2017

Federated Authentication using the Cloud (Cloud Aura)

Al Abdulwahid, Abdulwahid Abdullah

Federated Authentication using the Cloud (Cloud Aura)

By

Abdulwahid Abdullah Al Abdulwahid

A thesis submitted to the University of Plymouth

in partial fulfilment for the degree of

Doctor of Philosophy

School of Computing, Electronics and Mathematics

Faculty of Science and Engineering

February 2017

Abstract

Federated Authentication using the Cloud (Cloud Aura)

Abdulwahid Al Abdulwahid *(MSc)*

Individuals, businesses and governments undertake an ever-growing range of activities online and via various Internet-enabled digital devices. Unfortunately, these activities, services, information and devices are the targets of cybercrimes. Verifying the user legitimacy to use/access a digital device or service has become of the utmost importance. Authentication is the frontline countermeasure of ensuring only the authorised user is granted access; however, it has historically suffered from a range of issues related to the security and usability of the approaches. Traditionally deployed in a point-of-entry mode (although a number of implementations also provide for re-authentication), the intrusive nature of the control is a significant inhibitor. Thus, it is apparent that a more innovative, convenient and secure user authentication solution is vital.

This thesis reviews the authentication methods along with the current use of authentication technologies, aiming at developing a current state-of-the-art and identifying the open problems to be tackled and available solutions to be adopted. It also investigates whether these authentication technologies have the capability to fill the gap between the need for high security whilst maximising user satisfaction. This is followed by a comprehensive literature survey and critical analysis of the existing research domain on continuous and transparent multibiometric authentication. It is evident that most of the undertaken studies and proposed solutions thus far endure one or more shortcomings; for instance, an inability to balance the trade-off between security and usability, confinement to specific devices, lack or negligence of evaluating users' acceptance and privacy measures, and insufficiency or absence of real tested datasets. It concludes that providing users with adequate protection and convenience requires innovative robust authentication mechanisms to be utilised in a universal manner. Accordingly, it is paramount to have a high level of performance, scalability, and interoperability amongst existing and future systems, services and devices.

A survey of 302 digital device users was undertaken and reveals that despite the widespread interest in more security, there is a quite low number of respondents using or maintaining the available security measures. However, it is apparent that users do not avoid applying the concept of authentication security but avoid the inconvenience of its current common

techniques (biometrics are having growing practical interest). The respondents' perceptions towards Trusted Third-Party (TTP) enable utilising biometrics for a novel authentication solution managed by a TTP working on multiple devices to access multiple services. However, it must be developed and implemented considerately.

A series of experimental feasibility analysis studies disclose that even though prior Transparent Authentication Systems (TAS) models performed relatively well in practice on real live user data, an enhanced model utilising multibiometric fusion outweighs them in terms of the security and transparency of the system within a device. It is also empirically established that a centralised federated authentication approach using the Cloud would help towards constructing a better user profile encompassing multibiometrics and soft biometric information from their multiple devices and thus improving the security and convenience of the technique beyond those of unimodal, the Non-Intrusive and Continuous Authentication (NICA), and the Weighted Majority Voting Fusion (WMVF) and what a single device can do by itself. Furthermore, it reduces the intrusive authentication requests by 62%-74% (of the total assumed intrusive requests without operating this model) in the worst cases.

As such, the thesis proposes a novel authentication architecture, which is capable of operating in a transparent, continuous and convenient manner whilst functioning across a range of digital devices – bearing in mind it is desirable to work on differing hardware configurations, operating systems, processing capabilities and network connectivity but they are yet to be validated. The approach, entitled *Cloud Aura*, can achieve high levels of transparency thereby being less dependent on secret-knowledge or any other intrusive login and leveraging the available devices capabilities without requiring any external sensors. *Cloud Aura* incorporates a variety of biometrics from different types, i.e. physiological, behavioural, and soft biometrics and deploys an on-going identity confidence level based upon them, which is subsequently reflected on the user privileges and mapped to the risk level associated to them, resulting in relevant reaction(s). While in use, it functions with minimal processing overhead thereby reducing the time required for the authentication decision. Ultimately, a functional proof of concept prototype is developed showing that *Cloud Aura* is feasible and would have the provisions of effective security and user convenience.

Table of Contents

List of Figures

List of Tables

Acknowledgements

First and foremost, all praise and gratitude is due to Allah the All-Compassionate and All-Merciful for everything He has provided me throughout my life, in general, and for giving me the potential and patience to persevere and reach this stage of my PhD research, in particular. Without Him, I would not have achieved anything or even existed.

I also owe a debt of gratitude to my beloved parents for their considerable encouragement and support, and passionate love and prayers for my success even though I have fallen short of being worthy of all what they do and have done for me. Any success that might be resulted, hopefully, should help me make them proud and happy of me. May Allah reward them the best.

My unreserved love, thanks and appreciation must go to my wife (Nouf) and children (Jawaher, Hattan, Abdullah, Joory, and Hala "means Aura") who have been very patient, understanding, and inspiring to me throughout this endeavour, spending days, nights, and sometimes even holidays without me. Hope that the potential success of this research will compensate some of what they have missed. May Allah bless them.

I should not forget my dear siblings who have been always supportive to me whenever I am in need and without any reservation. Many thanks to them.

This thesis would not have been completed on time without the invaluable guidance, wholehearted support, timely feedback and utmost professionalism from my Director of Studies Professor Nathan Clarke. I would like to express my special thanks and admiration to him. It has been really a pleasure and an incredibly rewarding experience to work with him and I am looking forward to continue doing so in future.

Thanks must also go to my other supervisors: Professor Steven Furnell, Professor Christoph Reich and Professor Ingo Stengel, who have spent a lot of time and efforts proof reading papers and my thesis, in addition to providing helpful advices throughout my studies.

I would like to thank all my friends and colleagues, either in the UK or in the KSA, who have contributed positively towards my progress by any means even if it was just a smile. Many of them deserve mentioning but it is difficult to state all the names. However, it is inevitable not to express my sincere thanks to my older brother-like friend Saad for all kinds of support he has provided throughout my PhD journey. Moreover, my friend and office mate Ayad Al-Adhami has been of great support and inspiration to me so he deserves many thanks from me. I wish them all success in all their current and future endeavours.

Finally, I would like to acknowledge with thanks and appreciation the government of the Kingdom of Saudi Arabia and my employer, the Royal Commission for Jubail and Yanbu, for granting me a scholarship and sponsoring my PhD studies.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

Work submitted for this research degree at the Plymouth University has not formed part of any other degree either at Plymouth University or at another establishment.

This study was financed with the aid of a scholarship from the Kingdom of Saudi Arabia.

Relevant scientific seminars and conferences were attended at which work was often presented and several papers were published and prepared for publication in the course of this research project. Other research skills development courses were also attended.

Word count of main body of thesis: 60,418 words

Signed.……

Date……

1 Introduction and Overview

1.1 Introduction

There are 7.6 billion mobile subscribers currently in existence and they are anticipated to reach 9 billion by 2020 (GSMA, 2016), many of which are increasingly utilising smartphones and other devices with a wide range of capabilities. Smartphones are capable of making telephone calls, texting, surfing the Internet, checking emails, playing games, viewing documents, transferring money, shopping online and storing confidential information. This leads individuals, corporations and governments to rely heavily and prevalently on computing systems (i.e. PCs, servers, laptops, tablets, phablets and mobile phones) for accessing, storing and processing personal, financial, medical and business information that are considered sensitive and confidential. This can be realised from the enormous growing number of Internet users around the world, 2.4 billion, along with the accelerated rise of 150% per year in mobile traffic (Meeker & Wu, 2013). Moreover, IDC (2014) states that the worldwide market share of smartphones and phablets is 70% of the total smart connected device market and is forecasted to grow to 75.6% by 2018. Furthermore, this is also proportional with the worldwide total number of smartphone users which was 2.1 billion in 2016 and is projected to reach 2.87 billion in 2020 as illustrated in Figure 1-1 (Statista, 2016).

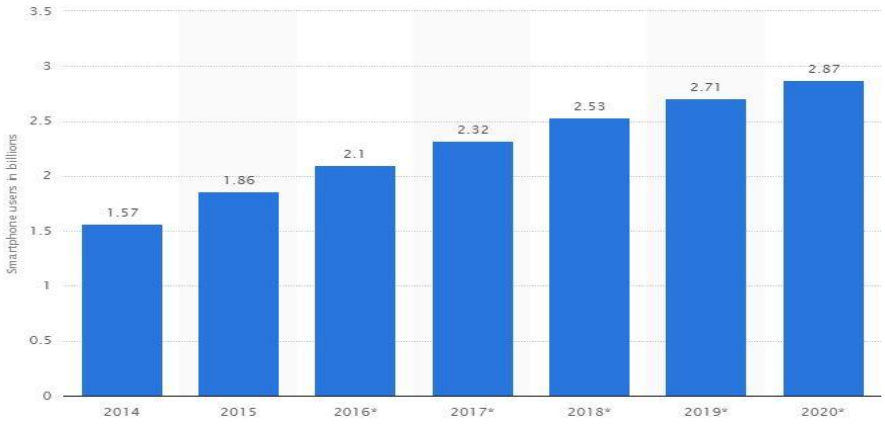

Figure 1-1: Worldwide Smartphone Users 2014-2020 (Statista, 2016)

However, unfortunately, these devices, activities, services and information are becoming targets of cybercrimes. For example, 35% of CSID (2012) survey respondents' accounts or personal information were compromised or stolen by imposters. In the Symantec Corporation (2013) report, it was revealed that there was a 42% increase in targeted attacks. Additionally, the average number of identities exposed per breach was 604,826 of which 23% were caused by theft or loss of device. In addition, another credible report showed that the use of stolen, weak, and default credentials was at the top of the data breach threats and represented 63% of the data beach incidents in 2016 (Verizon, 2016). Furthermore, three quarters of financial and travel organisations encountered customer impersonation and identity fraud (PwC, 2013), highlighting that even those organisations running and holding critical information suffer from cyber attacks.

Therefore, close attention has been drawn to the immense importance to strongly secure them from any unauthorised access. To secure any system or information, it is crucial that it must fulfil the CIA triad principles: confidentiality, integrity and availability (Furnell et al., 2008). In order to maintain the first two, it is paramount for a system to uniquely identify legitimate users by an effective user authentication technique, which, if achieved, enables functional authorisation and accountability. Thus, it is evident that authentication is a cornerstone of information systems security and is a key security control for any computing system, whether that is a PC, server, laptop, tablet, phablet or mobile phone.

Authentication is categorised into three major approaches: something the user knows (e.g. password and PIN), something the user has (e.g. smart card and token) and something the user is (i.e. biometrics) (Wood, 1977). Whilst various methods of authentication exist, they are traditionally poorly served thereby falling foul of a variety of drawbacks (Clarke & Furnell, 2007). Knowledge-based authentication has still been the standard means for user authentication on computing systems, making up approximately 3 out of 4 of authentication

events (TeleSign, 2016). Furthermore, besides using several digital devices, almost half of the surveyed respondents stated that they have more than 10 accounts with distinct usernames and passwords (Barker, 2016). Consequently, 73% to 84% of TeleSign (2016) and Gigya (2016) surveys participants, respectively, use the same password for various accounts to mitigate the burden of memorising and recalling numerous different passwords. Nevertheless, doing so violates the recent strict password policies, where users are required to remember multiple, complex, longer, non-recycled, unshared and changing passwords, which if met would augment security control while compromising users' convenience. Token-based authentication seems to solve some password shortcomings; however, they have higher cost and fundamentally authenticate the presence of the token rather than the individual. Usability also becomes an issue when the user is required to carry multiple tokens for accessing a variety of services (Dinesh, 2012; Furnell et al., 2008). Due to these weaknesses, further attention has been placed upon the final form of authentication, biometrics. They arguably have high availability, strong defence against repudiation and good levels of usability as the burden from the user to recall passwords or carry tokens is removed. However, it is not impossible to forge single static biometrics, and the likely need for additional reader devices and their accuracy are questionable (Clarke, 2011; O'Gorman, 2003).

The problem is further magnified as users are now in possession of an ever-growing number of advance digital devices; each one with its own associated security requirements. As an instance, 73% of 470 respondents own smartphone and tablet and 83% would like to have seamless experience across all their devices (Salesforce, 2014). Thus, it is apparent that a more innovative, convenient and secure solution for user authentication is essential. Some attempts have been emerged to counteract the aforementioned weaknesses of traditional authentication including deploying two/multi-factor authentication, such as the combination of password and token or two/multi-layer authentication, such as the combination of PIN and

graphical password (Aloul et al., 2009; Cryptomathic, 2012). However, these techniques, on one hand merely augment security, but on the other hand degrade user friendliness.

Furthermore, it is proven that the aforementioned approaches mostly remain point-of-entry. In spite of the fact that re-authenticating the user periodically or as and when needed for higher sensitive services is imperative to increase the level of authentication beyond the standard point-of-entry technique, it is not viable because of its intrusiveness as they require the explicit interaction of the user and thus affecting the users' experience (Grenga, 2014). The potential aim is to use more advanced techniques that would enable periodic or continuous re-verification of the user without compromising the convenience. Therefore and to enhance these solutions, a number of studies have upheld the need for more innovative authentication approaches that endeavour to balance the trade-off between security and convenience, such as transparent authentication system (TAS) (Clarke, 2011) and implicit authentication (Yazji et al., 2009) (which are introduced in sections 2.4.3 and 2.4.4, and then discussed in 3.8). Nonetheless, these technologies merely focus upon individual platforms rather than providing a universal and federated authentication approach that can be used across different technologies and services. The advent of cloud computing, its universal connectivity, scalability and flexibility (Grobauer et al., 2011), offers a new opportunity of achieving convenient authentication seamlessly in a technology and service independent fashion, thereby deploying it to host a centralised authentication. However, relying upon such an environment also introduces a range of technology, privacy and trust-related issues that need to be considered in any proposed solution.

1.2 Research Aims and Objectives

The proposal builds upon existing research on transparent and distributed authentication, with a view of capitalising upon the benefits that cloud computing provide. An authentication

system built upon this would provide a more secure, user-friendly, universal and technology independent environment. As this proposed framework evolves, further research will be undertaken to consider the human-aspects of security, including the privacy of highly sensitive biometric data and the operational factors that must be incorporated within the architecture to ensure a convenient but highly secure system.

In order to achieve this, the following research objectives are established:

- To develop a current state-of-the-art understanding of authentication methods including both the problems and available solutions.
- To investigate the leading authentication technologies provided by various sectors and the biometric authentication techniques including its applications in the existing research on continuous, transparent and distributed authentication.
- To explore end-users' perceptions and attitudes towards security, privacy and usability in order to assess the acceptability of such proposal.
- To validate whether prior TAS models function on real live user data and what their actual performance will be in practice.
- To conduct a series of experiments aiming at evaluating the effectiveness of utilising the Cloud for such universal authentication and seeking to identify the attributes required for a successful authentication mechanism.
- To design a novel and holistic architecture that will enhance security, user-friendliness, universality, and will operate in a technology independent fashion.
- To develop a functional prototype exemplifying the federated Cloud Aura authentication framework to have a tangible understanding of how such approach would function in practice.

1.3 Research Novel Contributions

The research has fulfilled the aforementioned objectives and has made positive contributions to the field of user authentication, and specifically in biometric identity verification domain. The core novel contributions of this research are:

- Conducting an exhaustive literature survey of the existing research in the domain of multibiometric continuous and transparent authentication.
- Surveying end-users' perceptions and attitudes towards security, privacy and usability in order to assess the acceptability of the research proposal, including their perceptions and satisfaction of associated current and alternative authentication approaches alongside their usability in addition to their awareness and attitudes towards related privacy issues.
- Developing a biometric data capturing software sought to create a real dataset of a significant number of real users for a significant period of time of real usage in totally uncontrolled conditions, aiming at employing it in the research experiments. Forty-seven subjects were recruited and their usage data was collected over 2-week period.
- Modelling and undertaking a baseline set of experiments to determine the nature and performance of the potential contributing transparent biometrics and soft biometric data; namely, facial verification and geolocation.
- Modelling and replicating a well-established framework (NICA) to validate whether prior TAS models would function on real live user data, whether they were based on valid assumptions, and what its actual performance is in practice.
- Modelling and developing an enhanced model utilising multibiometric fusion and time windowing within a device, aiming at investigating whether employing a fusion mechanism that encompasses all available biometric samples at a given time-frame is

viable in practice and to what degree it improves the performance from the individual unimodal approaches.

- Conducting a series of experiments aiming at evaluating the effectiveness of utilising the Cloud for such a universal authentication approach and seeking to determine whether it is viable, convenient and secure to authenticate users based upon their digital devices activities and other captured biometrics, so that it would be possible to gather a single user profile from the range of devices a single user may use.
- Proposing a novel federated biometric authentication approach addressing the main research gap, thereby shifting the burden of both the authentication processing and management responsibility to a centralised Managed Authentication Service Provider (MASP). Accordingly, an intelligent, modular and holistic *Cloud Aura* architecture has been designed enhancing system security, user-friendliness, and universality that will operate in a location, service, and technology independent fashion.
- Developing a functional proof of concept prototype exemplifying the federated Cloud Aura authentication framework to have a tangible understanding of how such an approach would function in practice.

1.4 Thesis Structure

This thesis is organised into eight chapters to address the aforementioned objectives, commencing by Chapter one that introduces the research problem and outlines the overall research aim and objectives and the structure of this thesis.

Chapter two describes the authentication methods with the aim of developing a current state-of-the-art understanding of them including both the problems and available solutions along with their applicability to the proposed research. It also provides an overview of some of the current provided authentication technologies by service providers and devices manufacturers

in order to explore whether they solve some issues related to the research area. Furthermore, a number of featured authentication frameworks is discussed in terms of the benefits they offer as well as their shortcomings.

Chapter three reviews biometric authentication from a number of perspectives, including its system components, requirements, techniques, performance measures and standards, with a view of examining its potential to be incorporated in the research proposal. This is followed by an intensive literature survey of the existing research on continuous and transparent authentication focussing on those employed multibiometrics.

Chapter four presents the results of a user survey conducted in order to address aspects of the problem that the literature has not covered, aiming at exploring their technology usage and security practices, and at investigating their perceptions and satisfaction of associated current and alternative authentication approaches alongside their usability. Furthermore, it sought to analyse users' awareness and attitudes towards related privacy issues.

Chapter five seeks to initially establish an experiment exercise to capture and collect real data of a set of biometric techniques and coexisting device' sensors from a real and live usage without any environmental or usage constraints. The collected data is utilised in a series of studies aiming to eventually investigate the appropriateness and effectiveness of utilising them for such a universal solution with a view to identify the attributes required for a successful authentication mechanism. Accordingly, three experimental studies were undertaken beginning with a baseline set of experiments to understand the nature of transparent biometrics and soft biometric data and determine their potential contribution to the system performance. Followed by a replication study to explore whether prior TAS models function on real live user data and what their actual performance will be in practice. The chapter then concludes by an enhanced model utilising multibiometric fusion and time

windowing within a device, aiming at investigating whether employing a fusion mechanism that encompasses all available biometric samples at a given time-frame is viable in practice and to what degree it improves the performance from the individual unimodal approaches.

Chapter six builds upon the knowledge of Chapter five to introduce a novel federated biometric authentication approach that addresses the main research gap thereby shifting the burden of both the authentication processing and management responsibility to a centralised Managed Authentication Service Provider (MASP). The Chapter continues to examine the argument that it would help towards building a better user profile and thus improving the security and convenience of the technique beyond what a single device can do by itself.

Chapter seven presents the architectural design of the Cloud Aura, accompanied with description of its key components, functionalities and operational considerations. The architecture is designed in an adaptable, modular and scalable manner in order to be interoperable considering the divergent platforms of today's digital devices. A functional prototype is developed and elucidated, incorporating a number of the aforementioned architectural features to ensure that the system is viable in practice.

Chapter eight is the final chapter summarising the conclusions arising from the research and highlighting the key contributions, achievements and limitations. It also contains a discussion on potential areas for future research.

A number of appendices are supplemented at the end of this thesis in support of the main discussion, including experimental ethical approvals, consent forms, and programming scripts, in addition to a number of published papers arising from the research programme.

2 User Authentication Approaches

2.1 Introduction

Protecting any IT system against unauthorised user activities is usually provided via user identification or authentication which enable successful authorisation and subsequently accountability – these concepts together are referred to as AAA (Conrad et al., 2012). The identity of a user is required by a system to authenticate/verify user's credentials against an authentication database to decide whether he/she is the legitimate claimed individual. For instance, a username is a way of claiming an identity and a password is one method for providing authentication. Proceeding to a successful verification, authorisation is established based on the predefined devices and/or services the verified user is allowed to access on a system with specified privileges. Accountability provides the means to attribute activities each user performs on a system and keeps track of them – usually through logs.

Therefore, managing appropriate authentication is arguably the pivotal concept for implementing information security within an IT system. Achieving a high level of confidentiality, integrity, authorisation, and accountability of an IT system would not be possible without carefully considering a sensible, robust and usable authentication approach. Authentication can be achieved by utilising one or more of the three fundamental approaches: something the user knows (including passwords, PINs, graphical passwords, and cognitive questions), something the user has (including SIMs, smart cards, certificates, mobile phones, and hardware/software one-time password (OTP) tokens) and something the user is (biometrics) (Wood, 1977).

The first two authentication approaches have been employed in most security systems surrounding today's digital society. However, the third one has emerged gradually from being research and utilised mainly by governments (e.g. in the context of forensics and borders

control), to becoming more available in the public domain (biometrics are now deployed in a wide range of applications that can be considered fairly mainstream – passports, mobile phones, schools, and police). For better appreciation of various authentication approaches, a thorough overview of their conventional and contemporary uses is required.

2.2 Conventional Authentication Approaches

This section describes the common authentication approaches aiming at developing a current state-of-the-art understanding of them including both the problems and available solutions along with their applicability to the proposed research.

2.2.1 Secret Knowledge-based Approach

This approach refers to the process where the user has to remember a secret which is a particular sequence of inputs, typically made up of numbers only (PIN); numbers, characters and/or symbols (password and passphrase); answer(s) to predefined question(s) (cognitive knowledge); or images (graphical password) (Zekri & Furnell, 2006). This secret is set initially by the user or generated by the authenticating system. Thus, it is known mutually by both the user (brain) and the system (database) and there must be an exact match between them to be able to have access. This means that it is a Boolean authentication process – its outcome is either one (totally true secret thus allow access) or zero (totally false secret thus deny access). As a result, there is an integral reliance on individuals' memory and ability to recall the secret exactly as and when prompted regardless of its length, sophistication, and uniqueness. Furthermore, it does not defend well against repudiation as the so called secret is transferable, guessable and can be watched by others through shoulder surfing (O'Gorman, 2003).

2.2.1.1 Personal Identification Number (PIN), Password and Passphrase

A PIN is considered the simplest knowledge-based authentication technique. It is available to be used within mobile phones: for the mobile handset itself (switch on or unlock) and/or for the Subscriber Identity Module (SIM) card (to authenticate with the cellular networks) and with cash/credit cards. Typically, a mobile PIN ranges from 4 to 8 digits only. As numbers only are relatively easier to recall, they are easier to guess and to steel. Passwords, which can be longer and are made of some or all of numbers, letters and symbols, mitigate the possibility of being predicted. They are believed to offer effective protection if they are established and employed appropriately.

Despite the fact that passwords are still the most ubiquitous authentication method perhaps because of its perceived convenience and inexpensive implementation as they are conceptually quite simple to design, manage and use, they are vulnerable to be misused by users. PINs/Passwords protections are often compromised through the failure or unwillingness of individuals to correctly practice the password policy to protect and administer sensitive information (Clarke & Furnell, 2005; Kurkovsky & Syta, 2010). For instance, 45% of the former survey respondents never changed their PINs. Worse than that, it was also revealed in the latter survey of 330 young people aged 18 to 25 that over 71% of the participants do not even use PINs or any other authentication methods to lock their mobile phones (though these methods are available to them). Furthermore, a recent survey conducted by Crawford and Renaud (2014) showed that 30% of the participants do not enable any security measure on their mobile devices although sensitive information resides on them. Whilst some practice improvements are notable, the small population (30 participants) of this survey is an issue but, even so, when factoring this percentage to the worldwide mobile users it would be significant.

More recently, many digital services create password policies and guidelines to encourage good practice, which are adopted by many organisations to be utilised by their employees. Some of these policies are difficult to ensure they are being followed and hence they can be avoided. For instance, it is possible to violate these policies by using dictionary words, using them on multiple systems, writing them down and not or rarely changing them. For example, 61% of 1200 surveyed respondents reuse the same password on multiple websites, besides 44% of them change their passwords merely once a year or less (CSID, 2012). Others are enforceable, such as the length of password, complexity and its lifetime. Accordingly, when users are faced with the need to memorise multiple passwords and change them periodically, they tend to forget them, write them down, and select easily guessed ones (O'Gorman, 2003). Therefore, the problem is exacerbated as they would become more susceptible to be stolen. Moreover, additional administrative costs would be posed by frequent passwords resetting (O'Gorman, 2003). The above-mentioned studies also implied that some people would rather setup the same but very sophisticated password on multiple accounts; however, this exasperates the issue if one of these accounts is compromised, all others may follow, as the intruder would be able to reuse the same cracked password to login to them.

Passphrases come as an alternative endeavour to balance the trade-off between the simplicity of remembering a secret by the genuine user and the difficulty of predicting it by intruders. Passphrases are a sequence of words built to be used as a credential secret. They are usually without spaces but possibly with digits replacing letters or words; for example, "Going for a long journey" is transformed to "Going4al0n9journey". It can be noted that they are similar to passwords in terms of usage and appearance except that the former are longer normally thus more robust. On the other hand, it is argued that passphrases are easier to remember than passwords especially if they carry an associated meaning. However, if they consist of common words from a language dictionary, they would be vulnerable to be broken with less

effort. In addition, common substitutes, such as “4=for” and “0=o”, render it less secure and more confusing to recall.

Brute-force attack tools (attempting every possible combination automatically), such as Brutus and OphCrack, are notorious against most of knowledge-based authentication techniques (Shankdhar, 2014). Some countermeasures have been proposed against them and to reduce the likelihood of a system or device being abused by imposters during the usage session and before it ends. For instance, the account would be temporary blocked or further credentials would be requested after three failed access attempts or the user would be required to re-authenticate again after specific or lapse time dependent upon the system settings or the user’s preference. Even though that this seems to move the PINs, passwords and passphrases from being a mere point-of-entry technique, it most probably hinders the user due to its constant intrusiveness.

2.2.1.2 Cognitive Knowledge Question

Cognitive knowledge which comes in a form of question(s) seeks to alleviate the load of users memorising desperate passwords thereby deploying associative question(s) (Clarke, 2011). These cognitive questions are typically about personal information and can be in two forms – factual (e.g. first school, mother’s maiden name, and city of birth) and subjective (e.g. favourite colour, food, and teacher). The former are potentially easier to establish than the latter. Therefore, it is evident that this technique lacks one of the main characteristics of secret knowledge-based authentication approach, i.e. secrecy. By predicting or conducting online search or social engineering, it is possible to have the correct answer(s) – the higher the possibility of an answer to deduce or associate, the higher it is vulnerable to crack.

So, it is apparent that this approach cannot be dependable as a standalone authentication approach. This could be overcome by requiring a user to answer a group of cognitive

knowledge questions or alternatively utilising it besides another authentication approach (as explained in 2.2.4). Whilst this solution probably enhances security by adding another layer, it potentially increases the burden on the user thereby lengthening the time of authentication and requiring them to recall and provide multiple secrets (i.e. the password and the answers of the cognitive questions). However, this approach offers opportunities of supporting the security level of other than secret-knowledge ones, such as one-time password (OTP) tokens. Furthermore, it can be used as a remedial approach for resetting the password when users, for instance, forget their password or are locked-out due to exceeding the maximum failed login attempts.

2.2.1.3 Pattern and Graphical Password

Solutions have been suggested to mitigate the downsides of PIN, password and passphrase, some of which solely concern about guidelines promoting increasing the entropy of passwords. However, human inability to memorise and remember multiple complex passwords is not addressed by them. It has been proven that the human brain is more capable to store and remember pictorial information than textual (Nelson et al., 1976). As a result, pattern password authentication has emerged, with which a user is required to recognise and sequentially draw a pre-set outline on nine (three by three) dots grid that appear on a screen. Therefore, it is argued that it will be much more convenient to the user to recognise a pattern than an alphanumeric password. In addition, Weiss and Luca (2008) showed and argued that repeated entry of pictorial password would be with "lower cognitive load and higher memorability" to the user. Mobile devices with touch screens make it reasonably plausible to utilise pattern password, which is used in Android devices, to improve the memorability of the secret.

However, in the current functioning pattern passwords, users are able only to stroke and drag (draw a direct line between) two adjacent dots, which in turn limit the number of permutations. As a result, the typical application of it is more vulnerable to brute-force attacks. Some attempts have been conducted to overcome this shortcoming. For instance, De Luca et al. (2012) extend this typical pattern password to allow skipping dots (as demonstrated in Figure 2-1), thus enhancing its resilience to brute-force attacks by allowing more combinations. Nevertheless, its accuracy is quite low (77%) with a 19% false rejection rate and 21% false acceptance rate. Furthermore, besides the fact that this approach is still secret-knowledge based and hence inherits most of its drawbacks, such as shoulder surfing, it is susceptible to a so-called smudge attacks when a secret pattern can be simply determined on a greasy screen (Aviv et al., 2010).

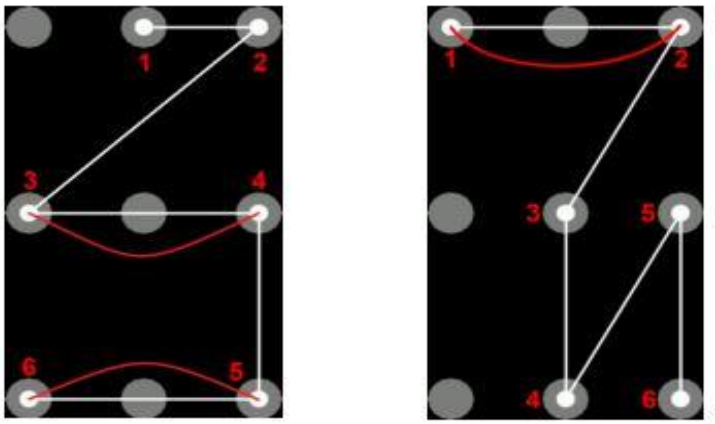

Figure 2-1: Pattern with the Possibility of Points to be Skipped (De Luca et al., 2012)

To obtain the most from the advantages of people's ability to remember graphical over alphanumeric secrets, a number of approaches have been proposed. For example, with click-based graphical authentication, there is a generic image where the user is required to click on pre-specified obscured points (Wiedenbeck et al., 2005). Albeit evaluations have demonstrated its usability improvement in relation to memorability, it is relatively difficult to click precisely on a point, especially if the point space is small and while using finger tips on

touch screens. This leads to increase authentication failures that might frustrate the user. Moreover, poor selection of background images that have likely selectable points yields to being easily predicted, for instance a study by Oorschot and Thorpe (2011) found an average of 7–10% of user passpoints (click-based) passwords within 3 guesses only.

Further to the work on click-based concept, proposals about choice-based or PassImages graphical authentication have risen (Charrau et al., 2005; English & Poet, 2011). There are a set of images on sequential grids; the secret is among them in a form of a series of images that should be pressed or clicked on a specific order, one at each grid. To overcome shoulder surfing attacks, the distribution of images on each grid should be randomised. Likewise, Passfaces (2007) product capitalises on the psychological theory that human's brains recognise and recall faces better than any other picture or object (Ellis et al., 1979). Users are able to use familiar personal photos that are stored on the ones PC or on the web to form a passfaces, with which the possibility of forgetting them is very rare. In the login process, the user is encountered by a 3 by 3 grid that contains one of the pre-set photos among 8 others. Similar to the other graphical password methods, there are three consecutive grids to identifying all three faces. The time taken to pass all the steps of graphical authentication could be an issue of inconvenience. Additionally, poor selection of photos makes them susceptible to be known by imposters. Moreover, given that it is a secret-knowledge approach, it can be shared and left not changed.

2.2.2 Token-based Approach

To overcome some of the abovementioned downsides of secret knowledge-based approach, tokens have been developed. Generally, the token-based authentication approach has various applications ranging from physical to logical accesses to systems and services. Based on the external appearance and the need for additional devices, they can be categorised into two

types: hardware tokens and software tokens (Aloul et al., 2009). With the former type, a separate physical device is produced and provided, usually, by the service provider, such as bank smartcard and HSBC Secure Key OTP token (HSBC Bank plc, 2014). On the other hand, with the latter type, there is a utilisation of a user's existing device as is, such as when sending OTP via SMS to the user's registered mobile phone, or there is a need to install a software (an application) on the user's smartphone or PC (Aloul et al., 2009), such as Google authenticator (Google, 2014).

A typical authentication token either stores static but complex passwords or generates a one-time password (OTP) for each session (Furnell et al., 2008). The user is required to enter the generated password on the system or service they are authenticating to or it is synchronised directly. From one prospective, they have some advantages over the secret knowledge-based methods in that they are capable of storing, recalling and generating multiple and sophisticated passwords, thus lifting this burden from the human's brain. However, the reliance on the individual is still existent as it is assumed that the token is in the possession of the legitimate user – they merely verify the presence of the token not the authorised user.

Tokens provide compromise detection, for example if three failed attempts threshold is exceeded, as well as countermeasure against denial-of-service attacks (O'Gorman, 2003), albeit they are not fail-safe – the breach of RSA SecureID tokens in 2011 evidences this (BBC, 2011). Therefore, it is evident that this approach cannot stand by itself to be effective at inhibiting masquerade attacks. As a result, typically, it is employed with at least another authentication factor to form an approach called multi-factor authentication which is elaborated in the 2.2.4 sub-section. Having said this, in recent tokens, a PIN is prompted to validate the user for a subsequent legitimate use of the token; however, the token can be lent, lost or stolen and the PIN can be shared.

It is apparent that the cost of issuing, maintaining and recovering them is higher. Simply issuing (or reissuing if lost or stolen) SIM, smart cards or hardware tokens is adding an additional cost over passwords. This is worsened if specialised devices are required, such as card readers. For example, if a bank plans to employ hardware tokens to access its online banking, there is a need to purchase tokens/token readers for all its customers, implement and maintain them, along with providing technical support and potential replacement in case they are lost or malfunctioned. Moreover, time synchronisation between the token and system might be difficult with those time-synchronous tokens (Furnell et al., 2008) especially in out of coverage areas. Furthermore, users' convenience is an issue, in particular when users need to carry a variety of tokens for different accounts and services from different providers which make it cumbersome and probably impractical.

2.2.3 Biometrics

In seeking a more reliable and robust authentication approach, attention has turned to biometrics. Biometrics-based authentication is commonly acknowledged as a reliable solution that provides enhanced authentication over the secret knowledge-based and token-based approaches. Unlike the previous approaches, biometrics enables both identification and verification processes (Furnell & Clarke, 2005; Woodward et al., 2003). Regardless of whether the user has claimed an identity initially or not, the high level of uniqueness biometrics offers facilitates the process (Vallabhu & Satyanarayana, 2012). It also removes the reliance upon the individual to either memorise and recall complex and various passwords or carry and secure tokens. However, whilst the resulting decision of other approaches is (at least in theory) with complete accuracy (i.e. a Boolean decision), biometrics results in a confidence measure, with a pre-determined threshold deciding on whether the confidence is sufficient to accept or reject access. Thus, there is a margin for this decision being wrong; either by allowing access to an imposter or denying access of authorised user. Accordingly,

the performance of a typical biometric technique is measured based on its error rates, such as False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER) (Jain et al., 2002; Nanavati et al., 2002).

Biometrics is dependent upon measurable and distinctive characteristics of an individual. They can be categorised based upon their underlying characteristics into: physiological and behavioural approaches (Jain et al., 2008; Nanavati et al., 2002). Physiological biometrics are those based upon a unique physical aspect of the body, such as a fingerprint, face, or iris, whereas behavioural biometrics utilises the distinctive way in which humans behave, such as voice, keystroke and signature, to identify and/or verify a user. Both categories are believed to uniquely (with a varying level of accuracy) identify individuals, be non-transferable to others, unforgettable, cannot be easily lent or stolen, and difficult to reproduce, change or hide (Saevanee et al., 2012). As such, they offer a strong defence against repudiation (Schouten & Jacobs, 2009). However, biometric systems error rates and cost, together with usability have been hindering their widespread adoption (Clarke & Furnell, 2005); notwithstanding, recent years have shown that this has been alleviated by significant enhancement in biometric systems capabilities (FBI, 2014; Goode Intelligence, 2011). Nevertheless, stable uni-biometrics can be forged albeit some with difficulty (O'Gorman, 2003). For instance, traditional facial recognition can be fooled by a photo of the authorised person and voice recognition can be faked by imitation or voice recording. Therefore, they can be used in combination with a token that can store the user's identity or a password (as elucidated in the following sub-section) or additional data is required to determine whether a sample is alive. Liveness detection have been suggested and implemented to determine whether the provided biometrics sample is from a living legitimate user utilising some biological indicators, such as blood flow and blinking for iris scan, and temperature and pulse for fingerprint systems (Clarke, 2011; Furnell et al., 2008; NSTC, 2011). Whilst these metrics

have added a level of protection, some of them suffer from their own weaknesses and hence are forgeable. For instance, an impersonator can hold a photo of an authorised person with two eye holes, stand behind it and blink (or even hold a video of him/her blinking) in front of a facial recognition system (Moren, 2015). However, devising a biometric system deploying a set of countermeasures would overcome the downsides and thus making it robust and difficult to compromise. Alternatively, multibiometrics would offer a more resilient authentication solution (and is discussed in section 3.6).

2.2.4 Multi-Factor and Multi-Layer Authentication

To improve and augment the level of protection, two or more authentication techniques can be employed in combination. It has, even, been recommended by the European Central Bank (2013) that financial service providers should deploy "strong authentication" in all their online transactions. It can comprise multiple techniques from the same authentication approach (multi-layer authentication), such as password and cognitive questions, or from different authentication approaches (multi-factor authentication), such as PIN and smart card, password and facial recognition, or fingerprint and OTP generator token. This can then be reinforced by elements such as predefined user location which can be based on either the mobile cellular network (i.e. cell ID), the global positioning system (GPS) (i.e. longitude, latitude) (Conrad et al., 2012), or/and the IP address.

The multi-layer method lacks adherence to regulations of some sensitive sectors, such as banks where it is not compatible with the Federal Financial Institutions Examination Council regulations that emphasised clearly that these factors are required to be from two or more of the authentication categories (Federal Financial Institutions Examination Council, 2005). Therefore, it can be deduced that multi-factor authentication is considered stronger than multi-layer one – that is perhaps why the banking sector has utilised multi-factor

authentication in one way or another, such as the bank card and PIN or password and OTP token for online banking. On the other hand, although some recent smartphones are equipped with a built-in facial recognition or fingerprint sensor, they operate separately as an alternative single authentication method not multi-factor, i.e. the user has the option either to enable PIN or the fingerprint not both of them together. Hence, to the author's best knowledge no multi-factor authentication method has been utilised to access mobile phones thus far.

Nevertheless, while the aforementioned approaches increase the level of security, they add a further burden, from the perspective of the user, and remain at the point-of-entry. Re-authenticating the user periodically is not viable because of its intrusiveness. Furthermore, they increase the cost of provisioning, managing and implementing various authentication methods.

2.3 An Overview of Current Use of Authentication Technologies

It can be perceived that the integral aim of any IT authentication system is to safeguard resources against any illegitimate access. Therefore, service providers as well as device manufacturers require or offer a form of authentication technologies to protect them from any unauthorised access. Authentication technologies vary perhaps dependent on the data sensitivity involved and the users requirements, and each has its own benefits and weaknesses. This section investigates some of the available provided authentication mechanisms, with the aim of identifying their capabilities for accomplishing the aim of this research.

A number of service providers and devices manufacturers offer a variety of authentication technologies seeking to fill the gap between high protection and usability. Thus, it is useful to provide an overview of some of these attempts with the current authentication technologies employed with/by a sample of leading service/device providers; namely:

- HSBC (HSBC Bank plc, 2014),
- NatWest (NatWest, 2014),
- Lloyds (Lloyds Bank, 2014),
- SAMBA (Saudi American Bank) (Samba Financial Group, 2014),
- Windows 8.1 Laptop/PC (Microsoft, 2014; White, 2013),
- Android (Samsung Galaxy S5) (O'Boyle, 2014; Samsung, 2014),
- iPhone 5S (Apple, 2014; Mogull, 2013) and
- Google Authenticator (Google, 2014).

This set was selected because it is believed that they represent a wide range of services and providers that offer a variety of advanced authentication methods. Moreover, due to the fact that banks hold highly sensitive financial data, they are expected to strive to deploy the most advanced robust identity verification procedures. Other less critical and/or less common service providers and services are deemed not to utilise such resilient protection tools. Thus, half of the selected list is banks in addition to the most dominant operating systems (IDC, 2016). Google Authenticator is also included for the sake of diversity and inclusion as it has a different approach than the remaining listed technologies and it works with many leading websites, such as Amazon Web Services, Dropbox, and Facebook (Macworld, 2014).

Table 2-1 reveals an overview of these authentication technologies in order to better appreciate whether they have solved and mitigated the issues of traditional authentication flaws by enhancing security as well as improving the usability of authentication.

	Secret-based	Token-based	Biometrics-based	Point-of-entry	Re-Authentication
HSBC	✓ User ID ✓ Cognitive question ✓ PIN	✓ Separate Hardware OTP	-	✓	(New OTP) ✓ New payee ✓ Transfer money
NatWest	✓ User ID ✓ PIN ✓ Password	✓ Separate Hardware OTP (Card-Reader) ✓ Digital banking card	-	✓	(New OTP) ✓ New payee ✓ New standing order ✓ Change password ✓ Change phone
Lloyds	✓ User ID ✓ Password ✓ Cognitive question	-	-	✓	(New OTP with Automated call to registered mobile) ✓ New payee ✓ Transfer money
SAMBA (Saudi American Bank)	✓ User ID ✓ Password	✓ Separate Hardware OTP OR ✓ Mobile (SMS) OTP	-	✓	(New OTP) ***OR*** (ATM login) ✓ New payee ✓ Transfer money
Windows 8.1	✓ User ID ✓ Password ✓ Picture password	-	-	✓	✓ Websites accounts
Android (Galaxy S5)	✓ PIN ✓ Pattern ✓ Password	-	✓ Face ✓ Fingerprint	✓	-
iPhone (5S)	✓ PIN ✓ Password	-	✓ Fingerprint	✓	✓ Access iTunes ✓ New purchase
Google Authenticator	✓ User ID ✓ Password	✓ Mobile OTP	-	✓	-

Table 2-1: An Overview of Some of Current Authentication Technologies

Accessing all of the services mentioned in Table 2-1 above requires a form of secret-based information, including user ID, PIN, password, pattern, and/or cognitive question(s) all of which are needed to be memorised and recalled by users. All of these services except Lloyds bank augment their authentication process by offering the option of employing two-factor authentication or imposing it. To be able to unlock an Android (Galaxy S5) or iPhone (5S) device, a user selects to provide either a secret (i.e. PIN or password (for both), pattern (for Android)) or biometrics (i.e. face/fingerprint, or fingerprint, respectively).

On the other hand, accessing HSBC and SAMBA online banking systems must happen by entering secret information (i.e. user ID and cognitive question or password), in addition to having a separate hardware token for either banks, or using the user's mobile as token that generates One Time Password (OTP) or via SMS, respectively. However, two of the services employ two-layer authentication for the initial access: NatWest and Lloyds banks. The

former asks only for user ID and password whereas the latter adds them with a cognitive question to login. Nevertheless, the user will be prompted to provide an additional credential, OTP, when a critical service is requested, such as creating new payee. To do so, NatWest customers ought to have digital banking card with a separate PIN number to use with their Card-Reader to generate the OTP while Lloyds customers will see a OTP on screen and they will receive an automated phone call to their pre-registered mobile for confirmation.

These techniques might be perceived as a sensible trade-off between security and convenience. However, they arguably on one hand merely augment security but on the other hand degrade user friendliness, or the vice versa. For example, with HSBC, NatWest and SAMBA, the user must carry a separate token which only proves its presence not the legitimacy of the user. Additionally, logging in Lloyds online banking requires the user to recall 3 distinct secrets. Given the difficult users' experience with remembering secrets and tokens, these approaches merely serve to increase this burden.

The Google Authenticator app can offer an alternative solution as it is available in different platforms including iOS, Android and Blackberry and is easier to use than separate tokens as smartphones are carried around by users most of the time. Conversely, the backup secrets (that can be used if there is a difficulty in receiving the automatically generated code) can be stored in the device in an unencrypted text file (Google, 2014). Once it is lost or stolen, the service is susceptible to be accessed by the unauthorised holder of the device.

On the other hand, there are some encouraging signs and endeavours regarding classifying the services according to their level of sensitiveness when prompting re-authentication to access those ranked higher, such as transferring money to other accounts, adding a new payee and purchasing from iTunes. Despite their indication to reflect the reality of fluctuating

confidence on the user and services varying risk levels, should this procedure occur very often, the user is likely to get frustrated.

A few other attempts to utilise biometrics to the mainstream appear with some service providers and handsets, such as HSBC, Galaxy S7 and iPhone 7S. For example, HSBC has declared that they will utilise voice and fingerprint biometrics to access their mobile banking systems; however, it would only be available on the mobile banking app and only with touch ID-enabled Apple devices, which confines its universal application (HSBC News and Media, 2016). Similarly, Galaxy S7 and iPhone 7S employ the fingerprint scanner on their home button not only to unlock the device but also to purchase from their stores and to access some third party websites and apps, such as PayPal and iTunes (Apple, 2017; Guiding Tech, 2016). Nevertheless, offering the option of bypassing the fingerprint for PIN or password, even if they are enabled, may render the feature not being used at all or render this process to be exploited by attackers where the drawbacks of secret codes remain.

2.4 Featured Authentication Frameworks

A number of researchers have upheld the need for more innovative authentication methods that aim to balance the trade-off between security and convenience. The following sub-sections discuss a number of these featured authentication frameworks, namely single sign-on, federated identity, transparent authentication and authentication aura, in terms of the benefits they offer as well as their shortcomings.

2.4.1 Single Sign-On

An attempt to increase convenience and reduce the burden (of remembering many passwords and of entering the user's credentials on each resource and application) from the user has evolved – single sign-on (SSO). SSO provides the user transparent access to all services that they have the privileges to access within an organisation after a single successful login

(Furnell, 2005; O'Gorman, 2003; Sandhu, 2004). They, therefore, only need to set and recall one password to authenticate to a resource and subsequently attain the permission to access other services under the same domain without being prompted to authenticate again. A popular example is Google with which the account holder is required to enter their credentials once to be able to use its services, such as Gmail, Google drive and Google calendar, during the same session.

Besides the usability benefits from the users' perspectives, SSO is perceived to be beneficial for organisations. It induces a level of cost effectiveness thereby reducing the load for administrating numerous credentials to access various services. Rather, there is a need to administer one single credential for every user regardless of the number of services they are authorised to access. Identity Access Management (IAM) systems leverage this process (within one domain) which enables user-centric authentication. However, it should not be merely deployed to replace all logins with a single password; otherwise, this would be at the expense of protection. If this single login is cracked, it would then allow the intruder access to all participated services. Therefore, some standard protocols have been developed to secure the credentials exchanging between services, such as Security Assertion Markup Language (SAML) (Sandhu, 2004).

Securing the authentication process in the first place is still crucial which, if it is done by utilising the aforementioned approaches, would yield to keeping their downsides, such as the need for a complex and lengthy unrepeated password as well as the burden of memorising and recalling it. Additionally, SSO assumes that the authorised person who has been granted access initially is the one continues accessing the service throughout the usage session; which is not always the case. Moreover, typical users have other systems that are under other autonomous domains and organisations. As a consequence, the encumbrance of cognitive memory load and carrying tokens may persist.

2.4.2 Federated Identity

To bridge the gap between separate domains and thus alleviate the burden on users, federated identity management has risen thereby extending the SSO concept from being confined to a sole domain. It aims at granting access for users of one organisation to resources offered by other organisations seamlessly. To achieve this, an inter-organisational trust relationship should be established (Clarke, 2011; Stihler et al., 2012).

Thus, there is a need to ensure the security of these cross-domains credentials whilst they are being communicated, which in turn leads to the development and deployment of standards, such as OpenID, WS-Federation, and Shibboleth (CSA, 2012; Stihler et al., 2012). Whilst some of these standards, in one way or another, act as third party federated IAM providers, whereby an identity provider or manager coordinates the authentication process among the member parties of the federation which are the services providers (Madsen et al., 2005), users' credentials and some other information might be passed from one service provider to another. For instance, holders of Facebook account are able to use the credentials to access Yahoo services although they are distinct organisations. Hence, Facebook might send some basic information about the user, such as name, email, mobile number and photo. Accordingly, user privacy concerns must be overcome so that the user should have the discretion to decide which of their data can be shared, with whom and when.

Equally important, it is argued that federated identity is fragile to breach proliferation if one of the associated services providers' credentials hacked (Madsen et al., 2005); however, they claimed that some of the mentioned standards offer mechanism to contain such a breach by de-federation. Nevertheless, the time scale until such containment occurs is critical and dependent on whether it has been detected. As a result, an efficient federated IAM system must provide an effective auditing feature which poses issues on how to manage it on

heterogeneous domains. In addition, whereas a federated IAM approach offers promising usability advantages, still replacing all passwords with a single password is against good security practice of differing passwords for each system. Moreover, it is still performed at the point-of-entry leaving the system at risk of misuse afterwards. Furthermore, it focusses upon system/service level authentication – rather than actually looking at what the user is doing.

2.4.3 Transparent Authentication

Point-of-entry authentication, which solely and initially establishes identification of the user at the beginning of the session but not throughout, has a number of flaws. The vulnerability increases when the identity of the user has been verified at login and the device is left on for long periods of time. For instance, 85% of mobile phone users who responded to Clarke and Furnell (2005) kept their mobiles on for more than 10 hours a day. This can lead to a high-risk environment in which an imposter targets the device following a legitimate login. If this occurs and the device is kept on and active, free and open misuse can be conducted for a substantial period of time. It was even pointed out in the original specifications for security in third generation (3G) networks that "It shall be possible for service providers to authenticate users at the start of, and during, service delivery" (3GPP, 2001) – the emphasis here is on authenticating users during service delivery.

Therefore, it is imperative to increase the level of authentication beyond the standard point-of-entry technique. The potential aim is to use more advanced techniques that would enable periodic or continuous re-verification of the user without compromising the convenience. All authentication techniques are considered intrusive as they require the explicit interaction of the user. However, biometrics can also be deployed in a more usable fashion that allows the samples to be collected spontaneously. They cannot easily be compromised, can be deployed in a non-intrusive manner and thus eliminate the potential threat posed by social engineering.

Thus, the use of transparent authentication using biometrics would enhance both the requirement for a robust authentication mechanism and the user's need to eliminate any inconvenience during the authentication process. For this reason, Clarke and Furnell (2007) proposed transparent/non-intrusive continuous authentication using behavioural biometric techniques. This approach has the effect of moving away from a Boolean authentication result to a more meaningful and appropriate confidence measure. As illustrated in Figure 2-2, there is a disconnect in current authentication schemes that rather assume authenticity wherever an access control decision is made. However, through more closely aligning the authentication process with the access control decision, a more reliable and secure decision is made (as illustrated in Figure 2-3). Furthermore, the approach also takes into consideration that all authentication approaches are not equal and they have varying levels of authentication performance.

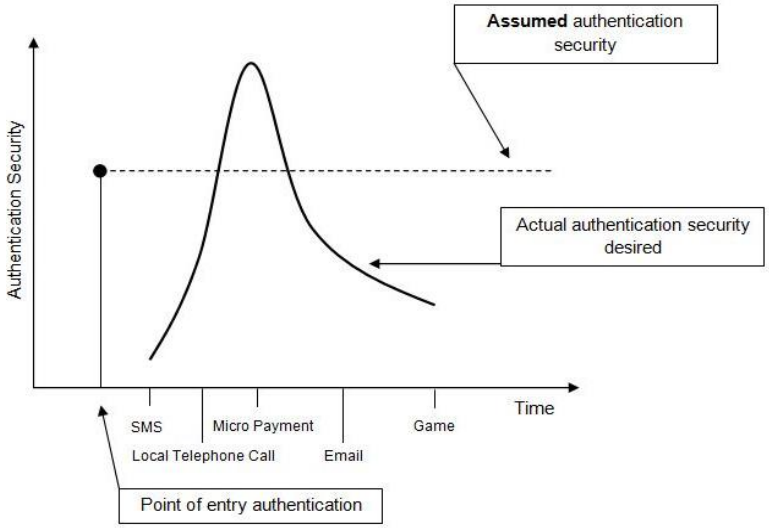

Figure 2-2: A Model of Traditional Authentication Security (Clarke, 2011)

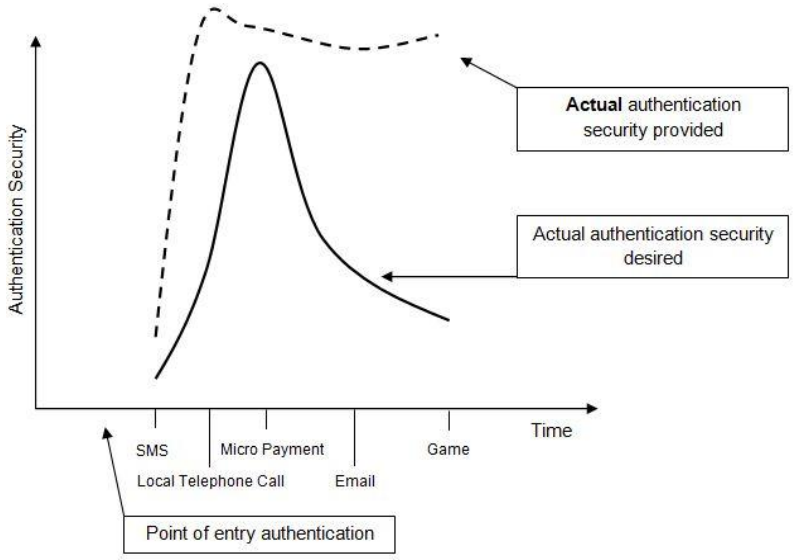

Figure 2-3: A Model of Continuous Authentication Confidence (Clarke, 2011)

Whilst transparent authentication approach can be appreciated as a solution to effectively remove the reliance upon the human aspects to ensure a robust and usable authentication, its applicability and universality have to be considered as it is confined to a single device. With every device requiring biometric setup and enrolment, user configuration and management, risk assessment and continual refinement.

2.4.4 Authentication Aura

The number of individuals having several digital devices to carry and/or use concurrently has increased. For example, it is common place for people to have mobile phone (in many cases more than one), tablet, laptop, PC, and game console. It is likely that similar authentication techniques are applied across distinct devices possessed by the same individual. The repeated intrusive authentication process for each device is likely to be annoying and time consuming. To counteract this burden, communicating the identity confidence between devices would be useful. In the one hand, collective identity knowledge controlled by the array of secured devices operated by an individual at any given time offers an opportunity to enhance security and usability. Accordingly, this has led to the proposal of deploying and sharing the

credentials of the individual's devices authentication confidence in a distributed and cooperative fashion, enabling a near field adaptive security envelope to be established and maintained around the individual – the user's Authentication Aura (Hocking et al., 2011). Authentication Aura enables the individual and distinct devices to communicate their own authentication status and confidence, and hence to establish an accumulative level of confidence.

Distinct devices are likely to employ different methods of authentication as shown conceptually in Figure 2-4. For instance, a laptop has an inbuilt fingerprint scanner, a smart phone has a PIN number, voice recognition and an inbuilt front camera, and a PDA has handwriting recognition. If a user has initially logged-in to a device by any authentication technique, the established combined confidence can be utilised to provide specific access to other trusted devices within a close proximity via a near field communication (NFC) channel. Consequently, the potential case is to acquire consolidating multibiometrics samples, which in turn mitigates some of the limitations of uni-modal biometrics by enhancing recognition accuracy, security, and usability (Ross et al., 2006). Confidence adaptation and degradation is applied over the time of missing or error acquired credentials and based on the un/known locales. Locking the system and asking for re-authentication would be necessary to re-determine the user's credentials when an inappropriate level of confidence has been reached.

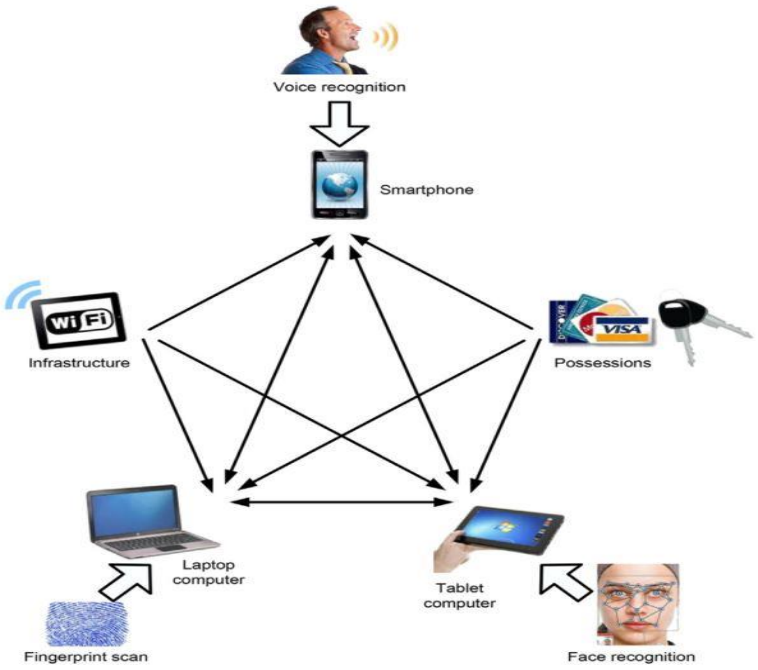

Figure 2-4: The Potential Intra-Device Relationship and Authentication Techniques (Hocking et al., 2013)

The approach further improves the level of security being afforded whilst reducing the burden of users' inconvenience. However, the approach to authentication is still disparate, with individual authentication approaches being supported on a number of technologies. Furthermore, the effective performance being achieved is highly correlated to the biometric software – a cheap facial recognition will experience a significantly different level of recognition accuracy to an expensive military-grade system. It is therefore not appropriate to merely have devices that support biometric capturing but also recognition capabilities with a good level of performance. Establishing trust in such an environment is complicated further. It also requires each device to support the Aura-framework and thus be capable of supporting a level of biometric processing, configuration and management.

2.5 Conclusions

Verifying the authenticity of a user to use a digital device or service has become crucial. Individuals, businesses and governments undertake an ever-growing range of activities online and via mobile devices and unfortunately these activities, services and information are the

targets of cybercrimes. Authentication is at the vanguard of ensuring only the authorised user is given access; however, it has historically suffered from a range of issues related to the security and usability of the approaches. Further to this, they are still mostly functioning at the point-of-entry and those performing sort of re-authentication executing it in an intrusive manner.

Research has suggested novel approaches to authentication such as transparent authentication and cooperative and distributed authentication. However, these technologies either merely focus upon individual platforms rather than providing a universal and federated authentication approach that can be used across technologies and services, or require each participating device to be capable of supporting a level of biometric processing, configuration and management in order to achieve a good level of performance.

In order to provide the users' digital devices with adequate protection and convenience, innovative robust authentication mechanisms have to be utilised in a universal level, so they operate in a transparent, continuous and user-friendly fashion. Biometrics can be deployed in a usable manner that enables non-intrusive samples capturing. It is non-transferable to others, unforgettable, cannot be easily lent or compromised, and thus eliminate the potential threat posed by social engineering. Therefore, the use of transparent authentication using biometrics would enhance both the requirement for a robust authentication mechanism and the user’s need to eliminate any inconvenience during the authentication process. However, devising a federated biometric authentication model requires detailed insight about main biometrics related aspects in order to take them into consideration.

3 Biometric Authentication

3.1 Introduction

Having established the need for a novel, secure, convenient and universal authentication system that can be accomplished seamlessly in a location, technology and service independent fashion, biometrics is envisaged to be the authentication approach that can be deployed to serve such a system. Thus, this chapter presents and discusses the use of biometric authentication as a potential crucial cornerstone to solving the research problem including highlighting its applicability and capability to be implemented in a transparent manner. It begins by describing the generic biometric processes and operational modes as well as the main components. An overview of the requirements of the biometric system and the factors that affect its performance is outlined. Additionally, an analysis of biometric techniques is presented, highlighting the features of the deployment of multibiometrics and their standards, concluding by a review of some key relevant frameworks and their specific applicability within TAS.

Throughout history, people have been using human traits (biometrics) to identify others. For instance, it is possible to identify an acquaintance by recognising their known faces, voices and/or odour. Their high level of uniqueness to a distinct person has been adopted for identifying and authenticating users accessing environments that require high security, such as governments, borders and military. After over 50 years of comprehensive research and development of biometric authentication mechanisms, they further have evolved in the last 10 years to be deployed in numerous daily mainstream applications and devices, ranging from smartphones, laptops, keyboards, mice to ATMs and time and attendance. Accordingly, the biometrics market is predicted to grow over 304% between 2016 and 2022 to exceed $32.7 billion (Markets and Markets, 2016). Furthermore, it is anticipated that the market of

smartphone biometrics products and services, in particular, would grow from one billion in 2016 to surpass two billion by 2022 (Acuity Market Intelligence, 2017).

Nanavati et al. (2002) and Woodward et al. (2003) introduces compatible definitions of biometric system that can be consolidated as an automated identification or verification of an individual using measureable distinct behavioural or physiological traits. It is apparent from the definition that automation of the process involved is fundamental. Generally, any biometric system comprises of two processes to perform (Figure 3-1). The first stage is enrolment, during which a discriminative sample (or perhaps a number of samples dependent on the technique used) of an individual's trait is collected, classified and then stored as a template. It is imperative that this process is conducted with a high degree of quality, accuracy and assurance that the template created is of a genuine user (Clarke, 2011; Jain et al., 2008). During the second process – authentication, the user provides biometrics sample(s), which are then classified (and possibly fused with other biometrics) and subsequently compared with the stored template resulting on a value of the degree of matching between them (Jain et al., 2008). Based on this resultant value and the predetermined threshold (i.e. the tolerable degree of dissimilarity), a decision is made whether to grant access or not. Determining this threshold is pivotal due to its effect on both usability and security; if it is set too low, it would increase security but at the same time reduce the usability level as most probably legitimate users would have many access failures (i.e. False Rejection Rate (FRR)). In contrast, setting it too high may lead to falsely granting access to illegitimate users (i.e. False Acceptance Rate (FAR)). These two errors are explained in section 3.4. Both enrolment and authentication processes and their underlying phases should be conducted in an automated or semi-automated (i.e. when the user establishes the enrolment intrusively) manner to comply with the aforementioned definition of biometric system.

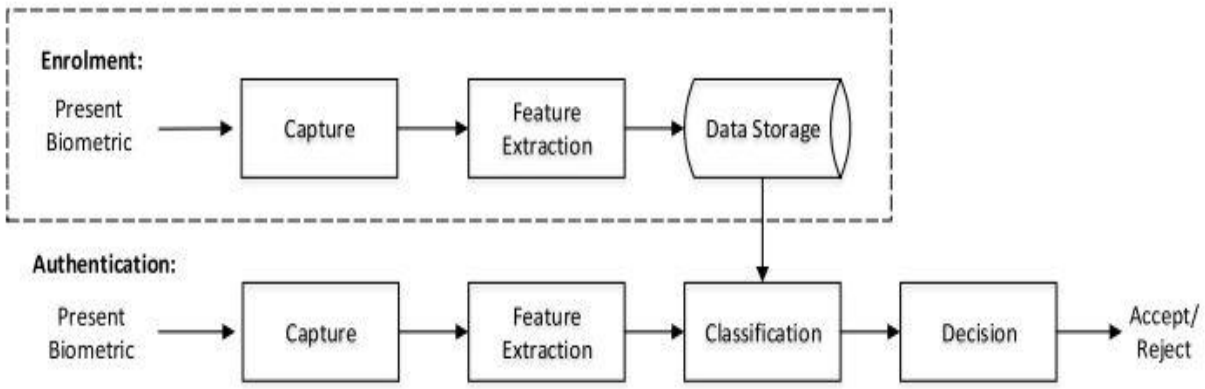

Figure 3-1: The Two Processes of a Generic Biometric Authentication System (Saevanee, 2014)

It is also noteworthy to highlight that there are two operational modes of biometric systems: verification and identification (Furnell & Clarke, 2005; Jain et al., 2008; Nanavati et al., 2002; Woodward et al., 2003).

- **Verification**: seeks to verify that a claimed identity is matched with that on the database.
- **Identification**: seeks to determine whether the identity exists on the database (open-set identification), or who the person is assuming they already exist on the database (closed-set identification).

During verification mode, the matching process is between sample(s) of claimed person and the stored template of that person; thus, it is a one-to-one comparison. In contrast, the comparison is one-to-many in identification mode; anonymous sample(s) is compared with every stored template to decide whether there is a match. This means that there is a possibility that the user's template does not exist at all in the database. Therefore, the result of the former mode confirms that claimed identity is true or false whereas the latter determines whether the user is identified or not.

These two distinct modes are dependent on the application context; if the user has claimed having enrolled in the system by presenting an identity, for instance a username or token with

a biometrics, the former mode operates, otherwise the latter does so (Vallabhu & Satyanarayana, 2012). Moreover, other aspects should be considered when deploying either of the two modes – they are different with respects to performance and privacy (Clarke, 2011; Nanavati et al., 2002) as well as cost and users' convenience (Clarke, 2011). Furthermore, the time needed for identification is usually longer because it involves more complexity and computation. Having said this, it is evident that identification requires higher level of system's accuracy and uniqueness of traits than verification.

The aforesaid biometric system definition states that it utilises physiological and behavioural biometrics. The former category refers to those traits related to people physical appearance, such as fingerprint, facial recognition, iris and retina scan, and hand geometry. On the other hand, the latter one refers to the way people behave, such as voice and gait recognition, and keystroke dynamics. Both categories are linked (with varying accuracy) directly to the user alone; with which users cannot deny their responsibility of the access/incidence occurred. However, typically, behavioural biometrics are less unique, thus they would not be suitable for identification mode that requires a high precision, especially in a large scale application (Saevanee et al., 2012). In spite of the effectiveness of biometric systems in guarding against theft, forgetting, counterfeit, reproduction, and hiding (O'Gorman, 2003; Schouten & Jacobs, 2009), they are vulnerable to falling foul in any of these pitfalls if only one modal (trait) is deployed (O'Gorman, 2003).

3.2 Biometrics Requirements

Selecting a biometric authentication approach to employ is not only dependent upon its level of uniqueness and performance, but also upon other requirements, which are important to be considered. The appropriateness of the potential biometric authentication technique is

determined based on the availability of the following requirements on the associated trait as proposed by (Jain et al., 2002):

- **Universality**: The utilised trait should be possessed by every individual of users population, such as if all users have hand, it would be possible to use hand geometry as biometric technique.
- **Uniqueness**: The selected trait should have sufficient level of distinctiveness to each user proportional to the application environment. For instance, whilst face trait would be suitable for accessing a smartphone, accessing military information requires a more unique trait such as iris.
- **Permanence**: It is imperative for the chosen trait to be constant or less changing over time. The more the frequent changing of a trait, the more the need to update the biometrics template and hence the cost of maintenance (Clarke, 2011). For example, whereas individual retina scan remains invariant, their keystroke behaviour varies due to device, mode, and text familiarity.
- **Collectability/Measurability**: To decide whether a specific biometrics characteristic is suitable for a biometric system, the ease to collect and then measure it digitally is critical. Collecting some biometrics is very intrusive – it requires specialised devices and/or explicit user interaction, such as retina. Conversely, others can be collected easily with normal daily devices and interactions, such as capturing voice samples while having a phone call.
- **Performance**: The accuracy and scalability of the technologies required to acquire the trait's samples should be considered with their applications and constraints.
- **Acceptability**: End-users of an adopted biometrics should be willing to provide their traits and utilise the technique, in terms of, for instance, privacy and convenience. Otherwise, they would resist or avoid using it.

- **Circumvention**: The degree to which a trait is vulnerable to be forged should be taken into account. For instance, iris scan is almost impossible to imitate, unlike ordinary facial recognition (which does not support liveness test).

It can be deduced that a perfect biometrics trait to be deployed in an authentication system should meet all the above-mentioned requirements. However, none of them is perfect, but depending on the application requirements, a number of them are acceptable to some extent (Jain et al., 2008). For instance, even though retina is one of the most unique biometrics, permanent and difficult to circumvent, its capturing process requires special equipment and user acceptability is an issue due to many reasons such as ease of use and user privacy. On the contrary, voice recognition tends to have a high user acceptability and simpler sample acquisition; however, its stability and robustness against impersonation are challenges.

3.3 Components of Biometric System

In order to achieve biometric authentication, a typical biometric system consists of five incorporated components as illustrated in Figure 3-2 (Clarke, 2011; NSTC, 2006a):

- **Sample Capturing (Acquisition)**: The biometrics samples are acquired from a genuine user using an applicable capturing device or method. Whereas some biometric techniques require specialised sensors, such as hand geometry, others may either employ normal affordable separate devices or embedded technologies, such as facial recognition using a webcam or mobile front camera.
- **Feature Extraction (Processing)**: Deploying specific algorithms, the unique characteristics of the captured sample(s) are processed aiming at generating a feature extraction template. For instance, after a fingerprint sample is captured, a number of algorithms are performed to extract its distinctive features, such as the curvature and width of ridges, to create the template.

- **Template Database**: It stores the biometric template resulted from the sample feature extraction process – perhaps along with other user's information. This stored template is used as a reference in the matching process afterwards.
- **Matching (Classification)**: When an individual attempts to have access by providing current biometrics samples, the features of these samples are extracted and subsequently compared to the stored reference template(s) using a matching algorithm. Accordingly, a match score is given representing their degree of similarity, based upon which the authentication decision is followed.
- **Decision**: A comparison between the matching score and the set threshold is performed – if the former equals or exceeds the latter, the access is granted; otherwise the access is denied or restricted.

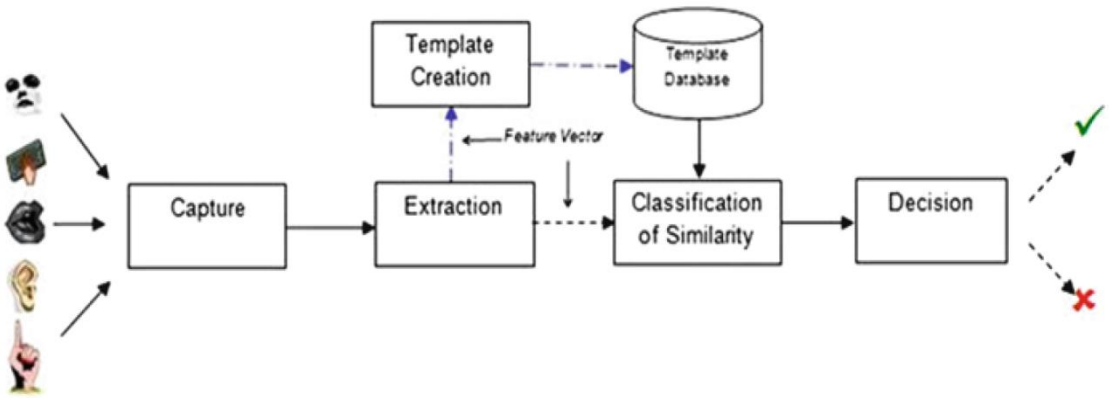

Figure 3-2: The Components of a Biometric System (Clarke, 2011)

3.4 Biometrics Performance Metrics Factors

Having stated that the decision of a biometric authentication process is based on the result of comparing the pre-enrolled template of legitimate user with the captured sample(s), achieving a precise 100% match is unlikely due to a variety of issues, such as environment noise and trait variability (Furnell & Clarke, 2005). This affects the biometrics performance that leads

to probability of mislead results which grant access to adversaries or deny access of authentic users. These performance metrics are referred to as (FAR) and (FRR), respectively. Jain et al. (2002) and Woodward et al. (2003) defined these error rates as follows:

- **FAR (False Acceptance Rate)**: It measures the rate of biometric technique errors in accepting illegitimate individuals.
- **FRR (False Rejection Rate)**: It measures the rate of biometric technique errors in rejecting legitimate individuals.

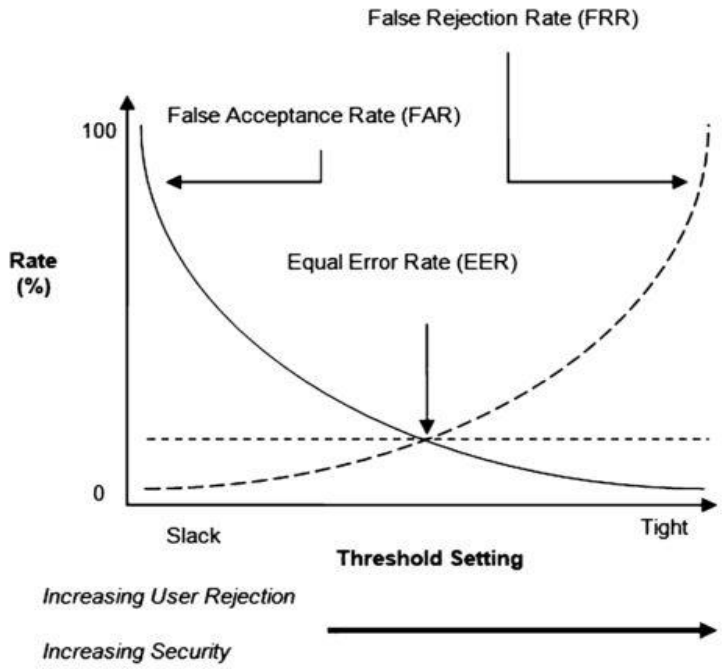

Figure 3-3: Biometrics Performance Metrics Factors (Clarke & Furnell, 2005)

Based on the pre-set threshold, which controls the tolerable level of each metric, the security of biometric systems and the user's convenience can be determined. As illustrated in Figure 3-3, these two performance metrics have an inverse relationship. If the threshold is set tighter (i.e. requiring a high matching level), it may yield to legitimate users being denied access (i.e. FRR), thus increasing the protection thereby minimising the potential of unauthorised users obtaining access (i.e. FAR). Consequently, legitimate users might frustrate from repeated authentication failure – thus hindering the adoption of such a system. On the

contrary, if the threshold is set more relaxed (i.e. requiring a low matching level), it increases the likelihood of impersonators being accepted (i.e. FAR). Even though that this tends to provide a more convenient authentication process to genuine users by reducing the possibility of being rejected (i.e. FRR), it would be at the expense of security. Therefore, a balance between system security and user-friendliness should be considered carefully.

The FAR and FRR are widely accepted as measure factors for biometric systems along with a third one named Equal Error Rate (EER) that is also depicted in the same previous figure. The EER is the point where FAR curve intersects with FRR curve – i.e. where FAR equals FRR – and is used for the comparison between different biometric systems (Clarke & Furnell, 2005; Jain et al., 2002; Nanavati et al., 2002; Woodward et al., 2003).

It can be interpreted that the lower EER, the better the overall performance of a biometric system. However, the desirable EER would be sought based on users and applications needs and capabilities and tolerance slack to both types of errors. For instance, an increased FRR could be bearable in accessing financial accounts in exchange for securing them by having a reduced FAR.

On the other hand, in practice, there are other complications users might encounter besides the aforementioned error rates. Although they are referred to synonymously in some literature such as in (Jain et al., 2008; Woodward et al., 2003), the False Matching Rate (FMR) and False Non Matching Rate (FNMR) can be considered subsets of FAR and FRR, respectively (Clarke, 2011). The FMR and FNMR measure the performance coming out of the matching stage whereas the FAR and FRR measure it at the decision stage. The FAR/FRR metrics are more inclusive; in that they also encompass the Failure to Enrol (FTE) and Failure to Capture (FTC) rates.

- **FTE (Failure to Enrol)**: It shows the rate of unsuccessful biometrics registration where individuals are unable to create an initial template (Furnell & Clarke, 2005; Jain et al., 2008; Nanavati et al., 2002; Wayman, et al., 2005; Woodward et al., 2003).
- **FTC (Failure to Capture)**: It is also known as Failure to Acquire (FTA) – indicates the rate of biometrics sensor device fails to acquire/capture a biometrics sample and locate it on the templates database (Clarke, 2011; Jain et al., 2008; Woodward et al., 2003).

The FTE is a consequence of the FTC occurrence but not the opposite as the latter could be at a later stage after the initial enrolment. Both errors may be caused by a variety of reasons, including but not limited to: missing the main related trait (e.g. missing finger or hand completely); poor quality of the biometrics sample that could be attributed to sensor deficiency (e.g. those caused by wear and tear); environmental effects (e.g. noise or poor lighting); users mistakes (e.g. wrong posture for facial recognition); or inconsistent measured pattern (e.g. changing on the way of user's typing on keyboard).

Precautious practices might mitigate these errors, such as selecting the most appropriate biometric system to the targeted users population where the utilised trait(s) is/are available typically as well as consistent; maintaining the sensor periodically; designing the system in a way avoiding the impact of surroundings along with a usable interface; and offering an efficient and easy method to update templates.

Given these different performance metrics factors, it is apparent that they, in one way or another, affect other biometrics requirements mentioned in the previous section. For instance, the FAR provides an indication about the uniqueness of biometrics characteristics (Wayman et al., 2005). In addition, quantifying universality can be done by the FTE whereas collectability by the FTC (Wayman et al., 2005). Furthermore, all the mentioned metrics (i.e.

FAR, FRR, EER, FTE and FTC) contribute to the appraisal of biometric system performance, the degree of circumventing the associated trait, and users' acceptance of employing that system. Therefore, envisaging a correlated picture of such a system involving all of these metrics gives better understanding of it although it might vary in the real use due to the lack of controlled conditions guaranteed during the evaluation process (Clarke, 2011).

3.5 Biometric Techniques

As mentioned in the previous section, biometric techniques are categorised into two main categories based upon the nature of the deployed discriminative trait: physiological and behavioural. Whilst a variety of technologies have been proposed and adopted, those of the former category are the most embraced. The Biometrics Institute Industry 2013 Survey reveals that the order of which biometrics the respondents are involved in begins with fingerprint recognition and then facial recognition, followed by iris recognition, multimodal (i.e. the combination of two or more biometric modalities), and voice recognition respectively (Biometrics Institute, 2013). Given that voice recognition is the only behavioural biometrics of the survey list and it is at its end, it is evident that physiological biometrics are more established and hence have the biggest users' adoption to date.

This section briefly outlines a number of leading biometric techniques with a view of the applicability of utilising them on the research proposal – each has its own pros and cons and is more appropriate to and used in specific domains. The list of biometrics provided, however, should not be considered comprehensive due to unforeseen suitability of some other techniques to the research proposal or due to immaturity of others which are still in the infancy stage of being researched and produced.

3.5.1 Physiological Biometrics

Physiological Biometrics methods aim at distinguishing an individual based upon specific physical characteristics, such as fingerprint and face, which tend to be invariant, thus applicable to be utilised for both identification and verification (NSTC, 2006a).

3.5.1.1 Fingerprint Recognition

Fingerprint recognition is the oldest and most prevalent deployed biometric (Biometrics Institute, 2013; Jain et al., 2002; Woodward et al., 2003) due to its heritage with forensics applications, besides the emerging use in immigration, attendance, and computing/mobile systems. These applications encompass both physical and logical access control. This might be owing to the fact of extensive research have been conducted and empirically proven that fingerprint recognition method has high level of individuality to each finger and thus person, matching accuracy, permanence, maturity, and affordable sensors (Jain et al., 2008; Maltoni et al., 2009).

Fingerprint recognition compares ridges, valleys and patterns of an individual fingerprint utilising one of the three matching classification approaches: correlation-based, minutiae-based, and ridge feature-based (Jain et al., 2008; Maltoni et al., 2009). It had been in use manually by law enforcement for more than one hundred years (with ink on cards), up until the 1960s when it became automated with the Automated Fingerprint Identification System (AFIS) (Jain et al., 2002; Maltoni et al., 2009). The Federal Bureau of Investigation (FBI) developed it, in 1999, with respects to response time and capacity as well as including the ten fingerprints to be the Integrated Automated Fingerprint Identification System (IAFIS) (NSTC, 2006a; Woodward et al., 2003).

Whilst these applications are used primarily for identification mode by forensics agencies where a suspect does not claim or declare an identity, fingerprint recognition has been

integrated in other ubiquitous verification based applications where the user claims an identity while, for instance, accessing his/her own device, such as laptops (e.g. HP EliteBook 2570p (HP, 2014)), and smartphones (e.g. Apple iPhone 5S (Apple, 2014; Mogull, 2013) and Samsung Galaxy S5 (O'Boyle, 2014; Samsung, 2014)).

This permeated deployment, notwithstanding; still it suffers from performance and usability issues. Fingerprint readers might endure wear and tear effects over time and fingerprints themselves might be covered by dirt or have small cuts, for example. This would deteriorate the performance by increasing the error rates and accordingly increase users' inconvenience. On the other hand, spoofing attacks (e.g. silicon replicas) were risen as concerns along with the possibility of steeling fingerprints of persons from touched objects or even from distance using a standard camera (Chaos Computer Club, 2014). However, current fingerprint readers are augmented by liveness sensor with which some data are extracted to decide whether the sample is taken from a living person (Clarke & Furnell 2005; Maltoni et al., 2009).

3.5.1.2 Palmprint and Hand Geometry

Palmprints were employed in 1858 manually with ink on employment contracts in India (NSTC, 2006b). Thus, it can be deemed as the second oldest used biometrics in official transactions after the fingerprint; however, unlike the fingerprint trait, it has not evolved to be automated until 1994 in Hungary (Woodward et al., 2003). Since then different palmprint recognition solutions have been developed and adopted gradually within the commercial and state domains up until embedding it into the FBI's IAFIS and subsequently their recent Next Generation Identification system (NGI) in which palmprint capability added to it (Mears, 2013; National Science and Technology Council, 2011).

Palmprint recognition system identifies individuals based on the unique features of their inner hand palm. It shares the comparison criteria with fingerprint recognition system – it compares

the geometry features, i.e. sizes, as well as ridges and minutiae features of the palm (Jain et al., 2008).

Therefore, it can be used for identification and verification modes. However, it has some shortcomings in addition to those of the fingerprint techniques; for instance, the large capturing machine, the relatively larger template size compared to fingerprint, and the probability of palms geometry features to change due to aging or weight.

Similarly, hand geometry measures some of the hand characteristics but from the outer surface; in particular, length, width, thickness and surface area of the back of the hand and four fingers (Nanavati et al., 2002; Woodward et al., 2003). However, despite the early automated implementation (i.e. Identimat) in the early 1970s and other successive patents, hand geometry systems can only be utilised to verify not identify users because these characteristics are not very distinctive (Jain et al., 2008).

It has been utilised for a variety of purposes, including time and attendance, physical access and border crossing as a standalone or in combination with other biometrics, such as palmprint or facial recognition (Jain et al., 2008). Whilst its use is perceived as straightforward, it is intrusive as the user should be cooperative to collect the samples. As the hand samples are extracted and generated in a silhouette format, the template size tends to be relatively small and so does the memory required. In addition, hand geometry devices are typically built to function even in challenging environments, such as outdoors. Nonetheless, their current large physical size is perhaps prohibitive to daily use personal computing applications (Clarke, 2011).

3.5.1.3 Facial Recognition and Facial Thermogram

Recognising and identifying known people based on their faces has been utilised since the commencement of creating people; however, it is up until the first semi-automated facial

recognition system was developed in the 1960s (Li, 2012). The maturity of its classification algorithms have been researched, developed and adopted steadily to be used in various scenarios, from passport identification and surveillance applications, to physical/virtual access control, to more recently smartphones authentication. It is considered the second biometric after fingerprint with respect to users adoption and the sale rate (Biometrics Institute, 2013).

This is, perhaps, attributed to its capability to be utilised in a transparent fashion (i.e. without cooperation or interaction of the user) leveraging ordinary camera, such as a webcam, as the capturing sensor. The measured characteristics are usually dimensions of the eyes, nose, mouth, ears, cheekbones, and distance between most or all of them based on different proprietary algorithms (Clarke & Furnell, 2005). The effectiveness of such algorithms vary depending upon several factors: the stability of the extracted face features over time, surrounding illumination, image resolution, face distance and position from the camera, and liveness test provisioning.

A number of solutions to tolerate or control some of these factors have been proposed. Using a three dimensional image might assist in mitigating the effects of face orientation and lighting conditions, albeit the need for 3D camera/sensor would thwart its acceptance and propagation (Clarke, 2011) as they tend to be more expensive and slower to respond (Jain et al., 2008). Furthermore, Clarke et al. (2008) proposed a more sophisticated composite model in which a number of user's face images in different sizes, illumination and orientations are collectively stored as a template – when a sample is taken, it will be compared with the stored composite template (as illustrated in Figure 3-4). Nevertheless, the trade-off between user friendliness and security is an issue since the likelihood of rejecting a genuine user declines and that of accepting an imposter increases.

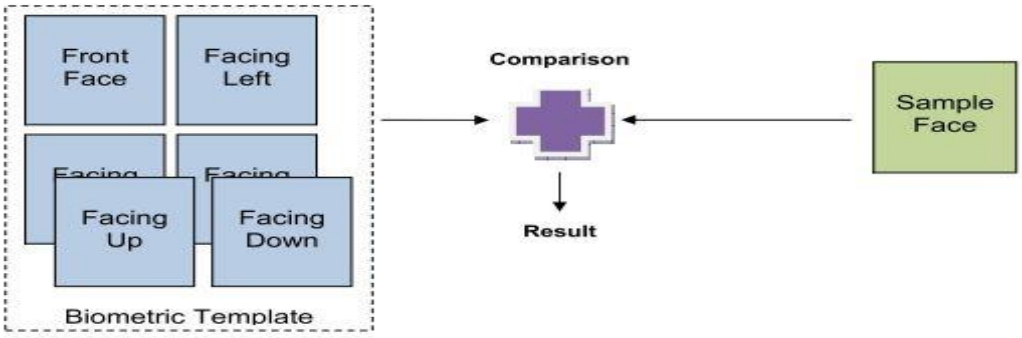

Figure 3-4: Facial Recognition with Various Orientations (Clarke et al., 2008)

Facial thermogram, also, has evolved as another solution to counter some of the drawbacks of facial recognition, such as poor illumination, poor image resolution and lack of liveness test. Facial thermogram captures the pattern of facial heat produced by the distinguishing blood flow under the skin that forms unique structure of veins and tissues utilising an infrared (IR) camera (Woodward et al., 2003). This thermal data that can typically be extracted with minimal environment inference and users interaction may enable transparent deployment. However, its performance alone has not reached the applicability for identification unless it is implemented in combination with other modalities, such as facial recognition with which the overall authentication performance would improve significantly (Socolinsky & Selinger, 2004). Moreover, given that the facial thermogram might disclose some confidential personal data, for instance, health conditions from blood liquidity or swelling (Woodward et al., 2003), privacy concerns might rise yielding to probable low users' acceptance.

3.5.1.4 Iris Recognition and Retina Recognition

Iris recognition is based upon distinguishing individuals in accordance to their irises which is the round coloured tissue formed of many furrows and ridges and surrounding the pupil of the eye (Woodward et al., 2003). It is believed the most accurate biometrics method due to the very distinctive complex irises patterns that are persistent throughout the life and

available in all ordinary people (Daugman, 2004). As a consequence, it can be used to verify as well as identify individuals.

The uniqueness of the iris of each individual had been empirically proposed and proven by different ophthalmologists throughout the last century until the patent of Leonard Flom and Aran Safir, in 1985 (Flom & Safir, 1987); based upon which a few years later patented algorithms were developed founding the automated iris recognition by John Daugman (Daugman, 1994).

Since then numerous iris recognition techniques and applications have been proposed, gained trust and put in practice by governments and companies (Roy & Biswas, 2011); ranging from borders control (e.g. in UAE since 2001, UK since 2004, Canada and USA since 2011), national identity (i.e. Aadhaar India's UID project since 2009), police (i.e. in USA since 2010), to websites and apps login (e.g. Eyelock device since 2011) (Markets and Markets, 2014). Having said that, iris recognition is the third adopted biometrics characteristic (Biometrics Institute, 2013) and even it has more growth potential in the next five years (Markets and Markets, 2014).

These optimistic anticipations can be owing to the promising features in terms of protection and users' convenience, coupled with the fact that the digital iris image can be acquired from distance without the need for users to have direct physical contact. Yet, some factors may lead to reducing the performance, such as blinking, eyelashes/eyelids occlusion, movement, and pose from camera. Nevertheless, these factors can be circumvented; therefore, developers have been producing a number of novel solutions and extraction classifications aiming at utilising any camera regardless of and/or to overcome the aforementioned issues (Daugman, 2007; Roy & Biswas, 2011). However, the more effective liveness detection solutions would require a high quality camera (recognition device), such as those of Chen et al. (2012) and

Galbally et al. (2012). The former proposal uses multispectral images that need less user cooperation opening the door for employing it in a transparent manner.

In relation to human eyes characteristics and similar to the accuracy and stability of iris recognition or even better, retina pattern distinctiveness was acknowledged in 1935, but the automated retina recognition technique was not developed until 1970s and commercially available in 1980s (Woodward et al., 2003). Using an infrared camera for illumination at a close distance, retina recognition systems read the unique pattern of blood vessels in the back of the eye (Clarke, 2011). The secrecy level of the pattern is very high as capturing it is not overtly available without special devices and users cooperation.

Consequently, it is considered very intrusive leading to narrow domains applicability and hence low adoption. Furthermore, directing the infrared wave to such a sensitive organ, the eye, may raise some healthy issues which might let users hesitant to accept being exposed to it. However, it is still useful and used for physical access control to locations of high security, such as military buildings (Nanavati et al., 2002).

3.5.1.5 Ear Geometry

Ear geometry recognition technique distinguishes individuals based upon the unique structure pattern of their ears, including concha, helix, antihelix, and other discriminative features (Ross, 2011). The potential of these features in identifying people was considered in 1890 by Alphonse Bertillon but has not been empirically proven until Iannarelli (1989) developed his system and since then it has been implemented manually in law enforcement and forensics domains (Arbab-Zavar & Nixon, 2011). Since then a number of proposed automated ear recognition systems and related classification algorithms have emerged, such as Cummings et al. (2010) that achieved 99.6% success rate. Therefore, it can be used for identification and verification modes.

It has been evidenced that the ear unique characteristics are relatively stable throughout the life span unlike those of the face that have noticeable effects of aging (Wu, 2011). In addition, they can be recognised from distance and they are not impacted by surrounding factors (e.g. illumination), apart from varying angles and hair and earrings occlusion which can be controlled and normalised (Abaza et al., 2013; Arbab-Zavar & Nixon, 2011). Albeit these promising features and high accuracy, there is no any commercial ear geometry product (Clarke, 2011; Ross, 2011). However, the aforementioned attributes and the fact that the ear is normally universal along with the specifications of smartphones that are equipped with front camera could enable its transparent applicability, i.e. when the ear samples can be acquired while the user normal call interaction (Clarke, 2011).

3.5.2 Behavioural Biometrics

Behavioural Biometric techniques discriminate individuals based upon measuring characteristics and pattern of their way of usage, such as speaking and typing on a keyboard (Woodward et al., 2003). Despite the less degree of uniqueness and permanence caused by the erratic nature of these behavioural traits due to different reasons, such as changing mood, health, and environment, they tend to be more universal, transparent, and hence usable than the physiological ones (Clarke, 2011).

3.5.2.1 Voice Recognition

It can be implied from its name that voice recognition verifies the identity of users by the distinctive aspects of their voice. Depending on the employed classifier, these aspects can be either of low level, including quality, duration, intensity dynamics, and pitch of the signal and/or high level, including rhythm, speed, modulation, intonation, pronunciations and education level (NSTC, 2006c). It is also called speaker recognition and voice verification

but it is worth noting to differentiate it from speech recognition system in which the focus is on what is being said rather than the way of saying (Nanavati et al., 2002).

Voice recognition operates in two modes: constrained (text-dependent) and unconstrained (text-independent) (Woodward et al., 2003). With the former, the user speaks a predefined phrase or given number(s) whereas the spoken input is free with the latter. Whilst both of them are viable, it is argued that the text-dependent mode offers lower error rates (Woodward et al., 2003) though with higher intrusiveness, where the user cooperation is pivotal.

Gunnar Fant, in 1960, pioneered an x-rays based model for the acoustics of speech production (NSTC, 2006c). Since then many related research groups (e.g. the NIST Speech Group) have been founded; many related patents have been issued; many studies and evaluations have been conducted striving to enhance the voice recognition systems (Jain et al., 2008). Accordingly, it is currently the most deployed behavioural biometrics and the fifth among all biometrics (Biometrics Institute, 2013).

Likewise facial recognition, voiceprint recognition, in most algorithms, is able to leverage existing hardware on the devices the user normally interacts with, such as smartphone and PC microphone. Further to the abovementioned development and the ease of use, the embedment of speech recognition technology in the recent smartphones (e.g. Siri in Apple iPhone and iPad) may offer a promising future for voice recognition (Huntington, 2012). However, there are some issues to consider with it, encompassing those affecting the quality of the sample, for instance sickness and ambient noise; and those for enhancing the detection capability of imitator or recorded voice. Various countermeasures to vulnerabilities have been produced, such as suppressing background noise and incorporating it with another authentication method. The latter can be indirect, for example by requesting the user to speak out a password, or direct by augmenting it with another biometrics modality. Therefore, it tends to

be used to verify rather than identify users. Even so, it may be an effective transparent authentication technique.

3.5.2.2 Signature and Handwriting Recognition

Handwritten signature and general handwriting are considered as attributes of an individual. Thus, handwritten signature has been used commonly for numerous law, official, business and financial transactions to certify the identity authority, e.g. signing a contract. According to Woodward et al., (2003) and Jain et al., (2008), the first acknowledgment of its potential in verification was published by Osborn in 1929, and then evolved from being purely manual using pen and paper to a digitised recognition system in 1980s. Subsequently, the proliferation of touchscreen devices has led to apply the similar individuality to handwriting verification.

Verifying the authenticity of the handwritten signature and handwriting can be conducted using static (off-line) or/and dynamic (on-line) approaches (Alonso-Fernandez et al., 2009). The former is merely carried out by examining the handwriting appearance, i.e. the curvatures, angles and patterns of letters or symbols and comparing it with the genuine image. On the other hand, information about how the handwriting was generated is involved with the latter, including pace, movement changes and pressure (Guse, 2011).

It is plausible to capturing the samples while a user is entering word(s), e.g. taking notes on a tablet PC or signing on a point-of-sale terminal. This makes it a viable candidate of non-intrusive transparent authentication. Furthermore, a promising performance was achieved by (Clarke & Mekala, 2007) with 0% FAR and 3.5% FRR in a controlled environment and 0% FAR and 1.2% FRR in a feasibility environment. However, the number of participants of that experiment is small and the effect of the written word length should have been focussed upon on the experiment. Moreover, although it is more difficult to forge the dynamic approach,

given the likelihood of variations in handwriting, even if they are done consecutively by the same person, it is still sufficient for verification not identification mode.

3.5.2.3 Keystroke Analysis

Keystroke analysis (or dynamics) is meant to verify individuals based upon their discriminatory typing patterns on a keyboard or keypad. The patterns data is extracted thereby deploying characteristics include: inter-keystroke latency (the interval time between two successive keystrokes), hold time (the interval time between pressing and releasing a key) (Clarke & Furnell, 2006), and possibly other augmenting features, such as the finger pressure on keys (Saevanee & Bhatarakosol, 2008).

Various studies revolving keystroke analysis have been undertaken since its inception as an applicable verification technique in 1970s, using different characteristics (mentioned previously) and classification methods (e.g. statistical and neural network) (Bergadano et al., 2002; Brown & Rogers, 1993; Gaines et al., 1980; Joyce & Gupta, 1990; Leggett & Williams, 1988; Spillane, 1975). Most of the studies have presented satisfactory performances feasible for verification mode or for identification only and only if combined with other authentication methods.

Analysing the keystroke dynamics can be categorised into (Banerjee & Woodard, 2012):

- **Static (text-dependent)**: with which the user keystroke behaviour is analysed while typing a predetermined text either at the point-of-entry (e.g. username and password) or possibly at a later stage during the normal interaction.
- **Dynamic (text-independent)**: there is no any particular predetermined text, so the user keystroke features are analysed whilst typing any text and comparing them against the reference template created during the enrolment stage.

Despite it may require a greater time and effort to train the classifier, the latter can be performed in a non-interfering and continuous manner making it more suitable to transparent authentication whilst the user is composing a text message, scheduling a meeting, or typing a document.

As keystroke analysis is claimed to be utilised on those varying devices that have keyboards or keypads with different interfaces and involving one or more fingers, a number of studies have examined some of these issues, such as (Karatzouni & Clarke, 2007; Saevanee & Bhatarakosol, 2008). Further advantage of keystroke analysis is the ability of employing it without the need for additional hardware; albeit, deploying the pressure feature may lead to the need for a pressure sensitive screen or keyboard which are not available on the ordinary ones.

Although it has been researched since the 1970s, it has not been developed and deployed extensively, except a few commercial solutions that incorporate it with other authentication techniques, for instance analysing the keystroke of typing the username and password. Nonetheless, whereas this may add a layer of security, it inherits some drawbacks of the other combined methods (i.e. the password in this example).

3.5.2.4 Behavioural Profiling

Behavioural (or service utilisation) profiling classifies the users based upon the distinct pattern(s) of their usage of devices' applications and/or services, such as which specific applications and websites they access, at which specific time of the day, for how long (Aupy & Clarke, 2005). A profile template is created from the user historical behavioural interactions to be utilised, subsequently, at the authentication process whilst the normal usage interaction to determine whether it is the genuine user identity or vice versa when the usage pattern deviates.

Research into behavioural profiling started in the late 1990s. However, the focus has been mainly on utilising profiling mechanism in intrusion (IDS) and fraud detection of telephony and credit card systems, such as the research of (Stolfo et al., 2000). This case is also applied on the commercial applications; to best of the author's knowledge, the available solutions in the market are limited to IDS and fraud detection system rather than conclusive behavioural profiling authentication systems.

The technique has been researched taking various aspects into consideration, such as network-based, device/host-based, desktop or mobile environments, and deploying it alone or coupled with other authentication techniques (Aupy & Clarke, 2005; Li et al., 2011; Saevanee et al., 2012). The user's location information also can be incorporated based on either the mobile cellular network (i.e. cell ID), the global positioning system (GPS) (i.e. longitude, latitude), or/and the IP address. Nevertheless, it might be considered as a fourth approach of authentication as proposed by the International Information Systems Security Certification Consortium (ISC2) and called someplace the user is (Conrad et al., 2012). Notwithstanding, it can be argued that it is under the behavioural profiling biometrics because location alone would not be sufficient to verify the user; hence it is an approach rather than a category.

Although behavioural profiling biometrics has the potential to monitor behavioural patterns on most categories of devices without interrupting the users from their typical interaction, which makes it a good alternative for transparent and continuous authentication, it suffers from privacy and acceptability issues. Fearing from private information leakage that might occur during the behaviour monitoring tends to affect the level of users' acceptance. Furthermore, comparative high probability of changing over time along with the low individuality of user behaviour (as most of the behavioural biometrics) it is probably more feasible to be incorporated with a multi factor/biometric authentication system.

3.5.2.5 Gait Recognition

Gait recognition is based upon discriminating people according to the patterns associated with their walking stride. The person's gait data is initially captured and enrolled to create a template, which is consequently used to be compared against; if the samples match it, the user is considered legitimate; otherwise, some security measures should be taken.

Cutting and Kozlowski (1977) were the pioneers in experimenting and proving the plausibility of identifying individuals on the basis of their gait. Since then, a number of studies have emerged revolving gait recognition from various perspectives, shifting it from being utilised mainly for surveillance purposes, to being deployed to authenticating users using wearable sensors (Gafurov & Snekkenes, 2009) or on mobile devices (Tanviruzzaman et al., 2009).

For the monitoring purpose, a camera is used to capture the gait motions to be analysed in a later stage when needed. This means that it is used from distance and without user cooperation. Different sensors are worn in the wearable type depending on the limb where it is put, such as on ankles, hip, or arms. In contrast, there is no need for additional equipment when smartphones capabilities are leveraged, in which the user's gait information can be collected while they interact with the device or even carry it on their pocket.

Thus, it is evident how applicable this technique is to non-obtrusive and continuous authentication. Nevertheless, its relatively low distinctive level as well as permanence over time, affected by many factors (e.g. footwear, health condition, and ground condition), lead to conclude that it is not sufficient for identification but for verification combined with other modalities.

3.5.3 Summary of the Biometric Techniques

In order to establish an insight about the usefulness of these biometric techniques to a universal innovative authentication solution, Table 3-1 demonstrates the aforementioned biometric techniques against the biometrics requirements discussed in Section 3.2 in addition to the transparency feature (where H, M and L represent High, Medium and Low respectively). At large, whilst it is evident that physiological biometric techniques tend to be better in terms of uniqueness, permanence and performance, they fall short concerning the collectability, user acceptability, and transparency unlike their behavioural counterparts.

It is also apparent that none of the biometric techniques outperforms all the others based on all requirements and none of them is free from scoring L (low). Therefore, no single biometric modality is ideal and fulfils all the requirements. However, dependent upon the application and context requirements, a number of them would perhaps be suitable to some extent. Moreover, this would be enhanced significantly if a combination of these techniques were utilised as part of a multimodal approach.

Biometric Techniques		Requirements							
		Universality	Uniqueness	Permanence	Collectability & Measurability	Performance	Acceptability	Resistance to Circumvention	Transparency
Physiological	Fingerprint Recognition	H	H	H	M	H	M	M	L
	Palmprint & Hand Geometry	H	M	M	L	H	M	M	L
	Facial Recognition	H	M	M	H	M	M	L	H
	Facial Thermogram	M	M	M	H	L	L	H	H
	Iris Recognition	H	H	H	M	H	L	H	M
	Retina Recognition	H	H	M	L	H	L	H	L
	Ear Geometry	H	H	H	M	M	M	L	M
Behavioural	Voice Recognition	H	M	L	M	M	H	M	H
	Signature & Handwriting Recognition	H	M	L	M	M	H	M	M
	Keystroke Analysis	M	L	L	H	L	M	M	H
	Behavioural Profiling	H	M	L	H	M	M	M	H
	Gait Recognition	L	L	L	H	L	H	M	H

Table 3-1: Biometric Techniques against their Requirements

3.6 Multibiometrics

Given the aforementioned presentation of leading biometric techniques, it is apparent that they can be offered as a single/uni-modal or multimodal biometrics. It is perceived that employing such a system stems some flaws depending on the particular utilised trait and classifications – making it probably inadequate for some applications, cases and populations. For instance, locations that require high security, such as borders and military bases, do not tolerate specific error rates most of uni-modal biometrics methods have. Another example is when a proportion of targeted users are not able to provide the utilised uni-trait, either permanently (e.g. a wheelchair person cannot have gait samples) or temporarily (e.g. a person with broken hand cannot have hand geometry samples).

These drawbacks can be mitigated by fusing and consolidating the resultant information presented by multiple biometrics sources within a system referred to as multibiometrics (de Oliveira et al., 2010). A number of researchers have proven that multibiometric systems outperform the uni-modal biometrics in improving: matching performance, universality, and resistance against spoof attacks (Jain et al. 2005; Ross et al., 2006; Sim et al., 2007), thus enhancing the overall system accuracy, reliability and robustness. Nonetheless, typically, cost, processing load, and vendor-specific solutions have to be profoundly considered before developing and adopting such a system.

3.6.1 Multibiometric Systems Categories

A multibiometric system can be one of the following categories based upon the contributing biometrics source(s) that are illustrated in Figure 3-5 (Ross et al., 2006; Jain et al., 2008; Clarke, 2011):

- **Multimodal**: multiple biometrics approaches are used (e.g. finger and face or keystroke dynamics and behavioural profiling).

- **Multi-instance**: using more than one subtype of the same biometrics (e.g. the right and left index fingerprints of an individual).
- **Multi-sensor**: multiple sensors are employed to capture a single biometrics modality of an individual (e.g. optical and capacitive fingerprint sensors).
- **Multi-sample**: a single sensor is utilised to capture more than one sample of the same biometrics trait taking account of their potential variations (e.g. frontal and side image of an individual face).
- **Multi-algorithm**: utilising more than one classification algorithm on a single biometric feature to subsequently consolidate the output to have an improved matching performance (e.g. minutiae-based and texture-based fingerprint classifier algorithms).
- **Hybrid**: a subset of the abovementioned categories is employed, aiming at optimising the recognition accuracy, for instance combining multimodal and multi-algorithm systems (e.g. two voice recognition algorithms integrated with three face recognition algorithms).

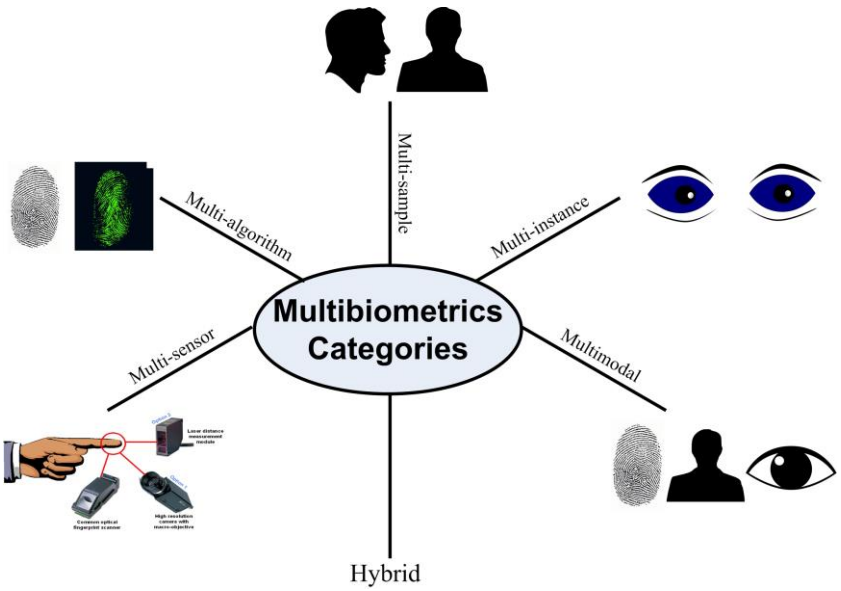

Figure 3-5: Multibiometrics Categories

3.6.2 Multibiometric Fusion Types

This variety of multimodal, multi-instance, multi-sensor, multi-sample, multi-algorithmic, and hybrid approaches seeks to optimise the authentication decision. Combining the information from these differing sources is called fusion. As illustrated in Figure 3-6, a multi-algorithmic approach would enable utilising a range of biometrics classification algorithms (each crafted to focus on differing aspects of the problem) and combine the results through fusion.

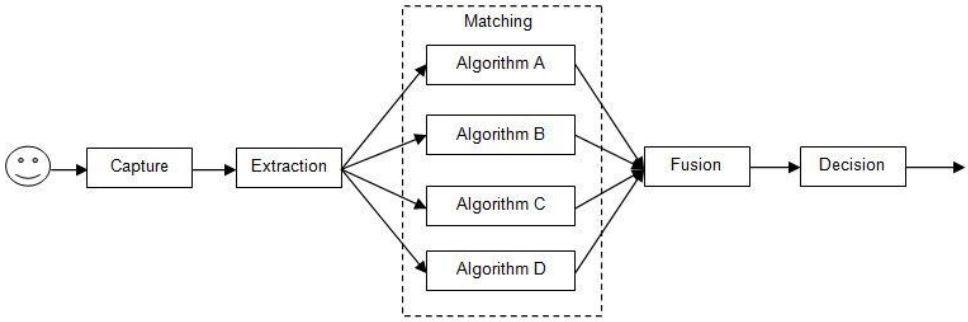

Figure 3-6: Multi-Algorithmic at Matching Score Level Fusion (Clarke, 2011)

Generally, as illustrated in Figure 3-7, fusion can occur at various phases of the authentication process; sensor, feature, matching score, and/or decision level (Clarke, 2011; Ross, 2007; Sim et al., 2007).

- **Sensor level fusion**: The raw biometrics data is consolidated prior to feature extraction these data were captured by multiple sensors or by a single sensor acquiring multiple samples (e.g. fusing different face images from one or different cameras).
- **Feature level fusion**: After obtaining multiple samples from one or more biometrics traits, the feature vector is extracted from each sample using a variety of algorithms. These feature vectors are then fused together to be used in the following matching phase (e.g. fusing the feature vectors of the face and iris).

- **Matching score level fusion**: The produced results of multiple biometrics classifiers are joined at this level to produce a new accumulated match score to be utilised for the subsequent decision process, as depicted in Figure 3-6. It is believed to be the most accurate and thus the most widely utilised fusion type (Ross et al., 2006).
- **Decision fusion**: This fusion occurs when each incorporated biometric system has provided its own decision to enable a final authentication decision.

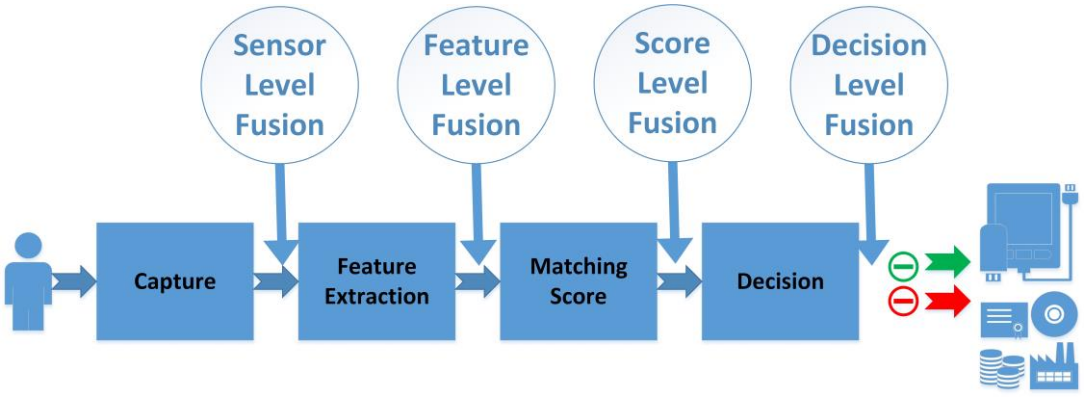

Figure 3-7: Fusion Types

This approach to the optimisation of authentication accuracy provides a very strong indicator as to the authenticity of the user. For example, as illustrated in Table 3-2, the use of multimodal systems can result in a significant improvement in the classification performance (Jain et al., 2005).

Classifier	FRR at a FAR=0.1%
Finger	16.4
Face	32.3
Hand	53.2
Multimodal (Minmax Norm)	2.2
Multimodal (Tanh Norm)	1.5

Table 3-2: Multimodal Performance using Finger, Face and Hand Modalities

This substantial enhancement in the whole performance of the biometric system the multibiometrics approaches offer leads to developing various large-scale applications, some of which will be listed in the following sub-section. However, issues should be taken into consideration to be eliminated for use in a TAS, such as overhead computation and potential

incompatibility between vendor-specific solutions. The former should be examined throughout the development process depending on the system/user requirements whilst the latter can be overcome thereby abiding by the available standardisation of biometrics (which are discussed in 3.7).

3.6.3 Multibiometrics Large-Scale Applications

The advancements provided by multibiometric systems have driven a number of large-scale governmental applications. The United States Visitor and Immigration Status Indicator Technology (US-VISIT) system verifies the passports of foreign visitors to the United States at the borders utilising fingerprints; it was initiated employing only right and left index fingers of a person and extended to all ten flat fingerprints (Ross, 2007).

Another high profile multibiometrics application is the FBI's Integrated Automated Fingerprint Identification System (IAFIS) which employs all ten fingerprints to create a criminal repository in order to be compared against during legal and forensics cases, or employment in sensitive positions (National Science and Technology Council, 2011). It is then expanded to include multiple modalities, such as palm, face and iris in its transitioned version Next Generation Identification (NGI), seeking to improve accuracy thus improving jurisdiction cases. For instance, whereas IAFIS offers an accuracy of 92%, NGI achieves 99.6%. NGI also deploys advanced matching algorithms which minimised the response time. For example, while IAFIS may take 2 hours to give a decision, NGI would not exceed 10 minutes when comparing against more than 60 million individual records repository (FBI, 2014; Mears, 2013).

Another endeavour and perhaps the largest multimodal biometrics identification system to date is the India's Aadhaar programme, aiming to eventually provide a national ID for about

1.2 billion Indians. It encompasses fingerprint, face and iris traits and have collected nearly 600 million multimodal records thus far (Collins, 2014; Onin, 2014).

Accordingly, as multibiometric systems have improved dramatically in performance and scalability supported by intense research in the area, there is a potential to further deploy them in large-scale civilian and commercial applications.

3.7 Biometrics Standards

Given that each biometric technique has its own differing types of sensors and algorithms (each is perhaps developed and offered by varying vendors), it is apparent that implementing a multibiometric system (e.g. multimodal and multi-algorithmic) is sophisticated. For such multibiometric systems to exist in a vendor- and modality-independent fashion, agreed upon standards are essential to be developed and conformed with. Typically, having multiple biometrics products each follows different data format, structure and metrics would yield to users being locked-in with a specific vendor regardless of the variety of performance and cost incurred (National Science and Technology Council, 2011).

Biometrics standards have been developed nationally and internationally concerning particular modality or the overall biometric system, enabling interoperability between various systems thereby, for instance, specifying unified biometrics data interchange formats. Interoperability is a pivotal aspect for implementing multibiometric systems. For example, images attained by one sensor must be compatible with those attained by another sensor besides it must be possible that both of them are interpreted by a third provider product.

One key standard in the arena is the Common Biometric Exchange Formats Framework (CBEFF) standard. It is developed by national and international standards development bodies (InterNational Committee for Information Technology Standards (INCITS) Technical

Committee M1 – Biometrics and ISO/IEC Joint Technical Committee 1 (JTC 1) Subcommittee SC 37 – Biometrics) to promote interoperability of multiple biometrics-based devices, applications and systems (NIST, 2008), thereby enabling the exchange of biometric information efficiently between system components (National Science and Technology Council, 2011). Some of the large-scale applications of biometrics have adopted and implemented this standard, such as the India's Aadhaar programme.

Furthermore, International Standards Organization (ISO) and International Electrotechnical Commission (IEC) have introduced dominant standards supporting the generic aims of biometrics standards: interoperability and data interchange among applications and systems. According to Podio (2011) and JTC 1/SC 37 (2013), ISO and IEC under Joint Technical Committee 1 (JTC1) Subcommittee 37 (SC37) determine that the main aspects covered by these standards are:

- common file frameworks (ISO/IEC 19785);
- biometric application programming interfaces (BioAPI) (ISO/IEC 19784);
- biometric data interchange formats (ISO/IEC 19794);
- related biometric profiles (ISO/IEC 24713);
- methodologies for performance testing and reporting (ISO/IEC 19795); and
- cross jurisdictional and societal aspects (ISO/IEC 24779).

Therefore deploying ISO standards such as ISO 19794, 19785, 19784 would avail incorporating any selected biometrics approaches – something individual devices would never be able to achieve due to prohibitive costs and processing requirements (ISO, 2006a, 2006b, 2011).

3.8 A Review of Continuous and Transparent Multibiometric Authentication Systems

Despite the benefits that biometrics has over conventional counterparts of knowledge- and token-based approaches, if they are applied at the point of session entry, they would arguably be insufficient to secure sensitive resources. With point-of-entry authentication only, the system is left vulnerable to being hijacked or misused afterwards as there is no post-of-entry assurance of the authenticity of the user. Continuous authentication has emerged to address this issue; however, usability issues have arisen when the user is prompted to intrusively and perhaps repeatedly re-verify to the system. Transparent authentication has then been proposed as a favourable solution which utilises biometrics to validate the user continuously in the background without requiring explicit abnormal user interaction (Crawford & Renaud, 2014; Traore & Ahmed, 2012).

After a thorough analysis of the related literature, a number of relevant search keywords have been identified within user authentication domain, i.e. “transparent”, “continuous”, “implicit”, “active”, “passive”, “non-intrusive”, “non-observable”, “adaptive”, “unobtrusive”, and “progressive” from various eminent academic databases. Accordingly, 93 studies have been reviewed, most of which (70%) only employ single biometric.

However, despite that these frameworks (shown in Table 3-3) have arguably contributed to solving the flaw of point-of-entry verification only by providing further consideration to on-going identity confidence, they have merely proposed uni-modal biometrics and hence have significant drawbacks.

	Modality	Studies
Behavioral	**Keystroke**	(Bergadano et al., 2002; Dowland et al., 2001; Furnell et al., 1996; Gunetti & Picardi, 2005; Hempstalk, 2009; Hossain et al., 2012; Leggett & Williams, 1988; Mahar et al., 1995; Marsters, 2009; Messerman et al., 2011; Monrose & Rubin, 2000; Obaidat & Sadoun, 1997; Roth et al., 2014; Shepherd, 1995; Umphress & Williams, 1985)
	Mouse	(Ahmed & Traore, 2007; Aksari & Artuner, 2009; Feher et al., 2012; Gamboa & Fred, 2004; Jorgensen & Yu, 2011; Lin et al., 2012; Mondal & Bours, 2013; Pusara & Brodley, 2004; Shen et al., 2009; Stanic, 2013; Zheng et al., 2011)
	Signature	(Clarke & Mekala, 2007)
	Gait	(Derawi et al., 2012; Gafurov & Snekkenes, 2009; Juefei-Xu et al., 2012; Kale et al., 2002; Lu et al., 2014; Mäntyjärvi et al., 2005; Morris, 2004; Nickel et al., 2012; Tanviruzzaman & Ahamed, 2014)
	Voice	(Abdullah et al., 2014; Kunz et al., 2011; Martucci et al., 2012; Woo et al., 2006)
	Behavioral Profiling	(Aupy & Clarke, 2005; Jakobsson et al., 2009; Li et al., 2014; Saevanee et al., 2011; Yazji et al., 2009)
Physiological	**Face**	(Clarke et al., 2008; Janakiraman et al., 2005; Klosterman & Ganger, 2000; Liu & Chen, 2003; Xiao & Yang, 2010)
	Ear	(Fahmi et al., 2012; Hurley et al., 2000; Islam et al., 2008; Rodwell, 2006)
	Finger	(Feng et al., 2012; Koundinya et al., 2014)
	Palmprint	(Kisku et al., 2012)
	Iris	(Chen et al., 2012; Du et al., 2011; Matey et al., 2006; Mock et al., 2012; Proença & Alexandre, 2006; Sui et al., 2012; Wildes, 1997; Yang & Du, 2011)

Table 3-3: Single Biometric Transparent Authentication Systems

As each of the above-mentioned models utilises a sole modality, they continue in carrying its shortcomings, thus enduring low matching performance, limited universality and higher vulnerability to spoofing attacks. Fusing more than one biometric (multimodal) can arguably contribute to overcoming or at least alleviating these flaws. As discussed previously in 3.6, a number of researchers have proven that multibiometric systems outperform the uni-modal biometrics. This section reviews the domain, focussing in particular upon the role that multibiometrics has and its viability in practice.

3.8.1 Continuous and Transparent Multibiometric Authentication Systems

Based upon a comprehensive analysis of the prior art on continuous and transparent multibiometric authentication systems, 28 research studies have been specified and are categorised into: physiological transparent multibiometric systems; behavioural transparent multibiometric systems; hybrid transparent multibiometric systems; distributed transparent multibiometric systems; and web-based transparent multibiometric systems. The first three

categories are according to the nature of the utilised biometric modalities, whereas the last two ones are according to their operational deployments that distinguish them from the others. The commentary on the sub-sections that follow describes the key achievements and milestones that have taken place. With respect to the performance criteria adopted to discuss these studies, they are based on the common declared varied metrics (i.e. FAR, FRR, EER, FMR, Matching score, Verification score, Recognition rate) on the results of the studies under each category. The concept of intrusive authentication utilised throughout this analysis refers to the occurrence when the user is interrupted by a system/application and required to provide credentials explicitly, e.g. password or biometric sample. Accordingly, the reduction percentage of intrusive authentication is quantified by comparing the number of explicit events a genuine user needs to authenticate to access the device explicitly while using the transparent framework to that number with a conventional authentication framework.

3.8.1.1 Physiological Transparent Multibiometric Systems

Table 3-4 demonstrates a number of studies that have investigated utilising physiological biometrics only aiming to continuously verify the legitimate user. From this perspective, Sim et al. (2007) experimented with the deployment of facial and fingerprint recognition characteristics within a biometric system. These modalities were holistically fused using Hidden Markov Model (HMM). According to the output of the verification along with the elapsed time, the authentication system responds by continuing granting user access, freezing some processes, or locking the system. They claimed that the traditional performance metrics, i.e. FAR, FRR, EER, are not suitable for such a continuous authentication system due to negligence of time within the calculation. Therefore, their system was evaluated based upon newly invented metrics: Time to Correct Reject (TCR), Probability of Time to Correct Reject (PTCR), Usability, and Usability-Security Characteristic Curve (USC). Nonetheless, to the best knowledge of the author, these metrics have not been adopted commonly to evaluate

other forthcoming continuous and transparent authentication frameworks making the comparison not possible. Although it was experimented using real data on a Windows XP desktop computer, the focus was only on testing the usability and it was not extensive enough to be generalised – only 11 participants carried out the experiment over 30 minutes each.

Author(s)	Platform	Biometrics			Performance (%)				Experiment Demographics	Mode	Limitations	Features
		F*	FP*	I*	Match	FAR	FRR	Verification				
Sim et al. (2007)	PC	√	√	-	-	-	-	-	11 participants 30 minutes	Real	New performance metrics	Holistic fusion Extendable
Azzini and Marrara (2008)	PC	√	√	-	48.6-72.5	-	-	-	300 minutes	Simulation	Intrusive login (FP)	-
Kwang et al. (2009)	PC	√	√	-	-	-	1	-	90 participants	Prototype	26-42% added processing overhead	-
de Oliveira and Motta (2011)	PC	√	√	-	-	-	-	-	40 participants	Simulation	Intrusive login (secret)	Multibiometric security API
Tsatsoulis et al. (2012)	PC/Laptop	√	-	√	-	3	-	84-97	61 participants 5 minutes	Real	Intrusive login (I)	-

* **F** = Face; **FP** = Fingerprint; **I** = Iris

Table 3-4: Physiological Transparent Multibiometric Systems

Similarly, Azzini and Marrara (2008) proposed a multimodal continuous system; however it only uses facial recognition for the ongoing user identity verification whereas the fingerprint is prompted whenever the threshold of the confidence on the authorised user is not met. Given that its achieved matching score ranged between 48.6 and 72.5%, it is evident that it suffers from low accuracy as it can, operationally, be considered unimodal. It was not even evaluated with real data – it was merely simulation (the same as de Oliveira and Motta (2011)) and thus no performance result was revealed. Likewise, although that Kwang et al. (2009) obtained a promising FRR of 1% with 90 participants, they had an additional 26-42% of processing computation overhead. This might lead to user frustration (if they are left waiting for the authentication decision) and/or higher power consumption. Further study in this domain was conducted by Tsatsoulis et al. (2012) who examined the feasibility of the system using iris and face recognition with 61 real users. They reached a verification rate of

84-97% and a FAR of 3%. However, it fell short in achieving a complete transparency due to having the user to intrusively login to the system using their iris (which is not checked after the login).

3.8.1.2 Behavioural Transparent Multibiometric Systems

The hindrance of transparently employing physiological biometrics has been evident; thus, a shift to behavioural counterparts was sought (as shown in Table 3-5). Further studies within the similar context were separately introduced relying only on behavioural biometrics (Li et al., 2011; Saevanee et al., 2014). The former study deployed the dynamic user profile of the usage of calling, text messaging, and general applications services on mobile phone with an EER of 5.4%, 2.2% and 13.5% respectively and an overall EER of 7.03%. The latter, on the other hand, disclosed that linguistic profiling, keystroke dynamics and behaviour profiling can be used to distinguish users continuously and transparently with an EER of 12.8%, 20.8% and 9.2% respectively and an overall EER of 3.3%. It was even claimed that their proposed approach reduces the number of intrusive authentication requests of conventional approaches by 91%. Despite these promising results, they were fully or partially acquired based upon desperate and limited off-line datasets not live ones. Therefore, they did not represent the real usage of a user. Although there were thousands of logged activities, the number of participants is considered limited. Furthermore, the dataset is dated back to 2004-2005, during which a few number of applications were available to users as well as the capabilities of the mobile phones were limited. What is more, is that the latter framework's experiment utilised separate datasets simulating that they were for the same users which was not the reality. Therefore, they perhaps did not reflect the real time and current practice nor the results.

Author(s)	Platform	Biometrics						Performance (%)			Experiment Demographics	Mode	Limitations	Features
		V*	M*	K*	B*	G*	T*	FAR	FRR	EER				
Ahmed and Traore (2005)	PC	-	√	√	-	-	-	0.651	1.312	-	22 participants 9 weeks	Real	-	IDS Client-server
Vildjiounaite et al. (2006)	Mobile	√	-	-	-	√	-	-	-	2-12	31 participants	Offline experiment	-	-
Pusara (2007)	PC	-	√	√	-	-	√	14.47	1.78	-	61 participants 10 days	Real	Detection time 2.20 minutes	IDS
Li et al. (2011)	Mobile	-	-	-	√	-	-	-	-	7.03	76 participants	Simulation	Off-line dataset	Analysed telephony, texting & apps services
Crawford et al. (2013) Crawford and Renaud (2014)	Mobile	√	-	√	-	-	-	-	-	(K) 10 (V) 25	30 participants 7 tasks	Real & Simulation	-	67% reduction of intrusive authentication
Saevanee et al. (2014)	Mobile	-	-	√	√	-	-	-	-	3.3	30 participants	Simulation	Off-line dataset & Real	91% reduction of intrusive authentication
Bailey et al. (2014)	PC	-	√	√	-	-	√	2.24	2.1	-	31 participants 3 tasks	Real	-	-

* **V** = Voice; **M** = Mouse; **K** = Keystroke; **B** = Behavioural profiling; **G** = Gait; **T** = Touchalytics

Table 3-5: Behavioural Transparent Multibiometric Systems

In line with providing authentication in a transparent and continuous manner using behavioural biometrics, Crawford et al. (2013) and Crawford and Renaud (2014) proposed a framework for mobile devices utilising keystroke dynamics and voice recognition. The study showed that it enhanced the usability, thereby reducing the number of explicit authentication requests by 67% from those of traditional counterparts. However, this explicit authentication was configured to be PIN which is secret knowledge not biometrics, thus still the user is prone to cognitive burden. Furthermore, no common overall security performance measures revealed to allow comparative studies but solely for each individual deployed biometrics – EER of 10% and 25% of keystroke dynamics and voice recognition respectively. Equally important, it would be ideal if an extensible evaluation was undertaken rather than experimenting it involving merely 30 participants with seven tasks. On the other hand, its applicability and universality have to be considered as it is confined to a single device – with

every device requiring biometric setup and enrolment, user configuration and management, risk assessment and continual refinement.

This is also applied to other studies in the domain (Ahmed & Traore 2005; Pusara 2007; Bailey et al., 2014). They investigated the feasibility of using keystroke and mouse biometrics to authenticate the user continuously. The first two studies were also featured as Intrusion Detection Systems (IDS). Conducting real evaluations on desktop PCs with varying number of participants, their performance results were (FAR of 0.651, 14.47 and 2.24; FRR of 1.312, 1.78 and 2.10) respectively. Despite augmenting their systems by Graphical User Interface (GUI) interactions of the user, the last two experiments undesirably showed lower accuracy. This perhaps is attributed to the arguable low uniqueness of the added GUI events. Moreover, the real usage and thus performance would differ from those under controlled environment where specific pre-set tasks are given to the participants to perform during the evaluation. Another related investigation was carried out by Vildjiounaite et al. (2006) fusing voice recognition with gait recognition of the user while mobile phone usage. They employed 31 users to experiment their proposed system offline. Nonetheless, even though they spent sufficient differing times training the classifiers of each modality, they accomplished divergent performance results (EER 2-12%), rendering it to be unstable.

All the aforementioned frameworks can only operate on a distinct device (a mobile or PC). Given that users nowadays use typically at least one from each of these platforms, extra care should be taken to their applicability and universality.

3.8.1.3 Hybrid Transparent Multibiometric Systems

Researchers have realised the difficulties of deploying physiological biometrics only together with the instability of behavioural biometrics only in a transparent manner, which in turn may increase the incidences of users being locked-out and required to re-authenticate explicitly.

Therefore, various studies have been proposed deploying a mixture of physiological and behavioural or soft biometrics (e.g. colour of face), as summarised in Table 3-6. One of the early studies that consider employing a set of biometrics for continuous authentication was proposed by Carrillo (2003) to safeguard aircraft cockpit and flight deck throughout. Her proposal provided two designs with regard to the location of processing: on board or distributed verification. However, there was no implementation nor evaluation as it was conceptual only.

Author(s)	Platform	Biometrics								Performance (%)					Experiment Demographics	Mode	Limitations	Features
		F*	FP*	V*	M*	K*	B*	G*	SB*	Match	FAR	FRR	EER	Recognition				
Carrillo (2003)	Flight Deck	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Conceptual	No experiment	2 designs: on-board & distributed verification Several biometrics
Altinok and Turk (2003)	PC	√	√	√	-	-	-	-	-	-	-	-	-	-	24 participants	Virtual data	-	Integration with time
Clarke and Furnell (2006)	Mobile	-	-	-	-	-	-	-	-	-	$2^{*}10^{-4}$	0.4	-	-	-	Conceptual	Intrusive login (secret)	Several biometrics
Kang and Ju (2006)	PC	√	-	-	-	-	√	-	-	-	-	-	-	-	-	Simulation	Intrusive login (secret)	-
Asha and Chellappan (2008)	PC	-	√	-	√	-	-	-	-	-	-	-	-	-	-	Conceptual	No experiment	e-Learning
Ojala et al. (2008)	Wearable & Laptop	√	-	-	-	-	-	-	√	40-60	-	-	-	-	-	Prototype	Intrusive login (F) Wristband	-
Clarke et al. (2009)	Mobile	√	-	√	-	√	-	-	-	-	-	-	0.01	-	27 participants 45 minutes	Real	-	Extendable Standalone & client-server
Soltane et al. (2010)	PC	√	-	√	-	-	-	-	-	-	-	-	0.087	-	30 participants 3 sessions	Simulation	-	Adaptive Bayesian fusion
Niinuma et al. (2010)	Laptop	√	-	-	-	-	-	-	√	-	0	4.17	-	-	20 participants	Real	Intrusive login (secret)	-
Muaaz (2013)	Mobile	√	-	√	-	-	-	√	-	-	-	-	-	-	-	Conceptual	No experiment	Fuzzy Crypto
Tsai et al. (2014) Khan et al. (2011)	Laptop	√	-	-	-	-	-	-	√	-	-	-	-	86.88	7 participants	Real	-	Swarm intelligence algorithms

* **F** = Face; **FP** = Fingerprint; **V** = Voice; **M** = Mouse; **K** = Keystroke; **B** = Behavioural; **G** = Gait; **SB** = Soft biometrics

Table 3-6: Hybrid Transparent Multibiometric Systems

The frameworks of Asha and Chellappan (2008) and Muaaz (2013) were also conceptual. Whilst the former employed fingerprint and mouse dynamics for e-learning environment, the latter utilised gait, face and voice recognition on mobile. Altinok and Turk (2003) suggested a multimodal continuous authentication system using voice, face, and fingerprint biometrics. It focused on the integration of biometrics modalities at a specific time to establish a level of certainty (confidence) using a Gaussian model, ensuring that the authorised user is present whilst this level degrades over time with absence of biometrics samples. However, there was no overall integrated system performance revealed. Moreover, evaluating such a system needs to be on the basis of real data not merely simulated as was the case in their work – they simulated just 24 virtual identities. Another proposal, without declared performance, simulated using the face and its behavioural features to implicitly assure the legitimacy of the user after an intrusive login using secret code (Kang & Ju, 2006).

Clarke and Furnell (2006) proposed a mobile-based system, Intelligent Authentication Management System (IAMS), using a combination of the secret knowledge-based approach and selected/available biometric techniques to provide transparent and continuous authentication. It was framed to operate in both standalone and client-server modes. Although it was expected to achieve a desirable performance (a worst case of FAR of 0.00002% and FRR of 0.4%), the evaluation was not comprehensive and not based upon real data. Furthermore, the flaws of using the secret knowledge-based approach are inherited, given it would potentially rely upon it if no other biometrics sample were available. It did however propose a general model for all transparent modalities.

An expanded subsequent implementation of TAS, the Non-Intrusive and Continuous Authentication (NICA), was conducted by Clarke et al. (2009). It was built upon the work suggested by IAMS utilising a mixture of secret knowledge authentication coupled with several chosen available biometric techniques. It is capable of choosing individual biometric

techniques to verify a mobile user based upon the configuration of their device. For instance, if a mobile device is not equipped with an inbuilt camera, NICA will only choose keystroke analysis and voice verification to verify the user. NICA does also consider the assumption that different services and data require different security provisions. Through understanding the risk associated with particular user actions and services, the protection level required can vary from almost none for checking the time, medium for texting, to significantly high for online banking. The level of confidence is continuously fluctuating based upon the biometric samples captured which is subsequently reflected on the privileges to access services and applications, enabling the device to shutdown functionality if insufficient confidence exists. Its evaluation was carried out involving 27 participants who completed specified tasks over an average of 45 minutes, whereby 60 biometrics samples were collected. As a result, it accomplished a performance of below 0.01% EER. However, it was a scripted evaluation that sought to understand users' opinions. It did not collect samples from real-world use. Having real participants conducting the trial with real but free tasks for a longer time and interval sessions may provide a more accurate insight of the system. Moreover, reducing the threshold to alleviate the error rates of deployed in-house biometrics algorithms would impact the accuracy of this result.

Soltane et al. (2010) attempted to overcome this by experimenting with integrating face and voice traits of 30 users for 3 separate sessions. The resulting EERs of the face and the voice verification studies were 0.449% and 0.003% respectively. These results, however, are questionable with the low number of users and even evaluated samples (merely 16 face images and 4 voice samples from each user). Interestingly, when using an adaptive Bayesian fusion method, the overall EER was 0.087%, that is better than that of face only but worse than the voice's. However, having multibiometrics is still desirable because it would harden

the system against spoofing attacks as if a modal is compromised the other one contributes to system protection. Furthermore, this result might be affected by the particular fusion method.

Studies were proposed blending the physical biometrics (i.e. face) with soft biometrics (e.g. face skin colour and clothes colour) aiming at providing continuous but passive authentication (Niinuma et al., 2010; Khan et al., 2011; Tsai et al., 2014). The last research is a successor of the work in Khan et al. (2011), so they are referred to here as one. Both studies were experimented on laptops deploying intrusive login (password or face) and then constantly comparing the soft biometrics histogram against what was collected at the login stage. Niinuma et al. (2010) achieved a zero FAR and 4.17% FRR with a sample of 20 participants whereas the recognition score of Tsai et al. (2014) using swarm intelligent algorithms was 86.88% with only 7 participants. Apart from the relatively small samples that would not resemble the reality, the variation of lighting throughout the usage session may contribute to frequent need to obtrusive re-verification leading to users' inconvenience.

From a different perspective, today's typical computer/technology users are nomadic and not confined to one location, Ojala et al. (2008) presented a prototype of a wearable continuous and transparent authentication device – a wristband. Users are authenticated by their fingerprints at the login stage and their presence is verified continuously by measuring the skin temperature, heart rate and the body capacitance. In spite of the novelty of the proposal, it suffers from a number of issues. There is an intrusive login when requesting the user to present their fingerprints. Additionally, even though the prototype threshold was set low at 25%, the matching scores were low (between 40 and 60%). It might be deteriorated further if the threshold is increased, thus resulting in an unacceptable performance. Furthermore, it does not leverage the available devices capabilities because it requires an additional device which is considered a token. As a consequence, the drawbacks of using tokens persist. Nevertheless, the breakthrough of mobile devices competencies, such as the heart rate sensor

of Samsung Galaxy S5 (Samsung, 2014) would open the horizons of employing them rather than additional devices.

3.8.1.4 Distributed Transparent Multibiometric Systems

All the aforementioned frameworks did not consider the current fact of a user in possession of various digital devices. Therefore, the studies presented in Table 3-7 have been conducted. An attempt to exploit the advantageous features of transparent authentication method among various devices the user owns was proposed by Chowdhury et al. (2010). They presented a framework utilising physiological signals (e.g. blood pressure and heart beat) and behavioural profiling capable to work in ubiquitous environment, where the probable ratio is one user to many devices. Nonetheless, it was just conceptual without feasibility study. Stemming from this notion, a progressive authentication framework was prototyped leveraging the widespread of inter-devices connectivity to enable the authentication information among the user's devices (Riva et al., 2012). Incorporating the biometrics of face, voice and behavioural profiling, alongside proximity to fellow logged-in device(s), the prototype was run on a mobile and a PC with 9 users only. From usability standpoint, it was declared that there was a 42% reduction of requested explicit authentication whilst the security standpoint was not considered.

Author(s)	Platform	Biometrics				Performance (%)			Experiment Demographics	Mode	Limitations	Features
		F*	V*	B*	PS*	FAR	FRR	EER				
Chowdhury et al. (2010)	PDA	-	-	√	√	-	-	-	-	Conceptual	No experiment	One user to Many devices
Riva et al. (2012)	Mobile & PC	√	√	√	-	-	-	-	9 participants	Prototype	-	42% reduction of intrusive authentication
Hocking et al. (2013)	PDA & various devices	-	-	√	-	-	-	-	20 participants 14 days	Real & Simulation	Utilises Secret & Token	74% reduction of intrusive authentication

* **F** = Face; **V** = Voice; **B** = Behavioural profiling; **PS** = Physiological Signals

Table 3-7: Distributed Transparent Multibiometric Systems

A similar but more thorough study was conducted by Hocking et al. (2013) – Authentication Aura. It enables the separate and differing devices of a particular user within a close proximity to communicate their own authentication status and confidence, thus establishing an accumulative level of confidence. It is also capable to utilise personal dumb items, such as a wallet and car key that are RFID tagged, to incorporate to the confidence level of the user. Their experiment involved 20 participants to have their usage observed for 14 days. Even though that the sample seems small, the dataset was created based on 1.23 million recorded observations. There were no error rates revealed but it indicated that users' convenience would increase as a result of decreasing the number of explicit authentication the user would be prompted to by 74% in a typical day compared with the occurrences of secret knowledge-based authentication. However, its scalability, architecture complexity and processing load executed on each participating device have to be examined thoroughly as well as the performance. In addition, utilising active communication technologies, such as WiFi and Bluetooth, besides the RFID would have contributed to a better viability study of the framework.

3.8.1.5 Web-based Transparent Multibiometric Systems

Author(s)	Platform	Biometrics				Performance (%)		Experiment Demographics	Mode	Limitations	Features
		F*	V*	K*	M*	FMR	EER				
Traore et al. (2012)	Web	-	-	√	√	-	(M) 22.41 (K) 24.78 Fused 8.21	24 participants 8 weeks	Real	Intrusive login (secret)	Bayesian fusion
Ceccarelli et al. (2014)	Web	√	√	-	-	(V) 10 (F) 2.58	-	-	Prototype	Intrusive login (fingerprint)	-

* **F** = Face; **V** = Voice; **K** = Keystroke; **M** = Mouse

Table 3-8: Web-based Transparent Multibiometric Systems

Table 3-8 demonstrates alternative solutions that have been proposed to move the potential processing burden from the user devices to a web server (Traore et al., 2012; Ceccarelli et al., 2014). The former combined mouse and keystroke dynamics to ensure the identity of a web service user after an initial conventional password login. Their overall EER was 8.21% using

Bayesian fusion. The universality of their approach, however, is an issue, in particular when users accessing the services on mobile phones where acquiring the mouse/keystroke features might be implausible. The latter presented a multimodal biometrics verification protocol applied in an Internet system called Context Aware Security by Hierarchical Multilevel Architecture (CASHIMA). It is deemed to operate securely in any web service from a variety of client devices, utilising available biometrics sensors of fingerprint, voice, face, and/or keystroke dynamics samples. It implements a changing level of trust in the user similar to the concept of TAS confidence, in that it is determined according to the intervals and quality of the acquired samples. The trust level reflects on the subsequent services the user is granted access to and the risk level associated to them, leading to relevant reaction ranging from allowing access to high sensitive services, restricting access to some services, to locking out the system completely and asking for re-authentication. The classification and authentication decisions are both performed on the online server side not the client. Thus, privacy issues must be given more consideration and assessment.

Albeit this proposal demonstrated some encouraging features that may contribute to solving some of other TAS framework pitfalls, it fell short in proving the feasibility of the solution empirically – it was evaluated only on a fully functioning prototype. Additionally, just two biometrics traits were incorporated in the prototype: face and voice, which achieved independently (not an overall) an FMR of 2.58% and 10% respectively on a smartphone. Therefore, some critical issues were not possible to be tested, such as the scalability and response time of the protocol and battery consumption of mobile phones. Furthermore, it was stated in the proposal that it involves an explicit authentication process at establishing the session where fingerprints can be used. This yields not to have a complete transparent authentication system.

3.8.2 Users' Perceptions of Transparent Authentication Systems (TAS)

Clarke et al. (2009) and Crawford and Renaud (2014) investigated the users' perceptions and acceptance of transparent authentication. They found that 92% of 27 participants and 73% of 30 participants, respectively, believed that transparent authentication provided a more secure environment than other conventional authentication. Accordingly, 90% of the latter's participants stated that they would use the transparent authentication technique if it is offered to them. Moreover, another study was conducted by interviewing 20 users of both smartphone and tablet revealed that they preferred being offered an authentication mechanism allowing them to access about 50% of their applications without performing intrusive unlock (Hayashi et al., 2012). The relative small samples of these studies notwithstanding, TAS can be appreciated as a remarkable solution to effectively remove the reliance upon the human aspects to ensure a robust and usable authentication. On the one hand, 83% of 470 respondents who owned smartphone and tablet would like to have seamless experience across all their devices (Salesforce, 2014).

3.8.3 Discussion

It is found that studies have employed a variety of biometric techniques – physiological only, behavioural only and both, with the addition of soft biometrics or password. A few systems even incorporated intrusive initial login using secret code, fingerprint or iris, rendering them not to be complete transparent thereby suffering from intrusive authentication drawbacks. For instance, in case of the need for secret credential either at the login or re-login stage, the memorisation burden remains along with other documented passwords downsides.

The operational context also varies, including PC, mobile, wearable, various and varying devices, or the Internet and this has a significant impact on the underlying authentication techniques that can be utilised and thus subsequently on the performance that can be

achieved. Therefore, it is evident that there is a lack of an empirical solution that can be accomplished seamlessly in a location, technology and service independent fashion that is favoured by the majority of users. Even though that the few studies working on various devices and/or the web contexts may present a level of universality, issues of processing burden and privacy, respectively, have not been resolved. Despite the fact that most studies deployed an identity confidence/trust adaptation, a small proportion of them associated it to the differing risk level of a particular data, action, or service.

With respect to performance, many studies never performed an evaluation; others declared heterogeneous metrics (e.g. FAR, FRR, EER, FMR, Verification score, Recognition rate). Furthermore, various studies had no overall security performance results revealed but merely for each individual deployed modality, making a comparison implausible. The relatively small samples most evaluations involved might not resemble the real use of such a system. Moreover, the real usage and thus performance would differ from those under controlled environment and short durations/intervals where predetermined tasks are performed during the evaluation. Therefore, it would be ideal to conduct an extensible evaluation, having the participants piloting the trial for a longer time and interval sessions without restrictions in order to have a more accurate insight into the system.

Whilst transparent multibiometric systems have shown enhancement over their intrusive counterparts in terms of matching performance and user convenience thus improving the authentication decision reliability and robustness, still they are not popular nowadays. This can be attributed to the potential endured cost, processing overhead, complexity, and acceptability. For instance, the number of possible usage scenarios that are based on the availability and type of captured samples would increase the complexity of the system. Therefore, these and similar issues have to be thoroughly considered before developing such a system.

From the analysis, it is envisioned that proposing a successful continuous and transparent multibiometric authentication mechanism must address a number of characteristics:

- achieving a high level of transparency thereby being less dependent on secret-knowledge or any other intrusive login, e.g. iris;
- leveraging the available devices capabilities without requiring additional device, e.g. token or sensor;
- incorporating a variety of biometrics from different types, i.e. physiological, behavioural, and soft biometrics;
- deploying an on-going identity confidence level based upon the captured biometrics samples, which is subsequently reflected on the user privileges and mapped to the risk level associated to them, resulting in relevant reaction(s);
- functioning with minimal processing overhead in order to have high level of scalability thereby reducing the user's waiting for the authentication decision;
- providing an architecture capable to operate across a range of digital devices, bearing in mind the differing hardware configurations, operating systems, processing capabilities and network connectivity;
- implemented and evaluated extensively on real and live data;
- having sufficient number of participants conducting the evaluation trial for a long time or at least interval sessions with free use in order to provide a more accurate insight into the system;
- and taking into consideration some critical issues, e.g. trust, privacy, and biometrics templates management.

3.9 Conclusion

Even though the biometrics outweighs its counterparts of knowledge- and token-based approaches, they are still mostly functioning at the point-of-entry, and even those performing sort of re-authentication executing it in an intrusive manner. The majority of frameworks that were proposed to solve this issue deployed a single biometric to re-verify the user in a continuous but implicit fashion. Nonetheless, they have inherited the downsides of the utilised modality so they have issues regarding the universality and circumvention.

Therefore, a serious move towards employing two or more biometric modalities in TAS has been taken. However, most of the previous studies in this domain fall short in one or more drawbacks in relation to lack of full transparency, universality, interoperability, scalability, high performance, and real data on which their validations were conducted. In order to provide users with adequate protection and convenience, innovative robust authentication mechanisms have to be utilised in a universal level, so they operate in a transparent, continuous and user-friendly fashion.

To conclude, it is perceived that the success of a particular transparent and continuous authentication mechanism has the merit of ensuring effective authentication method together with users' acceptance. However, it is paramount to have high level of performance, scalability, and interoperability among and with existing and future systems, services and devices. Furthermore, all these requirements should be implemented and evaluated extensively on real data in order to prove that such a system is viable and should be put and deployed in an operational context to measure other key factors that are required for successful adoption, such as privacy, users' acceptance and usability.

4 Security, Privacy and Usability – A Survey of Users' Perceptions and Attitudes

4.1 Introduction

Users are now in possession of an ever-growing number of advanced digital devices (i.e. PCs, servers, laptops, tablets, phablets and smartphones) with a wide range of capabilities which are used for accessing, storing and processing personal, financial, medical and business information (some of which are often considered sensitive and confidential). Accordingly, each device has its own associated security requirements and configurations. Therefore, it is apparent that a more innovative, convenient, and secure solution for user authentication is essential.

As perceived throughout previous chapters, most of the undertaken studies and proposed solutions thus far endure one or more shortcomings; for instance, inability to balance the trade-off between security and usability, confinement to specific device, lack or negligence of evaluating users' acceptance and privacy measures, and insufficiency or absence of real tested datasets.

Hence, it is considered desirable to explore and address related aspects to the proposal that the literature has not addressed yet prior to implementing it or any alternative solution; for instance, the extent of using the technologies including devices, operating systems, and Internet services. To this end, this chapter presents details of a survey that was conducted to investigate the current security measures employed and compares these with the desired and appropriate protection together with the associated experience. The discussion also considers the acceptability of such proposals from the end-user perspective, as this is essential if measures are to see sufficiently widespread adoption amongst them.

4.2 Design and Methodology

The survey was designed to explore and assess users' technology usage and security practices, and to investigate their perception and satisfaction regarding current and alternative authentication approaches. Furthermore, it sought to understand the usability of these practices and to analyse users' awareness and attitudes towards privacy. This was to answer the following research-related aspects:

- whether users utilise multiple Internet-enabled devices;
- whether these devices are of diverse types and operating systems;
- whether users have access to various network technologies and their extent use;
- whether users employ security tools and maintain them properly;
- users' perception of several authentication techniques and associated login failures;
- and finally their real practices of privacy-related topics along with their acceptance of aspects related to the proposed authentication model (i.e. storing biometrics with, being monitored by, and passing management of authentication to a TTP).

The survey was meant to be and conducted over the Internet via an online questionnaire that was hosted within the Centre for Security, Communications and Network Research (CSCAN) at the University of Plymouth. A set of questions were drafted taking into account the target of achieving the survey aims, being understandable by public IT users, being objective, and being answered in an average of 10 minutes by about 350 participants. To fulfil this, a number of local researchers within the CSCAN were requested to act as participants, have pilot turns through the survey, and provide their feedback. As a result, the survey questions were repetitively refined and enhanced until they reached the final disseminated version.

The survey was structured to contain twenty-seven questions comprising a variety of closed-ended questions including drop down list, multiple choice, and Likert scale with an option for

the respondents to comment in some questions where the answer is not listed (Appendix C). The questions were divided into four sections, organised as follows:

1. **Demographic**: Exploring the participants' demographic characteristics, including questions related to gender, age, education and location.
2. **Technology Usage (Services and Devices)**: Establishing an understanding of persons' technology usage.
3. **Security Practices and Convenience**: Investigating the role and usability of security related to the aforementioned respondents' technology usage.
4. **Privacy**: Analysing respondents' experience and acceptance level of privacy-related topics.

The targeted participants were public users who are 18 years or above and, given that it is an online survey, obviously use technology services and/or devices. They were recruited via e-mail, predominantly targeting students in Plymouth University, staff and colleagues in the Faculty of Science and Engineering, as well as friends and relatives. Additionally, it was advertised on the International Student Advisory Service website. A news entry on the university staff/student portal also was requested and placed. Prior to displaying the survey questions, its aims and structure were briefed confirming that the respondents should be 18 years or older and they are free to withdraw up until the final submission of their responses (Appendix C). All of the information has been treated confidentially and respondents have been anonymous during the collection, storage and publication of research material. Accordingly, it is worth noting that the ethical approval (Appendix B) was obtained ensuring that this survey conforms to the ethical principles laid down by the University of Plymouth.

Due to the resultant ordinal data from the responses of the 5-point Likert scale questions, the following arithmetic mean equation is performed to calculate the central tendency of the responses in order to better interpret them.

$$\text{Arithmetic Mean} = \frac{\sum_{i=1}^{5} R_i C_i}{\sum_{i=1}^{5} C_i}$$

Where R= Response rate, and C= Count of responses/R.

4.3 Results Analysis

This section presents details of the survey that was conducted to investigate the current security measures employed and compares these with the desired and appropriate protection together with the associated experience.

4.3.1 Demographic

In total, 302 completed responses were received during a period of 8 weeks that the survey was active. This number is within the range of other surveys in the research domain and close to the expected and targeted figure.

An analysis of the survey shows that almost three quarters of the respondents are males against the remaining of females, as Table 4-1 illustrates. Being within an academic institution, nearly 79 per cent of the participants are within the age range between 18 and 39, in addition to the fact that the vast majority of them are either students or employed. Even though it is likely to skew the results with regard to the group and gender, the survey sample shows a proportionate representation of the general population – it is in line with the findings of the UK's Office of National Statistics where the age group (16 to 34) were the top users of the majority of the Internet activities with no significant penetration differences between males and females (Office of National Statistics, 2013). It can, also, be implied that the

majority of respondents are somewhat highly IT literate that entitles them to better understand the surveyed issues. With regard to the country of residence, approximately 74% of them reside in Europe or Northern America.

Demographic Factor	Characteristic	Count	Percentage
Gender	**Female**	66	21.85%
	Male	236	78.15%
Age (in years)	**18-29**	113	37.42%
	30-39	125	41.39%
	40-49	48	15.89%
	50-59	14	4.64%
	60+	2	0.66%
Employment Status	**Employed**	131	43.38%
	Self-employed	14	4.64%
	Student	151	50.00%
	Other	6	1.99%
Country of Residence	**Europe**	192	63.57%
	North America	30	9.93%
	Other	80	26.49%

Table 4-1: Summary of Respondents' Demographic Characteristics

4.3.2 Technology Usage (Services and Devices)

The survey proceeded by analysing the extent of users' technology usage. Unsurprisingly, as shown in Figure 4-1, users currently possess an increasing number of digital devices – about 75% of respondents have 3 Internet-enabled devices or more of which 62% have 4 or more.

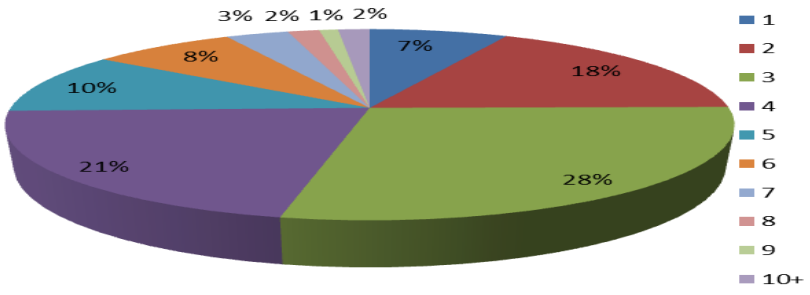

Figure 4-1: The Number of Internet-Enabled Devices in Use

These devices represent a variety of models from various manufacturers, thus running a range of differing operating systems (OS) (as illustrated in Figure 4-2). From the same perspective,

in terms of desktop/laptop computers, Windows OS outweighed its counterparts (Mac and Linux) by 86%. On the other hand, Apple's tablets prevail over those of its rivals as 45%, preceded by 26% for Android-based tablets. However, the iOS and Android smartphones had similar share of users' usages by 43% and 46% of respondents respectively, in addition to the use of other devices with distinct OSs such as game consoles which are used by almost 21%.

This distribution is not in line with the mobile phones market share that shows 87.6% of it is led by Google Android OS (IDC, 2016), making it not representative of the general population. Nonetheless, it is not likely to skew the results of this user survey because it is out of its related research questions (stated in Section 4.2) to know what the dominating OS is but rather to find out how diverse the devices and OSs that are being utilised by users.

The results of these two figures (4.1 and 4.2) draw attention to the fact that a typical today's user most probably owns/uses many digital devices with differing OSs. This, in turn, emphasises the need to consider universal applicability a crucial aspect in any proposed authentication mechanism.

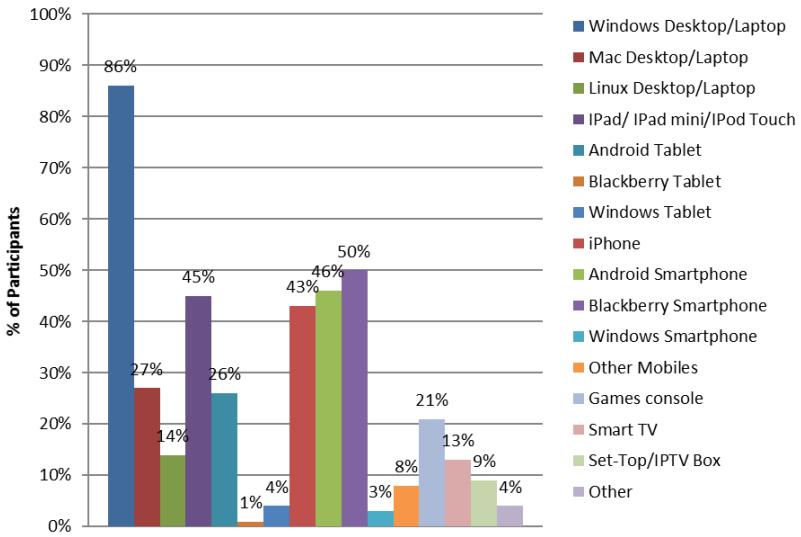

Figure 4-2: The Digital Devices in Use

When it comes to cloud services, Figure 4-3 reveals that only a small proportion of participants, less than 13%, do not use any cloud service. Having this ubiquitous employment of cloud computing, supported by the PwC (2013) survey results (four fifths of their surveyed participants store confidential data on the Cloud), it is likely that sensitive information would inevitably be involved. This would indicate that privacy concerns about the Cloud (or saving personal information remotely) might be diminished or the trust on the measures in place by the Cloud Service Providers (CSPs) might be established. Accordingly, this makes the Cloud a plausible environment for any solution aiming at broad spectrum of universality and acceptability so users are familiar with and able to access it whenever and wherever they need.

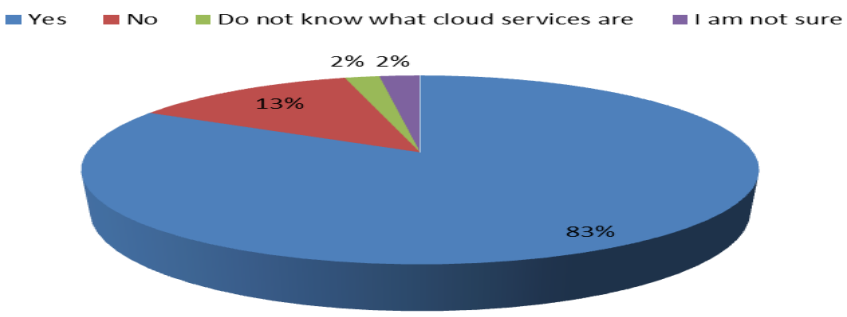

Figure 4-3: Cloud Services Usage

The high connectivity can be perceived as most of respondents have access to a wide range of network technologies, such as home WiFi (97%), public WiFi (61%), and 3G/4G (81%). As a result, 53% spend more than half of the day online while nearly 19% are always connected, as depicted in Figure 4-4. During their online presence, they use diverse services (e.g. messaging, email, and online banking) in varying frequencies (e.g. hourly, daily, weekly). It can be assumed, therefore, that accessibility to an online authentication solution is likely to be positive. On the other hand, as a large number of those questioned are online most of the day, securing the used devices and services throughout these long periods of time against misuse

arises as an issue. Prompting users to re-verify periodically is very disruptive and thus apparently inconvenient.

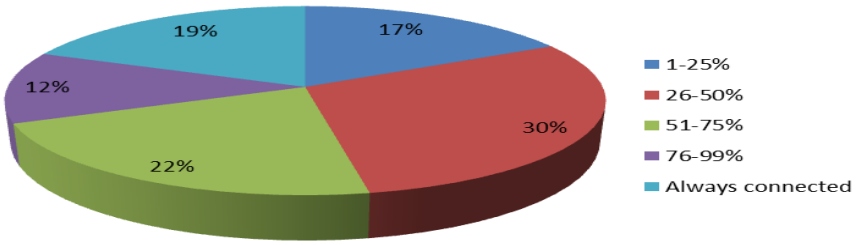

Figure 4-4: The Percentage of a Day Spent Online

4.3.3 Security Practices and Convenience

Moving forward to exploring the users' security practices and the ease of use incurred, Figure 4-5 illustrates that nearly two thirds of users are required to authenticate to 51-100% of the services and devices they use. Additionally, 37% of the participants need to enter their login credentials several times in a typical day, ranging from frequently (11 times) to too many to remember (above 20 times). As a consequence, this added authentication burden experienced by the users would lead them to either avoid using it when they have the choice whether to enable the authentication feature, or they do not deploy it appropriately.

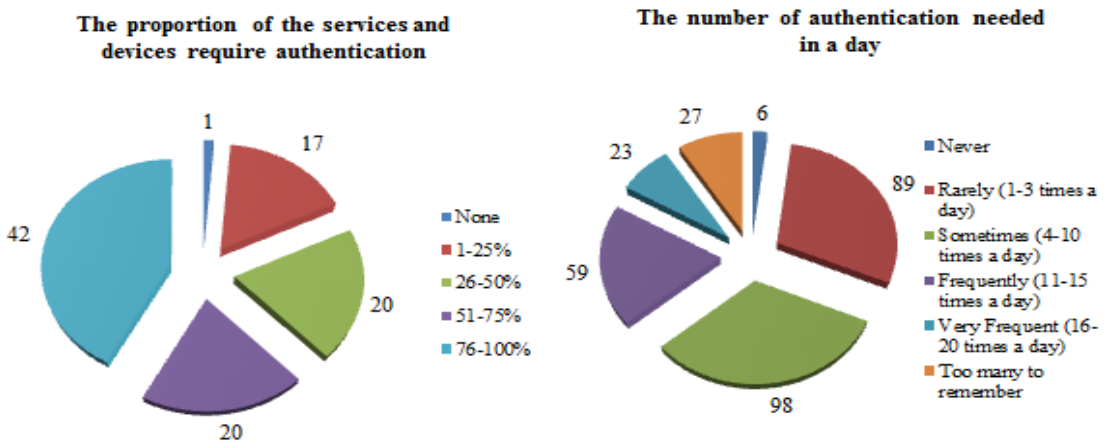

Figure 4-5: The Extent of Authentication Repetition

The former is reiterated by the finding that only 49 per cent of the respondents use the authentication tool on their digital devices. Furthermore, an example of the latter, i.e. not complying with authentication's good practices, can be seen from Figure 4-6; only 9 per cent of participants change their password of the most important account on a regular basis (weekly or monthly) whilst 27 per cent never changed it. Therefore, it is evident that principally relying upon users to secure their IT assets by practising security policies is impractical.

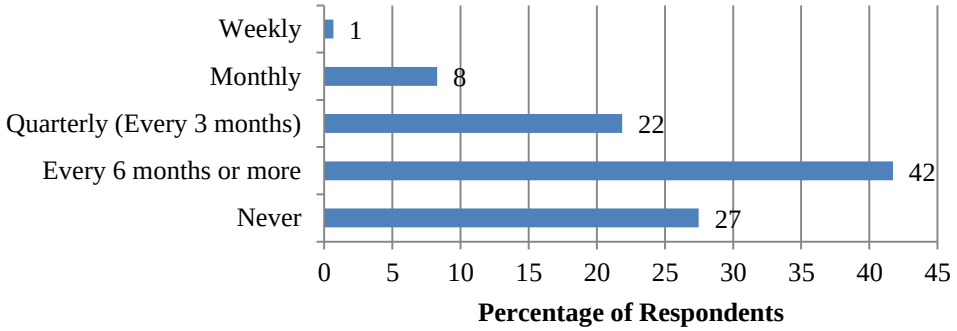

Figure 4-6: Respondents Changing the Password of Their Most Important Account

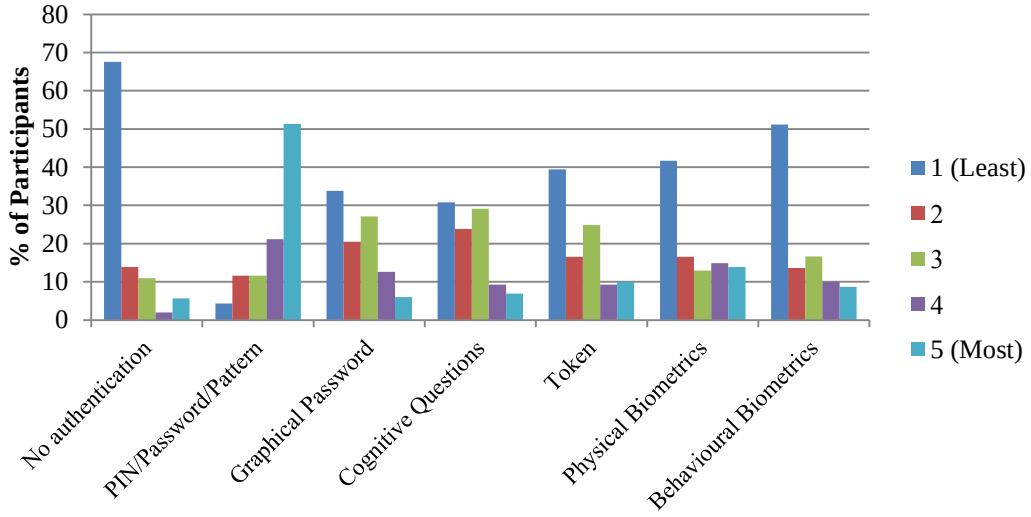

Figure 4-7: Participants Preferences of Authentication Methods

Despite the fact revealed by Figure 4-7 that PIN/password/pattern authentication methods are either the preferable (4) or most preferable (5) to 72% of participants, there are some issues

related to complying to their good practice measures (security) as seen previously, alongside with the inconvenience caused by them (usability) which can be seen in the succeeding figures. Interestingly, a high percentage of respondents (82%) preferred not to be without authentication. Thus, it can be perceived that users recognise the importance of security. Further noteworthy point in this figure is the comparable perception of both physical and behavioural biometrics. When combining the responses of ranking 4 and 5 of each category and excluding the PIN/password/pattern, the result shows that participants favoured physical biometrics the most (29%), followed by behavioural biometrics, graphical password, and token (19% each), and cognitive questions the least (16%).

Figure 4-8 demonstrates that about 94% of respondents experienced authentication failure of which 22% experienced it several times a week. Accordingly, two thirds of them stated that they had been frustrated by those failures as shown in Figure 4-9.

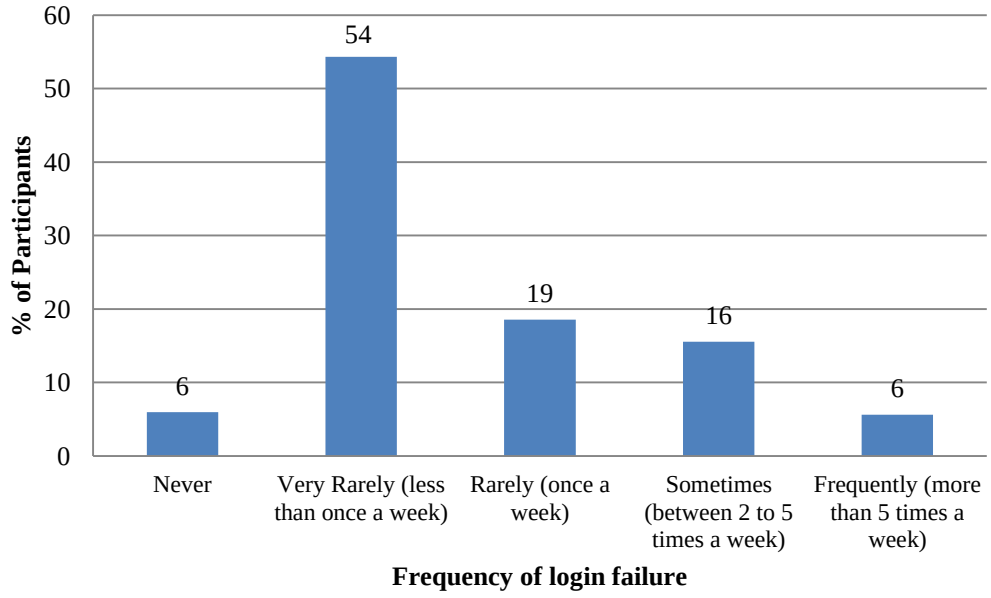

Figure 4-8: Percentage of Participants Experienced Login Failure vs. the Frequency of Login Failure

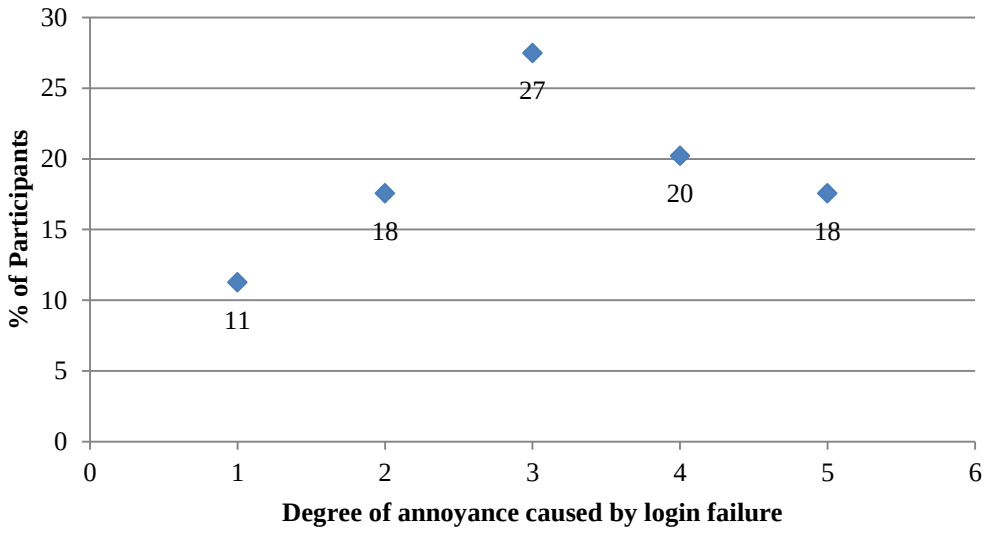

Figure 4-9: Degree of Annoyance Caused by Login Failure to the Participants

Furthermore, authentication techniques that rely mainly on people to remember or recognise secrets or to carry additional devices continue to be the prime contributors to users' inconvenience because most authentication failures are related to them. The results illustrated in Figure 4-10 show that the prevalent causes of those experienced failures are forgetting (67%) or mistyping (55%) the secret code, followed by the absence of the token/mobile (11%). This, however, could be proportional with the authentication approaches the participants use. The more the users utilise biometrics, the more associated login errors perhaps occur. Even so, users might not be the chief responsible cause of them – biometric errors can be as a result of sensors, environment, and/or classification issues, which can be alleviated in many ways. As a consequence, it can be implied that biometric approaches have the potential to obtain users' acceptance if they offer a less users cumbersome solution than what other authentication approaches cause.

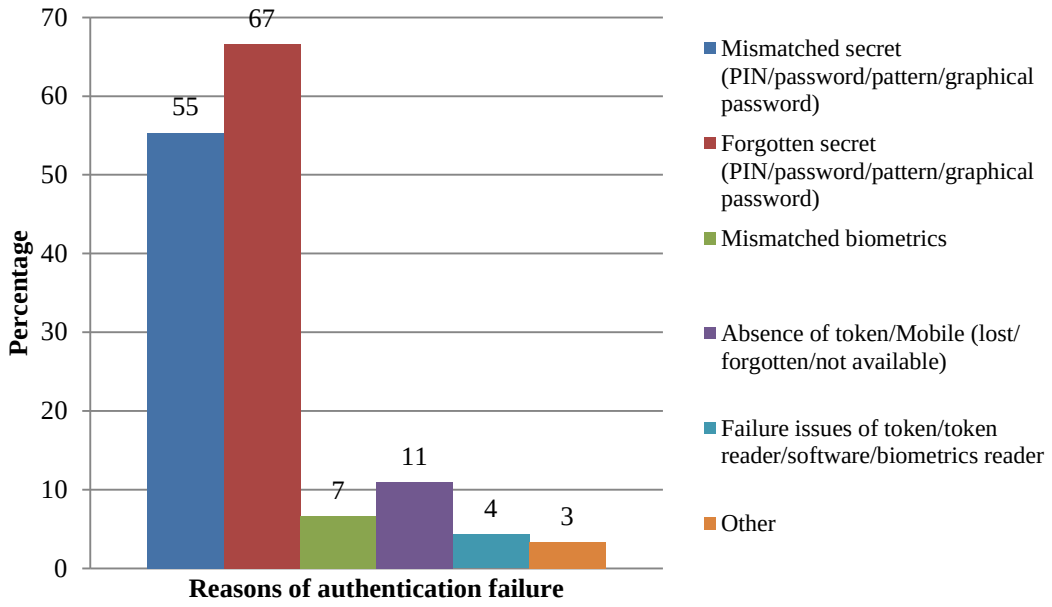

Figure 4-10: Percentage of the Reasons of Authentication Failure

When considering participants concerns about technology-related key aspects, according to the arithmetic mean of the responses ranking, respondents expressed that they were most concerned about privacy (4.06), followed by security (3.93), abuse (3.66), and then convenience (3.62), as demonstrated in Figure 4-11. The overall insight of this figure conveys clearly that respondents are somehow highly concerned about all these issues closely, indicating that an effective authentication solution should vigilantly guarantee all of them. Given privacy at the top of respondents concerns implies a reasonable level of privacy awareness they have but their according practices compliance are questionable. Hence, further exploration about privacy-related issues is needed. These results also suggest that a significant proportion of users' data are considered sensitive to them, thus providing a stronger authentication without compromising the ease of use is fundamental. For instance, employing intrusive multi-factor authentication mechanism (e.g. password and hardware token) would promote the protection but lower the usability alike.

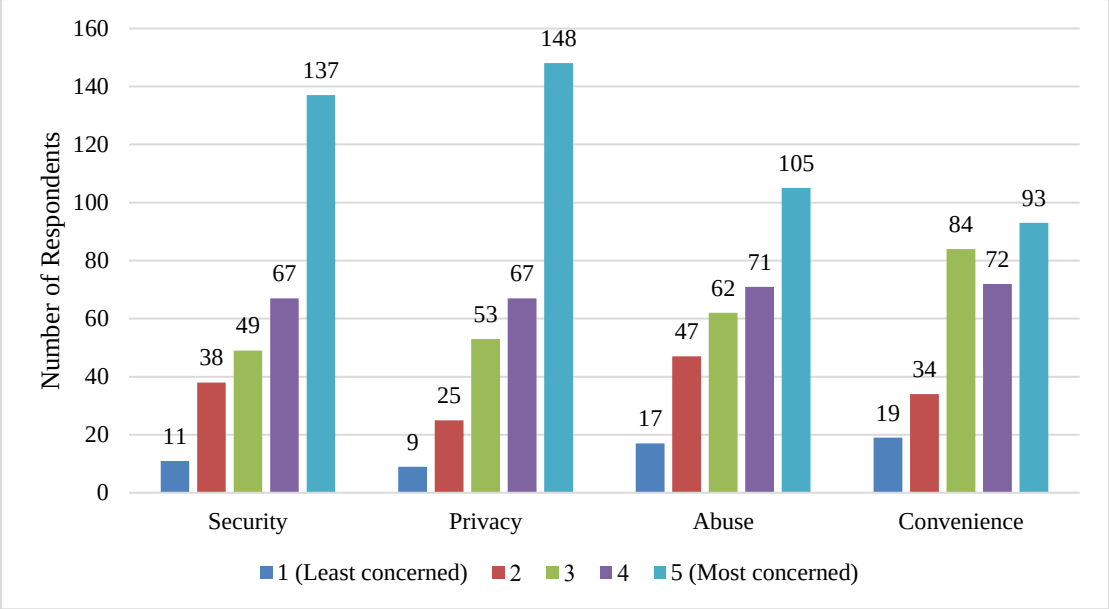

Figure 4-11: Ranking of Participants Concerns about Technology-Related Key Aspects

Specific questions were asked to investigate users' usability perspectives regarding the use of some authentication mechanisms offered with current devices and services. It seems that there was an inclination from the respondents to the notion that those biometrics-based authentication mechanisms are more usable and easier to use. Figure 4-12 shows that iOS Touch ID, which employs fingerprint login on the home button, was rated the second highest usable of the alternative mechanisms by achieving 55% of surveyed respondents rated it somewhat usable (3), usable (4), or most usable (5), preceded by Android pattern unlock (63%) and followed by Amazon 1-Click (52%). Although Android face unlock attained only 39% of the same rate, it can be considered significant because this relatively low percentage might be attributed to the fact that 34% of respondents were not aware about or had not used it so they responded by N/A.

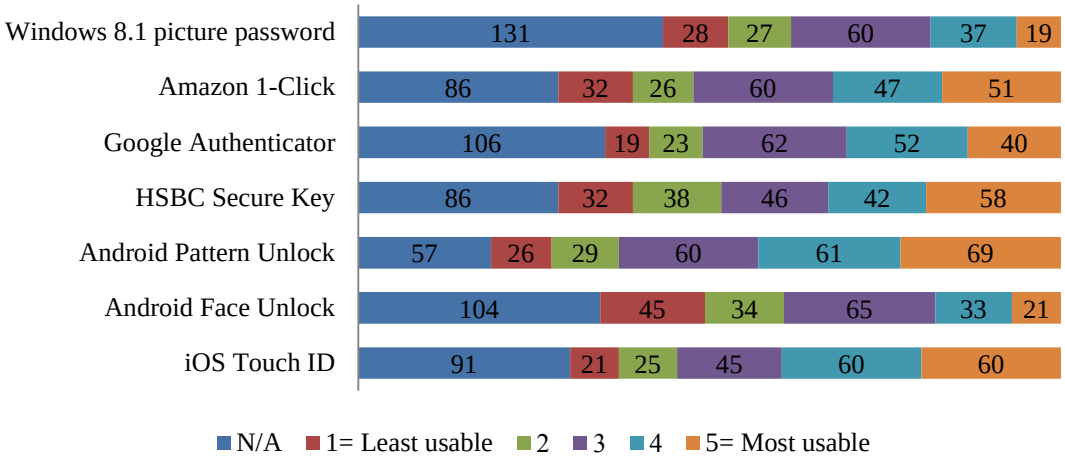

Figure 4-12: Respondents' Perspectives of the Usability of Current Authentication Mechanisms

Furthermore, Figure 4-13 presents interesting normalised results of the relatively high ratings of the approaches once the N/A responses are taken out. iOS Touch ID became the joint first most usable with Google Authenticator (79%) followed closely by Android pattern unlock (78%). It can also be inferred that users tend to prefer using an authentication method that involves minimal effort, with the HSBC Secure Key being considered the least usable.

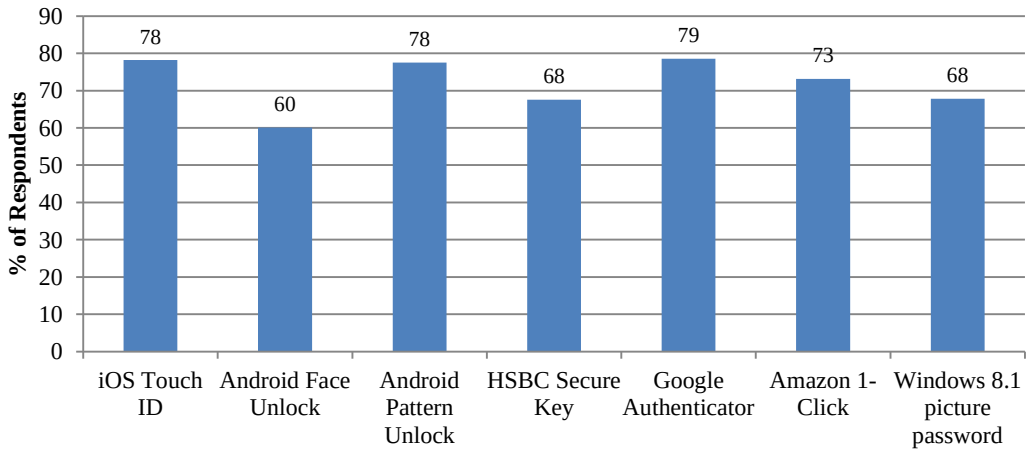

Figure 4-13: The Percentage of Respondents Rated Some Authentication Mechanisms by "Somewhat usable", "Usable", or "Most Usable" After Excluding N/A Responses

4.3.4 Privacy

In relation to participants' practices and attitudes towards privacy-related aspects, one of the countermeasures that users can scrutinise to safeguard their sensitive data against leakage is

the End-User License/agreement/App permissions (EULAs). Even though privacy issues gained the highest concerns of the participants as shown in Figure 4-11, the findings in Figure 4-14 and Table 4-2 are perhaps contradictory to that result. 77% of respondents have never or rarely read the EULAs. Likewise, 68% of them have never or rarely decided not to use/install or uninstalled a service or application due their EULAs despite the fact that some of them, for instance, access user location unnecessarily. This contradiction between the respondents' perceptions and real practices can be attributed to various possibilities. It perhaps pinpoints the so-called herd behaviour; for instance, there have been a number of privacy awareness campaigns and media attention probably as a reaction to some data breaches and leakages, making users alerted about the buzzword privacy; however, in practice they do not take reasonable care for their privacy or they do not know how to protect it. Another possibility could be the fact that users get used to trust specific service providers historically leading them to tend to accept any further service or update they may offer. Furthermore, other issues may play a role in this negligence, such as cultural tendency towards avoiding reading and the annoying design of such licenses and agreements (e.g. very lengthy, and full of jargons).

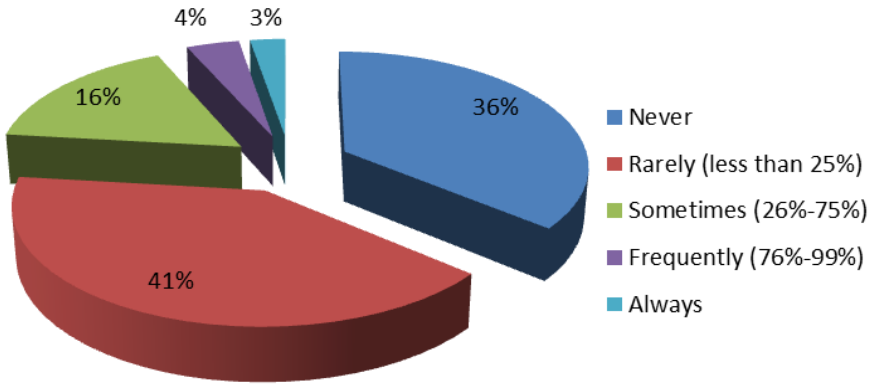

Figure 4-14: Frequency of Reading the EULAs

Response	Percentage
Never	38
Rarely (1-3 times)	30
Sometimes (4-10 times)	21
Frequently (11-15 times)	8
Very Frequent (16-20 times)	3
Too many to remember	0

Table 4-2: Frequency of Not Using or Uninstalling Services Due to the End-User License/Agreement/App Permissions

A subsequent question in this domain was about the respondents' confidence in storing their biometrics with a TTP, highlighting that this would enable utilising them to perform authentication anywhere to use different devices and services. As appears in Figure 4-15, an accumulated 41% of participants stated that they are confident or very confident storing their biometrics with a TTP, against only 30% who are unconfident or very unconfident. Given that 29% had neutral confidence in this issue, the compound result gives an arithmetic mean of 3.1 which indicates that there is a slight tendency towards adopting the concept.

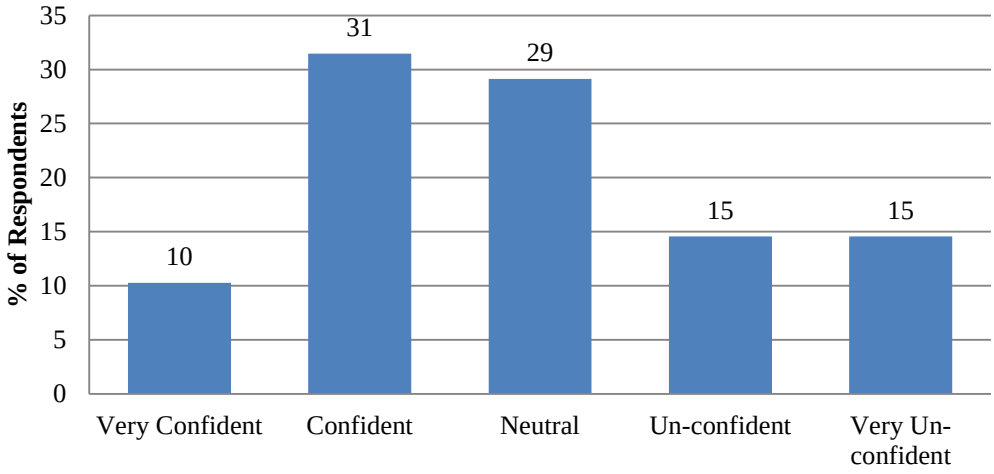

Figure 4-15: The Confidence in Storing Biometrics with a TTP

However, Figure 4-16 depicts that 57% of the surveyed users would prefer storing their biometric templates on their own devices only or together with other locations, i.e. 11% prefer storing them with network operators (e.g. ISP, mobile operator) whereas 26% with a TTP. On the other hand, there is a low proportion of them (13%) reject the idea of storing the biometrics anywhere, meaning that they do not favour the use of biometrics at all.

Nevertheless, users already trust service providers with their authentication credentials. Additionally, it is likely that recognising the benefits of such a method would shift the preference towards keeping the biometric templates with a TTP or both on the device and the network operator or a TTP as proposed by Karatzouni et al. (2007). For example, biometric templates stored off-board/remotely would remove the processing overhead away from the device, hence saving memory and energy, and allowing better universality and applicability. On the contrary, storing the templates on-board would eliminate the potential time lag introduced through the network traffic. Nevertheless, this is only important if the system is waiting for a response (i.e. point-of-entry) – in a transparent mode, this is not typically the case. Therefore, having a hybrid approach storing templates between the own device and the operator or a TTP is reinforced by the variety of responses and by some of current deployments – as already many apps on mobile devices do this (often transparently to the user) such as Siri, iCloud, and Dropbox.

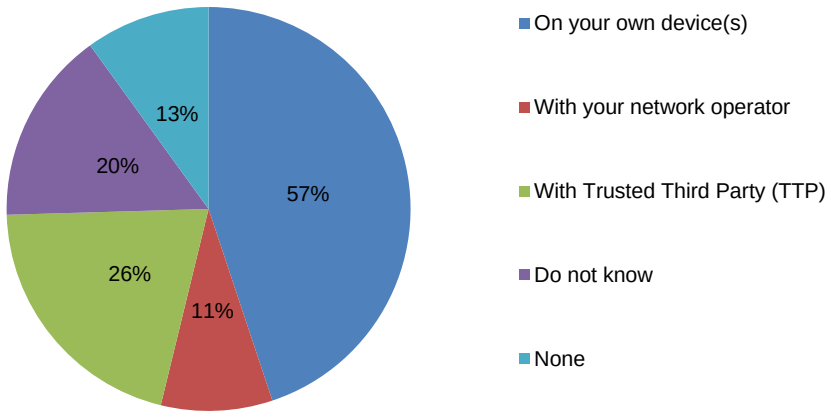

Figure 4-16: Respondents' Preferences of the Location(s) of Storing Biometrics Templates

From a similar perspective, Figure 4-17 reveals an interesting result where the respondents expressed greater acceptance (58% accepted, leading to an arithmetic mean of 3.6) of their device/service usage being monitored, given that no private data is collected. This supports

the previous assumption that whenever the benefits of adopting any proposed solution are clearly elaborated and justified, it would gain higher level of acceptability. It is even supported by the results of two credible surveys (PwC, 2012; Salesforce, 2014), where three quarters of respondents were willing to share some personal information in return to the benefits they will receive.

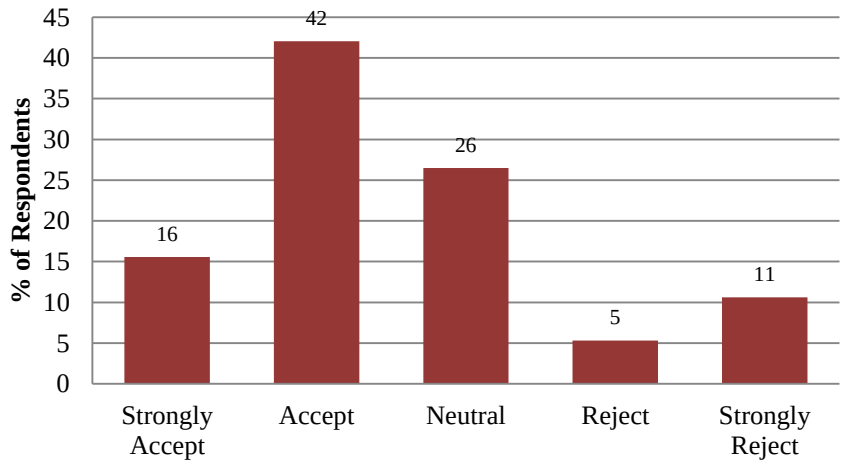

Figure 4-17: Acceptance Level of Participants' Usage Behaviour Being Monitored

Lastly, Figure 4-18 shows that when exploring the extent of participants' willingness to pass the responsibility of managing authentication to a TTP, there was a decline compared with the outcome of Figures 15, 16 and 17 above (where participants were more towards accepting the notion of storing biometrics with and being monitored by a TTP). Only 23% rated their inclination to the idea by responding by (willing "4" or very willing "5") whereas the majority (40%) were in the middle of the scale between the willingness and unwillingness. Even though these results are not in line with those represented earlier, the preparedness rate is not that low given that the arithmetic mean is 2.7. In addition, the way of asking this question without any further explanation regarding the potential advantages of doing so may had an adverse effect.

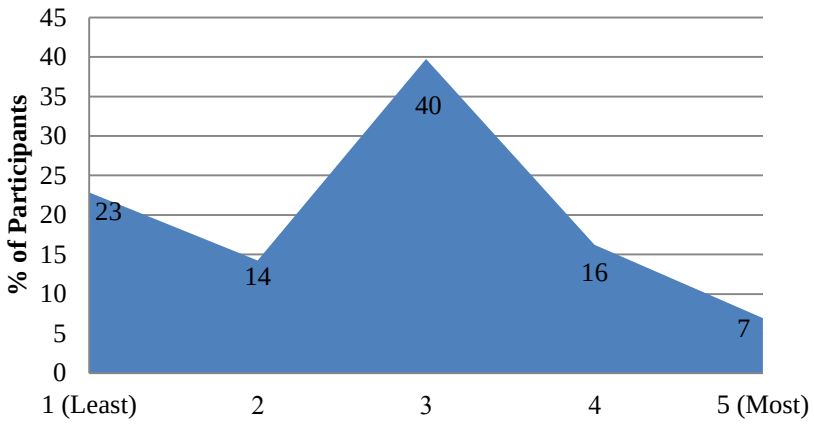

Figure 4-18: Willingness to Pass the Responsibility of Managing Authentication to a TTP

Again, users who better understand a mechanism and the implications involved will more likely have a more informed decision about it. Moreover, in the reality, users have been delegating the responsibility of managing their login credentials to service providers who run Identity Access Management (IAM) systems in many examples either while using SSO or federated identity (where in one way or another, one of the participating parties in the federation or of the communication standards acts as third party) (Madsen et al., 2005; Stihler et al., 2012).

4.4 Discussion

The results of the survey are derived from a range of participants' with a variety of backgrounds in terms of gender, age, employment, and countries. It is evident the respondents profoundly interact with digital devices, especially those providing Internet access which is being utilised for many online services a significant proportion of the day. Some of these services are categorised sensitive and confidential. As a large number of those questioned are online most of the day, securing the devices and services throughout these long periods of time against misuse arises as an issue. Prompting users to re-verify periodically is very disruptive and thus apparently inconvenient. It is also found the respondents' devices operate various operating systems and have a broad set of

communication technologies. Therefore, the requirements to protect users' information have come to the utmost importance.

Although participants state that they use one or more of the security tools on their devices (e.g. antivirus), they fall foul in using authentication as less than half of them enable it. Even so, they are prompted to authenticate to access their devices as well as services many times a day with which the majority of them encounter frequent login errors and have got annoyed by that. These errors are caused mainly by secret-knowledge approaches (mismatched and/or forgotten secrets) followed by token-based approaches (absence of token/mobile). Furthermore, non-compliance with password policies by respondents (e.g. 69% of them have never or rarely changed their passwords despite being for the most important account) can be attributed to users attempts to avoid the above-mentioned nuisance. There is an apparent contradiction between the widespread interest in more security and the quite low number of respondents using or maintaining the available security measures.

It is also perceived that albeit of the high percentage of login failure occurrences, the relatively amplified level of frustration caused by these failures, and being the dominant reasons of them, secret knowledge-based authentication approaches are still preferred by the respondents. This might be due to the fact that most of the users have not been exposed to other techniques, such as biometrics, they have used other alternatives but in a very intrusive manner, or they have associated them with their leading and historical use in criminology and forensics. However, physical biometrics is the second preferred authentication approach by 29% of the participants outweighing graphical password, cognitive questions and tokens.

These results along with the significant proportion having the information security on top of their concerns show that there is a desire for added but convenient security, which is lacking on the most utilised existing authentication technique – the secret-knowledge. It seems that

users do not avoid applying the concept of authentication security but the current available common authentication technique. As such, a move towards continuous and transparent authentication may provide the trade-off between users' convenience and higher security.

The plethora of users with many devices and services which each may has its own security configurations and requirements, together with the widespread access to a wide range of communication technologies and cloud services, yielding to a high success possibility of a prospect cloud-based authentication solution. Such solution that centralise the task of authentication to a TTP would enable providing it in a device and service independent fashion, relieving users of the burden of enrolling and authenticating to each device and service separately and the devices of a significant volume of data processing and storage. This is also supported by and would even improve the comparatively positive responses regarding storing biometric templates with a TTP as well as having usage behaviour being monitored.

4.5 Conclusions

The survey findings reinforce the observation that users utilise a variety of Internet-enabled devices to carry out a wide range of activities, many of which are considered sensitive. Whilst the most adopted authentication approach is still the secret knowledge-based, it is (followed by tokens) the chief reason of login errors; consequently high proportion of users either inactivate it or misconduct its use. For instance, two third of participants never or rarely changed the password of their most important account. On the contrary, respondents are overwhelmingly concerned about protecting their information, devices and accounts, revealing that a disjoint between users' perceptions towards security and real practices is in existent. Therefore, it is evident that users do not avoid applying the concept of authentication security but the drawbacks of current available common authentication technique.

Thus, alternative security measures are apparently required given that they do not heavily rely upon users to secure them. Biometrics may have the merit of providing this as physical biometrics is the second preferred authentication approach by 29%. The revolutionary growth of personal digital devices' capabilities may open the horizon to leverage them for biometrics capturing.

The survey also demonstrates that users are online most of the day performing a wide range of sensitive tasks that are required to be secured throughout the usage session. The respondents incline towards storing biometric templates with a TTP as well as having their usage behaviour being monitored. Advanced connectivity technologies and cloud services are capable to be deployed for a novel authentication security solution managed by a TTP to offer a federated, transparent and continuous authentication in order to be used on multiple devices and services. Nevertheless, such mechanism must be designed attentively ensuring various related aspects, such as the security of biometric templates on and during the transmission to the Cloud.

5 Real-World Analysis of TAS

5.1 Introduction

It is evident from the literature survey conducted in 3.8 section that prior research has suggested various novel approaches to authentication such as transparent authentication and cooperative and distributed authentication. For instance, Clarke (2004) proposed a mobile-based model called (IAMS) for continuous and transparent authentication and then extended and enhanced it in a number of studies (Clarke & Furnell, 2006; Clarke et al., 2009) to surface the NICA frmaework. Subsequently, Karatzouni (2014) undertook experimental modelling on NICA. However, these studies amongst the others were evaluated based upon simulated or semi-simulated off-line data so most of the systems were experimented on virtual user data. In addition, to the best of the author's knowledge, even those a few studies that experimented on real data, they evaluated it on a small number of users, short durations, specified tasks, and controlled environments. As a result, there is an apparent lack of publicly available multimodal dataset acquired in a real-world unconstrained environment over a reasonable period of time. Thus, there is a need to implement these models with real data to understand how they work in practice for different users.

A few previous studies (i.e. those of Ceccarelli et al. (2014), Clarke and Furnell (2006), and Clarke et al. (2009)) also did take into account the risk levels and authentication requirements of the actions being carried out and services being accessed by users. Consequently, this renders it difficult to understand and appreciate the dynamic between the real use and authentication and security requirements. Furthermore, they merely focused upon individual platforms rather than providing a universal and federated authentication approach that can be used across technologies and services in a convenient fashion. Building upon existing research on TAS, a cloud-based solution would offer these premises but before moving to

what it might look like, establishing an empirical understanding basis about whether these existing models might work and how well in real practice using real life data (captured for the purpose of this research particularly) is needed.

Having stated this, a number of derived research questions need to be addressed and investigated experimentally. Accordingly, three experimental studies were developed to be carried out with the aim of resolving them. These are the experiments and the related questions they sought to address:

- **Experiment 1 – A baseline study on transparent and soft biometrics**: a baseline set of experiments to understand the nature of transparent biometrics and soft biometric data and determine their potential contribution to the system performance.
- **Experiment 2 – A replication study**: a replication of a well-established previous study (i.e. NICA) in order to validate whether prior TAS models function on real live user data and what their actual performance is in practice.
- **Experiment 3 – Multibiometrics-based continuous authentication decisions**: an enhanced model to utilise multibiometric fusion and time windowing within a device, aiming at investigating whether employing a fusion mechanism that encompasses all available biometric samples at a given time-frame is viable in practice and to what degree it improves the performance from the individual unimodal-based approaches.

Therefore, this chapter seeks to initially establish an experiment to capture and collect real data of a set of biometric techniques and coexisting device' sensors from a real and live usage without any environmental or usage constraints. The collected data is employed in a series of studies evaluating the appropriateness and effectiveness of utilising them for such a universal solution with a view of identifying the attributes required for a successful authentication mechanism.

5.2 Experimental Methodology

This section presents the scientific methodical approach followed while conducting the data collection along with each of the aforementioned three experiments.

5.2.1 Methodology of Data Collection

In general, the research seeks to explore how users' profiles can be constructed and intelligently utilised for authentication based on the biometric features captured during real and live unconstrained use of the mobile device. A biometric data collection exercise was sought to create a real dataset of a significant number of real users over a significant period of time of real and totally uncontrolled use. It was apparent that a software would be required, so a biometric data collection software was developed (described in detail in 5.2.5).

With the biometrics requirements in mind (in particular universality, collectability and acceptability discussed in 3.2), four modalities were selected to be incorporated in the software; face, voice, app usage, and gait, along with the location information. The utilised traits should be possessed by every participant, easy to collect by normal daily devices and interactions, and accepted to be provided in terms of, for instance, users' privacy and convenience. Another reason for this selection is the fact that they represent a variety of biometric techniques – physiological (face), behavioural (voice, app usage, gait), and soft biometrics (geolocation), offering a better insight about the system and its potential enhancement.

Those biometric samples were planned to be automatically, continuously and transparently collected and stored on their devices' local storage without any interference upon participant's normal activities (i.e. without the need for any additional actions from the users and without interrupting them) for 2 weeks to get as much data as possible. Furthermore, looking at it pragmatically, getting both weekdays and weekends data to show the different

nature of the user behaviour to draw the research model for different usage scenarios was deemed important. However, there was also a need to trade this off with being able to encompass the data collection exercise in an appropriate time-frame. Therefore, it was felt that 2-week worth of data was a super volume of data to base this upon. After several refinements, specified capturing intervals of the aforementioned biometric modalities data were decided (elaborated in 5.2.5) aiming at avoiding the substantial battery drainage might be encountered by participants and hence thwarting them from taking part in the study.

Accordingly and prior to the recruitment for participation, 6 users were asked to undertake a pilot study by having the developed application installed on their smartphones and tablets to examine the application functionalities. After a number of refinements (resulted from the pilot study) and ensuring that the application is working as required, ethical approval was acquired from the university's Research Ethics Committee (Appendix D), and participants were sought and invited to participate in this biometric data capturing experiment. In order to facilitate a meaningful analysis, the targeted total number of subjects was 40 as a minimum which is considered a sufficient baseline based upon other previous research that were conducted using similar sample sizes (Beautement & Sasse, 2010). They were briefed about the nature of this research and probed to ask any questions regarding the experiment, followed by giving them the consent form at the beginning of the study (Appendix D) should they wish to carry out the study. In order to ensure meeting the stated requirements of the targeted dataset being a true representation of natural usage pattern, the following were confirmed to be followed:

1) Participants were not given any specific task to carry out.

2) No specific usage environment or conditions was specified so it should be totally uncontrolled.

3) All participants had the software installed on their own devices to eliminate effect of hardware change.

Once participants gave their consent, the application was installed on their Android smartphones (and tablets where appropriate). Upon completing the experiment duration, the captured biometric samples were generated in a database format files on the participants' devices' local storage. The data was shown to the participant – once they were happy to transfer it, the files were taken by the principal investigator. They were then anonymously and securely stored within the Centre for Security, Communications and Network Research (CSCAN) at the University of Plymouth in a way that introduces an element of abstraction and/or encoding to be converted to specialised measurements and feature vectors, only to be analysed anonymously by a machine.

It is not the purpose of this research to examine whether executing the concerned algorithms on the devices themselves or on a server/cloud is practical. Therefore, upon the completion of the data capturing process, the pattern classification analysis of all these studies was implemented on the collected dataset offline (i.e., not on the participants' devices themselves).

5.2.2 Methodology of Experiment 1

Prior to undertaking the second and third experimental studies that are going to incorporate a single modality or a combination of individual's modalities within the dataset, a baseline set of experiments needed to be conducted to determine the nature and performance of the potential contributing modalities. These can be physiological/behavioural biometrics and/or soft biometrics. In a transparent mode, the nature of biometrics works in a different way than it is in the conventional intrusive mode. Therefore, fundamentally, there is a need to understand what the values of these individual biometric techniques are and what the sensors additional information may provide. However, it was out of the scope of this PhD research to

create and evaluate a unimodal biometric technique of each of the biometrics that could be used in the proposed system. Hence, a couple of preliminary investigations were designed and undertaken on an example of one of each category – the most available and highest performing biometrics (i.e. facial recognition) in terms of biometrics, and GPS information in form of soft biometric information. An evaluation of those within the transparent authentication context would aid to gain an insight about how useful they may be.

As reviewed in Section 3.8, there were prior studies on the performance of transparent facial verification and geolocation. However, they were calculated in this research because it is believed that the published studies may differ when they are applied on such a dataset of real and un-controlled live usage data with all varying conditions, including illuminations, orientations, distance, and capturing times (to name but a few). On the other hand, despite the geolocation is arguably considered as a distinct authentication approach (Conrad et al., 2012), there have not be any study investigating its performance separately (to the best knowledge of the author). In this research, it is not counted as an independent biometric technique but it is an example of how information could be used to help provide better discrimination. Moreover, just for better understanding, it was calculated in what would be the EER for location to suggest that it is actually quite discriminative. As such, it is presented as a measure of similarity to understand how unique it is and whether if it is augmented by other pieces of information, it will add to the process constructively. Thus, it is regarded in this research as a smart information source or soft biometrics that can be utilised to improve the robustness of such federated cloud-based authentication model. In addition, in terms of moving forward with the other experiments, published EERs from the prior literature were used in addition to the results of these preliminary experiments to provide a basis for them.

5.2.3 Methodology of Experiment 2

The ultimate aim of this research project is to build upon existing research on transparent and distributed authentication (which albeit exist, they have not been used on real data). Most of the previous TAS frameworks were scripted evaluations on simulated data (without collecting samples from real-world use) and controlled environment/parameters, which might not resemble the real use of such a system. Moreover, the real usage and thus performance would differ from those under controlled environment and short durations/intervals where predetermined tasks are performed during the evaluation. Therefore, it would be ideal to conduct an extensible evaluation of one of the previous TAS framework at which this research is built upon, having the participants piloting the trial for sufficient period of time without restrictions in order to have a more accurate insight into the system.

Had this research proceeds with another piece of simulated work based on the assumptions of a previous simulated model, there would be a risk of building it upon inaccurate or biased parameters, assumptions and/or results. Furthermore, it would be difficult to generalise findings from experiments because they might not be true to real-world dynamics. In the one hand, establishing the empirical feasibility investigation and analysis on real data would be useful to provide a fair insight about the performance. Thus, it would be wise to start with replicating one of the previous studies (i.e. NICA) in order to establish a knowledge on whether they work, to investigate the real performance and to understand what actually happens in practice with real data. Moreover, it would aid to assure the previous results are reliable and valid, and to determine whether extraneous variables exist to consider in the research novel model, such as the drop value of degradation function.

With the aim of aiding the performance evaluation of the NICA framework utilising the collected real dataset thereby replicating its functionalities in practice, vital data inputs are

required – i.e. the risk level of each application the user accessed and their related security requirement levels (i.e. integrity level). For the experimental purposes, there should be a benchmark scientific method to set various risk levels for different used applications/services in the dataset for each user. Furthermore, the risk level of a common application among the participants should be consistent to avoid any skewness in the results (though this might not be the case in reality as every user has their own security perceptions and needs). The rigorous study of Ledermuller and Clarke (2011) that proposed a risk assessment model for mobile devices was adopted (demonstrated in Table 5-1).

Asset Category	**Risk Level**
E-Mail (corporate)	8
E-health	8
E-banking	7
Remote access (corporate)	7
Stored business documents	7
Remote access (private)	6
Voice communication	5
Physical device	5
Personal information (online synchronised)	4
E-Mail (private)	4
Web access (browser)	4
Messaging	4
Social networking	3
Personal information	3
Stored documents Maps	2
Maps & Navigation	2
News client	1
Utilities	1

Table 5-1: Device's Asset Categories and their Associated Risk Levels. *adapted from* Ledermuller and Clarke (2011)

They stated that each mobile application category has its distinct associated risk level dependent upon a number of measures, e.g. their asset values, threat levels, and vulnerability levels. Accordingly, the security requirement can be applied for each application based upon their risk level – the higher the risk level of an application, the higher the associated security. That is, the applications/services that are associated with private information or expensive services would require a high level of security whereas the normal applications/services would require a low level of security. For example, the online banking app is assigned level

7, voice call is level 5, and 1 for weather forecast app. If the integrity level (IL) is greater than or equal to the specified associated security level, a transparent access is granted, otherwise an intrusive authentication request is required in order to proceed with the service. Thus, all applications used by the participants in the acquired dataset were ranked based upon the afore-mentioned risk assessment model in order to be the baseline thresholds to feed the algorithms and to compare against in this and all subsequent studies.

5.2.4 Methodology of Experiment 3

Going beyond the results of the replication study, another thorough study using multibiometric fusion approach would provide an empirical validation whether it offers a better level of security and users' experience, and whether it is more appropriate to an innovative authentication architecture.

As the biometric samples can be captured by one or different biometric techniques, the following approaches are implemented so one or a set of them is applied as appropriate (elaborated in 3.6.1):

- **Multi-Sample approach**: deploying multiple inputs of the same modality in order to have a more informed identity verification decision and to offset the existence of samples of low quality.
- **Multimodal approach**: deploying a single sample of multiple modalities to alleviate the malfunction of some incorporated biometric techniques or sensors.
- **Hybrid approach**: dynamically deploying single or multiple samples of multiple modalities. This would fine-tune the algorithm in order to achieve a desired performance, crafting a more multi-layered method.

Referring to the review in 3.6.2, these samples need to be fused effectively at certain phase of the biometric system: sensor, feature, matching score, and/or decision level (Clarke, 2011; Ross, 2007; Sim et al., 2007). The approach to be adopted in this experiment is the decision-level fusion of available multimodal and multi-sample decisions. Even though it is not the most accurate multibiometric fusion type (Ross et al., 2006), the decision-level fusion approach is the most appropriate one for the available information of the captured dataset and it also has the merit of encompassing any number of classifiers without the need to re-train the system. This objective aims at producing such a scalable, flexible and dynamic framework, thereby enabling multiple diverse classification schemes, in order to have a more robust authentication decision.

The implemented multibiometric authentication system is tasked with taking the binary decisions and subsequently performing an accumulative decision taking into account the variability factors of the biometric information. This fusion can be as max, min, median, or majority vote combinations (Kittler et al., 1998). However, security needs more consideration, e.g. single biometrics should not have much value. In order to produce a balanced decision considering the effect of the inputs from modalities of different EERs yet different accuracies, consideration needs also to be given to the weight each individual contributing technique has on the fused decision.

Probability fusion can be an option but unlike the matching-level fusion, the adopted decision-level fusion lacks the richness of information that can be used as probabilistic inputs. However, there is an approach that can be implemented at the decision-level fusion whilst taking the proportional different verification performance of the contributing biometrics into account – the weighted majority voting. For instance, typically, the facial verification performs better than the gait recognition and thus would have a greater weight and effect on the final fused decision. This would also support the flexibility and dynamic of the approach

when employing classifiers/biometrics of changing nature, based at which their weights would be updated accordingly.

Therefore and for evaluation purposes, MATLAB scripts were developed to investigate the Weighted Majority Voting Fusion (WMVF) of facial verification, voice verification, gait recognition and behavioural profiling.

Given enough time in samples, any combination of multibiometric systems could potentially exist. In order to manage the data, this weighted majority voting formula is devised; knowing that the weights are assigned to the individual biometric techniques inversely proportionate to their EERs – the lower the EER, the higher the weight than those of high EER.

$$\text{Weighted Majority Voting} = \frac{\sum_{i=1}^{N}\sum_{x=1}^{M}((D_i)_x * W_i)}{\sum_{i=1}^{M} x_i}$$

Where: i= the number of the biometric technique;

N = the total number of available biometric techniques within the specified time window;

x = the number of the sample of the biometric technique;

M = the total number of samples of the same biometric technique within the specified time window;

D = the decision of the biometric sample;

W = the weight of the biometric technique.

Based upon the existence of the samples, the Alert level algorithm would correspondingly respond taking into account their number, confidence level(s), weight(s), and individual

classification decision(s). The result of this formula is compared with the threshold associated with the risk level of the accessed application/service.

An investigation tool was required to facilitate the pattern classification processing of these studies. Hence, the specialised mathematical modelling software package MATLAB (R2015b release) that is developed by MathWorks was employed on a Windows 7 Enterprise 64-bit Operating System with Intel Core i5-4310 CPU, 2.7 GHz and 16 GB RAM. It is utilised extensively for the modelling and validation of the studies of this research because of its common use and well-acceptance throughout scientific and engineering communities in the analysis of mathematical problems. A number of scripts were written and then generated in order to perform a variety of tasks to implement the experiments (Appendix F). In all these studies, the data of each participant was split into two datasets: 60% for training the classifiers and generating the user profile and 40% for validation and testing the performance. Accordingly, the latter was performed considering one participant acting as the valid authorised user whilst the remaining other participants as imposters and then repeating to ensure all users have the opportunity of acting as the authorised user. Results are then averaged across the population sample.

5.2.5 Data Collection Software

The contemporary digital devices (e.g. smartphones and tablets) are capable of capturing multiple biometric modalities alongside other pieces of information from built-in sensors (e.g. GPS) without affecting the users' normal interactions. In order to facilitate the subsequent experiments set to evaluate and determine potential and feasible attributes to prove the research concept using a wide real dataset, a software utilising these smart devices was needed to be developed for biometric data collection purpose.

Even though the findings of Section 4.3.2 demonstrate that the utilisation of the iOS slightly outweighs the Android by the surveyed users, Android environment was selected because:

- Most of the data to be collected may be considered sensitive so the software and data need to be installed and collected off-line. Not all respondents of that user survey are accessible to meet face to face for the installation and collection procedures. Accordingly, a preliminary pilot study of those reachable potential participants showed that about two thirds of them use devices running Google Android OS.
- It is currently dominating the mobile phones market share by 87.6% (IDC, 2016).
- It is an open source and easy to manipulate.
- Its security model details are publicly available.
- Unlike iOS, it enables access to device detailed sensors data from background services without the need to root/jailbreak the devices (it is unlikely for the participants to accept that).

This would enable recruiting more participants on the data collection process and offer a reasonable opportunity to acquire data from different sensors unlike other locked platforms. As a consequence, a mobile application was developed using Android Studio development environment in order to be installed on participants' devices (both an Android smartphone and a tablet where appropriate) for a real data collection. This application is devised to capture the biometric samples from the users and store them as templates on the participants' devices' local storage in order to analyse and utilise them in developing the subsequent authentication model and prototype.

It was crucial to develop the software in an appropriate way to capture the information required in an efficient and convenient fashion. Thus, there were no additional sensors or

equipment required for the data collection other than the personal participants' devices. Those devices should have the following minimum specifications:

- A smartphone and/or a tablet operating an Android OS version of 4.0.3 and above;
- A front camera;
- GPS location feature.

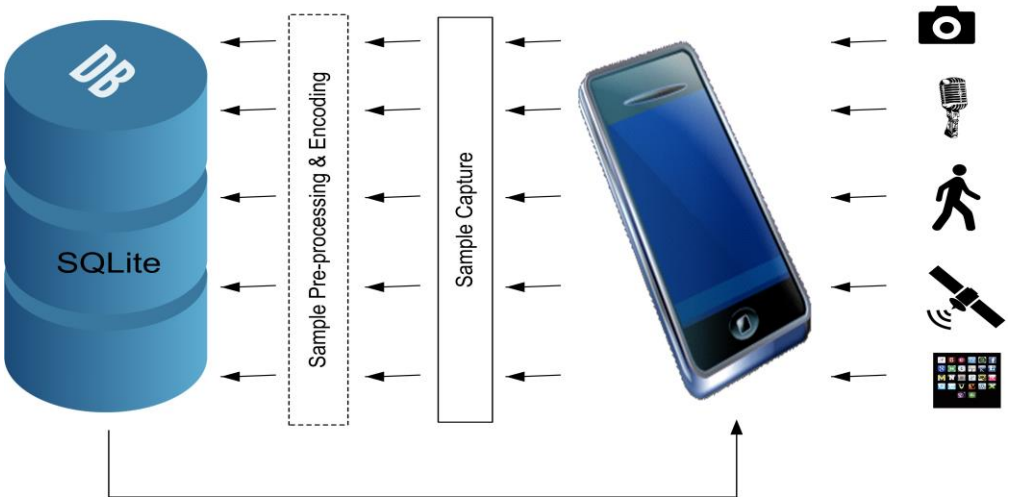

Figure 5-1: Cloud Aura Data Collection Software Architecture

As illustrated in Figure 5-1, the following 5 biometrics are captured and stored on an SQLite database on the local storage of participants' both smartphones and tablets (if available):

1) Facial recognition

   Images samples are captured at the initiation of the Cloud Aura app and then every 3 minutes (if a face is detected) – i.e. when there are no face features captured in the image, it is discarded in order to eliminate database memory unnecessary overload. These images are to be compressed and stored along with their timestamps in the SQLite database. Instead of storing their raw versions, they are pre-encoded in Base64 String format in order to simplify the database structure and thus their generation overhead is decreased. Moreover, they are prepared for future analysis work where the encoded data

will be easier to check for integrity and unlikely to be modified in transit. Furthermore, it adds a level of obfuscation making it not easy for human's observation – it is only read and analysed by machine.

2) Voice recognition

Voice samples are captured at the initiation of the Cloud Aura app and then every 3 minutes. However, linking it with actions such as phone calls would have been more practical but this was avoided in order not to put participants away from taking part in such an experiment due to privacy concerns. A noise cancellation method is applied to reduce the unwanted surrounding sounds. The captured samples are to be compressed and stored together with their timestamps in the SQLite database. Similar to face samples, instead of storing their raw versions, they are pre-encoded in Base64 String format in order to simplify the database structure and thus their generation overhead is decreased. Moreover, they are prepared for future analysis work where the encoded data will be easier to check for integrity and unlikely to be modified in transit. Furthermore, it adds a level of obfuscation making it not easy for human's observation – it is only read and analysed by machine.

3) Apps Usage

All device's applications usage of a user are captured as soon as they are accessed based on their associated timestamps and then are stored in the SQLite database accordingly.

4) Gait (Walking pattern)

The Cloud Aura app counts the number of steps the user walks together with the distance they cover in each specific hour of a day, and then stores these figures in the SQLite database accordingly.

5) Geolocation (GPS)

The Cloud Aura app monitors and captures the geographical location (from either the GPS sensor or the WiFi hotspot) of the device as soon as it is in use and the location changes per specific hour a day. The captured GPS coordinates (longitude and latitude) are stored in the SQLite database accordingly.

All related capturing packages were encapsulated in one single Android Application Package (APK). Native Android was used to develop the Could Aura application whilst XML to design its graphics and user interface, Java for the front-end app development, and SQLite as the app database. Enabling the software to capture the above-mentioned information was facilitated by employing and deploying a number of Android APIs (apart from other supplementary basic APIs) as follows (Appendix E):

- Android Media API – Face Detector
- Android Hardware Camera2 API
- Android Media API – Audio Manager
- Android App Usage API
- Android User Availability API
- Android Hardware API – Sensor Manager
- Android Location API
- Android Database File Upload API

5.3 Experimental Results and Analysis

This section seeks to firstly outline the gathered experimental data. A thorough discussion and analysis of the results of the three set experiments is then performed and presented.

5.3.1 Overview of the Acquired Dataset

Cloud Aura biometric data capturing software was initially installed on the devices of 58 subjects, 11 of which were removed from the inclusion in the final dataset for various reasons, such as incompatibility frequent crashing, odd battery drainage, and lack of generated core

files. As a result, as shown in Table 5-2, the data captured from the 47 participants (4 users have 2 devices each and 1 user has 3 devices) can be considered rich enough to enable a meaningful analysis. Even though the recruited subjects were asked to let the software run for 14 days, some had above than the requested period and a few less.

Total Number of All Users	47
Total Number of All Devices	53
Total Number of Days	761
Average Number of Days per Users	14.36
Total Number of Usage Hours	1,005

Table 5-2: The Overall Final Captured Dataset Statistics

The participants' devices also represented a wide range of manufacturing devices (e.g. Samsung, Sony, HTC, Google, Motorola and Huawei) as well as Android OS versions (ranging from 4.0.3 to 6.0.1), thus giving a better reflection of how the real world practice is. Designing and developing such a solution must be performed taking into account compatibility and interoperability.

Table 5-3 demonstrates the total logs and samples of each captured biometric modality. The 15,322 face samples counted are those timestamped images taken while a user using the device. This includes all those images taken throughout the day, in all environmental conditions, orientation angles and even those not of the authentic authorised device user (in case it was used by for instance a colleague during the study). The only exclusion was those images with no face exists, such as when the front camera facing the ceiling. This was applied to avoid over consuming the devices' available memories as the storing database resides on the devices themselves at the data capturing stage.

Furthermore, geolocation and gait timestamped logs were utilised in full for this study without any erroneous issues. Nevertheless, despite having applications usage, there were many daily hours without any logs from these two modalities (i.e. geolocation and gait)

caused by a number of possibilities, such as disabling the GPS and the WiFi concurrently and remaining seated during these hours. However, this is not considered a shortcoming as this is expected in the normal daily smartphones use.

Total Number of Face Samples	15,322
Total Number of Voice Samples	10,810
Total Number of Apps Usage Logs	46,204
Total Number of Geolocation Logs	11,625
Total Number of Gait Logs	1,128

Table 5-3: Statistics on Each Captured Modality

It can also be noticed from the above table that the final dataset contains a rich amount of applications usage information having the total number of its logs (46,204) is the highest amongst all other collected modalities. This number is assumed to be the number of the total authentication requests the users were prompted to when they accessed the applications. Therefore, it is used in a number of calculation metrics throughout the forthcoming experiments, especially when calculating the number of transparent and intrusive requests. As depicted in Figure 5-2, the number of days during which the data was collected for each user were roughly analogous with an average of 14.36 days per user. Conversely, the total apps usage over that period and thus the average number of apps usage per day for each user vary markedly, signifying the diversity of usage interactions between users. This observation is more noticeable with those participants having multiple devices – perhaps due to the fact that solely one device is utilised as primary whilst the others are for secondary use.

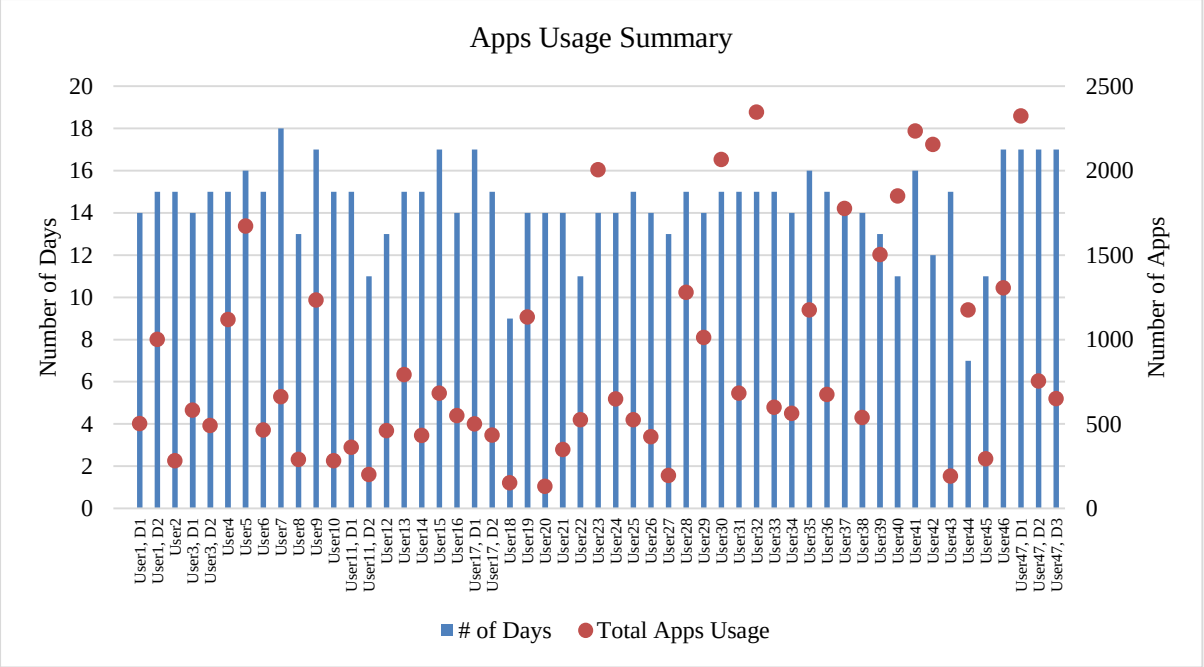

Figure 5-2: The Overall Statistics of the Final App Usage Dataset

The breakdown of the final app usage dataset in Table 5-4 illustrates its immense diversity and size, offering the opportunity to utilise it as a behavioural profiling modality given the detailed information it provides. Based upon it, the information of how a digital device is operated can be identified, including the name of the application, the time, frequency and duration at which it was accessed – and then all those can be linked with the geolocation at which it was used (if available).

Avg # of Apps per User	29.87	**Avg # of Used Unique Apps per Device**	26.49
Avg # of Apps Usage per User	983.06	**Avg # of Apps Usage per Device**	871.77
Avg # of Daily Usage hours	18.96	**Avg # of Apps Usage per Day**	61.68

Table 5-4: The Breakdown of the Final Apps Usage Dataset

The average number of applications used per user (983.06) is utilised as a distinctive basis between the high active users and low active users, yielding to what Table 5-5 demonstrates, 27 participants are categorised as low active (below average) and the remaining 20 are high active (above average).

Usage Level	Participants' Numbers
Low Active	2, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 24, 25, 26, 27, 31, 33, 34, 36, 38, 43, 45
High Active	1, 3, 4, 5, 9, 19, 23, 28, 29, 30, 32, 35, 37, 39, 40, 41, 42, 44, 46, 47

Table 5-5: Users Categories based upon their Apps Usage Levels

It was observed that the majority of device usage/interactions occurred between 6 A.M. and midnight; with a very few interactions outside this period of time by a few participants which can be attributed to being their usual sleeping time or any other personal reasons. The usage data during this relatively idle period was deemed insignificant with regard to the experimental analysis. Therefore and to avoid any data inconsistency and to aid un-skewed interpretation and representation, this period was not considered during the experiments, including calculating the system integrity, user confidence as well as their illustrative plots.

As it is not practical nor beneficial to present the user interactions of all subjects during all experiment days, Figure 5-3 and Figure 5-4 depict examples of the 18 hours of user applications usage associated with their risk levels excerpted from User 31 (a low active user) and User 4 (a high active user). The high degree of variation in the number of applications used throughout the day and their security requirements indicating the need for considering this diversity in any proposed authentication solution. Furthermore, examining these figures, which represent the whole experiment population, it is evident that more observed interactions with the device were conducted after the working hours (i.e. 17:00) despite accessing the apps of the highest risks during the working hours. Even though this was not overwhelmingly the case with all subjects, it was quite common observation, implying that the time and location at which users utilise their devices may have a major effect on their way of use.

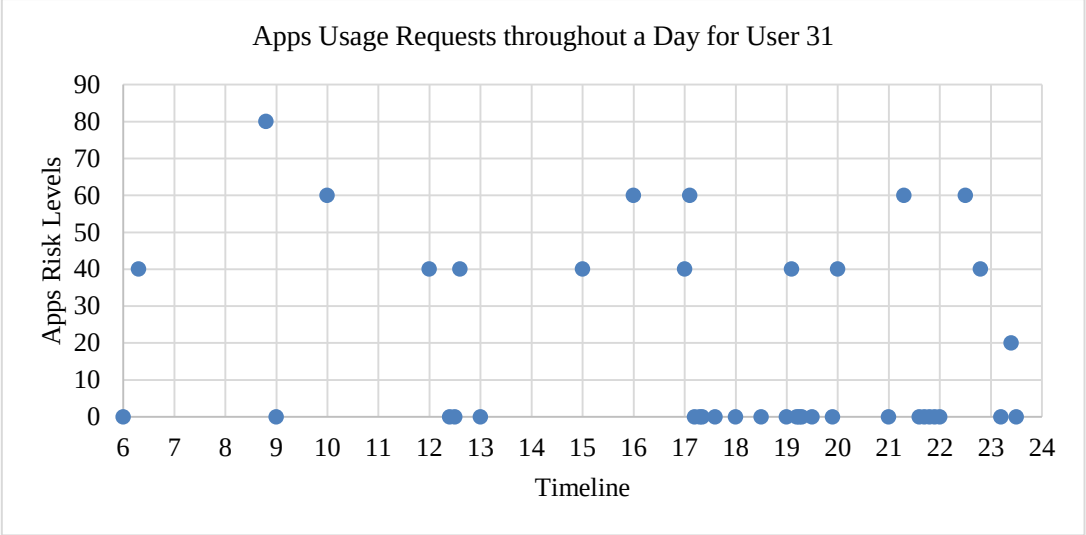

Figure 5-3: Apps Usage Requests throughout a Day for User 31 (Low Active User)

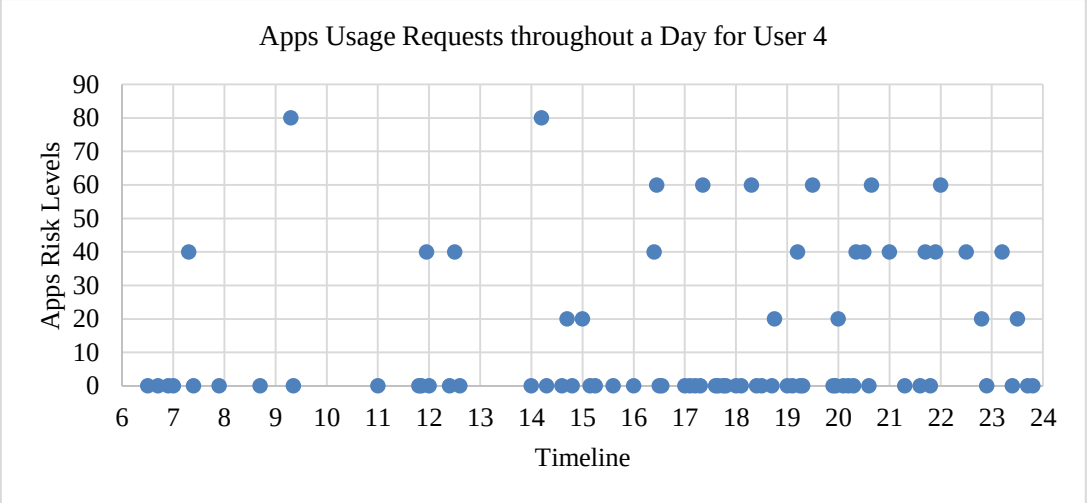

Figure 5-4: Apps Usage Requests throughout a Day for User 4 (High Active User)

5.3.2 Experiment 1: A Baseline Study on Transparent and Soft Biometrics

The succeeding two sub-sections outline and analyse the baseline set of experiments undertaken to determine the nature and performance of the potential contributing modalities; namely, facial verification and geolocation.

5.3.2.1 Facial Verification Performance

All 15,322 face samples from the collected data set (an average of 333 images per user) were used to calculate the performance under totally un-constrained data collection. It is also worth

noting that due to the malfunctioning of the front-facing camera of the mobile phone of User 27, there were no face images from this subject. It is therefore not included in calculating the average performance of face verification though it is to be considered with other modalities elsewhere in these experimental series. As previously mentioned, a face detection tool was applied prior to capturing any image, making the dataset almost free from images with no face exists. Adopting a MATLAB Computer Vision and Pattern Recognition (CVPR) toolbox running Fisherfaces face recognition method – which tends to tolerate large illumination variations – the feature vector was generated. It derives a low-dimensional space and then uses pixel intensities in the face images as identifying features (Belhumeur et al., 1997). Subsequently, the orientation of each facial image was corrected and the enrolment was performed and the verification performance was calculated.

To ensure that the classifier could cope with the variabilities in angles of facial orientation, a customisation was deployed on the script enabling it to accept a group of facial images as an enrolment template. Accordingly, five randomly selected facial images were utilised to create the template, against which the remaining images of that participant were compared. Specifying this number was due to what is likely to be in real practice where having such a lengthy enrolment process would inhibit the users' acceptance (Clarke et al., 2008). Images of other participants were used as imposters while measuring the algorithm accuracy. That is, the images of all remaining 45 subjects were considered imposter samples and used to calculate the FAR. This was subsequently repeated with each user taking the role of the authorised user.

Figure 5-5 demonstrates that the average face verification EER varied markedly between participants ranging from 0 (for Users 7, 8, 9, 10, 13, 16, 32, 37, 40, 42) to between 18 and 20 (for Users 11, 15, 17, 34, 36, 41, 44, 46, 47). As far as the extent of use of these 2 extreme subsets is concerned, they also differ significantly so no correlation was observed between

them and the endured EERs of the same users. For instance, whilst the number of applications used by Users 7, 13 and 16 are quite similar to those of Users 11, 15, 34 and 36 (i.e. both groups are of low active users), their EERs are divergent completely – with the former being of the lowest EER and the latter being of the highest EER. Therefore, there does not appear to be a correlation between the EER achieved and the number of applications used.

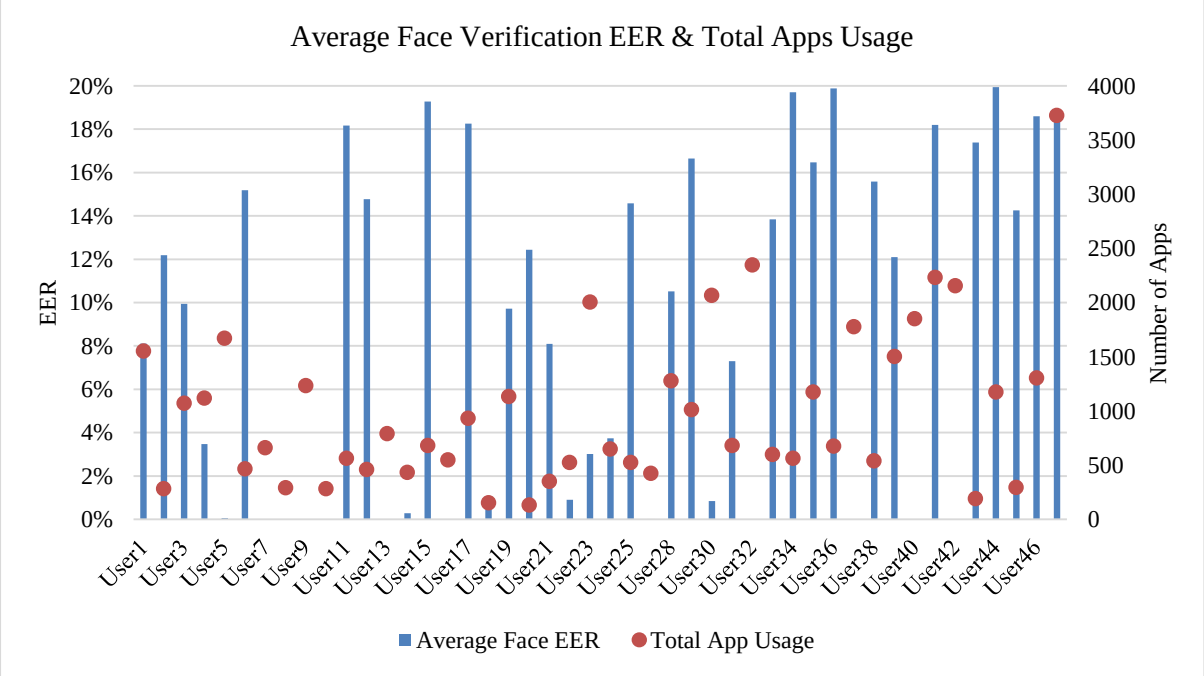

Figure 5-5: Average Face Verification EER & Total Apps Usage for each User

The level of user identity confidence was calculated continuously based upon the face samples captured and their associated verification decisions when compared against the template. The decision can be a number between zero and one. No degradation was applied in this experiment so the confidence fluctuates only depending on the facial verification decision of the coming samples at the time.

Figure 5-6 illustrates that the face authentication confidence levels did not reveal significant difference dependent upon the level of usage. Taking examples of one high active participant (4) and another low active one (31), they both experienced constantly high identity confidence throughout a selected day. Hence, the variety of performance levels can be

attributed to factors other than the usage degree such as differences in camera resolutions, personal way of use, environmental and lighting conditions, and occlusions. Another observation on the same figure is that the face verification technique performed well in such un-obtrusive and continuous fashion.

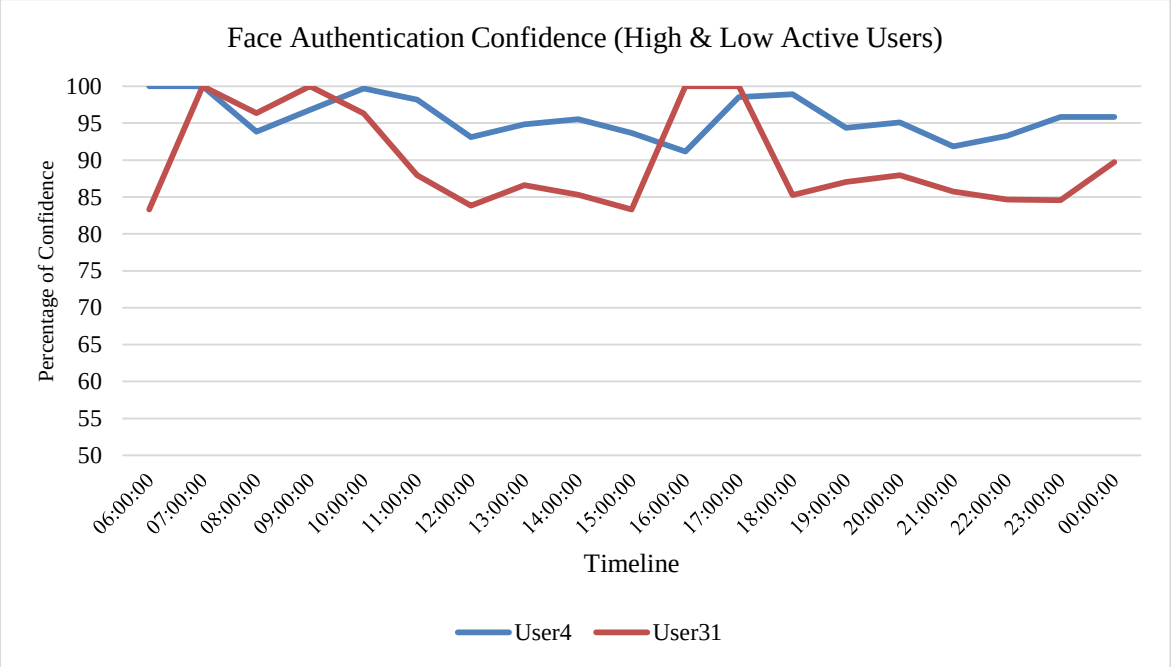

Figure 5-6: Face Authentication Confidence (High & Low Active Users) throughout a Day

The overall resultant EER was 6.05%. Despite being slightly higher than other published facial verification EERs, the nature of capturing the dataset (un-constrained and task-free) makes this result closer to reality. For example, whilst facial recognition approaches are well accepted, they are designed to operate within very tight environmental conditions (i.e. specific levels of illumination and facial orientation). Such assumptions in a transparent application are unlikely to hold true – implementing it on a mobile phone, it would be expected to capture a user's face in a variety of orientations and during differing times of the day. Equally so, if this biometric is fused with other modalities while mapping the fused decision with the security requirements of the applications accessed and actions performed, this would probably improve the performance (which is to be investigated in 5.3.4). The

relative high EER may also be due to the high possibility of the dataset having numerous partial images, affecting the features matching with the templates of complete images to be difficult to perform well.

5.3.2.2 Geolocation Performance

A fair number of geolocation samples were collected with a total of 11,625 logs from 44 subjects, yielding to an average of 264 GPS samples per user (as seen in Table 5-6). Albeit the participants' devices were all equipped with GPS sensor and had access to WiFi, the collected dataset had no geolocation information at all from only 3 participants (Users 4, 12 and 28). This might be attributed to the fact that there were no restrictions what so ever on users (i.e. participants were not instructed to enable the GPS/WiFi all or at specified times). Another issue found upon investigation of the GPS data that there were portion of certain days missing for some users. Although it was unclear why exactly this was the case, speaking with participants confirmed that this was because they might switch the GPS off or put their device on flight mode for a period of time for personal reasons. A possible reason for the tendency to disable the GPS could be the high power consumption might be encountered by some participants when turning it on all the time. Nonetheless, taking this into operational consideration would alleviate the issue of missing geolocation data thereby, for instance, deploying a periodic GPS capturing or utilising a more efficient location API such as the Google location services. This however, does not remove or minimise the capability of doing a meaningful analysis and model given the distribution of captured data between users.

User ID	Total of GPS	User ID	Total of GPS	User ID	Total of GPS	User ID	Total of GPS
User1	416	**User14**	116	**User25**	140	**User37**	476
User2	75	**User15**	182	**User26**	114	**User38**	144
User3	287	**User16**	147	**User27**	102	**User39**	403
User5	448	**User17**	250	**User29**	271	**User40**	496
User6	124	**User18**	91	**User30**	553	**User41**	598
User7	177	**User19**	303	**User31**	182	**User42**	577
User8	78	**User20**	135	**User32**	628	**User43**	151
User9	331	**User21**	93	**User33**	160	**User44**	315
User10	76	**User22**	140	**User34**	151	**User45**	78
User11	151	**User23**	537	**User35**	314	**User46**	350
User13	212	**User24**	173	**User36**	181	**User47**	698

Table 5-6: Number of GPS Captured Samples for each Participant

To avoid having unreasonable high error rates, the data for each user were pre-processed to eliminate those periods when no GPS data recorded as the geolocation classifier ideally should not be triggered without inputs. They were consequently aggregated based on the timestamps at which they were collected. The coordinates captured were represented on decimal format, such as 50.3758239, -4.1413622 where the former number is the latitude decimal degree and the latter is the longitude decimal degree. These can be converted to degrees, minutes, and seconds (DMS) when required prior to entering the classifier.

The Mobility Markov Chains (MMC) model was adopted successfully for similar purposes in prior art (Gambs et al., 2012; Mahbub et al., 2016). Thus, MMC was utilised for this experiment to be able to predict the next location of an individual based upon a number of observations of their mobility behaviour over the previous period of time and the locations they have visited on particular time-frames. It produced a probability score after comparing each geolocation pair with the historical and predicted locations of the concerned user. Not only that, consideration was also taken to the marginal differences between the GPSs of close proximity to tolerate. For example, the GPSs captured on Monday between 15:00 and 16:00 are slightly different than those on Tuesday of the same time (e.g. by 10-20 meters) which is an accepted margin and would not deteriorate the probability score sharply.

As conducted in face verification, the geolocation dataset of each subject were divided into 60% for training the classifier and creating the user template and 40% for testing and validation. Figure 5-7 exhibits that a significantly wide range of geolocation performance was calculated with 2.60% of User 32 being the best and 24.22% of User 14 being the worst. It was found that 5 participants (Users 31, 32, 37, 40 & 42) achieved an EER of less than 10% each whilst another 6 (Users 2, 5, 9, 13, 14 & 27) accomplished an EER of more than 20% each. Only one subject of the former was categorised as low active user whereas, in contrast, a sole subject of the latter was high active user. Therefore, a closer analysis encompassing the whole dataset was required to comprehend whether a relation existed between the usage level and the geolocation performance.

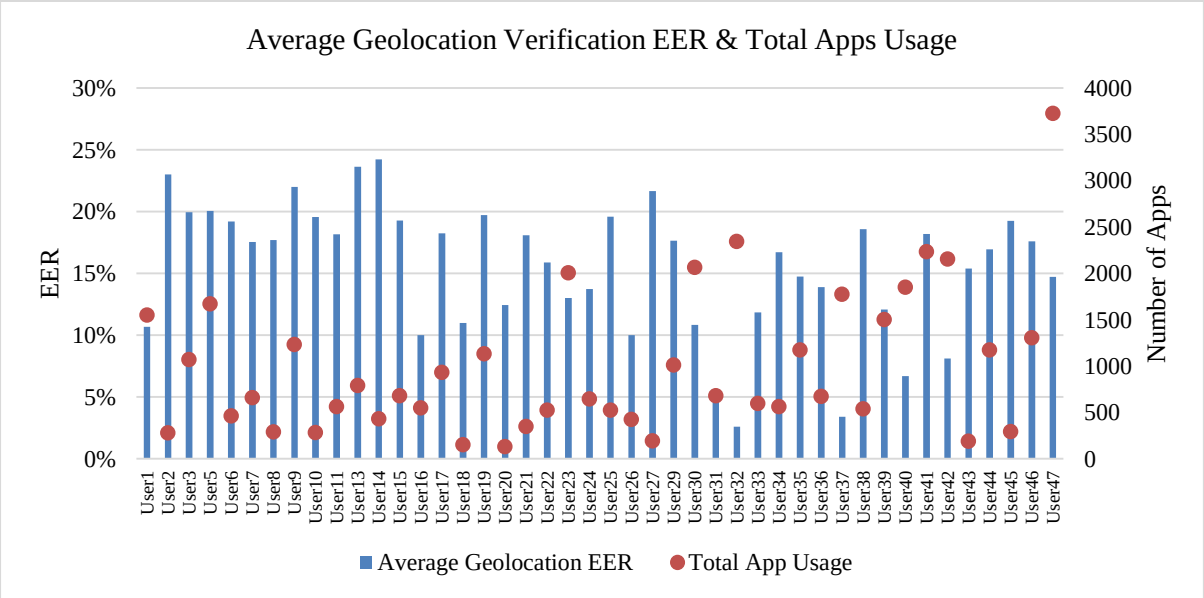

Figure 5-7: Average Geolocation Verification EER & Total App Usage for each User

Table 5-7 shows that the 26 low active subjects had an average EER of 17.95% even though that the 18 high active subjects had a better EER of 13.61% (with a difference of 4.34%). This could be due to the enriched acquired samples on which the classifier was trained, making the decision made more reliable. Furthermore, those high active users perhaps tend to have a more stable pattern of life, in particular in terms of their usual visited places.

Usage Level	Participants' Numbers	Average Geolocation EER%
Low Active	2, 6, 7, 8, 10, 11, 13, 14, 15, 16, 17, 18, 20, 21, 22, 24, 25, 26, 27, 31, 33, 34, 36, 38, 43, 45	17.95
High Active	1, 3, 5, 9, 19, 23, 29, 30, 32, 35, 37, 39, 40, 41, 42, 44, 46, 47	13.61

Table 5-7: Average Geolocation EER based upon the Usage Level

The overall classification resulted in an EER of 15.78%, making it a positive smart contributor to accomplish a well-informed authentication fusion system. Even though it is not a biometric and cannot be used alone, it was included and measured in biometric terms just to understand how unique it is. For instance, being used as soft biometric so additional information being used as part of the decision-making process of a wide biometric system or it can be used as a feature within a particular modality such as behavioural profiling where it is utilised along with other features to understand the nature of individuals' behaviour.

5.3.3 Experiment 2: A Replication Study

A framework called Non-Intrusive Continuous Authentication (NICA) was selected for evaluation because it is believed to be very close to the approach of this research, it has the virtue of taking part in tackling aspects of the research problem, besides the fact that it is well-documented allowing a straightforward replication (as reviewed in 3.8.1).

5.3.3.1 NICA Theoretical Foundation

NICA is a mobile-based solution that utilises a mixture of secret knowledge authentication coupled with several chosen available biometric techniques to provide transparent and continuous authentication despite the cognitive intrusive initial login (Clarke et al., 2009). It can be configured to choose what to include for classification from individual biometric techniques. NICA does also consider the assumption that different services and data require different security provisions. Through understanding the risk associated with particular user

actions and services, the protection level required can vary from almost none for checking the time, medium for texting, to significantly high for online banking. The level of confidence is continuously fluctuating based upon the biometric samples captured which is subsequently reflected on the privileges to access services and applications, enabling the device to shutdown functionality if insufficient confidence exists.

In order to establish the device's security provision and the system usability, the Integrity Level (IL) and the Alert Level (AL) are regarded the pivotal operations of the NICA framework to be defined and mapped with confidence levels. As Table 5-8 demonstrates, confidence levels are aligned with the FAR of the incorporated authentication techniques.

Biometrics				**Secret Knowledge**			
Confidence Level	**FAR Level**	**+ OR - Value**	**Max IL**	**Confidence Level**	**Input Required**	**+ OR - Value**	**Max IL**
B0	10-20%	0.5	2	S0	PIN/Cognitive	NA	NA
B1	5-10%	1	3	S1	PUK (Operator)/ Administrator Password	None - IL set to 0	NA
B2	2-5%	1.5	4				
B3	0-2%	2	5				

Table 5-8: NICA Confidence Levels and the Corresponding IL

On the other hand, the corresponding Integrity Level (IL) of the system ranges between -5 and +5 – where -5 is the lowest IL and +5 is the highest IL. The IL changes based upon the result of the authentication requests, the confidence level of the utilised authentication technique, and the time that has elapsed between them. A specific value is assigned to each of the confidence levels to be added to or deducted from the current IL dependent upon whether the identity verification is successful, up to a predefined maximum system IL (as also shown in Table 5-8). With the aim of alleviating the risk of misuse while the device is idle, a degradation function is enforced thereby decreasing the IL periodically – 0.5 drop every 30 minutes for frequent users and 50 minutes for infrequent ones.

With regard to the Alert Level (AL), it is run by the authentication manger which is invoked every 10-25 minutes and decides which is the most recent sample with the best performance within the specified time window to be used for authentication and what the subsequent action to take, as illustrated in Figure 5-8.

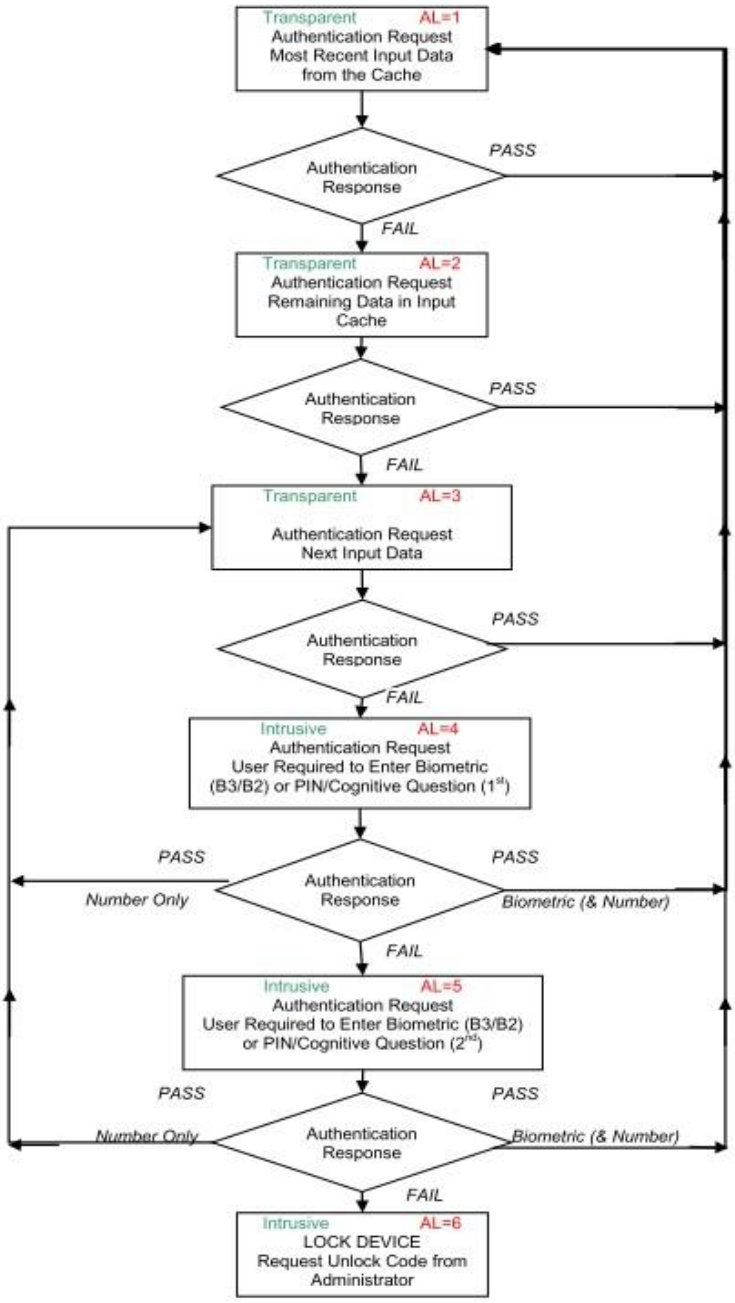

Figure 5-8: NICA Alert Level Algorithm (Clarke et al., 2009)

Depending upon each authentication decision/request made by the AL, the IL is utilised when the user triggers a request to access a service/app that the system has set to be protected. NICA provides the protection capability to certain services/apps by associating an integrity value as a threshold not to be broken in order to grant the user access to them. Hence, if the IL is sufficient to access the service/app, then access will be authorised, otherwise the user will be prompted with an intrusive request.

5.3.3.2 NICA Integrity Performance - Authorised User

The main contribution of this thesis is not to develop new biometric classifiers/algorithms or optimise a specific one, but rather enhancing the mechanism of managing the biometric signals received to have a more informed identity verification decision in a more convenient and secured manner. Therefore, the performance of selected well-established studies (reviewed in Chapter 3) were adopted along with the EERs resulted from Experiment 1 to be incorporated as inputs in this and forthcoming experimental studies (as presented in Table 5-9) whilst mapping them with the associated actual recorded timestamps of the dataset.

Category	**Biometric Technique**	**EER %**
Physiological Biometrics	**Facial Verification**	6.05
Soft Biometrics	**Geolocation**	15.78
Behavioural Biometrics	**Voice verification** (Woo et al., 2006)	7.80
	App Usage (Behavioural Profiling) (Li et al., 2011)	7.03
	Gait (Derawi et al., 2012)	20.10

Table 5-9: The Biometric Techniques Performance (EER) to be Employed in the Following Experiments

In this study in particular, the EERs of 4 biometrics are used – i.e. face verification, voice verification, behavioural profiling, and gait. The core focus of evaluating the NICA framework is on the concept of transparent user authentication at an operational level – where in case of misuse by an impostor or insufficient confidence in the authorised user, an

intrusive authentication is requested, otherwise, the user is not interrupted. In addition, no consideration to the action(s) resulting in failing intrusive authentication is given in this evaluation – a successful authentication is assumed and the AL is reset to Level 1 whereas for an impostor it would lead to lock the device.

As explained in the preceding sub-section, the NICA framework was conceptualised to operate the AL time window to be 10-50 minutes and the IL time window (of the degradation function) to be 30 minutes for heavy users and 50 for light ones. Although these time windows would enhance the usability of such system from the end-user perspective, it might be relaxed in terms of security due to being susceptible to misuse in between the triggering times. Therefore, varying smaller time windows were configured for this evaluation in order to investigate their effect on the framework operational performance and, if possible, determine whether a specific combination perform better with specific type of users. However, as the combinations of these timings (i.e. AL and IL) can be infinite, just 4 combinations were tested; namely, AL 2 min/ IL 10 min; AL 5 min/ IL 5 min; AL 5 min/ IL 10 min; and AL 5 min/ IL 20 min.

There are many ways to analyse the data but a set of them are to be followed to help explain the nature and dynamic of the model. Evaluating the NICA framework is set to assess its security and usability on previously mentioned time windows based upon the averages of all users, the worst and best cases, and in relation to the different accessed apps risk levels. The former focuses on measuring how the integrity level is maintained with an authorised user as well as an imposter besides how long it takes to identify and lock out an impostor at differing levels of AL whilst the latter focuses on examining its transparency through the frequency of interrupting the user to request them to perform an explicit authentication.

The primary focus of this sub-section is to gain a better insight into how system integrity would be maintained and vary across each time window as a means to determine how secure the NICA framework is. Preserving a fair level of integrity while the device is in use by an authorised user is an indication of the robustness of the system. Table 5-10 demonstrates the average system integrity (out of 5) of all authorised users over the differing time windows.

NICA				
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**
Average Integrity	3.51	3.69	3.71	3.85

Table 5-10: NICA Average Integrity over Different Time Windows (Authorised User)

It is apparent that the average integrity of the NICA framework is less in lower time windows as triggering the AL and IL at short intervals increases the probability of not having samples in between and thus does not allow for keeping or even increasing the integrity. As a result, the FRR would be higher with shorter windows. Although the smaller windows (AL=5, IL=5) can be considered performing well with an integrity average of 3.51 out of 5, it is increasing with the greater time windows – the significant difference is noticed with changing the IL. This performance can be attributed to the fact that during the larger window (i.e. IL=20) the integrity is sustained as the degradation function is not called other than thrice an hour. Notwithstanding, this might be at the expense of exposing the device to un-authorised access before the next IL drop.

A further investigation was conducted to see how divergent the accomplished integrities were across these time settings. As shown in Table 5-11, User 44 had the worst calculated average integrity throughout all time windows whilst three different participants (Users 45, 9, and 18) scored the best cases. Even though the performance spectrum looks wide ranging from 0.94 to 4.87, almost 60% of participants experienced an average integrity of above 3,

enabling granting the legitimate user access to those applications of risk levels above 3 resulting in a fair degree of transparency.

NICA				
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**
Worst Case Integrity	1.17	1.05	1.08	0.94
User ID	44	44	44	44
Best Case Integrity	4.85	4.75	4.86	4.87
User ID	45	9	18	18

Table 5-11: NICA Worst and Best Integrity Cases over Different Time Windows (Authorised User)

Another observation here is with respects to the extent of user interaction revealing that no direct correlation existed between it and the achieved integrity across all participants. For instance, from those users of worst and best cases, whilst Users 44 and 9 were of the high active users, the former was the worst case and the latter was the best with the AL of 2 minutes and the IL of 10 minutes. Despite the possibility of the lack of available samples while utilising small time windows hence causing constant dropping integrity due to the degradation function, the framework still achieved quite acceptable positive integrity. In a nutshell, the role that varying time windows play in the process of the framework is evident and can vary from one user to another.

5.3.3.3 NICA Integrity Performance - Imposter User

Having investigated the NICA framework with the authorised user regarding maintaining a representative confidence on the user, the security aspect of the framework needs to be further examined considering an impostor exploiting the system.

The average integrity of the system for an impostor across the four time windows is shown in Table 5-12. The lower the integrity of the system, the higher the security. With integrities less than (-4), the user would not only be rejected from accessing applications/services of high risk levels but also from accessing those of low risk level, leading to barring the whole

device. The shorter time windows outperform the longer ones albeit this might be in favour of security but not usability as this would increase the FRR. Therefore, a balanced trade-off between security and usability based upon the user requirements and preferences together with the risk nature of data/apps/services is needed.

NICA				
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**
Average Integrity	-4.84	-4.67	-4.64	-4.41

Table 5-12: NICA Average Integrity over Different Time Windows (Imposter User)

In order to further examine the system integrity against the illegitimate access, worst and best cases were recalled besides the average time of detecting and locking out the imposter (Table 5-13). The worst and best integrities with imposter were comparative to those with authorised user, but with 3 other participants (Users 20, 32, and 35) getting the best results. Even so, the absence of direct relation also occurred between the usage level and the performance – given that half of the reported best cases are categorised as high active (Users 32 and 35) and the other half as low active (Users 20 and 45).

NICA				
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**
Worst Case Integrity	-1.47	-1.33	-1.35	-1.17
User ID	44	44	44	44
Best Case Integrity	-4.99	-4.86	-4.95	-4.97
User ID	35	32	20	45
Average Detection Time (min)	5.670	2.155	5.360	5.166

Table 5-13: NICA Worst, Best Integrity Cases and Detection Times over Different Time Windows (Imposter User)

The results of the table also presented that the system security was sound being able to identify and prevent the imposter from accessing the applications/services within a few minutes proportionate to the operated AL time. The acceptability of these detection times is dependent upon the user requirements and utilised applications risk levels. Furthermore, it is envisaged that these times would be reduced if the imposter starts by requesting a high risky

application which is higher than the system integrity at the time, at which the imposter will have an immediate failed authentication leading to a quicker integrity drop.

5.3.3.4 NICA Usability Performance

Although it can be deduced that the framework manages to maintain a certain level of transparency, a closer look into the extent of intrusive authentication requests is desired. Therefore, the percentages of these intrusive requests of each user throughout the usage period were averaged to get the overall system usability performance. In line with the security results, Table 5-14 elucidates that there is a correlation between the IL and the number of explicit authentication requests. As the time windows rise and the better the average integrity, the lower the number of intrusive requests is.

NICA				
Total Requests	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**
	% of Intrusive requests	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**
46,254	19.85	16.16	15.79	12.99

Table 5-14: The Average Percentage of Intrusive Authentication Requests of NICA

It can be interpreted that longer time windows introduce fewer intrusive authentication requests on average as invoking the degradation function in short intervals is not as frequent. This supports the conclusion that the degradation function has a noticeable effect on such a framework. Moreover, taking merely the most recent sample and ignoring the rest of samples and the ceiling being posed on the confidence level of each biometric (to which this sample belongs) to contribute towards raising the integrity above certain levels (elicited in the NICA model) besides the short time between AL requests might be the cause of enduring more intrusive requests.

The performance results of the NICA framework (ranging from an average of 12.99% to 19.85% intrusive requests of all requests to access applications) show that it offers a fair level

of security and usability. However, these numbers being averages mean that there were cases achieved worse results so it is worth investigating the effect of including more or all available samples (rather than only one in NICA) within the time window to calculate the authentication decision and thus the integrity level and how this would be reflected on the performance.

A further analysis was pursued to appreciate which category/categories of applications/services risk levels spawned more intrusive authentication requests, and thus affected the users' convenience. Table 5-15 illustrates the differing app risk levels that signify the required level of user' confidence alongside the percentage of intrusive authentication requests that the user prompted to when attempting to access the apps.

NICA				
App Risk Level	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**
	% of Intrusive requests	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**
0	0	0	0	0
1	0.45	0.37	0.36	0.30
2	1.43	1.16	1.14	0.94
3	2.07	1.69	1.65	1.36
4	4.11	3.35	3.27	2.69
5	11.78	9.59	9.37	7.71
Worst Case User(s) ID	59.66	56.60	54.47	49.26
	44	44	44	41
Best Case User(s) ID	0.00	0.00	0.00	0.00
	2	2	2	2

Table 5-15: The Percentage of Intrusive Authentication Requests of NICA based on the App Risk Levels, Worst and Best Cases

The table shows that the majority of the highly risk apps generated more intrusive authentication requests while with lower app risk levels the system became way more transparent, i.e. very less intrusive authentication requests. Whereas the average percentage of intrusive requests reached more than 50% of the total app requests in the worst cases (with Users 41 and 44), the highly secured apps that require trust level of 5 produced the majority

of them. However, the apps with trust required 4 and less acquired gradually descending intrusive requests to nearly complete transparency whilst the best case reached that – User 2 had no intrusive requests at all.

Given that more than two thirds of the users encountered less than 20% obtrusive requests, it is evident that the model is capable of accomplishing rational high levels of integrity for the period of usage whilst retaining a reasonable level of users' convenience although higher levels of system integrity and thus transparency are desirable.

5.3.4 Experiment 3: Multibiometrics-based Continuous Authentication Decisions

Given the aforementioned experimental findings on the NICA model, it is evident that it solely incorporates single sample neglecting the capabilities of capturing many samples within certain periods the contemporary advanced digital devices have. Whilst it is envisaged that this can be mitigated by making use of these capabilities and combining them in a way to enhance the overall performance, this needs to be validated empirically in order to propose a more robust approach than the NICA framework. Such a fusion must be executed in a constructive rather than destructive fashion.

The use of multibiometric approaches augments the authentication systems to rely upon more than one biometric technique or more than one sample of the same technique. This should be dynamic and intelligent in the method of selecting what modalities to encompass in the fusion process and how. For instance, when acquiring a face image is not possible, gait, voice and behavioural profiling would be able to accomplish an adequate level of security. As discussed in 3.6, the reliability of utilising multibiometrics would counteract the spoofing and circumvention risks. Accordingly, this experiment deploys a novel multimodal/multi-sample fusion method of facial verification, voice verification, gait recognition and behavioural

profiling in order to appraise the effectiveness of applying multibiometrics-based continuous authentication on the framework of this research.

The use of various classifiers might result in divergent data and outcomes subject to the activities the user is carrying out, thus enriching the decisions of multiple classifiers (Sim et al., 2007). All settings of the above-mentioned replication study were followed in this experiment with the addition of considering the inclusion of all available biometric samples within the specified time-frame.

This multibiometric fusion model is analysed by first looking at the average system integrity of the system over the whole experiment duration across various AL's and IL's including the users obtained the worst and best results with authorised and imposter user data comprising how long does it take to identify and shut out at impostor. Likewise, the integrity is calculated after reducing the degradation value and even disabling it completely. Finally, further analysis is undertaken to count the number of transparent versus intrusive authentication requests along with a breakdown based upon the different levels of app risk.

5.3.4.1 Weighted Majority Voting Fusion (WMVF) Integrity Performance - Authorised User

Using the same dataset of the previous experiment, Table 5-16 depicts the results of the average system integrity after the deployment of the Weighted Majority Voting Fusion (WMVF) fed by the data of the genuine user.

Weighted Majority Voting Fusion (WMVF)					
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min *(-0.25 Drop)***
Average Integrity	3.91	3.77	3.85	4.07	3.84

Table 5-16: Average Integrity of Weighted Majority Voting Fusion (WMVF) with Degradation Function (Authorised User)

As seen above, the WMVF achieved trust levels on the legitimacy of the user outperforming NICA albeit not significantly on all windows except (AL 5 min and IL 5 min) where the improvement was about 0.4 point (i.e. from 3.51 with NICA to 3.91 with WMVF). This quite better performance can be attributed to the inclusion of all available samples. However, being not that large can be due to various factors, such as bad captured samples stemming false decisions; the available samples that passed the decisions are of low confidence biometric techniques; the extent of usage; and the degree by which the integrity drops when the time set for degradation function passed without samples inputs.

Paying a closer attention to the worst and best cases in Table 5-17, there is an increase in the former compared with the NICA outcomes as much as 0.4 in shorter windows up to full 1 level jump in the longer ones. For instance, whilst the worst case achieved by NICA was 0.94 (with AL 5 and IL 20), it is improved to be 1.92 with the WMVF. This would minimise the intrusive requests significantly with those low risk levels apps (to be further investigated in section 5.3.4.3). In contrast, despite the improvement on average, the best cases diminished slightly across the different time window. Nevertheless, this is expected and accepted as the inclusion of all available samples within a specific time-frame would incur the probability of including low quality samples or even less accurate techniques.

Weighted Majority Voting Fusion (WMVF)					
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
Worst Case Integrity	1.56	1.42	1.51	1.92	1.01
User ID	41	41	41	41	41
Best Case Integrity	4.51	4.36	4.45	4.70	4.76
User ID	43	43	43	18	15

Table 5-17: Worst and Best Integrity Cases of WMVF with Degradation Function over Different Time Windows (Authorised User)

Further investigation is thus required to establish the consequence of changing the drop degree of the degradation function which was set originally at (-0.5). It was modified to be (-

.025) and the script was re-run on (AL 2 min and IL 10 min) in order to provide a further insight of whether this would affect the operation and balance the transparency and robustness of the model. As depicted in Table 5-16 and Table 5-17, compared to the average integrity of the same windows but original degradation degree, the new degree produced a slight higher averaged integrity (3.84 vs. 3.77) whereas the worst case deteriorated (from 1.42 to 1.01) albeit the best case was enhanced (from 4.36 to 4.76). Such variance reveals that determining the amount of the degradation function is an influential aspect on the system performance. Therefore, the most appropriate drop degree depends on the user requirements, how they utilise their device(s), and the device(s)' capturing capabilities.

Dependent upon the above differing results of different time window settings, it is worth exploring the effect of deactivating the degradation function completely. Therefore, the model and thus the script were modified and tested accordingly. This setting was for the system to have the decision without considering (adding to/subtracting from) the previous historical integrity, i.e. independent IL. This means that whenever the user attempts to access an app or service, the authentication system will look for the available biometric samples within the set time window and calculate the integrity of the system based on the authentication decision in a weighted fashion. If the calculated integrity outweighs the risk level of the requested app/service, the access to it is granted and then the integrity is reset to zero waiting for the next app/service access request. Otherwise, if the access is denied, the integrity will drop below zero by 0.5 until it reaches -5 at which the user will be locked out completely and prompted to provide other information such as a specified high secure obtrusive authentication. It is apparent from Table 5-18 that the use of not updating the IL every specified time and resetting it to zero raise the confidence on the authorised user to a quite higher level, which is arguably interpreted in high levels of security.

Weighted Majority Voting Fusion (WMVF) without Degradation			
Time Windows	**2 min**	**5 min**	**10 min**
Average Integrity	4.11	4.13	4.08

Table 5-18: Average Integrity of WMVF without Degradation Function (Authorised User)

The worst and best performance cases (demonstrated in Table 5-19) disclose that the lowest integrity accomplished by User 41 who had high interactions. Although this was also the case with activated degradation, the integrity here was far less than that with degradation. On the one hand, looking at the middle window (5 min) which achieved the highest overall average and best case integrity, it was noticed that only 2 participants (Users 41 and 44) were below 2 of average integrity and both were high active users. However, these 2 participants can be considered as special cases at which they had poor performing biometric modalities (i.e. their facial verification EER were about 18% and 20% respectively). Given the face samples were the second most contributing modality of the dataset, this will have a considerable impact on the fused result and hence relying only on the level of interactions to determine the appropriateness of a specific method might not be sufficient.

Weighted Majority Voting Fusion (WMVF) without Degradation			
Time Windows	**2 min**	**5 min**	**10 min**
Worst Case Integrity	1.01	1.01	0.92
User(s) ID	41	41	41
Best Case Integrity	4.80	4.81	4.71
User(s) ID	18	18	18

Table 5-19: Worst and Best Integrity Cases of WMVF without Degradation Function over Different Time Windows (Authorised User)

On the other hand, about 55% of those achieved an average integrity above 4.5 were of the high active users. Having said that and knowing that they represent 43% of the dataset, this method of independent IL and no degradation, arguably, tends to be more suitable for frequent users. This can be attributed to the fact that they would have such a rich set of samples which are utilised to verify them every time the IL is triggered and/or an app is requested. On the contrary, the original configuration with the degradation function might

suite the infrequent users who lack the activities on the device and samples, so they are in need to take the historical samples/decisions into account.

5.3.4.2 WMVF Integrity Performance - Imposter User

In order to investigate the capability of this fusion model to thwart an imposter from accessing sensitive applications and within how long, the script was run with the data of participants other than the genuine one. The results presented in Table 5-20 show that WMVF security levels when the device is in use by an impostor are proportional to and better than those of NICA with the differing time windows. The enhancement was obvious with AL 5 and IL 20 where which it was about a complete half level point (from -4.41 to -4.91).

The amendment of the degradation degree also has a slight positive outcome on security though it is envisaged to reduce the security by not allowing the integrity to drop enough keeping it high even if the device becomes on illicit hands but it would be for the sake of higher usability.

Weighted Majority Voting Fusion (WMVF)					
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
Average Integrity	-4.98	-4.84	-4.73	-4.91	-4.89

Table 5-20: Average Integrity of WMVF with Degradation Function (Imposter User)

Table 5-21 displays additional details with regard to the calculated worst and best cases and the average detection time to shut out an imposter. In line with the imposter average integrity and those of the authorised user, the worst and best cases were improved proportionally. Likewise, the detection time was reduced at all different levels of AL/IL especially in AL 5 min and IL 5 min at which the reduction was almost half a minute, which would mean a lot when it comes to an unauthorised access.

Weighted Majority Voting Fusion (WMVF)					
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
Worst Case Integrity	-1.76	-1.55	-1.70	-1.99	-1.14
User ID	41	41	41	41	41
Best Case Integrity	-4.99	-4.77	-4.98	-4.90	-4.99
User ID	43	43	43	18	18
Average Detection Time (min)	5.092	2.113	5.167	5.016	2.073

Table 5-21: Worst, Best Integrity Cases and Detection Time of WMVF with Degradation Function over Different Time Windows (Imposter User)

There is a link between the AL and the average detection time. That can be the reason of the shortest average detection time of an imposter was with the AL2/IL10 (2.113 and 2.073 minutes). The system even would not wait for the AL to be invoked when the imposter immediately attempts to access a high risky app whilst the confidence at the time is not sufficient for it. In such a case, the imposter will be prompted to submit an intrusive authentication, which would high likely fail causing the integrity to drop and the AL to be triggered accordingly until the system decides that it is an imposter and lock down the device.

Furthermore, the outcomes of running the script on imposter data excluding the degradation function (to have a standalone WMVF decision) were comparative to those of the authorised users as illustrated in Table 5-22. Accomplishing average integrities very close to the maximum (i.e. -5) renders the system to be considered robust against misuse. Nonetheless, a breakdown of the results is needed to validate this and to examine the other side of the results.

Weighted Majority Voting Fusion (WMVF) without Degradation			
Time Windows	**2 min**	**5 min**	**10 min**
Average Integrity	-4.92	-4.94	-4.88

Table 5-22: Average Integrity of WMVF without Degradation Function (Imposter User)

Table 5-23 shows the best cases comprised both high and low active users leading to the same previous outcome that the suitability of such a model is reliant upon individuals' nature of use, the performance of operating biometrics and their availability. Moreover, better intrusion detection times were achieved because by following this method there will be less

opportunity of misuse left open whereby eventually lessen the access probability to apps/services that required high level of integrity.

Utilising this method would enable the system to start reducing the integrity as soon as the impostor attempts to access an app of high risk – the independent standalone integrity check that is triggered from the bottom line of zero would instantaneously recognise that the calculated integrity of the imposter is less than the requested app requirement and then it continues to decline according to the specified AL until containing this by locking out the imposter from using the device. The inclusion of the authorised samples which have been collected during the time window prior to the access request (as in the main configuration) in the WMVF decision, would delay the detection of an imposter if they highjack the device straight after an authorised user, unlike using this independent WMVF approach that would increase the likelihood of denying the impostor access in a shorter time.

Weighted Majority Voting Fusion (WMVF) without Degradation			
Time Windows	**2 min**	**5 min**	**10 min**
Worst Case Integrity	-1.08	-1.08	-0.94
User ID	41	41	41
Best Case Integrity	-4.98	-4.99	-4.83
User ID	39	7	18
Average Detection Time (min)	2.034	5.058	10.249

Table 5-23: Worst, Best Integrity Cases and Detection Time of WMVF without Degradation Function over Different Time Windows (Imposter User)

On the other hand, if it happened to be a false rejection at the beginning whereby a legitimate user is the one utilising the device, the following AL decision should have the potential to recover and correct that. This would essentially better establish the trade-off between the system robustness and users' convenience than that of degradation function in particular with those of more interactions, thereby not exposing the access of sensitive apps/services whilst not restricting access to the vast majority of non and low sensitive apps/services of the device.

However, consideration should be paid to the scenarios where merely one sample exists when an authentication decision is needed to be made. With the standalone WMVF, it might be risky to rely upon this single sample especially if it is from a low confidence biometric technique and a level 5 app is requested. In contrast, employing the continuous confidence taking into account the previous integrity and authentication decisions would recover this risk, thus providing a more reliable mechanism.

5.3.4.3 WMVF Usability Performance

Triggering the AL too frequently may perhaps lead to overwhelming authentication and hence inconvenience consequences. This would be due to the intrusive manner of such a system when samples are not available. It arguably establishes the security of the framework but at the expense of relative usability.

As shown in Table 5-24 besides the previous experiments, the more often the AL algorithm gets initiated, the more intrusiveness endured because the integrity will be constantly updated before the degradation function is triggered unless in case of inactivity. Moreover, comparing the percentage of intrusive requests of AL 2 min and IL 10 min (14.69%) with the same windows but of 0.25 drop (13.23%), it presents that the less the integrity degree drops, the more convenience can be established. This further highlights the effect of the degradation function on the model.

Weighted Majority Voting Fusion (WMVF)					
Total Requests	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
	% of Intrusive requests	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**
46,254	11.87	14.69	13.01	8.53	13.23

Table 5-24: The Percentage of Intrusive Authentication Requests of WMVF with Degradation

Looking deeper into the role this effect played on the various levels of apps risk, Table 5-25 emphasises this although the difference can be considered insignificant compared to the total requests. However, the effect is getting more noticeable with higher app risk levels accordingly. The result of the worst cases underlines the evident consequence of both time windows on system operation. For example, the averaged percentage of intrusive requests of AL 5 min were 37.79, 50.04, and 33.87 with IL of 5 min, 10 min, and 20 min respectively for the same user. Albeit these percentages seem large, looking at the other side of the coin would show that there were considerable reductions of the supposed intrusive requests without operating this model. In addition, the best case of no intrusive requests at all gives an indication the system has the ability to achieve full transparency in specific circumstances.

Weighted Majority Voting Fusion (WMVF)					
App Risk Level	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
	% of Intrusive requests	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**
0	0	0	0	0	0
1	0.27	0.33	0.30	0.19	0.30
2	0.86	1.06	0.93	0.61	0.95
3	1.24	1.54	1.36	0.89	1.38
4	2.46	3.04	2.70	1.77	2.74
5	7.05	8.72	7.72	5.06	7.85
Worst Case User(s) ID	37.79	46.55	50.04	33.87	50.25
	44	44	44	44	41
Best Case User(s) ID	0.00	0.00	0.00	0.00	0.00
	2	2	2	2	2

Table 5-25: The Percentage of Intrusive Authentication Requests of WMVF with Degradation based on the App Risk Levels, Worst and Best Cases

On the other hand, a substantial improvement in decreasing the number of explicit authentication requests is apparent in Table 5-26 without degradation function. The minimum intrusiveness was experienced when triggering the AL mechanism at the intervals of 5 minutes. Furthermore, Table 5-27 shows the distribution of these obtrusive requests across

the levels of accessed apps/services. It is perceived that the system achieved a reasonable level of low intrusiveness with apps/services required lower security (less than 1% intrusive requests on risk levels 1, 2, and 3).

Weighted Majority Voting Fusion (WMVF) without Degradation			
Total Requests	**2 min**	**5 min**	**10 min**
	% of Intrusive requests	**% of Intrusive requests**	**% of Intrusive requests**
46,254	7.83	7.40	8.47

Table 5-26: The Percentage of Intrusive Authentication Requests of WMVF without Degradation

Full transparency could also occur as can be seen with a number of participants – 26%, 32%, and 23% of participants with the use of the time windows 2 min, 5 min, and 10 min respectively. Notwithstanding, this is not mandatory on such model thereby which the deviation between the confidence on the authorised user and the apps/services risk levels is continuously observed and acted upon when the latter outweighs the former in order to secure them. Thus, an acceptable number of intrusive authentication prompts can be tolerated especially with higher risk apps/services. Regarding to the extent of interactions, those users of best cases are mix between high and low active, meaning that such an approach cannot be suitable to merely specific category of users but rather many factors can affect that, such as the pattern of life, the multitude of operated devices and their capabilities, and the performance of the contributing biometrics.

Weighted Majority Voting Fusion (WMVF) without Degradation			
Time Windows	**2 min**	**5 min**	**10 min**
App Risk Level	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**
0	0	0	0
1	0.18	0.17	0.19
2	0.56	0.53	0.61
3	0.82	0.77	0.89
4	1.62	1.53	1.76
5	4.65	4.40	5.03
Worst Case User(s) ID	49.31	49.31	54.20
	41	41	41
Best Case User(s) ID	0.00	0.00	0.00
	2, 3, 4, 5, 8, 10, 13, 14, 16, 17, 20, 43	2, 3, 4, 5, 7, 8, 9, 10, 13, 14, 16, 17, 18, 20, 43	2, 4, 5, 8, 10, 13, 14, 16, 17, 20, 43

Table 5-27: The Percentage of Intrusive Authentication Requests of WMVF without Degradation based on the App Risk Levels, Worst and Best Cases

5.4 Conclusion

Given the aforementioned WMVF results, it can be concluded that the security as well as the transparency of the system is improved compared to those of NICA. The reason is the fact that NICA takes the most recent sample and ignore the rest of samples whereas WMVF makes use of all samples using multimodal and multi-sample approaches to fusing them.

In addition, the time windows appear to notably affect the operation of the framework as the frequency of authentication provides a trade-off between security and usability. Furthermore, both degradation degree manipulation and deactivation have considerable impact on the framework performance. Exploring their impact on the number of intrusive authentication requests, it can be suggested for the time windows, the degradation function and the drop degree to be configured dynamically and adaptively depending upon the extent of usage, the availability and performance of biometric techniques.

Still, the problem of not having full transparency exists although it is not the aim and it is difficult to achieve while balancing all requirements and therefore a certain intrusive level due to higher risk is expected and accepted. As such, further investigation could be sought to

determine how adding additional smart information about the genuine user (e.g. usual geolocations and security status of other user's devices) could improve upon security and usability as well as to reconsider the degradation function and its effect on the framework.

6 Federated Authentication using the Cloud (Cloud Aura)

6.1 Introduction

Having achieved promising experimental results in the preceding chapter validating the feasibility of utilising various multibiometric information in order to assure risk-based continuous identity confidence within a transparent context; however, there are a number of issues that would make their operational use challenging. With the current implementations, each user's digital device would need to establish and maintain separate biometric profiles and the required intelligent management infrastructure. In a world with a multi-device environment (surveyed in Chapter 4), this would result in each device requiring the feature extraction and classification algorithms for each contributing biometric technique which in turns would increase the licensing costs if credible and well performing solutions are sought. This would also pose an increased processing and storage overhead on each incorporated device – thus placing a significant configuration and maintenance burden upon the users especially with the extensive use of high sensitive information and services.

Furthermore, the invaluable rich information that can be obtained from other devices owned and utilised by the user is wasted unless a centralised approach is created and employed to facilitate disseminating the accumulated user confidence – thus relieving the burden upon these devices and providing highly secure, robust, multi-device and intelligent handling of every authentication decision. Therefore, further enhancements in terms of balancing the security and usability and making a more reliable authentication decision are envisaged to be viable thereby encompassing more smart information and operational improvements.

Before going to design a full architecture, this chapter proposes the concept of federated authentication using the Cloud (Cloud Aura), models it, and experimentally validates whether the philosophies behind it would work, and then proceeds to build the information system for

it in the subsequent chapter. This chapter pursues to develop a novel authentication mechanism, with a view of capitalising upon the benefits presented by cloud computing, its universal connectivity, scalability and flexibility. These promising features offer a new opportunity of achieving convenient authentication seamlessly in a technology and service independent fashion. The approach introduces a new dedicated authentication provider – the Managed Authentication Service Provider (MASP) – that is able to provide state-of-the-art centralised verification of user authenticity.

The chapter then continues to discuss an analysis of a number of experiments that were performed on a customised model (refined based upon the results of the previous experiments) with the augmentation of information from smart sources such as multi-devices and geolocation. The analysis seeks to determine whether it is viable, convenient and secure to authenticate users based upon their digital devices activities and other captured biometrics, so that it would be possible to gather a single user profile from the range of devices a single user may use. From the results of these experimental studies, expanded attributes of Cloud Aura will be identified for further architectural design and prototypical development.

6.2 Cloud Aura – A Novel Authentication Approach

Whilst transparent authentication can be appreciated as a solution to effectively remove the reliance upon the human aspects to ensure a robust and convenient authentication, its applicability and universality have to be considered as it is confined to a single device. With every device requiring biometric setup and enrolment, user configuration and management, risk assessment and continual refinement, the necessity for transparent, universal and federated authentication approach that can be used across technologies and services is becoming more apparent. Thus, the aim is to have a federated continuous authentication that

can be managed centrally to work over user's devices to enable access to services seamlessly in a location, technology, and service independent manner.

As illustrated in Figure 6-1, the MASP is hosted on the Cloud and receives biometric signals from and control the verification decision of the subscribed user's devices. These devices can benefit from the confidence level of each other as they are fused on the MASP and communicated to those participating devices. This accumulated identity confidence status is utilised in both device and service domains as MASP would verify the user identity continuously and transparently whilst they access services on the device or online depending upon their determined risk levels. For example, had the user logged into his smartphone using a fingerprint, they would, within specified period of time and proximity, automatically logged into their registered laptop transparently without having to re-enter their biometrics unless the user confidence status is below the risk level of the requested service.

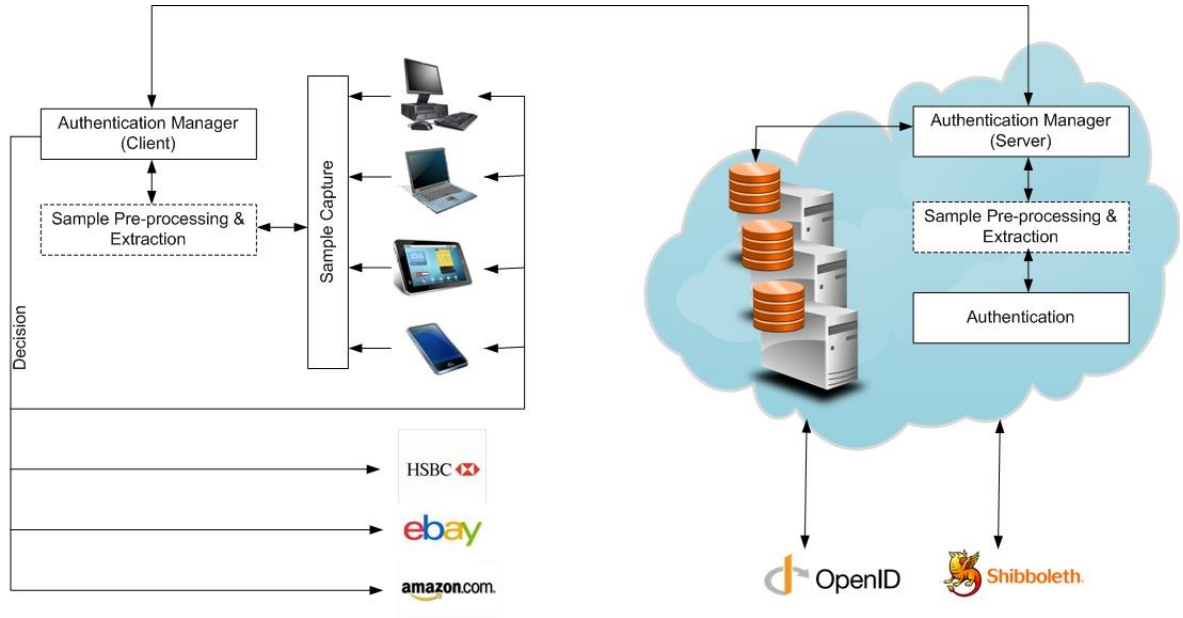

Figure 6-1: An Overall View of Federated Authentication using the Cloud

The concept of federated authentication using the Cloud (Cloud Aura) is to centralise the task of authenticating an individual to a Trusted Third-Party (TTP). Through providing a device and service independent authentication approach, the centralised authority benefits from

specialisation, enabling it to provide the most appropriate authentication technologies and essentially removes duplication as the user no longer needs to enrol on each device, configure each device and authenticate to each device. Instead, the user has a single authentication profile within the Managed Authentication Service Provider (MASP), where they are able to manage and monitor their profile. Any MASP-enabled device or service will merely send a request to the MASP and be informed of its current real-time identity confidence. In this manner, individual devices themselves are relieved of a significant amount of data processing and storage, including a large volume of duplicated activities that would be occurring with TAS and Aura enabled systems.

Federated authentication is similar to federated identity in that it extends the concept of authentication beyond an organisation or domain like single-sign-on does for federated identity. However, federated authentication is focused solely on the provision of authentication and not access control (as federated identity is). Indeed, combining the functionality of federated authentication with federated identity would provide the usability of multi-domain access control but with an increased and continuous level of trust upon the authenticity of the user. As such, extending the concept of the Authentication Aura (Hocking et al., 2011), this approach permits devices and services that are not biometrically enabled to benefit from stronger authentication approaches. For example, current password-based web services, such as Gmail, would now be able to transparently verify user's identity – requiring the user to merely access the web page and the background services will check whether the identity confidence is sufficient to provide immediate access. In cases where the confidence is not sufficient, the user would be asked to verify their identity.

An advantage of a centralised cloud solution is the ability to unify all authentication information, providing an in-depth understanding of what the user is doing (in terms of devices and services) and thereby providing additional identity intelligence of the user. For

instance, it is envisaged that an intelligent feature that MASP will offer is control dashboard where MASP administrators and perhaps the users themselves are able to vision the existing system state revolving the user's device(s) and services. For example, it will be possible to determine if two authentication requests are simultaneously made from different locations from devices that belong to the owner or otherwise – thus highlighting potential misuse.

The centralised approach also enables the use of multibiometrics and multi-factor authentication – providing a robust framework of authentication models that are stronger than any uni-modal or single factor authentication approach. For example, depending upon the available authentication approaches (which themselves will be dependent upon the devices and technology a user utilises), a variety of multi-instance, multi-algorithmic, and multi-modal approaches exist that seek to optimise the authentication decision. As illustrated in 3.6.2, a multi-algorithmic approach would enable a MASP to utilise a range of biometrics classification algorithms (each crafted to focus on differing aspects of the problem) and combine the result through fusion. Typically, cost, processing and vendor-specific solutions have prevented this from happening to date and continue to do so. As a centralised authentication service, the MASP, through ISO standards (i.e. ISO 19794, 19785, 19784) will be in a position to incorporate any and all approaches – something individual devices would never be able to achieve due to prohibitive costs and processing requirements (ISO, 2006a, 2006b, 2011).

Figure 6-2 illustrates a relatively simple multibiometrics model that incorporates varying degrees of multi-algorithmic processing and fusion at differing levels of the biometrics process. These models would be unique to the user, varying depending upon which samples are present. This approach to the optimisation of authentication confidence will provide a very strong indicator as to the authenticity of the user.

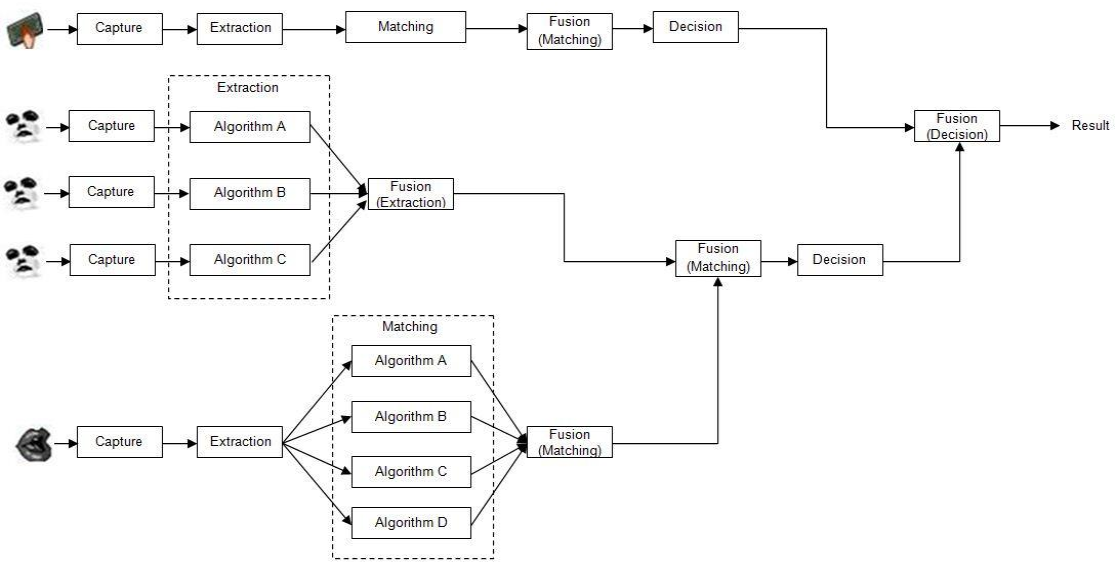

Figure 6-2: A Model for Multibiometrics within Federated Authentication (Clarke, 2011)

The centralised approach also overcomes another hurdle in the creation of effective biometrics classifiers – the availability of impostor data. Many modern classifiers utilise approaches that allow them to train the classifier to behave according to the valid or authorised user (e.g. neural networks); however, in practical live systems, the lack of availability inhibits the performance that can be achieved. Often this data needs to be simulated or created rather than being real user data. Moreover, many classifiers utilise full sample data, rather than derived statistics (such as a mean and standard deviation), making the creation of simulated data very challenging. Within a centralised system, anonymised impostor data will be available to all users for both initial enrolment and template refinement; ensuring classifiers are optimised. This, in turn, will allow to model the data to understand what other users' usage patterns and distinctive features look like and thus helping to generate patterns of anomalies and patterns of life, such as usual attended geolocation(s), accessing particular apps/services on regular basis at the same point of time every specific day and perhaps at specific geolocations.

Therefore, the succeeding sections examine the argument that Cloud Aura would help towards building a better user profile and thus improving the security and convenience of the technique beyond what a single device can do by itself.

6.3 Experimental Investigation of Cloud Aura

With the aim of investigating the Cloud Aura approach, a set of experiments exemplifying cloud-based authentication properties was developed in order to determine potential and feasible attributes that would provide a better system performance. There is a need to investigate whether additional information could be used as a contributing factor to provide a more reliable authentication decision-making process. Improvements that can be obtained by pushing the solution to the Cloud with regard to security and usability also need further exploration.

Within the limitations of what can be proven practically on the acquired dataset, a couple of metrics were identified to be used to help understand whether such information is useful – geolocation and multi-devices. It is by no means meant to be the definitive approach but they are examples of how additional information would aid enhancing this process.

In order to practically prove the concept of the proposed solution, the specialised mathematical modelling software package MATLAB (R2015b release) was utilised and implemented on a Windows 7 Enterprise 64-bit Operating System with Intel Core i5-4310 CPU, 2.7 GHz and 16 GB RAM. A number of scripts were modelled and implemented incorporating all information used in the previous experiments in addition to the information of the geolocation and that of other devices of the same participant – to establish its feasibility and potential to offer a successful authentication mechanism (Appendix F). Using the same dataset collected and discussed in Chapter 5, the data of each participant was split into two datasets: 60% for training the classifiers and generating the user profile and 40% for

validation and testing the performance. Accordingly, the latter was performed considering one participant acting as the valid authorised user whilst the remaining other participants as imposters. Accordingly, the following sections demonstrate the results.

6.3.1 Geolocation

Geolocation is one of the main elements of Cloud Aura. Incorporating the information of geolocation (via GPS sensor and/or WiFi signal) at which an application is accessed often – and possibly at specific time-frame(s) – can provide additional discriminatory information to support identifying users of digital devices. Moreover, defining trusted location(s) by the user during the enrolment or at a later stage will play a role on different related aspects, such as the required security threshold and degradation function. For instance, the required security prompted at home is adaptively less and the degradation function drops less than they do when at work or even in a totally unfamiliar location.

Geolocation, also, can add a further security layer to user authentication and access control decision, thereby determining that specified apps/services can only be accessed at specified location(s). For example, the user's home is the only authorised location from which they are authorised to access their online banking. The approved locations can be registered as a wider geographical zone (e.g. neighbourhood, city, county, and country). This would facilitate detecting illicit activities that occur in unusual locations – it would be more apparent when users using multiple devices each or one of which is in odd location unlike the other device(s). Similar use of geolocation in Cloud Aura can be for the re-enrolment and classifiers retraining processes. Specified geolocations can be authorised at which these processes are merely conducted, or even excluded from doing so.

For this experimental investigation purposes, the resulted geolocation EER from the preliminary study of section 5.3.2 and its associated timestamps were employed as additional

input into the same WMVF fusion formula utilised in 5.3.3 and 5.3.4. The following are the updated results after running the tests and settings of both aforementioned sections.

6.3.1.1 Cloud Aura Integrity Performance - Authorised User

Table 6-1 shows that the average integrity of Cloud Aura model (incorporating only the geolocation to the WMVF) achieved better average integrity scores than those of the previously reported WMVF in all differing AL/IL timings by an average of 0.2. This improvement elevated almost all the integrity averages to above 4 rendering the system to non-intrusively grant access to the vast majority of apps/services that reside on the user's device – knowing that a mere smart information (geolocation) is utilised in this calculation.

Going down to shorter AL/IL, the average integrity went down slightly due to the increasing probability of not having samples or even having weak samples at short intervals and thus not permitting for keeping or even increasing the integrity while active degradation function. Whilst the largest time windows (AL=5, IL=20) attained the highest average integrity of 4.17, it can be because of the less frequent invocation of the degradation function which might in turn be at the expense of exposing the device to un-authorised access before the next IL drop. Modifying the eroding degree of the degradation function (from -0.5 to -0.25) on AL=2 and IL=10 stemmed a comparable result to that of WMVF which accomplished a relative optimisation. Therefore, due care is needed while setting these timings and drop degree in order to suite the user requirements and security principles alike.

Cloud Aura					
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
Average Integrity	4.11	3.97	4.10	4.17	4.05

Table 6-1: Cloud Aura Average Integrity with Degradation Function (Authorised User)

The extreme achieved average integrity levels reveal an additional point supporting the extent of enhancement Cloud Aura can offer as presented in Table 6-2. Ranging from 2.24 to 4.97, the same User 41 scored the worst calculated average integrity throughout all time windows whilst 2 different participants (Users 15 and 18) scored the best cases. The improvement in the worst cases is notable in comparison to the previously reported WMVF outcome by an average increment of more than 1 utter level going past the 2 boundary. Moreover, 80.85 per cent of participants experienced an average integrity above 4 with 95.94 per cent over 3, allowing the system to un-obtrusively authorise the genuine user access to the vast majority of applications with a high level of transparency.

Cloud Aura					
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
Worst Case Integrity	2.55	2.40	2.53	2.24	2.49
User ID	41	41	41	41	41
Best Case Integrity	4.86	4.71	4.84	4.97	4.80
User ID	15	15	15	18	15

Table 6-2: Worst and Best Integrity Cases of Cloud Aura with Degradation Function over Different Time Windows (Authorised User)

When the user interaction level is concerned, a possible correlation existed between it and the achieved average integrity across all participants. For instance, the worst 2 cases were from high active users (29 and 41) who were the only users achieved an integrity below 3. On the other hand, the best cases were from low active ones (15 and 18). In addition, 52% of those gained an average integrity below 4.5 were low active users although they represented 40% of those above 4.5. Hence, no absolute link can be drawn between the interaction level and performance.

Furthermore, those with more interactions tend to reflect better with shorter windows though not for all of them. For example, whilst Users 32, 41, and 47 obtained 4.25, 2.53, and 3.96 respectively with AL=5 and IL 10, they acquired 4.12, 2.24 and 3.03 respectively with AL=5

and IL 20. This can be attributed to the richer available samples while utilising small time windows that sustained the integrity by inhibiting the constant degradation. Thus, Cloud Aura will have the potential of achieving a desirable integrity level. It is also evident that the variability of time windows will vary dependent upon the nature of each and every user's usage and device.

Cloud Aura without Degradation			
Time Windows	**AL 2 min**	**AL 5 min**	**AL 10 min**
Average Integrity	4.15	4.17	4.13

Table 6-3: Cloud Aura Average Integrity without Degradation Function (Authorised User)

Table 6-3 illustrates the consequence of turning off the degradation function completely. A very small enhancement over the WMVF counterparts' settings and the Cloud Aura with degradation is noticed by about half point. Notwithstanding, it can be arguably regarded as a high level of security. Digging deeper to gain an understanding of the relationship of these performances with the user profiles disclosed that the best integrity recorded was for User 18 who had low interactions and conversely the worst integrity recorded was for User 41 who had high interactions (as shown in Table 6-4). This is analogous with those of activated degradation but it is slightly better there.

Cloud Aura without Degradation			
Time Windows	**AL 2 min**	**AL 5 min**	**AL 10 min**
Worst Case Integrity	1.68	2.24	1.66
User ID	41	41	41
Best Case Integrity	4.83	4.97	4.81
User ID	18	18	18

Table 6-4: Worst and Best Integrity Cases of Cloud Aura without Degradation Function over Different Time Windows (Authorised User)

It was observed that only 2 participants (Users 29 and 41) – which were high active users – were below 3 of average integrity. Moreover, about 40% of those who achieved an average integrity above 4.5 were high active users and 54.55% of those with below 4.5 were low active users. These percentages are somewhat akin to the original participants' categories (in

terms of interactions) in the dataset. Further investigation within each category demonstrates that half of those with less usage encountered an average integrity less than 4.5 (35% of which were even below 4). On the contrary, solely one third of those with high usage faced less than 4.5 integrity on average (merely 7.5% of them suffered a below 4 integrity).

That being said, this approach can be considered to have a tendency towards being more appropriate for high active users who would have enriched samples to be fused (and subsequently an authentication decision be made) every time the AL is generated and/or an app is requested. In contrast, the original configuration with the degradation function would perhaps be more applicable to low active users who lack the interactions with the device as well as the availability of samples, yet they are in need to consider the historical samples/decisions. Nevertheless, both methods can perform well with all users' groups using the Cloud Aura model.

In spite of the evident increase on the average system integrity compared to those of the NICA and WMVF, it is worth assessing how quick the impostor would be detected and locked out from accessing apps and services of high risk levels.

6.3.1.2 Cloud Aura Integrity Performance - Imposter User

The average integrity of the system for an impostor across the varying time windows is seen in Table 6-5. It is apparent that all averages were fairly high across all AL/IL levels (the minimum was -4.75). This means that the user would be able to transparently access most if not all applications/services of high risk levels and below. The lower the AL/IL combination of the system, the higher the integrity and yet security.

Cloud Aura					
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
Average Integrity	-4.92	-4.99	-4.90	-4.75	-4.85

Table 6-5: Cloud Aura Average Integrity with Degradation Function (Imposter User)

The worst and best cases were calculated and demonstrated in Table 6-6 together with the average time of identifying and locking out the imposter. These cases of imposter were proportional to those of authorised user. Interestingly, both worst and best instances were with highly interactive participants, confirming that no absolute relation existed between the usage level and the performance, making the Cloud Aura works with all cases.

Cloud Aura					
Time Windows	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
Worst Case Integrity	-1.99	-2.11	-1.98	-2.26	-2.22
User ID	41	41	41	41	41
Best Case Integrity	-4.99	-4.82	-4.98	-4.99	-4.92
User ID	40	40	40	7	40
Average Detection Time (min)	5.077	2.107	5.098	5.004	2.062

Table 6-6: Worst, Best Integrity Cases and Detection Time of Cloud Aura with Degradation Function over Different Time Windows (Imposter User)

Identifying and thwarting the imposter from accessing the applications/services within a few minutes in line with the operated AL time were faster than those of the WMVF. These can be tolerable dependent upon the user requirements and risk levels of the utilised applications. It is also expected that these detection times would be shorter if the imposter immediately requests a high risky application higher than the system integrity at the time, at which the imposter will have an instant failed authentication leading to a quicker integrity erosion. Therefore, there is a clear need to trade-off system security and users' convenience based upon the user requirements and preferences together with the risk nature of the employed apps/services.

Furthermore, the results of imposter user without the degradation function were proportional to those of the authorised user, reaching average integrities very close to the optimum (i.e. -5) rendering the system to be very vigorous against misuse (Table 6-7). However, whilst this might provide a protection baseline from a variety of threat vectors, it would inevitably oversight a few cases – e.g. when a colleague/housemate (who has the same usual location of the legitimate user) attempts to misuse a device. Therefore, countermeasures need to be put in place. Nonetheless, other contributing modalities alongside the other information incorporated from other user devices registered under the same user profile (with the MASP of Cloud Aura) would certainly offset this shortcoming.

Cloud Aura without Degradation			
Time Windows	**AL 2 min**	**AL 5 min**	**AL 10 min**
Average Integrity	-4.96	-4.99	-4.94

Table 6-7: Cloud Aura Average Integrity without Degradation Function (Imposter User)

Table 6-8 provides a breakdown of these outcomes revealing that the worst cases encompassed both high and low active users whilst the best cases were of high active ones, leading to the same previous interpretation that the appropriateness of such model is reliant upon individuals nature of use, the performance of operating biometrics and their availability – not the usage level. Moreover, based upon accomplished enhanced intrusion detection times, following this method would offer fewer misuse vulnerabilities and ultimately alleviate the un-authorised access probability to apps/services of high risk level.

Cloud Aura without Degradation			
Time Windows	**AL 2 min**	**AL 5 min**	**AL 10 min**
Worst Case Integrity	-1.80	-2.26	-1.99
User ID	41	41	41
Best Case Integrity	-4.99	-4.99	-4.99
User ID	12	18	40
Average Detection Time (min)	2.015	5.012	10.128

Table 6-8: Worst, Best Integrity Cases and Detection Time of Cloud Aura without Degradation Function over Different Time Windows (Imposter User)

With ordinary activated degradation function, the model will include the recent samples within the time window along with the previous integrity which if the device has just been taken over will have a number of samples of the authorised user which, as a result, might make the process of identifying the imposter be belated. Unlike this, deactivating the degradation function and calculating an independent integrity instantly with the app/service access request would lead to a low confidence level on user, thereby eliminating the probability of including the authorised samples or letting this to be at the minimum. Furthermore, if an impostor begins with attempting to access an app of high risk, the system will promptly decrease the integrity and then continues to decline and ask for explicit authentication until containing this by locking out the imposter from using the device.

On the other hand, a false rejection at the beginning can be tolerable because the following AL decision should eventually recover and correct that. This would, in essence, offer a balanced approach between system sturdiness and users' satisfaction especially with those of more interactions.

6.3.1.3 Cloud Aura Usability Performance

To gain a more appreciation of the location effect on the performance of Cloud Aura, the extent of prompting the lawful user to provide authentication sample(s) was calculated. Table 6-9 demonstrates the high potential of the device to operate transparently with good improvements ranged from 2% to more than 5% in comparison with the WMVF. The least percentage of intrusive authentication requests was 6.51% which is quite satisfactory to have the desirable trade-off. Equally so, the results of the aforementioned sub-sections support the model to reach appropriate levels of integrity in the case of an authorised user and how well it establishes security in the event that an impostor tries to access the device assets.

Cloud Aura					
Total Requests	**AL 5 min IL 5 min**	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
	% of Intrusive requests	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**
46,254	7.71	10.67	8.05	6.51	8.97

Table 6-9: Cloud Aura Percentage of Intrusive Authentication Requests (with Degradation)

Further observation into the effect of using Cloud Aura on the various levels of apps risk was conducted and summarised in Table 6-10. The intrusive requests in levels 1, 2, and 3 are almost all under 1% thus minor variance occurred between the differing levels of AL/IL. However, the effect became more obvious with higher app risk levels (i.e. 4 and 5) accordingly. For the high risk ones, the larger the time window, the less intrusive the Cloud Aura – with a reasonable transparency in the middle windows. The potential aim of Cloud Aura is to maintain a resilient level of trust on user. However, intrusive authentication prompts are expected when high risk apps/services are requested in periods of inactivity or no adequate user confidence in existence.

Cloud Aura					
	AL 5 min IL 5 min	**AL 2 min IL 10 min**	**AL 5 min IL 10 min**	**AL 5 min IL 20 min**	**AL 2 min IL 10 min (*-0.25 Drop*)**
App Risk Level	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**
0	0	0	0	0	0
1	0.18	0.24	0.18	0.15	0.20
2	0.56	0.77	0.58	0.47	0.65
3	0.81	1.12	0.84	0.68	0.94
4	1.60	2.21	1.67	1.35	1.86
5	4.58	6.33	4.78	3.87	5.33
Worst Case User(s) ID	26.98	38.47	35.06	26.30	37.96
	44	44	44	44	44
Best Case User(s) ID	0.00	0.00	0.00	0.00	0.00
	2	2	2	2	2

Table 6-10: Cloud Aura Percentage of Intrusive Authentication Requests based on the App Risk Levels, Worst and Best Cases (with Degradation)

The result of the worst cases underlines the evident consequence of both time windows (AL and IL) on system operation. In spite of the fact that the worst percentage of intrusive requests looks high (38.47%), avoiding being interrupted by authentication 61.53% (of the total assumed intrusive requests without operating this model) is considered a substantial enhancement. In addition, the best case of no intrusive requests at all indicated that full transparency in specific circumstances can be achieved by Cloud Aura albeit not required.

It was helpful to extract the 14-day usage for a couple of representative users to show how authentication confidence builds, how the interactions are happening, and how the Cloud Aura model is enabling fewer of these intrusive requests. For this purpose, User 31 was selected to represent those users with low usage profiles and User 4 to represent high usage profiles. They had also varied performance on average integrity – the former achieved 7.49% and the latter 0.27% of intrusive authentication requests.

Figure 6-3 and Figure 6-4 illustrate the interactions of these 2 participants where the red line is the system integrity and the green circles and black triangles are the risk levels of accessed applications. For clarity, they are depicted in percentage instead of the original configuration of 0 to 5 levels. When the application risk level is less than or equal to the system integrity at the moment of access request, it is represented as a green circle. On the other hand, it is a black triangle if it is otherwise making it an intrusive request.

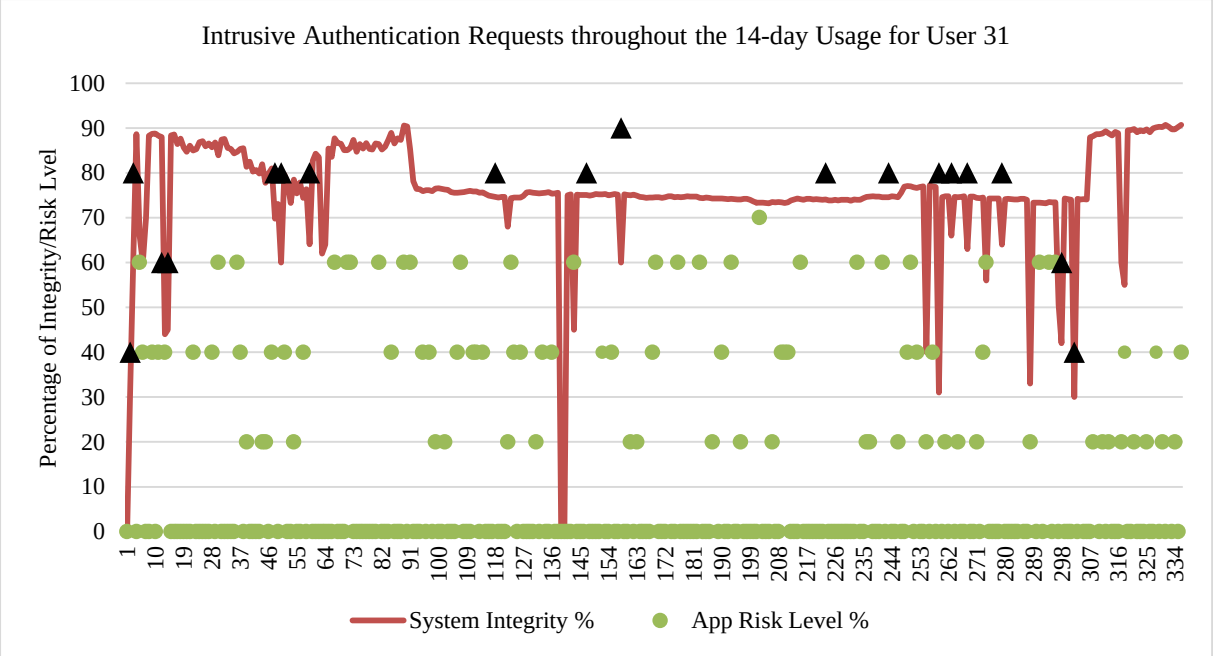

Figure 6-3: Intrusive Authentication Requests throughout the 14-day Usage for User 31 (Low Active)

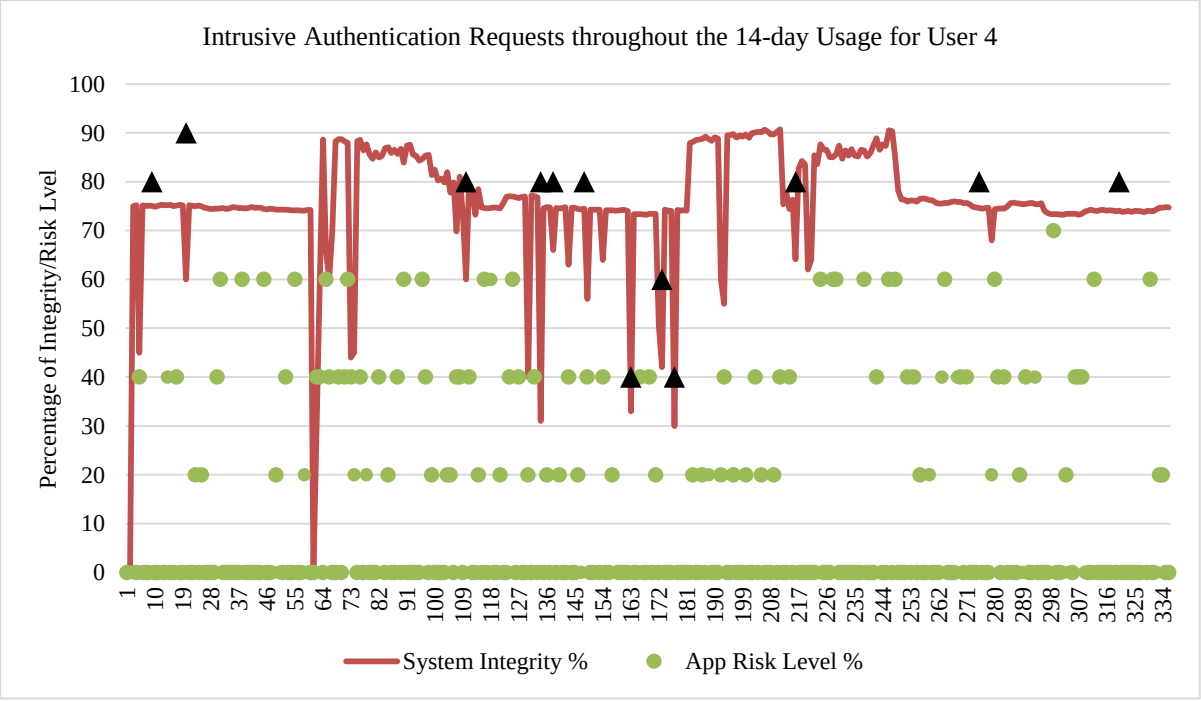

Figure 6-4: Intrusive Authentication Requests throughout the 14-day Usage for User 4 (High Active)

By examining the correlation between the percentage of intrusive authentication requests, the extent of use, and the required security of the accessed applications, it is shown that the low active users (User 31 in this example) had, on average, more explicit authentication than high active users (User 4 in this example). The is due to the system integrity decline after being

inactive for a period of time in order to avert illegitimate access to high risk applications. Therefore, if those applications were requested after this idle period, users were required to perform an intrusive authentication to confirm their identity and hence raise the confidence level again. Overall, the system demonstrated a fair level of maintaining the system integrity throughout the variable user interactions and, as a result, user-friendliness was improved thereby noticeably reducing the number of intrusive requests. In most cases and with most applications, the user was able to be authorised transparently without interruption.

On the other hand, a considerable improvement of reducing the number of explicit authentication requests by utilising Cloud Aura without degradation function is evident as shown in Table 6-11. The lowest intrusiveness was 6.64% with the AL of 5.

Cloud Aura without Degradation			
Total Requests	**AL 2 min**	**AL 5 min**	**AL 10 min**
	% of Intrusive requests	**% of Intrusive requests**	**% of Intrusive requests**
46,254	7.06	6.64	7.49

Table 6-11: Cloud Aura Percentage of Intrusive Authentication Requests (without Degradation)

Furthermore, Table 6-12 depicts that the system achieved a very low intrusiveness with apps/services required lower security (far less than 1% intrusive requests on risk levels 1, 2, and 3). Full transparency also occurred (as the best cases) with 26%, 32%, and 23% of participants with the ALs of 2, 5, and 10 respectively. Apart from this, this model should not require such performance always but rather keeping the required level of user confidence when needed to align the risk levels of requested apps/services. Thus, an acceptable number of intrusive authentication requests can be endured to safeguard the high risk apps/services. It is seen that even in the worst case, the number of intrusive requests has been almost halved and hence removes a significant amount of the users' inconvenience.

Cloud Aura without Degradation			
Time Windows	**2 min**	**5 min**	**10 min**
App Risk Level	**% of Intrusive requests**	**% of Intrusive requests**	**% of Intrusive requests**
0	0	0	0
1	0.16	0.15	0.17
2	0.51	0.48	0.54
3	0.74	0.69	0.78
4	1.46	1.38	1.55
5	4.19	3.94	4.45
Worst Case User(s) ID	40.04	37.89	43.31
	41	41	41
Best Case User(s) ID	0.00	0.00	0.00
	2, 3, 4, 5, 8, 10, 13, 14, 16, 17, 20, 43	2, 3, 4, 5, 7, 8, 9, 10, 13, 14, 16, 17, 18, 20, 43	2, 4, 5, 8, 10, 13, 14, 16, 17, 20, 43

Table 6-12: Cloud Aura Percentage of Intrusive Authentication Requests based on the App Risk Levels, Worst and Best Cases (without Degradation)

On the one hand, given the mixture of those best cases between high and low active users, such approach cannot be recommended for just a specific category of users. Rather, other various elements can influence this, such as the multitude of operated devices and their capabilities, and performance(s) of the contributing biometrics.

Based upon all aforementioned results of this section from both authorised and imposter participants, it is perceived that the verification time window does play an important role of balancing system security and usability. Very repeated user verification would render the user undergoes more intrusive authentication requests but, at the same time, recognising an imposter would be in a reasonable short period of time. In contrast, the user would be able to utilise the device more conveniently with less repeated user verification but, simultaneously, recognising an imposter and shutting out the device would take relatively longer period of time.

6.3.2 Multi-devices

Ideally, in the Cloud Aura approach, a user is able to establish a level of identity confidence through the capture of biometric samples on one device and then subsequently use that

confidence to access other devices and services. Thus, it can operate across multiple devices and services utilised by a user and registered in their Cloud Aura account/profile. The proposition of the centralised Cloud Aura solution is the ability to intelligently combine all possible provided authentication information from the different devices and techniques. This would, as a result, provide an in-depth insight of what the user is doing (in terms of devices and services) and in doing so, a more robust identity intelligence is performed. For instance, it will be possible to determine whether two authentication requests are concurrently made from different locations from devices that belong to the authorised user and thus highlighting potential misuse.

Moreover, when an access request is made to one of the user's devices, the score of their Cloud Aura confidence will determine whether they will be granted access to that device spontaneously (and to their other devices accordingly) or be required to carry out an intrusive authentication. This score will vary depending upon when and where the user last performed a successful authentication.

Whilst moving to a continuous multi-devices confidence based approach does not eliminate identity forgery completely, it does considerably complicate the forgery process – where the attacker will have to be able to constantly forge the biometric credentials throughout other user's devices (the supported biometric techniques can also differ across devices). The high cost and resources needed to continuously provide forged samples across a range of biometric techniques and devices make it a significantly more impracticable task than a targeted attack against a single device approach.

In order to analyse the effect of employing a multitude of devices in Cloud Aura, 5 participants (Users 1, 3, 11, 17, and 47) were found in the dataset having 11 devices in total (2 devices each except User 47 with 3 devices). Despite their limited number that makes it

difficult to generalise, it can provide a broad indication about the usefulness of such an approach. The average percentage of the intrusive requests on each device of a user were added to each other and then averaged to have a combined result. Even though that this accumulation can be done in an intelligent way considering, for instance, one of the devices as the main device and thus carrying higher contributing weight into the formula, this could not be established based on the information available. However, the average can be a representative of the neutral outcome where all devices have equal weights.

User#, Device#	Total Apps Usage	Average Intrusive Requests (each device)	Combined Average Intrusive Requests
User1, D1	502	10.45%	8.11%
User1, D2	1000	5.77%	
User3, D1	582	9.55%	9.95%
User3, D2	490	10.35%	
User11, D1	362	15.19%	18.17%
User11, D2	200	21.15%	
User17, D1	500	13.36%	18.25%
User17, D2	433	23.14%	
User47, D1	2322	7.89%	19.04%
User47, D2	754	19.32%	
User47, D3	650	29.92%	

Table 6-13: Breakdown of Intrusive Requests of Participants with Multiple Devices

Table 6-13 indicates that unifying the user identity confidence score of the various devices of a user's Cloud Aura would provide a more informing combined authentication decision. It is appreciated that the combined average of intrusive authentication requests is less than at least one of the participating devices (but not less than all of them). This can be caused by the fact that merely one device is being utilised as the primary one whereas the remaining devices are left for specific use, task(s), and environment(s). However, these secondary used devices can dramatically benefit from the maintained integrity of the main devices thus reducing their explicit authentication requests.

6.4 Conclusion

It is perceived that a particular transparent and continuous authentication mechanism would have the potential to ensure effective authentication method together with users' acceptance. However, it is paramount to have high level of performance, scalability, and interoperability among and with existing and future systems, services and devices. Furthermore, these requirements should be implemented and evaluated extensively on real data in order to prove that such a system is viable and should be put and deployed in an operational context to measure other key factors that are required for successful adoption (such as usability and economic benefits of biometrics licencing and processing).

The experiments showed that it is possible to gather a single user profile from the range of devices a single user may use and with the augmentation of information from various smart sources (multi-devices and geolocation as examples), it is viable, secure and more convenient to authenticate users. The model achieved appropriate levels of integrity in the case of an authorised user better than those of unimodal, NICA, and WMVF which accordingly established better security (detection time) in the event that an impostor tries to access the device assets. Furthermore, it reduces the intrusive authentication requests by 62%-74% (of the total assumed intrusive requests without operating this model) in the worst cases. These, in turn, demonstrated the added value of incorporating geolocation and multiple devices information in a centralised federated authentication using the Cloud that would provide a more reliable decision on the authenticity of the user in a high transparent fashion.

It is also evident that there is a dire need of having a model that is able to adapt according to particular usage profiles due to experimental results showing that the security and convenience aspects deviate and reflect depending upon what these settings are. Notwithstanding, with insufficient data on hand showing that particularly, it is nevertheless

arguably envisaged that actually with a larger and better dataset, the advantage of having the cloud-based authentication solution would increase beyond what was experimentally shown.

Building upon the previous experiments and the consequent needed refinements, a novel, flexible and scalable Cloud Aura architecture will be proposed and designed. An authentication system built upon this would provide a more secure, user-friendly, universal and technology independent environment.

7 Cloud Aura – System Architecture and Prototype

7.1 Introduction

With the aforementioned evolution of authentication mechanisms and of digital devices functionalities along with the extensive utilisation of them by users, the necessity for transparent, universal and federated authentication approach that can be used across technologies and services is becoming more apparent.

Having established the empirical experimental basis that have enabled showing how Cloud Aura would work and presenting the benefits of such an approach, this chapter seeks to design a novel information system that would help support those functionalities. Specified requirements would, also, be needed in the development of a holistic federated authentication platform, taking into account the security, usability, privacy and other related issues. Considering the operational aspects, that such a practical high intelligent authentication management system would require, is crucial to ensure its robustness, effectiveness and ease of use.

Benefiting from the promising features offered by cloud computing – its universal connectivity, scalability and flexibility – would enable a novel opportunity of achieving convenient authentication seamlessly in a technology and service independent fashion. The approach introduces a new dedicated authentication provider – the Managed Authentication Service Provider (MASP) – that is able to provide state-of-the-art centralised verification of authenticity. However, relying upon such an environment also introduces a range of technology, privacy and trust-related issues that must be considered and overcome.

An exhaustive description of the system architecture requirements, components, and processes is elucidated showing the flexibility of the integration of multibiometric techniques

in order to provide a centralised transparent and continuous authentication mechanism for multiple devices to access multiple services. Moreover, in order to practically prove that the concept of the proposed solution can work in practice, a functional cloud-based prototype is designed and developed.

7.2 Cloud Aura Requirements

Based upon the thorough analysis of the literature review (Chapter 0), the user survey (Chapter 4), and the results of the set of experiments (Chapter 5 and 6), and in order to offer an effective novel authentication mechanism, Cloud Aura system requirements have to be specified prior to the architecture design.

7.2.1 Essential Requirements

The following essential system requirements have been empirically established and thus must be addressed in the proposed architecture:

- **High security performance through the use of multimodal biometric system**

  As proved by Experiment 1 of Chapter 5, utilising a single modality would continue in carrying its shortcomings, thus enduring low matching performance, limited universality and higher vulnerability to spoofing attacks. Fusing more than one biometric (multimodal) can arguably contribute to overcoming or at least alleviating these flaws, as seen from Experiment 2 and 3 of Chapter 5.

- **High level of transparent operation**

  It is found from the analysis of the literature review of Chapter 3 and the user survey of Chapter 4 that it is imperative for the Cloud Aura architecture to operate in a full transparent fashion from even the initial login. Integrating any form of intrusive login

(i.e. secret or biometric) would lead them to carry the limitations of the secret-knowledge authentication approach, the single modality, and intrusiveness – thus reducing user convenience.

- **Continuous user identity confidence**

  The outcome of Chapter 3 shows that performing user verification merely at the point-of-entry leaves the system at risk of misuse afterwards. It also focusses upon system/service level authentication – rather than actually looking at what the user is doing. Therefore, user identity confidence should be maintained throughout the usage session(s).

- **Universality and Interoperability**

  Comparing the results of the WMVF (Section 5.3.4) with those after using the Cloud Aura concept (Section 6.3), it is evident that authentication mechanisms that are confined to work in a specific context and/or device are deemed to lack the universality and interoperability attribute that enables a seamless technology and service independent functioning. Accordingly, a centralised federated authentication approach using the Cloud would help towards constructing a better user profile encompassing multibiometrics and soft biometric information from their multiple devices and thus improving the security and convenience of the technique beyond what a single device can do by itself. As such, Cloud Aura should not require any additional capturing device or sensor and should be compatible with various platforms.

- **Services risk levels aligned with user identity confidence**

Considering the fluctuation nature of user identity confidence/trust should be mapped with the varying risk levels of conducted activities or accessed services, which reflects the real use, as shown from the diversity of apps risk levels the participants utilised in the experiments of Chapter 5 and 6.

7.2.2 Desirable Requirements

In addition to the afore-mentioned essential requirements, the following desirable system requirements need to be considered though they have not been validated in this research:

- **Flexibility and adaptability to deploy mixture of biometrics**

  Cloud Aura should be flexible, modular, and adaptable to the future of what new biometric techniques may emerge thereby using biometrics standards allowing to plug/include a new biometric into the system.

- **Work with autonomous service domains and organisations**

  The desirable architecture would be able to offer a federated authentication mechanism able to manage access control to heterogeneous service providers.

- **Minimal processing and storage overhead on user devices**

  Carrying out the feature extraction and classification algorithms for each contributing biometric technique on each device would increase processing and storage overhead on each incorporated device. Thus, there is a need to maintain an efficient and cost effective model for the biometric processing together with low footprint on users' devices with no adverse effect on the performance of the device.

- **Appropriate level of scalability**

The architecture should be scalable enough in order address the potential enlarging use of network and memory resources caused by the amplifying number of subscribed users and their interactions with the system.

- **Security and privacy protection**

  Measures to secure and manage biometric templates database and biometric samples in transient should be put in place to support users' acceptance of and trust in the system that would lead to better adoption.

The aforementioned requirements can be achieved by utilising the Cloud Aura system architecture, which is described in the proceeding section.

7.3 Cloud Aura Architecture

Stemming from the abovementioned essential and desirable characteristics and requirements, a federated biometric authentication framework is proposed, shifting the burden of both the authentication processing and management responsibility to a centralised Managed Authentication Service Provider (MASP). Cloud Aura fundamentally works as described in section 6.2, building upon existing research on transparent and distributed authentication, with a view of capitalising upon the benefits that cloud computing provide whereby residing in a cloud environment. An authentication system built upon this would provide a more secure, user-friendly, universal, adaptable, scalable and technology independent environment than a device-centric approach.

The specialisation of the MASP enables economies of scale with respect to the authentication processing algorithms that would not easy be achieved on an individual user basis. However, the significant benefit of the centralised approach is the ability to secure a host of devices and services that would not themselves be able to utilise strong biometric-level authentication

approaches. In a federated authentication approach, a user is able to establish a level of identity confidence through the capture of biometric samples on one device and then subsequently use that confidence to access other devices and services.

Figure 7-1 demonstrates an architectural Cloud Aura framework encompassing processes and elements held within the user device(s) together with those on the Cloud and their interconnectivity. The design of the Cloud Aura architecture is built upon the knowledge obtained from the conducted experiments of this thesis and the concepts of the Authentication Aura (Hocking et al., 2011) and IAMS/NICA (Clarke & Furnell, 2006; Clarke et al., 2009).

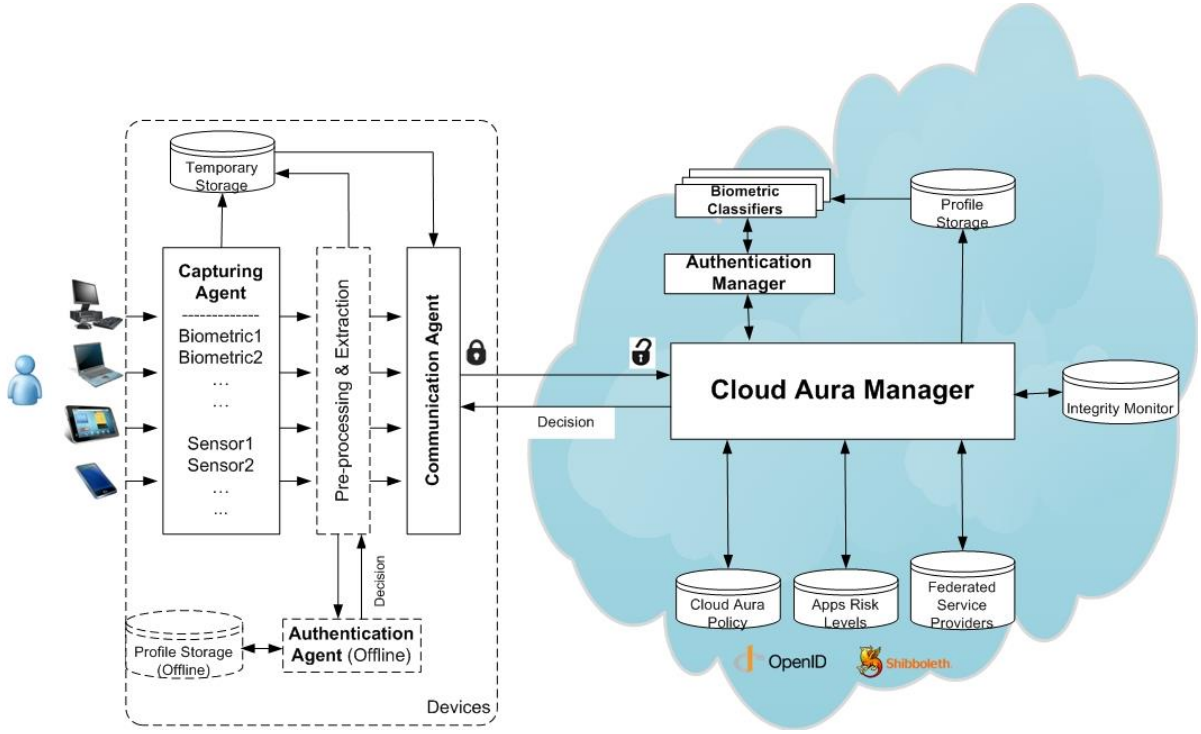

Figure 7-1: Cloud Aura Architecture

It incorporates functionalities on the device to capture (by the Capturing Agent) and pre-process (if necessary) authentication credentials, typically biometrics-based information and soft biometrics. This is a continuous process depending upon the device, its capturing capabilities and usage – the latter aspect being a key to achieving transparent authentication. Beyond capturing, however, (when the typical cloud-based mode is enabled) the

Communication Agent sends the pre-processed information to the Cloud Aura Manager (run by a MASP in the Cloud) which undertakes all remaining processing and responsibilities, removing any unnecessary processing and storage burden from the device. When utilising devices that the user does now own, this also serves to minimise privacy implications and the local storage of biometrics-based information.

The Cloud Aura Manager, being the heart of the Cloud Aura architecture, originates the Authentication Manager to process the appropriate Biometric Classifier(s) as configured in the Cloud Aura Policy. Dependent upon the verification result of the Authentication Manager, the Cloud Aura Manager, subsequently, utilises the various information from the Profile Storage, Integrity Monitor, Apps Risk Levels, and Federated Service Providers to take the appropriate subsequent response(s), such as granting access, requesting intrusive authentication, blocking some services, locking down the device(s), sending a security notification to the user, re-training the classifier, and updating the template. Furthermore, the resultant accumulated user confidence of the Integrity Monitor is disseminated to the other Cloud Aura-enabled devices of the user.

The following sub-sections explain in detail the integral Cloud Aura components required to work on the architecture in order to fulfil its requirements thereby maintaining security and minimising inconvenience.

7.3.1 Capturing Agent

The primary role of the Capturing Agent is to detect and collect biometrical information of a user both physiological and behavioural (e.g. fingerprint, face, voice and gait) alongside other smart or soft information from sensors of their device(s) (e.g. GPS and gyroscope). Given the range of biometric modalities that can be captured by a device and utilised by a user, their related agents are put into effect to capture their biometric characteristics simultaneously and

transparently at the set intervals. Moreover, the Capturing Agent does monitor and log the system activities and store this in the Temporary Storage in order to map the authentication and access control decisions to them.

Due to the unavailability possibility of some samples from some biometric techniques and/or sensors at a specific time, all raw samples are stored in the Temporary Storage database for future use, such as for pre-processing or by the Communication Agent. The Temporary Storage information consists of (but not limited to) the requested application name and its risk level, types of captured input data, date and time, besides the quality of the sample.

The varying quality of the samples in real life usage (as seen in the experiments of this research) poses issues of increasing FRR owed to the far mismatch with the templates (Clarke, 2011). For instance, face occlusion caused by posturing in front of the camera and surrounding noise with voice may lead to low confidence score although being from an authorised user. Thus, there should be a method for samples quality check prior to employing them for authentication decision. However, defining such a method can be within the design of biometric techniques which is not the aim of this research apart from being not vital for this system architectural design.

The architecture permits for a degree of client-side pre-processing of biometric samples in order to reduce the volume of data to be transmitted by the Communication Agent to the Cloud Aura Manager besides perhaps providing an increased level of privacy. This pre-processing phase may include extracting biometric features (if it is lightweight) dependent upon the concerned biometric technique, upon which it is performed differently and converted into feature vector. Both enrolment and verification processes benefit from this. During the former, the sample template is created and communicated to the Cloud Aura Manager to use and keep in the Profile Storage. However, during the latter process, the

sample template is used by the Authentication Manager to verify with the user's profile. These pre-processing and feature extraction processes are optional in the client-side if the cloud-based system is activated whilst they become core within the standalone mode.

Considering the multimodal and interoperability requirements, the system is not limited to current technologies of biometrics and sensors, so it can adapt to new modalities. Therefore, the architecture is constructed to be flexible, modular, and adaptable looking to the future of what new biometric techniques may emerge thereby using biometrics standards. Implementing the MASP to accept any current or emerged biometrics as long as it complies with ISO standards (i.e. ISO 19794, 19785, 19784) allows for flexibility and modularisation of the system – something individual devices would never be able to achieve due to prohibitive costs and processing requirements (ISO, 2006a, 2006b, 2011). Furthermore, having the classification and authentication undertaken in the Cloud, a wide range of devices can use such a system (e.g. smartphones, tablets, laptops, desktops), which vary in terms of their hardware configuration and operating system. This, in turn, enables the architecture to be plug in different operating systems being device-independent. Typically, cost, processing and vendor-specific solutions have prevented this from happening to date and continue to do so. Nonetheless, utilising these standards makes Cloud Aura an interoperable framework thereby providing a more rigorous and technology independent authentication approach.

7.3.2 Communication Agent

The Communication Agent plays as a communication bridge between the client (device) and the host (Cloud). Where the cloud-based mode is in use, the Communication Agent passes the captured samples from the device to the MASP so the Cloud Aura Manager works upon them accordingly. If the biometric samples were pre-processed, their feature vectors are the ones to

be sent. The communication process takes place in a trusted environment to a Trusted Third Party (TTP) and via the Secure Sockets Layer (SSL) security technology.

Once the authentication decision is made by the Cloud Aura Manager, the Communication Agent will receive the authentication result and the integrity status that enable the users to experience the outcome on the device(s) – ranging from granting access, requesting intrusive authentication, to locking down the device. Furthermore, in cases where less computationally complex functions suffice and/or where the standalone mode is in use, the Communication Agent will coordinate to ordain the authentication to be performed within the device by the Authentication Agent utilising the offline Profile Storage. The biometrics that can be employed in this way are defined in the Cloud Aura Policy.

7.3.3 Authentication Manager

The Authentication Manager is controlled by the Cloud Aura Manager, and performs the actual uni- and multi-modal authentication. When prompted, the Authentication Manager will perform the authentication by retrieving the required captured information set by the Communication Agent and supplying it to the appropriate biometric classifier(s), which will utilise the corresponding biometric template from the Profile Storage and produce an individual authentication decision. Dependent upon the type of captured sample, the Authentication Manager will utilise external Biometric Classifier to perform the relevant processing (e.g. facial recognition for face images, and voice verification for voice samples). The Authentication Manager will then obtain the verification result and inform the Cloud Aura Manager accordingly. The Authentication Manager uses the Profile Storage in the authentication process and the samples for re-generating or re-training the biometric template when needed. If the result of the Authentication Manager is successful, the captured samples

and information are kept in the Profile Storage for subsequent re-training and profile re-generation; otherwise, they are discarded or used to generate patterns of anomalies.

The initial process of profile template generation of physiological biometrics can be straightforward and thus can take effect instantly after the registration and enrolment stages. However, it can be a complex task when it comes to behavioural and soft biometrics where there is a need for a period of time and a number of samples in order to generate the templates.

As the biometric samples can be captured by one or different biometric techniques, the following approaches are implemented so one or a set of them is applied as appropriate (elaborated in 3.6.1):

- **Multi-Sample approach**: deploying multiple inputs of the same modality in order to have a more informed identity verification decision and to offset the existence of low quality samples.
- **Multimodal approach**: deploying a single sample of multiple modalities to alleviate the malfunction of some incorporated biometric techniques or sensors.
- **Hybrid approach**: dynamically deploying single or multiple samples of multiple modalities. This would fine-tune the algorithm in order to achieve a desired performance, crafting a more multi-layered method.

Referring to the review in 3.6.2, these samples need to be fused effectively at certain phase of the biometric system: sensor, feature, matching score, and/or decision level (Clarke, 2011; Ross, 2007; Sim et al., 2007). This objective aims at producing such a scalable, flexible and dynamic framework, thereby enabling multiple diverse classification schemes, in order to have a more robust authentication decision.

In order to produce a balanced decision considering the effect of the inputs from modalities of different EERs thus different accuracies, consideration needs also to be given to the weight each individual contributing technique has on the fused decision. Given enough time in samples, any combination of multibiometric systems could potentially exists. The weights are assigned to the individual biometric techniques inversely proportionate to their EERs – the lower the EER, the higher the weight than those of high EER. For instance, a fingerprint scan would be given a higher weight than that of gait recognition. When authentication fusion is performed successfully upon a user, the result score will be returned to the Cloud Aura Manager for use in the identity confidence calculation.

In spite of the fact that an overall successful decision of multibiometrics may contain a number of rejected samples, they can be actually of the authorised user, thus utilising them in the re-training process would aid having a better insight about the real interactions of the user.

7.3.4 Integrity Monitor

The Integrity Monitor holds the current and historical system integrity levels – one upon which the access control decision is made. The Cloud Aura Manager originates its process at the intervals defined in the Cloud Aura Policy. Following the same concept and algorithm outlined in Section 5.3.3.1, the level of integrity continuously fluctuates based upon the biometric samples captured, their authentication decisions, the elapsed time since those last decisions, and the current location. That integrity level is subsequently passed to the Cloud Aura Manager and accordingly reflected on the privileges to access services and applications (passed back to the Communication Agent), enabling the device to deny access to specific functionalities and request an intrusive authentication if insufficient confidence exists up until locking down the device completely when this status persists or gets deteriorated.

Reliant upon the period of inactivity, the Cloud Aura Manager will automatically degrade the system integrity according to the concerned settings in the Cloud Aura Policy, i.e. the degradation function including its invocation intervals and drop value. Doing so would contribute in mitigating the risk of misuse (especially of the high sensitive apps/services) in case the device is hijacked when the system integrity is quite high.

The Integrity Monitor does also provide another function – system integrity's feedback information. It shows the individual authentication results and locations per modality, per app/service, per device, and per user's Cloud Aura. Even though this informational guide might not be of use to some users, it offers a potentially useful appreciation about how their devices and Cloud Aura are being utilised, thus aiding to identify potential misuse as well as refinement and maintenance needed (e.g. template re-enrolment, classifier re-training, and modality disabling).

7.3.5 Applications Risk Levels

Intuitively, different apps and services have different risks that should be tied with authentication decisions. Other researchers have looked at this issue and identified that having different risks for different apps would be useful (Clarke et al., 2011b; Herland, 2015; Ledermuller & Clarke, 2011; Shabtai et al., 2010; Theoharidou et al., 2012; Vecchiato et al., 2016). In terms of defining a single approach to categorise these apps/services and calculate their risks, different researchers (including the abovementioned ones) have come up with different ideas and it is not the purpose of this work to come up of a new one. These apps risks are predefined based upon those models at the initiation of the Cloud Aura and as and when a new app is installed; however, the user still has the ability to override and change them should they wish to. Thus, in reality there might be variations between the risk level of

the same app utilised by different users as every user has their own security perceptions and requirements.

The adopted method in the experimental studies proposed that each mobile application category has its distinct associated risk level dependent upon a number of measures, e.g. their asset values, threat levels, and vulnerability levels (Ledermuller & Clarke, 2011). Each risk level is mapped with their related security requirement levels (i.e. integrity level) – the higher the risk level of an application, the higher the associated integrity level. That is, the applications/services that are associated with private information or expensive services would require a high level of security whereas the normal applications/services would require a low level of security. Hence, they are used as the thresholds to feed the algorithms and to compare against. If the integrity level (IL) is greater than or equal to the specified associated security level, a transparent access is granted, otherwise an intrusive authentication request will be required in order to proceed with the service.

7.3.6 Federated Service Providers

In order to achieve the aim of granting users access to resources offered by autonomous and heterogeneous providers seamlessly, the profiles of the subscribed service providers must be recognised and so a trust relationship with the MASP should be established. Since the MASP will be the chief controller of the user authentication on behalf of the Federated Service Providers (FSP) upon which they undertake the access control decision accordingly, trust management between the MASP and the FSP is thus pivotal. It can be dictated by a stringent Service Level Agreement (SLA) between them stipulating the minimum security requirements of federation clients. This can, for example, include the enforcement of adequate authentication measures such as specific biometric technique(s), specific number of them, and/or just a minimum integrity level. This data store is responsible for holding these

SLAs for all subscribed FSPs to be used by the Cloud Aura Manager in making the authentication and the subsequent authorisation decisions.

Having these different entities, there is a need to ensure the security of these cross-domains communications by deploying specialised standards, such as OpenID, WS-Federation, and Shibboleth (CSA, 2012; Stihler et al., 2012). Acting as a TTP federated MASP, whilst coordinating the authentication process among the member parties of the federation which are the service providers, user privacy concerns must be overcome so that the user should have the discretion to decide which of their data can be shared, with whom and when, in addition to the ability to de-federation.

7.3.7 Cloud Aura Policy

In order to achieve a commensurate level of security versus users' convenience on a given device, the architecture enables a Cloud Aura client to define a number of parameters in the Cloud Aura Policy. The Cloud Aura Policy holds the fundamental data needed to control the creation, operation and maintenance of the system. Upon registering on and activating the Cloud Aura, the Cloud Aura Manager will launch the Cloud Aura Policy to prompt the user to allocate values to the core parameters (which already have default values). The Cloud Aura Manager will use and work upon these parameters throughout regular operation of the Cloud Aura and allow the user to review and update them as and when preferred or needed. These parameters include:

- enabling/disabling Cloud Aura of specific device(s);
- enabling/disabling individual authentication techniques;
- Temporary Storage retention period;
- Degradation Function of system integrity;
- determining the time periods of Alert Level and Integrity Level;

- manual template generation/re-training;
- ranking the subscribed devices;
- assigning trusted geolocations;
- assigning the fusion weight to individual authentication techniques;
- determining what subsequent action(s) should be taken after each possible authentication result;
- determining the processing split (if needed) between the client and the Cloud;
- determining the authentication technique(s) of the standalone mode;
- and determining and reviewing subscriptions features with Cloud Aura.

Most of these parameters are straightforward or have been explained in different places of this thesis. The commentary that follows elaborates those that might be somewhat sophisticated.

Subscribed devices information and their ranks are used to control a device's contribution to the Cloud Aura integrity. This can be represented by an integer value indicating which devices have high significance and will contribute more to the integrity calculation – in case, for instance, a device is utilised as primary and thus always carried with the user whereas another device is secondary and sometimes left at home. Knowing that each user's device may have different set of biometric techniques, users are able to disable any of the enabled techniques in order to improve users' convenience, for instance due to frequent failures of that technique. Linking the techniques to the device they relate to would allow a user to enable a technique (e.g. facial verification) in one device but disable it in the other one for hardware issues or others – this may be desirable, in this example, if the camera of the latter device is of low resolution.

Another parameter that can be determined within the Cloud Aura Policy is the user geolocation(s) information. Having established how vital the geolocation information of the device is when utilising Cloud Aura authentication mechanism in Chapter 6, trusted geolocations can be defined and even given specified security requirements. For instance, for the sake of convenience, a user may opt to relax the thresholds (risk levels) of all or some apps while being at home, as the adversary probability is at minimal. Conversely, elevating the thresholds while at alien or even specific geolocations can be applied for the security purpose. Manipulating these parameters can reflect on the degradation degree of the system integrity over time and thus its transparency level.

As examined throughout the previous experiments of this research, aiming at mitigating the risk of misuse while the device is not being used by the genuine user, the degradation function is enforced thereby decreasing the IL periodically by 0.5 (by default but is adjustable) every x minutes. If no biometric samples captured for a specified time, the IL is going down by specified degrees. Once biometric samples come in, it takes the latest IL (after the last degradation) and adds to or subtracts from it based on their recent authentication decision and then resets the degradation function's time counter. For example, if the IL at 19:30 is 4 and the user would like to access an app at 20:15, it will not be sensible to give them access considering that IL recorded 45 minutes ago because the device might be on imposter's hands by this time. Furthermore, it might be nonsense to disregard that IL (i.e. 4) and start the IL from zero when an app is called, especially with infrequent users who rarely have samples available for authentication. For example, a genuine user might be eating lunch at these elapsed 45 minutes, so when immediately after lunch they want to access an app of high or medium risk, there might not be any biometric sample at that time. Thus, it is useful to encompass the previous IL but not as is.

It is dependent on two variables – elapsed time and the degradation degree. The degradation function of the IL (which should be stored on the Integrity Monitor and kept for the following IL calculation) should be implemented in x elapsed minutes from the last IL by y degrees if there is no biometric samples captured during these x minutes. Therefore, based upon the set degradation time (e.g. 10 minutes) and the degradation degree (e.g. 0.5), when an app is called, the Cloud Aura Manager will check what was the latest IL (from the Integrity Monitor). Then, it will calculate whether it was from more than 10 minutes (the degradation time) – if yes, the IL will be decreased by 0.5 (the degradation degree) for every passed 10 minutes. Consequently, this updated IL will be the basis of calculating the recent IL and hence the authentication decision.

Having perceived its impact on the number of intrusive authentication requests and that it may take many forms, its values vary even among those of the same interaction level, such as frequent and infrequent users. Therefore, offering the user with a degree of control, adjustability and influence over the confidence degradation would lead to choosing appropriate values based on trial.

Further features available for review and configuration through the Cloud Aura Policy are those related to the subscription with the Cloud Aura system. These include (but not limited to): SLAs between the client and the MASP, contact or payment details, price models and the service capacity and scalability options.

7.3.8 Cloud Aura Manager

The Cloud Aura Manager acts as the brain of the Cloud Aura architecture – administering and initiating the processes and liaising with and between the data stores as and when required. Its principal task is to maintain the level of security required commensurate with the

applications provided by the device(s) and services provided by the FSPs. It is hosted in the Cloud and conducts the following integral tasks:

- determining the operational mode;
- generating and maintaining the system Integrity Level;
- requesting profile generation and retraining;
- making authentication requests, both intrusive and non-intrusive;
- triggering what subsequent action(s) to be taken based upon the authentication result;
- and determining whether a user has the required system Integrity Level.

Upon registration, the Cloud Aura Manager guides the user to define system parameters that are administered by the Cloud Aura Policy. In addition, when the system is activated and functioning, the Cloud Aura Policy is also called to initiate operational parameters for ongoing running. During its continuous monitoring fashion, it receives the information transmitted by the Communication Agent and then employs the information held within the Profile Storage triggering appropriate processing procedures as required. Following the parameters set, the Authentication Manager is invoked. The result of the authentication is reported to the Cloud Aura Manager, dependent upon which is going to take a subsequent response taking into consideration other inputs such as the system integrity from the Integrity Monitor, the app risk level and the security requirements of the FSP.

The remaining responsibilities of the Cloud Aura Manager concern with control (either dynamically or by user), such as sending a template generation and re-training request to the Authentication Manager to update the biometric profiles and subsequently the Profile Storage.

Regarding the device-side Authentication Agent, it monitors the network connectivity to the Cloud Aura (via the Communication Manager) – should it be lost at any stage, the architecture will switch to a standalone mode to conduct independent operation. This could

be useful in a number of situations, such as poor network signal and network failure where the Authentication Agent will act as the Cloud Aura Manager temporarily with limited processes and modalities as configured in the Cloud Aura Policy. As such, it can be configured that at least one biometric technique always remains functioning on the device with the standalone mode. Quite not very strong level of protection this single technique is able to provide; notwithstanding, it would be able to provide a temporary effective means to authenticating the user whilst utilising local applications and utilities. Furthermore, in order to allow the use's devices to communicate in the absence of the Cloud connectivity, the system will operate the Authentication Aura concept (Hocking et al., 2011) via the NFC feature. As soon as the connection reinstated, the mode will revert to the cloud-based and the Cloud Aura Manager will re-establish its monitoring working until the device is disconnected again or shut down.

7.4 Correlation and Analysis of Cloud Aura

The system allows for both device- and service-level authentication. For device-level authentication, the user is required to initially install a service that will provide the interconnection between the local authentication mechanisms/services and the MASP. Once configured at start-up, this becomes a completely transparent process from the user perspective – with all future logins only required if sufficient confidence does not exist. For example, had the user in the morning, logged into his mobile phone using a strong biometrics approach they would, within an appropriate timeframe and proximity as defined by the Authentication Aura (Hocking et al., 2011), be automatically logged into his computer or any other device he owns.

The approach can also be utilised on devices the user does not own – providing a web-service level of integration. Upon initially connecting to the MASP identity through a web-based

biometrically-enabled login, a user will be able to access any of his web-based services transparently without having to repeatedly enter his credentials. This can be achieved in one of two approaches:

1) (Preferred) The MASP connects directly to a federated identity system (e.g. Shibboleth and OpenID) to provide seamless cross-domains single-sign on.
2) (Optional) The MASP provides a web-service credential database (i.e. password store) and releases the appropriate credentials to the web-service if sufficient confidence exists.

Cloud Aura authentication system works in a distinct way from how conventional authentication are carried out typically. Despite its apparent complexity over the existing provision, it does offer promising features. Having a cloud-based system would facilitate using multibiometrics, some of which require significant processing and storage. There would also be a need for single technique licensing and single instances (or at least lighter requirements on the licenses). In addition, getting that big trend in mobile computation, the use of cloud-based resources to do it would help relieve the mobile device from that. The lightweight framework for the mobile devices supports this, as the Cloud hosts the main software and no need to roll out all its code locally.

The Cloud Aura's control dashboard functionalities would be useful in identifying misuse thereby providing an in-depth understanding of what the user is doing (in terms of devices and services) and thereby providing additional identity intelligence of the user. For example, it will be possible to determine if two authentication requests are simultaneously made from different locations from devices that belong to the owner or otherwise – thus highlighting potential misuse. For instance, while using multiple devices, one of the devices has been stolen and being misused in another location. The dashboard flags it up and sends a message

out to the trusted user communication method (email). When the user logins after the notification, the dashboard should show something signifying that the Cloud Aura is here with these devices while one of them is at a different location and sending abnormal information/samples contradicting the normal usage coming from the other sources.

Furthermore, the dashboard would facilitate the review process of the historical events in order to check and see how things are working and reconfigure/respond to the system accordingly. For example, if the system is found to ask for intrusive authentication more frequently than usual, after checking the dashboard, it is noted that while the face and voice recognition always pass, the keystroke dynamics always fails. As a consequent, the user can re-train the keystroke classifier or switch off the technique. This would give the user the ability to:

- make an informed decisions about their own use of the system;
- confirm that the use they see are in fact their own one, i.e. there is no misuse;
- when the system detects misuse, the dashboard responds accordingly so the user can identify that and act accordingly by, for instance, blocking that device to restrict access and remotely wipe the device so the Authentication Agent of that system deals with that accordingly.

7.5 Operational Considerations

Cloud Aura provides a universal approach to identity verification that can be utilised by any network-enabled device or service. The introduction of such system architecture meets all set essential requirements of Section 7.2.1 (that have been proven experimentally) and considers the desirable requirements of Section 7.2.2 theoretically. Thus, it has the foundations for solving the authentication problems – both in terms of effective security and convenience.

However, it also introduces a range of further issues that need to be resolved in order for the system to operate effectively.

7.5.1 Trust

First and foremost is the need for users and organisations to trust a third-party provider with their authentication services. Fundamentally, to date, this is not a typical expectation and there might become a concern over doing so. However, users already trust service providers with authentication credentials, albeit not all in one place. Furthermore, federated identity has become widely popular and this is based on the use of a single authentication credential. Federated authentication that Cloud Aura deploys will offer a range of authentication technologies for inclusion within federated identity – extending the concept of federated identity but more thoroughly confirming the identity prior to the access control decision that is made. It arguably therefore should not be a complete leap in faith of organisations, but merely a logical extension of the services that are already being provided. Rigorous statements of SLAs and close and constant monitoring upon conforming to it would provide a baseline level of trust. This is also supported by the rather promising users' responses regarding storing biometric templates with a TTP as well as having their usage behaviour monitored by a TTP (investigated in the user survey of Chapter 4).

7.5.2 Cost

In spite of the gains offered by Cloud Aura, it does however change the paradigm under which authentication will be performed. Rather than a zero-cost solution as is (incorrectly) perceived to be cost of many secret-knowledge solutions, a federated authentication provider will need to charge at some level for the service it provides (perhaps on a per-authentication, per-user, monthly or organisational-basis). However, given the nature and scale of the authentication and security problem, the concept of paying to ensure appropriate

authentication security should be more than viable. Incurring cost on authentication is not strange because some businesses are releasing the true cost of their authentication solutions; for example, the financial sector investing in token-based approaches. Bearing in mind cost is an important factor, it would not necessarily be suitable to merely utilise more systems but rather better manage existing resources.

Likewise, it is worth noting that without the use of a cloud solution a user would have to buy licence for every biometric technique on every single multiple device – in the way which the industry works as per licence model making it incredibly expensive to do. However, with the idea of a centralised model where there is a centralised server to authentication – although it might not get away of just a single licence – there could be a need to obtain a mere single licence or at least fewer licences or some form that could be economically far cheaper (cost effective). Accordingly, this would allow the MASP (federated Cloud Aura provider) to offer their off-the-shelf biometric solutions to their customers to pay only for an instance of them instead of many instances. This would indeed offer organisations the opportunity to contract out the user identity management and maintenance, thus reducing their in-house cost.

7.5.3 Scalability and Response Time

With the technology itself, there are a number of areas that need to be considered operationally. Considerations such as the time taken to process and authenticate a sample – in particular the lag introduced through the network and the potential bottleneck at the MASP need to be given care. The latter can be addressed through the Cloud and successful capacity planning. However, adding all the additional time lags introduced in a networked solution over a device-centric model might reduce levels of acceptability – so care must be taken to ensure this does not have a serious impact. It is not envisaged to be a major problem, as the concept of network-based authentication already exists for devices in network domains, and

all users already login to remote services with the authentication process occurring on the remote server. Furthermore, the process of transparently authenticating individuals means that the capture and authentication of those samples will be undertaken continuously throughout the use of a service or device, not just at point-of-entry. Therefore, the user should not be left waiting.

Although the Cloud Aura is envisioned to be offered as a Software-as-a-Service (SaaS), MASP requirements will be largely dependent upon the number of users subscribed to the service, the number of active users and thus the volume of authentication decisions it needs to make at any point in time. With such variability in the level of service demand, a flexible and highly scalable processing and storage system is essential. Therefore, from the MASP perspective, whilst distributed computing paradigms would be a solution, cloud computing provides an ideal solution to this requirement. Platform-as-a-Service (PaaS) (perhaps provisioned from a Cloud Service Provider (CSP)) provides an effective model for developing the necessary architecture for a highly scalable and adaptive solution. Such a system deployed in a cloud PaaS would be high scalable in terms of computing power and storage. It would also provide multi-tenancy at the application level using a shared database service and the Implicit Filter Based Access Control Isolation pattern for data isolation so tenant-specific operations do not conflict with other tenants' data (Senk, 2014). Having such a modular and flexible system would help thereby load balancing and pushing data across these cloud tenants and resources.

7.5.4 Enrolment and Template Management

Operationally, consideration needs to be given to effectively managing enrolment and template renewal. In TAS systems, they often rely upon many biometrics approaches that are behavioural in nature and thus have features that are not time-invariant (as would be ideal). It

is therefore necessary to update and renew the template in a timely fashion to ensure it is a true reflection of the users current set of features. Knowing when to do this and the implications it will have upon the processing infrastructure (as template creation is a far more processing and memory intensive task than authentication) is essential to the smooth and seamless running of the MASP.

Dynamic profile update is an example of this, where the template is set to be generated by the most samples/behaviour of the last x days given they have passed the authentication with a minimum integrity level. Accordingly, all successfully verified logs will be included in the periodic template regeneration process at the end of the identified period whilst those rejected logs will be used to create imposter data to be utilised for re-training the classifiers. Thus, users ensure they are having true reflecting profile comprising their up to date features.

Furthermore, profile adaptation can be based upon biometrics performance. If the decisions out of the fusion process were to be positive with high confidence, the process would retrospectively look at each individual fused techniques – if there were negatives, that might be a basis for requiring a profile refinement and classifier re-training. Poorly performing biometrics can also be an indicator for this. If a biometric technique has not performed well across the usage of one or all users (with lots of rejections) but that was among other stronger biometrics having successes, it perhaps does not mean it is illegitimate user, but rather that particular biometric is not performing well. Therefore, the algorithm could switch it off and/or trigger re-training.

7.5.5 Security and Privacy

Further issues surround the use of biometrics information. From an end-user perspective, privacy is a key factor to consider. The storage, use and communication of biometrics samples must be achieved in a manner that minimises the threat of interception and misuse of

the information. The MASP architecture must be appropriately designed to provide separation and segregation of duties, hashing, and defence against client-side apps to ensure the opportunity of accessing the sensitive data is only possible to specific authorised entities. Therefore, in order to secure the actual information and its transmission, a range of standardised mechanisms can be put in place. A number of studies have been undertaken to tackle this issue (Gejibo, 2015; He, et al., 2016; Itani, et al., 2009; Shrishak, et al., 2016). For instance, the client-side uses the Pretty Good Privacy (PGP), which is an encryption method that offers cryptographic privacy and authentication for data communication. The encrypted data will then be sent to the server using the Secure Socket Layer (SSL). Moreover, biometric cryptosystems and cancelable biometrics exemplify a fair level of biometric template protection addressing these considerations and hence enhancing users' acceptance of adopting such a system (Rathgeb & Uhl, 2011).

Stringent SLAs may also ensure a level of privacy-aware countermeasures together with related additional regulations. Privacy can also be protected by using and retaining only that information which is needed for the authentication process and its accompanying intelligence, in addition to enabling users some control over the release of their shared information with both the MASP and even the FSPs.

7.6 Cloud Aura Prototype

This functional prototype is developed because almost half of the software was already developed for the data collection so a number of interfaces to connect that with the dashboard have been added. This with the design of the web-based pages helped in visualising and understanding better how the architecture would work in practice. Therefore, it is used as a useful learning tool in its design being an iterative process. For this purpose, a mobile application is developed (using an appropriate open source programming language) as well as

a counterpart web-based dashboard – both are connected with a database hosted in a web server (cloud) representing the MASP. The mobile application accepts the biometric samples from the users and gathers GPS information from their devices. Subsequently, that information is stored as templates on the MASP, utilised in making succeeding authentication decisions, and facilitated to control provisions to the user.

Cloud Aura prototype is designed to have a small memory and processing footprint on the device. It is capable of monitoring user's apps usage, face recognition, voice verification, gait recognition and GPS information and then verifying the legitimacy of the user accordingly in the Cloud.

As stated in section 5.2.5, given Google Android OS has the largest mobile phones market share by 87.6% (IDC, 2016) and it is an open source and easy to manipulate (in addition to other stated rationales), Android Studio development environment was used for developing the mobile app. Native Android was used to develop the Could Aura application; whilst XML to design its graphics and user interface; Java for the front-end app development; and SQLite as the app database. Additionally, Retrofit library was used for calling web service API; Picasso library for displaying server images; and Google Play Services library for capturing location. On the other hand, the web coding platforms were: HTML5, CSS3, Jquery and Javascript for font-end, in addition to PHP for back-end.

Enabling the software to capture the aforementioned information was facilitated by employing and deploying a number of Android APIs and classes (apart from other supplementary basic APIs) as follows:

- Android Media API – Face Detector
- Android Hardware Camera2 API
- Android Media API – Audio Manager
- Android App Usage API

- Android User Availability API
- Android Hardware API – Sensor Manager
- Android Location API
- Android Database File Upload API
- Activity Manager
- Broadcast Receiver

All related capturing packages were encapsulated in one single Android Application Package (APK) and uploaded to Google Play while keeping it downloadable by private invitations only.

The design of this app was conducted according to weighted percentage assigned to each biometric technique and information inversely proportionate to their EERs considering all possible scenarios of their availability. In addition, they can be enabled/disabled. Capturing location of a user occurs at the time of app request and saved temporarily at the device-end with its associated timestamp. When a user opens any app, the Cloud Aura software detects and logs the app name, user's current location, steps count and walked distance (all with their timestamps) and sends them to the server to compare each of them with their historical behavioural profiles and stores them. For instance, it compares the current location with other historical locations within the same time slot. If the location is within 100 meters, data of location is stored and percentage of location is calculated.

Figure 7-2 illustrates an overall view of the Cloud Aura class diagram and the relations between the main data stores.

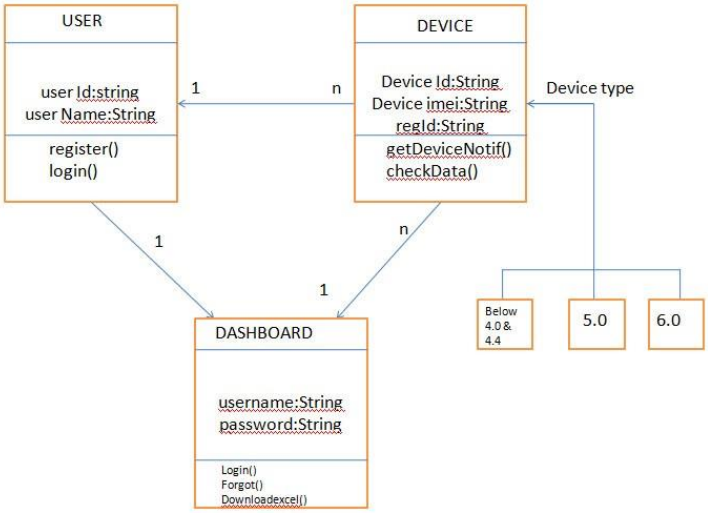

Figure 7-2: Class Diagram of the Cloud Aura Database

When a user installs Cloud Aura app for the first time, the registration/enrolment screen is prompted asking the user to set an email, password, and enrolling the physiological biometric samples (as shown in Figure 7-3). At the user registration screen, the user has to input an email and a password and capture 3 photos by clicking the camera button. When all details entered correctly, the user presses the register button to send all details to the server. It will send a confirmation email to the entered email with which the user has to verify their account.

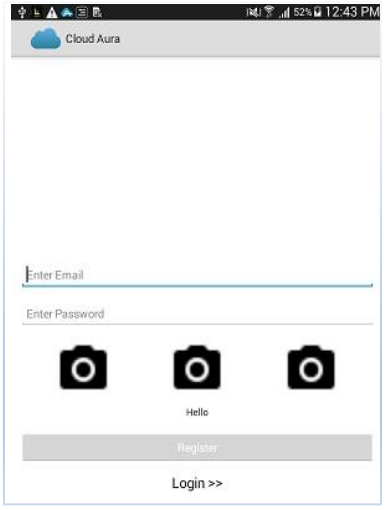

Figure 7-3: Cloud Aura App - User Enrolment/Registration

If the user is already registered, the login screen depicted in Figure 7-4 (Left) asks for the user credentials including the email, password and a voice sample forming a multi-factor

authentication. These credentials will be sent to the server for verification. If the login succeeds, the landing page appears (Figure 7-4 Right) and after setting the parameters, the app will continue working in the background unless the device is shut down or the app is disabled or uninstalled.

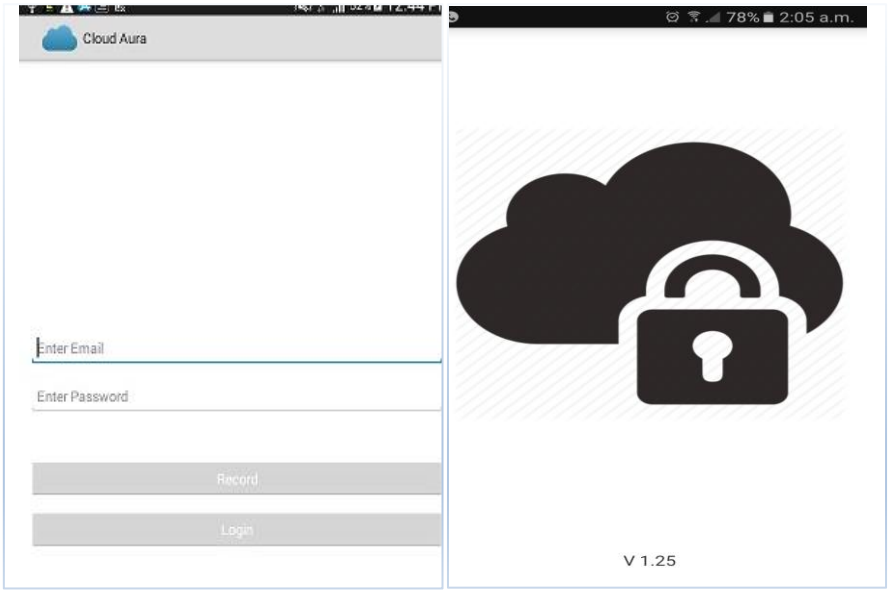

Figure 7-4: Cloud Aura App - User Login (Left) and Landing Page (Right)

One of the most critical parameter to define after the first login is the apps/services risk levels. As seen in Figure 7-5, a list of all installed applications and services on the device is demonstrated accompanied with three different risk levels (Low, Medium, and High), from which the user can select and submit initially and can re-visit at a later stage to update. All subsequent authentication decisions will be dependent upon these risks – when the resultant confidence is higher than the risk level of the requested app/service, the access is granted, otherwise an intrusive authentication is requested by asking for a voice or face sample.

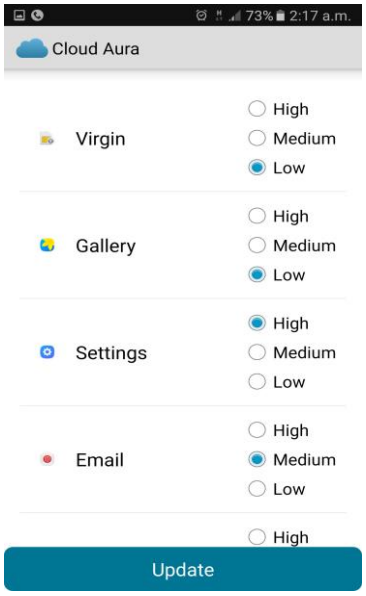

Figure 7-5: Cloud Aura App - Setting Apps and Services Risk Levels

The main page of the Cloud Aura app, through which three key functions can be undertaken, is exhibited in Figure 7-6. The first ON/OFF toggle button permits disabling and enabling the software temporarily or permanently from functioning on the device. For any reason, the user would prefer to stop the capturing processes. This would, arguably, enhance the users' acceptance and experience, thereby providing them a level of service control unlike the concept of a blanket-based opt-in or out completely. The second icon is for generating the collected information of that day in spreadsheets, allowing the user to review and monitor their data. The third button is to access the setting page, which will be shown in the next figure. Finally, a meter showing the current confidence of the device is displayed and can be attested by logging to the dashboard where the user can see this for all their registered devices. For example, the shown 75% in the figure conveys that this is the accumulated identity confidence that might come from a number of user's devices. In this case, the user will be able to access any service/app on their device(s) that have a risk level equivalent to or less than 75%.

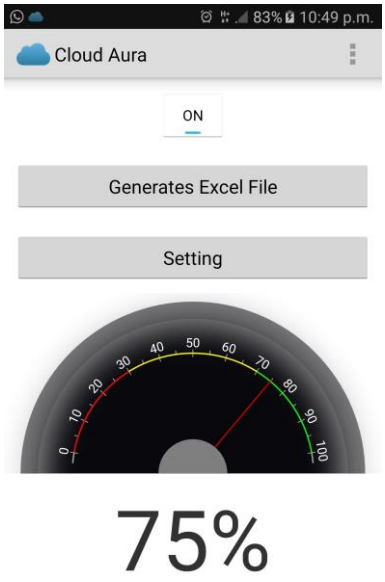

Figure 7-6: Cloud Aura App Main Page

When the user clicks on setting button of the above screen, it opens the enrolment settings screen revealing 4 icons; app risks setting, voice samples update setting, face samples setting and biometrics/sensors setting to enable/disable them (Figure 7-7). It is apparent that via the app setting, users can change risk levels of apps.

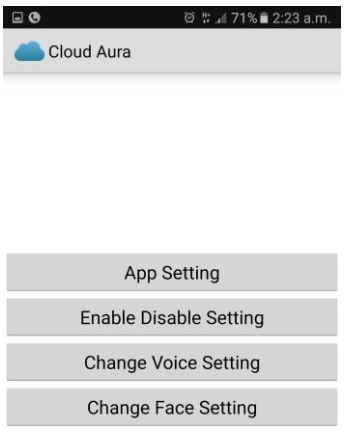

Figure 7-7: Cloud Aura App - Enrolment Settings

Due to the lack of text-independent voice verification classifiers that are freely available and/or open source, text-dependent method was utilised and believed to serve the purpose of this prototype. Thus, the user can enrol with up to three voice samples in the app, which can

be updated from the setting illustrated in Figure 7-8. The collected voice sample is matched with the three saved voice templates and its confidence is calculated.

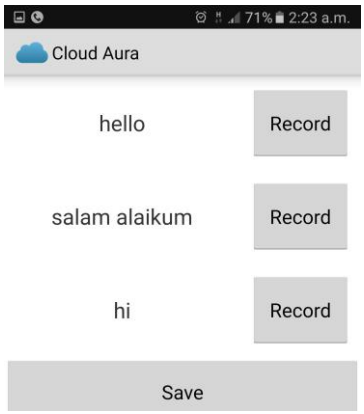

Figure 7-8: Cloud Aura App - Voice Enrolment/Re-Enrolment

Similarly, change face button shows the enrolled face images and the user can update one or all of them by capturing new image(s) and saving them on the dashboard (Figure 7-9).

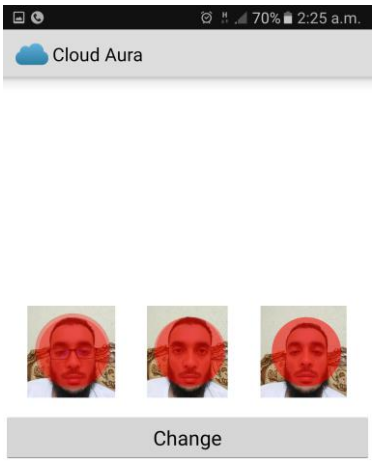

Figure 7-9: Cloud Aura App - Face Enrolment/Re-Enrolment

Image confidence calculation is undertaken on the server-side as follows:

1. Accepting the image (in jpg, png format)
2. Getting stored images for specific user at the time of registration
3. Recreating the images with the help of PHP function imagecreatefromjpeg() or imagecreatefrompng()

4. Resizing the images to 8x8 square
5. Filtering the images in grayscale
6. Getting the mean value of colours and the list of all pixel's colours
7. Comparing the colours, if the colour is bigger than the mean value, it gives 1 else zero
8. Finding out the hammering (change in shade) distances (between zero to 64) for both images and comparing both values to find the resultant value. If value < 9 ➔ images are similar, if value > 8 and value < 17 ➔ images are somewhat different, and if value > 16 ➔ images are completely different.

The last but not least setting, is related to the control of enabling and disabling specific biometrics/sensors, such as GPS, Fingerprint and Face features from being utilised by the Cloud Aura app. This can be seen in Figure 7-10 and will be reflected on the dashboard.

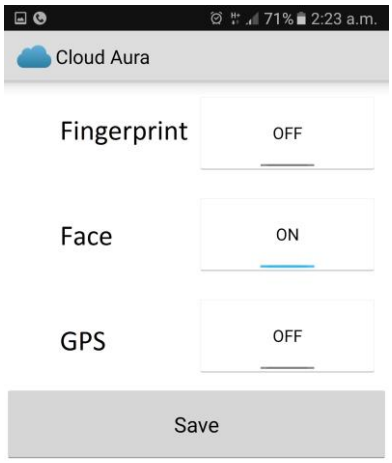

Figure 7-10: Cloud Aura App - Enable/Disable Biometric Capturing

As illustrated in Figure 7-11, a user can access the Cloud Aura's web dashboard using the same registration credentials and carry out some controlling and monitoring activities. General information is shown, such as the number of subscribed devices, their overall fused confidence, the registered email and the three face template images. Furthermore, there is

basic information about each registered device including the device name, the status of each of the biometrics and sensors besides the overall confidence of each individual device.

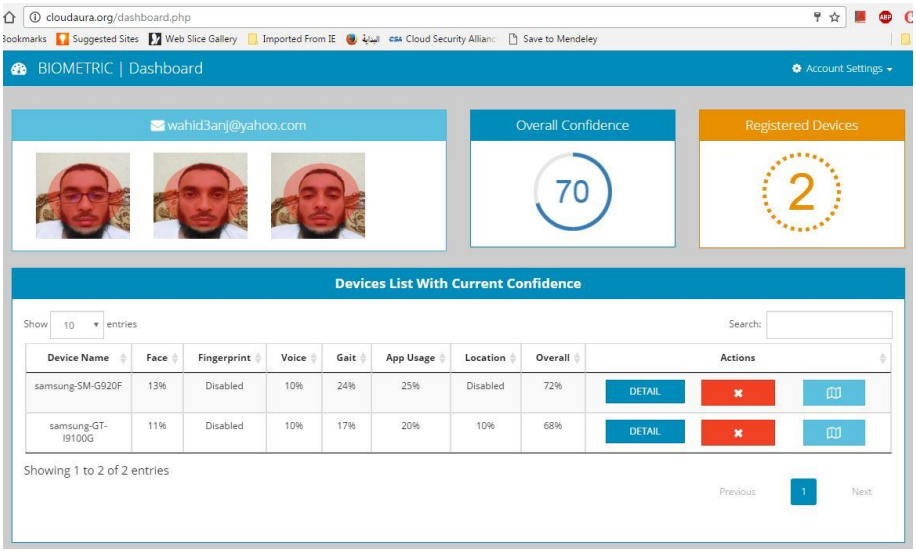

Figure 7-11: Cloud Aura Dashboard Main Page

With regard to the available actions, the red crossed icon allows for removing a device completely from the Cloud Aura. Additionally, the information icon displays the device location on Google map. By clicking on the detail button in front of a specific device, the user will be able to browse various log files (Figure 7-12) and review the historical overall identity confidence of each device as observed in Figure 7-13. These options would provide the user with information aiding to have better insight about the benefits of the system as well as how they use their devices leading to informed customisation to augment security and convenience

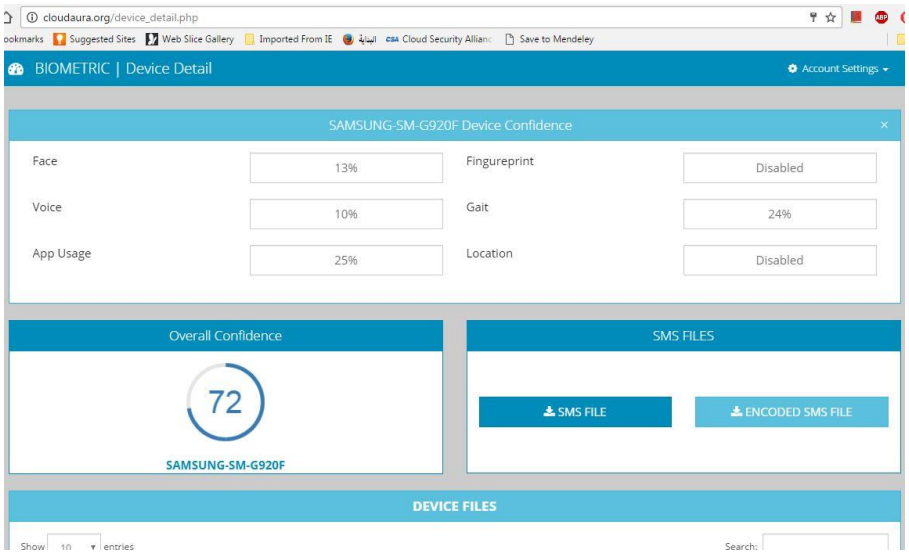

Figure 7-12: Cloud Aura Dashboard - Device Detail

Figure 7-13: Cloud Aura Dashboard - Device Fluctuating Identity Confidence

7.7 Conclusion

The requirements for achieving a novel Cloud Aura architecture have been established followed by a detailed practical architectural specifications designed in a modular and robust manner that would support such a system in practice considering the security, usability, privacy and other related operational issues. The architecture offers a cloud-based federated authentication mechanism accomplished by a Managed Authentication Service Provider (MASP) enables a high level of protection, transparency, adaptability, and universality seamlessly in a technology and service independent fashion.

A comprehensive description of the system architecture agents, components, and functionalities have been described. The Cloud Aura architecture has the potential to meet the laid requirements to offer the flexibility of the integration of multibiometric techniques in order to provide an intelligent centralised transparent and continuous authentication mechanism for multiple devices to access multiple services.

Even though it is not a risk-proof framework, a number of operational considerations have been addressed to be taken into account while developing and operating it. Moreover, a functional cloud-based prototype has been designed, developed and presented in order to practically prove that the concept of the proposed architecture would work in practice.

8 Conclusions and Future Work

This chapter concludes the thesis by outlining the key contributions and achievements of the research. This is followed by a summary of the limitations and obstacles encountered during it, and finally by an identification of potential areas of further research work.

8.1 Contributions and Achievements of the Research

The research has accomplished all the objectives originally stated in Chapter 1, with a series of undertaken experimental studies leading to the development of the Cloud Aura architecture. The key contributions and achievements of this research are:

- Investigating the leading authentication technologies provided by various sectors from a number of perspectives, including its system components, requirements, techniques, performance measures and standards, with a view of examining its potential to be incorporated in the research proposal. Building upon this, an exhaustive literature survey of the existing research in the domain of multibiometric continuous and transparent authentication was achieved.
- Exploring aspects of the research problem that the literature has not addressed related to end-users' perceptions and attitudes towards security, privacy and usability in order to assess the acceptability of such a proposal. It also included investigating their perceptions and satisfaction of associated current and alternative authentication approaches alongside their usability. Moreover, it sought to analyse users' awareness and attitudes towards related privacy issues.
- Developing a biometric data capturing software sought to create a real dataset of a significant number of real users for a significant period of time of real usage in totally uncontrolled conditions, aiming at employing it in the research experiments. Forty-seven subjects were recruited and their usage data was collected over 2-week period.

- Modelling and undertaking a baseline set of experiments to understand the nature of transparent biometrics and soft biometric data and to determine their potential contribution to the system performance.
- Modelling and replicating NICA framework to validate whether prior TAS models would function on real live user data and what its actual performance is in practice.
- Modelling and developing an enhanced model utilising multibiometric fusion and time windowing within a device, aiming at investigating whether employing a fusion mechanism that encompasses all available biometric samples at a given time-frame is viable in practice and to what degree it improves the performance from the individual unimodal approaches.
- Conducting a series of experiments aiming at evaluating the effectiveness of utilising the Cloud for such a universal authentication approach and seeking to determine whether it is viable, convenient and secure to authenticate users based upon their digital devices activities and other captured biometrics, so that it would be possible to gather a single user profile from the range of devices a single user may use.
- Proposing a novel federated biometric authentication approach addressing the main research gap, thereby shifting the burden of both the authentication processing and management responsibility to a centralised Managed Authentication Service Provider (MASP). Accordingly, an intelligent, modular and holistic *Cloud Aura* architecture was designed enhancing system security, user-friendliness, and universality that will operate in a location, service, and technology independent fashion.
- Developing a functional proof of concept prototype exemplifying the federated Cloud Aura authentication framework to have a tangible understanding of how such an approach would function in practice.

A number of papers related to the research programme have been presented and published in refereed journal and conferences (provided in Appendix A). As a result, the research is deemed having made positive contributions to the field of user authentication, and specifically in biometric identity verification domain.

8.2 Limitations of the Research

Whilst the objectives of this research have been met, a number of issues have arisen, which may have imposed limitations upon the work progress and findings in one way or another. The key limitations of the research are followed:

- There was insufficient data on hand that can be analysed to show the effect of unifying a user's profile from multiple devices. This was due to the difficulty encountered finding participants with multiple devices operating the Android platform and willing to partake in the data collection experiment. Thus, it is arguably envisaged that actually with a larger and better dataset, the advantage of having the cloud-based authentication solution would increase beyond what was experimentally shown.
- The lack of available open source biometric classifiers that accept the nature of the collected data. Thus and due to the scope of this research, published EERs from the prior literature were used as inputs in the experimental packages.
- The experiments concerned multibiometric fusion did not utilise the best fusion approach (i.e. matching level fusion). However, the decision level fusion approach was used because it is the most appropriate one for the available information of the captured dataset and it also has the merit of encompassing any number of classifiers without the need to re-train the system. Therefore, the study and the results might be even further improved if that extra information from matching systems would be utilised.

- The prototype's dashboard was hosted on a web-service. Developing a trusted cloud platform from which the fully operational Cloud Aura prototype will work would have provided a better insight about the effectiveness of utilising the Cloud for such a universal authentication and would have permitted evaluating specialised operational aspects required for a successful authentication mechanism, such as scalability and response time.
- The prototype was not evaluated with users in real life. It is desirable to conduct a series of scenario-based evaluations involving a number of stakeholders to appraise the practical usefulness of the proposed approach. However, it is argued that having already established the empirical feasibility investigation and analysis on real data has been useful and provided a fair insight about the performance.

Despite these aforementioned limitations, the research is believed to made valid contributions to knowledge and provided sufficient proof of concept for the ideas proposed.

8.3 Scope for Future Work

This research programme has advanced the field of user authentication in general and biometrics-based identity verification in particular. However, a number of areas of scope for future work exist, specifically related to this research. These suggestions are detailed below:

- The presented Cloud Aura agents are sending information, containing user specific data such as usage data and other arguably personal biometric features to a central managed authentication service provider. This research assumes that the Cloud Aura user trusts the cloud provider (offering the MASP) to handle this data reliably. However, this introduces privacy issues, which would not be tolerable for a real world implementation. Therefore, despite specialised measures have been suggested in the architecture, further practical consideration should be addressed in any future

enhancement. Moreover, more work is needed on securing the storage of biometrics-based information to reduce the privacy concern about centralising such information.

- While the proposed architecture proves to be plausible, it is not possible to fully appreciate its functionalities, including decision accuracy, response time and processing sophistication, unless it is thoroughly examined under various threat and attack vectors. Further experiments to assess impostor scenarios with real users could be beneficial.
- Further research could be sought to develop a number of applications that are capable of operating on various platforms, hardware capabilities and operating systems comprising smartphones, phablets, tablets and PCs/laptops to examine the prototype functionalities across deferring technologies, upon which expanded attributes of Cloud Aura would be identified and/or refined for further development.
- Developing a trusted cloud environment from which the fully operational Cloud Aura prototype will work is envisaged to provide a better insight about the effectiveness of utilising the Cloud for such a universal authentication and to enable evaluating specialised operational aspects required for a successful authentication mechanism, such as scalability and response time.

8.4 The Future of User Authentication

With the technology penetrating today's societies, the use of digital devices that have a wide range of capabilities is prevailing. Smartphones are capable of making telephone calls, texting, surfing the Internet, checking emails, playing games, viewing documents, transferring money, shopping online and storing confidential information (to name but a few of the tasks available!). This leads individuals, corporations and governments to rely heavily and prevalently on computing systems (i.e. PCs, servers, laptops, phablet, tablets and

smartphones) for accessing, storing and processing personal, financial, medical and business information that are often considered sensitive and confidential. Unfortunately, these activities, services and information are the targets of cybercrimes.

Authentication is a key security control for any of these computing systems. However, user authentication is traditionally poorly served, with existing implementations falling foul of a variety of weaknesses and, arguably, have not adequately advanced proportionally with the advancement of digital devices technologies as well as users requirements in providing a robust and usable solution. Biometrics has permeated and been integrated in the mainstream ubiquitous verification of digital devices, such as laptops and smartphones, and service providers, such as banks. Notwithstanding, still the majority of them also operate merely at the point-of-entry, providing little consideration to on-going identity confidence, leaving the system susceptible to misuse afterwards.

Research has suggested novel approaches to overcome these downsides without compromising the users' convenience by continuously and transparently authenticating the user throughout. However, the overwhelming majority of them merely focus upon individual platforms rather than providing a universal and federated authentication approach that can be used across technologies and services. The advent of cloud computing, its universal connectivity, scalability and flexibility, offers a new opportunity of achieving convenient authentication seamlessly in a technology and service independent fashion. The *Cloud Aura* approach proposed in this research capitalises upon these features to tackle the open issues of prior studies thereby introducing a new dedicated authentication provider – the MASP – that is able to provide state-of-the-art intelligent centralised verification of authenticity.

The future of user authentication implementations will have to consider seamless adaptation to include the evolution of wearables (e.g. smart glasses and watches) in particular and the

Internet of Things technologies in general. This would enable constructing richer user profiles, thus making more well-informed continuous and transparent context-aware verification decisions. The federated authentication will also need to give extra consideration to the Bring-Your-Own-Device trend, with which a user should be authenticated to access the organisation's assets through their personal devices.

References

[1] 3GPP. (2001). Universal Mobile Telecommunications System (UMTS); 3G security; Security threats and requirements. In 3GPP TS 21.133 version 4.1.0 Release 4. ETSI 3rd Generation Partnership Project (3GPP).

[2] Abaza, A., Ross, A., Hebert, C., Harrison, M. A. F., & Nixon, M. S. (2013). A survey on ear biometrics. ACM Computing Surveys, 45(2), 1–35.

[3] Abdullah, M., Bashier, H., Sayeed, S., Yusof, I., Azman, A., Ibrahim, S. Z., & Liew, T. H. (2014). Answering Incoming Call for Implicit Authentication Using Smartphone. Journal of Theoretical & Applied Information Technology, 61(1), 193–199.

[4] Acuity Market Intelligence. (2017). Biometric Smartphone Update. Retrieved from http://www.acuity-mi.com/BSP.php

[5] Ahmed, A. A. E., & Traore, I. (2007). A New Biometric Technology Based on Mouse Dynamics. IEEE Transactions on Dependable and Secure Computing, 4(3), 165–179.

[6] Ahmed, A., & Traore, I. (2005). Anomaly intrusion detection based on biometrics. In Proceedings of the 2005 IEEE Workshop on Information Assurance and Security (pp. 452–453). IEEE.

[7] Aksari, Y., & Artuner, H. (2009). Active authentication by mouse movements. In ISCIS 2009. 24th International Symposium on Computer and Information Sciences, 2009 (pp. 571–574). IEEE.

[8] Alonso-Fernandez, F., Fierrez, J., Martinez-Diaz, M., & Ortega-Garcia, J. (2009). Fusion of static image and dynamic information for signature verification. In 16th IEEE International Conference on Image Processing (ICIP) (pp. 2725–2728).

[9] Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. In 2009 IEEE/ACS International Conference on Computer Systems and Applications (pp. 641–644). IEEE.

[10] Altinok, A., & Turk, M. (2003). Temporal Integration for Continuous Multimodal Biometrics. In Multimodal User Authentication.

[11] Apple. (2014). iPhone 5s - Technical Specifications. Retrieved November 8, 2014, from https://www.apple.com/uk/iphone-5s/specs/

[12] Apple. (2017). Use Touch ID on iPhone and iPad. Retrieved February 16, 2017, from https://support.apple.com/en-gb/HT201371

[13] Arbab-Zavar, B., & Nixon, M. S. (2011). On guided model-based analysis for ear biometrics. Computer Vision and Image Understanding, 115(4), 487–502.

[14] Asha, S., & Chellappan, C. (2008). Authentication of e-learners using multimodal biometric technology. In International Symposium on Biometrics and Security Technologies, 2008. ISBAST 2008. (pp. 1–6). IEEE.

[15] Aupy, A., & Clarke, N. (2005). User Authentication by Service Utilisation

Profiling. In Proceedings of the ISOneWorld 2005. Las Vegas, USA.

[16] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge Attacks on Smartphone Touch Screens. In Proceedings of the 4th USENIX conference on Offensive technologies. WOOT'10.

[17] Azzini, A., & Marrara, S. (2008). Impostor Users Discovery Using a Multimodal Biometric Continuous Authentication Fuzzy System. Knowledge-Based Intelligent Information and Engineering Systems, 5178(2008), 371–378.

[18] Bailey, K. O., Okolica, J. S., & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. Computers & Security, 43, 77–89.

[19] Banerjee, S., & Woodard, D. (2012). Biometric Authentication and Identification using Keystroke Dynamics: A Survey. Journal of Pattern Recognition Research, 7, 116–139.

[20] Barker, I. (2016). 84 percent of people support eliminating passwords. Retrieved February 15, 2017, from https://betanews.com/2015/08/27/84-percent-of-people-support-eliminating-passwords/

[21] BBC. (2011). Security firm RSA offers to replace SecurID tokens. Retrieved May 5, 2014, from http://www.bbc.co.uk/news/technology-13681566

[22] Beautement, A., & Sasse, M. A. (2010). Gathering Realistic Authentication Performance Data Through Field Trials. In The sixth Symposium On Usability Privacy and Security (SOUPS). Redmond, WA, USA.

[23] Belhumeur, P.N., Hespanha, J.P., Kriegman, D.J.: Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. IEEE Trans. Pattern Anal. Mach. Intell. 19, 711–720 (1997).

[24] Bergadano, F., Gunetti, D., & Picardi, C. (2002). User authentication through keystroke dynamics. ACM Transactions on Information and System Security, 5(4), 367–397.

[25] Biometrics Institute. (2013). Biometrics Institute Industry Survey 2013.

[26] Brown, M., & Rogers, S. (1993). User identification via keystroke characteristics of typed names using neural networks. International Journal of Man-Machine Studies, 39, 999–1014.

[27] Carrillo, C. (2003). Continuous biometric authentication for authorized aircraft personnel: A proposed design. Naval Postgraduate School, Monterey, California.

[28] Ceccarelli, A., Montecchi, L., Brancati, F., Lollini, P., Marguglio, A., & Bondavalli, A. (2014). Continuous and Transparent User Identity Verification for Secure Internet Services. IEEE Transactions on Dependable and Secure Computing, 12(3), 270–283. https://doi.org/10.1109/TDSC.2013.2297709

[29] Chaos Computer Club. (2014). Fingerprint Biometrics hacked again. Retrieved January 12, 2015, from http://www.ccc.de/en/updates/2014/ursel

[30] Charrau, D., Furnell, S., & Dowland, P. (2005). PassImages: An alternative method of user authentication. In Proceedings of the f 4th Annual ISOneWorld Conference

and Convention. Las Vegas, USA.

[31] Chen, R., Lin, X., & Ding, T. (2012). Liveness detection for iris recognition using multispectral images. Pattern Recognition Letters, 33(12), 1513–1519.

[32] Chowdhury, M., Light, J., & McIver, W. (2010). A Framework for Continuous Authentication in Ubiquitous Environments. In Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), IEEE Press (pp. 1–6).

[33] Clarke, N. (2011). Transparent user authentication: biometrics, RFID and behavioural profiling. Springer London.

[34] Clarke, N., & Furnell, S. (2005). Biometrics–The promise versus the practice. Computer Fraud & Security, (September), 12–16.

[35] Clarke, N., & Furnell, S. (2006). A composite user authentication architecture for mobile devices. Journal of Information Warfare, 5(2), 11–29.

[36] Clarke, N., Karatzouni, S., & Furnell, S. (2008). Transparent facial recognition for mobile devices. In Proceedings of the 7th Security Conference. Las Vegas, USA.

[37] Clarke, N., Karatzouni, S., & Furnell, S. (2009). Flexible and Transparent User Authentication for Mobile Devices. In Gritzalis D And Lopez J (Ed.), Emerging Challenges for Security, Privacy and Trust, 24th IFIP TC 11 International Information Security Conference, SEC 2009 (Vol. 297, pp. 1–12). Pafos, Cyprus: Springer.

[38] Clarke, N., Karatzouni, S., & Furnell, S. (2011b). Towards a Flexible, Multi-Level Security Framework for Mobile Devices. In The 10th Security Conference. Las Vegas, USA.

[39] Clarke, N. L. (2004, March). Advanced User Authentication for Mobile Devices. University of Plymouth.

[40] Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones – A survey of attitudes and practices. Computers & Security, 24(7), 519–527.

[41] Clarke, N. L., & Furnell, S. M. (2006). Authenticating mobile phone users using keystroke analysis. International Journal of Information Security, 6(1), 1–14.

[42] Clarke, N. L., & Furnell, S. M. (2007). Advanced user authentication for mobile devices. Computers & Security, 26(2), 109–119.

[43] Clarke, N. L., & Mekala, a. R. (2007). The application of signature recognition to transparent handwriting verification for mobile devices. Information Management & Computer Security, 15(3), 214–225.

[44] Cloud Security Alliance. (2012). Identity and Access Management Implementation Guidance. In Cloud Security Alliance Security as a Service Implementation Guidance Version 1.0 (pp. 1–43). Retrieved from https://cloudsecurityalliance.org/research/secaas

[45] Collins, S. (2014, February 6). The public eye? Retrieved June 13, 2014, from http://www.cam.ac.uk/research/features/the-public-eye

[46] Conrad, E., Misenar, S., & Feldman, J. (2012). CISSP study guide. Elsevier Inc.

[47] Crawford, H., & Renaud, K. (2014). Understanding user perceptions of transparent authentication on a mobile device. Journal of Trust and Management, 1(7), 1–28.

[48] Crawford, H., Renaud, K., & Storer, T. (2013). A framework for continuous, transparent mobile device authentication. Computers & Security, 39, 127–136.

[49] Cryptomathic. (2012). Two-Factor Authentication for Banking: Building the Business Case (No. 1.2). Retrieved from http://www.cryptomathic.com/media/44262/cryptomathic white paper-2fa for banking.pdf

[50] CSID. (2012). Consumer Survey: Password Habits, A study among American consumers. Retrieved June 18, 2013, from http://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf

[51] Cummings, A. H., Nixon, M. S., & Carter, J. N. (2010). A Novel Ray Analogy for Enrolment of Ear Biometrics. In Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on Biometrics Compendium, IEEE. Washington, DC.

[52] Cutting, J., & Kozlowski, L. (1977). Recognizing friends by their walk: Gait perception without familiarity cues. In Bulletin of the psychonomic society.

[53] Daugman, J. (2004). How Iris Recognition Works. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 21–30.

[54] Daugman, J. (2007). New methods in iris recognition. IEEE Transactions on Systems, Man, and Cybernetics - Part B, Cybernetics, 37(5), 1167–75.

[55] Daugman, J. G. (1994). Biometric personal identification system based on iris analysis. US Patent 5,291,560. US Patent.

[56] De Luca, A., Hang, A., Brudy, F., Lindner, C., & Hussmann, H. (2012). Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In The SIGCHI Conference on Human Factors in Computing Systems, CHI 2012 (pp. 987–996). Austin, Texas, USA.

[57] de Oliveira, A. E., Henrique Matos Bezerra Motta, G., & Vidal Batista, L. (2010). A multibiometric access control architecture for continuous authentication. In 2010 IEEE International Conference on Intelligence and Security Informatics (pp. 171–171). IEEE.

[58] de Oliveira, A. E., & Motta, G. H. M. B. (2011). A Security API for Multimodal Multi-biometric Continuous Authentication. In 2011 Seventh International Conference on Computational Intelligence and Security (pp. 988–992). IEEE.

[59] Derawi, M. O., Gafurov, D., & Bours, P. (2012). Towards Continuous Authentication Based on Gait Using Wearable Motion Recording Sensors. In I. Traore & A. A. E. Ahmed (Eds.), Continuous Authentication Using Biometrics: Data, Models, and Metrics (pp. 170–192). IGI Global.

[60] Dinesh, T. C. (2012). What the Future of Online Banking Authentication Could Be. Retrieved from http://www.infosys.com/finacle/solutions/thought-papers/Documents/what-the-future-online-banking.pdf

[61] Dowland, P. S., Singh, H., & Furnell, S. M. (2001). A Preliminary Investigation of

User Authentication Using Continuous Keystroke Analysis. In 8th IFIP Annual Working Conference on Information Security Management and Small System Security.

[62] Du, Y., Arslanturk, E., Zhou, Z., & Belcher, C. (2011). Video-Based Noncooperative Iris Image Segmentation. IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, 41(1), 64–74.

[63] Ellis, H., Shepherd, J., & Davies, G. (1979). Identification of familiar and unfamiliar faces from internal and external features: Some implications for theories of face recognition. Perception, 8(4), 431–439.

[64] English, R., & Poet, R. (2011). Towards a metric for recognition-based graphical password security. In 5th International Conference on Network and System Security (NSS), 2011 (pp. 6–8).

[65] European Central Bank. (2013). Recommendations for the Security of Internet Payments - Final Version After Public Consultation. Germany.

[66] Fahmi, P. N. A., Kodirov, E., Choi, D.-J., Lee, G.-S., Mohd Fikri Azli, A., & Sayeed, S. (2012). Implicit authentication based on ear shape biometrics using smartphone camera during a call. In 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 2272–2276). IEEE.

[67] FBI. (2014). Next Generation Identification. Retrieved June 4, 2014, from http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi

[68] Federal Financial Institutions Examination Council. (2005). Authentication in an Internet Banking Environment. Retrieved May 8, 2014, from http://digitallibrary.kcci.com.pk/handle/32417747/701

[69] Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., & Schclar, A. (2012). User identity verification via mouse dynamics. Information Sciences, 201, 19–36.

[70] Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunar, B., Jiang, Y., & Nguyen, N. (2012). Continuous mobile authentication using touchscreen gestures. In 2012 IEEE Conference on Technologies for Homeland Security (HST) (pp. 451–456). IEEE.

[71] Flom, L., & Safir, A. (1987). Iris recognition system. US Patent 4,641,349. US Patent.

[72] Furnell, S. (2005). Authenticating ourselves: will we ever escape the password? Network Security, 2005(2), 8–13.

[73] Furnell, S., & Clarke, N. (2005). Biometrics: no silver bullets. Computer Fraud & Security, 2005(8), 9–14.

[74] Furnell, S. M., Katsikas, S., Lopez, J., & Patel, A. (2008). Securing Information and Communications Systems: Principles, Technologies, and Applications. Artech House.

[75] Furnell, S. M., Morrissey, J. P., Sanders, P. W., & Stockel, C. T. (1996). Applications of keystroke analysis for improved login security and continuous user authentication. In Information systems security (pp. 283–294). London, UK: Chapman & Hall, Ltd.

[76] Gafurov, D., & Snekkenes, E. (2009). Gait Recognition Using Wearable Motion Recording Sensors. EURASIP Journal on Advances in Signal Processing, 2009(1), 415817.

[77] Gaines, R., Lisowski, W., Press, S., & Shapiro, N. (1980). Authentication by Keystroke Timing: Some Preliminary Results. In RAND CORP SANTA MONICA CA (No. RAND-R-2526-NSF) (pp. 1–51).

[78] Galbally, J., Ortiz-lopez, J., Fierrez, J., & Ortega-garcia, J. (2012). Iris Liveness Detection Based on Quality Related Features. In 2012 5th IAPR International Conference on Biometrics Compendium, IEEE Biometrics (ICB) (pp. 271–276). IEEE.

[79] Gamboa, H., & Fred, A. (2004). A behavioral biometric system based on human-computer interaction. In Defense and Security, International Society for Optics and Photonics (pp. 381–392).

[80] Gambs, S., Killijian, M.-O., & Cortez, M. N. del P. (2012). Next Place Prediction using Mobility Markov Chains. In Proceedings of the First Workshop on Measurement, Privacy, and Mobility (pp. 1–6). Bern, Switzerland: ACM.

[81] Gejibo, S. H. (2015). Towards a Secure Framework for mHealth A Case Study in Mobile Data Collection Systems. University of Bergen.

[82] Gigya. (2016). Death of the Password. Retrieved from https://www.gigya.com/resource/whitepaper/death-of-the-password/

[83] Goode Intelligence. (2011). Mobile Phone Biometric Security – Analysis and Forecasts 2011–2015. Retrieved from http://www.goodeintelligence.com/report-store/view/mobile-phone-biometric-security-analysis-and-forecasts-20112015

[84] Google. (2014). Install Google Authenticator. Retrieved November 5, 2014, from https://support.google.com/accounts/answer/1066447?hl=en

[85] Grenga, A. J. (2014). Anroid Based Behavioral Biometric Authentication via Multi-Modal Fusion. Air University.

[86] Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. IEEE Security & Privacy Magazine, 9(2), 50–57.

[87] GSMA. (2016). GSMA Mobile Economy 2016. Retrieved February 6, 2017, from http://www.gsma.com/mobileeconomy/

[88] Guiding Tech. (2016). 5 Additional Uses of Samsung Galaxy S7's Fingerprint Sensor. Retrieved February 16, 2017, from http://www.guidingtech.com/57450/more-uses-galaxy-s7-fingerprint-sensors/

[89] Gunetti, D., & Picardi, C. (2005). Keystroke analysis of free text. ACM Transactions on Information and System Security, 8(3), 312–347.

[90] Guse, D. (2011). Gesture-based User Authentication on Mobile Devices using Accelerometer and Gyroscope. Berlin Institute of Technology.

[91] Hayashi, E., Riva, O., Strauss, K., Brush, A. J. B., & Schechter, S. (2012). Goldilocks and the Two Mobile Devices: Going Beyond All-or-Nothing Access to a Device's Applications. In Proceedings of the Eighth Symposium On Usable

Privacy and Security (SOUPS) 2012.

[92] He, D., Kumar, N., Khan, M. K., Wang, L., & Shen, J. (2016). Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services. IEEE Systems Journal, PP(99), 1–11.

[93] Hempstalk, K. (2009). Continuous typist verification using machine learning. The University of Waikato, New Zealand.

[94] Herland, K. (2015). Information security risk assessment of smartphones using Bayesian networks. Aalto University.

[95] Hocking, C. G., Furnell, S. M., Clarke, N. L., & Reynolds, P. L. (2011). Authentication Aura - A distributed approach to user authentication. Journal of Information Assurance and Security, 6(2), 149–156.

[96] Hocking, C. G., Furnell, S. M., Clarke, N. L., & Reynolds, P. L. (2013). Co-operative user identity verification using an Authentication Aura. Computers & Security, 39, 486–502.

[97] Hossain, M., Balagani, K. S., & Phoha, V. V. (2012). New impostor score based rejection methods for continuous keystroke verification with weak templates. In 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS) (pp. 251–258).

[98] HP. (2014). HP Notebook PCs - Using Fingerprint Reader to Login to Applications and Web Sites. Retrieved June 13, 2014, from http://h20566.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay

[99] HSBC Bank plc. (2014). Secure Key: two-factor authentication | HSBC UK. Retrieved November 5, 2014, from http://www.hsbc.co.uk/1/2/customer-support/online-banking-security/secure-key

[100] HSBC News and Media. (2016). HSBC and first direct bring biometric banking to the mainstream.

[101] Huntington, G. (2012). Using Voice and Other Biometrics - User Friendly Authentication and Authorization Architecture. Retrieved from http://www.authenticationworld.com/Papers/Creating a User Friendly Authentication and Authorization Architecture.pdf

[102] Hurley, D., Nixon, M., & Carter, J. (2000). Automatic ear recognition by force field transformations. In IEE Colloquium on Visual Biometrics (Ref.No. 2000/018) (pp. 2–6). London: IET.

[103] Iannarelli, A. (1989). Ear identification. Freemont, CA: Paramont Pub; Revised edition. Retrieved from http://www.amazon.co.uk/Ear-Identification-Forensic-Series/dp/0962317802

[104] IDC. (2014). A Future Fueled by Phablets. Retrieved November 11, 2014, from http://www.idc.com/getdoc.jsp?containerId=prUS25077914

[105] IDC. (2016). IDC: Smartphone OS Market Share 2016 Q2. Retrieved December 4, 2016, from http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[106] Islam, S., Davies, R., Mian, A. S., & Bennamoun, M. (2008). A Fast and Fully

Automatic Ear Recognition Approach Based on 3D Local Surface Features. Advanced Concepts for Intelligent Vision Systems, Lecture Notes in Computer Science, 5259(2008), 1081–1092.

[107] ISO. (2006a). ISO/IEC 19784-1:2006 - Information technology - Biometric application programming interface - Part 1: BioAPI specification. Retrieved October 14, 2013, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33922

[108] ISO. (2006b). ISO/IEC 19785-1:2006 - Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification. Retrieved October 14, 2013, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41047

[109] ISO. (2011). ISO/IEC 19794-1:2011 - Information technology - Biometric data interchange formats - Part 1: Framework. Retrieved October 14, 2013, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50862

[110] Itani, W., Kayssi, A., & Chehab, A. (2009). Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 711–716.

[111] Jain, A. K., Bolle, R., & Pankanti, S. (2002). Biometrics: Personal Identification in Networked Society. Kluwer Academic Publisherss.

[112] Jain, A. K., Flynn, P., & Ross, A. A. (2008). Handbook of Biometrics. Springer.

[113] Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. Pattern Recognition, 38(12), 2270–2285.

[114] Jakobsson, M., Shi, E., Golle, P., & Chow, R. (2009). Implicit authentication for mobile devices. In the 4th USENIX conference on Hot topics in security, HotSec'09.

[115] Janakiraman, R., Kumar, S., & Sim, T. (2005). Using Continuous Face Verification to Improve Desktop Security. In 2005 Seventh IEEE Workshops on Applications of Computer Vision (WACV/MOTION'05) - Volume 1 (pp. 501–507). IEEE.

[116] Jorgensen, Z., & Yu, T. (2011). On mouse dynamics as a behavioral biometric for authentication. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (pp. 476–482). New York, NY, USA: ACM.

[117] Joyce, R., & Gupta, G. (1990). Identity Authentication Based on Keystroke Latencies. Communications of the ACM, 33(2), 168–176.

[118] JTC 1/SC 37. (2013). BUSINESS PLAN FOR JTC 1/SC 37 "BIOMETRICS" for the PERIOD COVERED: October 2012 - September 2013.

[119] Juefei-Xu, F., Bhagavatula, C., Jaech, A., Prasad, U., & Savvides, M. (2012). Gait-id on the move: pace independent human identification using cell phone accelerometer dynamics. In 2012 IEEE Fifth International Conference on

Biometrics: Theory, Applications and Systems (BTAS) (pp. 8–15). Arlington, VA: IEEE.

[120] Kale, A., Rajagopalan, A. N., Cuntoor, N., & Kruger, V. (2002). Gait-based Recognition of Humans Using Continuous HMMs. In Proceedings of the Fifth IEEE International Conference on Automatic Face and Gesture Recognition (FGRí02) (pp. 1–6). IEEE.

[121] Kang, H.-B., & Ju, M.-H. (2006). Multi-modal Feature Integration for Secure Authentication. In D.-S. Huang, K. Li, & G. W. Irwin (Eds.), Proceedings of the 2006 international conference on Intelligent Computing (Vol. 4113, pp. 1191–1200). Berlin, Heidelberg: Springer Berlin Heidelberg.

[122] Karatzouni, S. (2014). Non-Intrusive Continuous User Authentication for Mobile Devices. Plymouth University.

[123] Karatzouni, S., & Clarke, N. (2007). Keystroke analysis as an authentication method for thumb-based keyboards on mobile handsets. In Advances in Network & Communication Engineering 4 (pp. 213–221).

[124] Karatzouni, S., Clarke, N. L., & Furnell, S. M. (2007). Device- versus Network-Centric Authentication Paradigms for Mobile Devices: Operational and Perceptual Trade-Offs. In 5th Australian Information Security Management Conference (pp. 1–13). Mount Lawley, Australia.

[125] Khan, M. K., Tsai, P.-W., Pan, J.-S., & Liao, B.-Y. (2011). Biometric Driven Initiative System for Passive Continuous Authentication. In 7th International Conference on Information Assurance and Security (IAS), 2011 (pp. 139–144). IEEE.

[126] Kisku, D. R., Gupta, P., Sing, J. K., Tistarelli, M., & Hwang, C. J. (2012). Low Level Multispectral Palmprint Image Fusion for Large Scale Biometrics Authentication. In I. Traore & A. A. E. Ahmed (Eds.), Continuous Authentication Using Biometrics: Data, Models, and Metrics (pp. 89–104). IGI Global.

[127] Kittler, J., Hatef, M., Duin, R. P. W., & Matas, J. (1998). On Combining Classifiers. IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3), 226–239.

[128] Klosterman, A., & Ganger, G. (2000). Secure continuous biometric-enhanced authentication. In Technical Report CMU-CS-00- 134, Carnegie Mellon University. Retrieved from http://repository.cmu.edu/compsci/2113/

[129] Koundinya, P., Theril, S., Feng, T., Prakash, V., Bao, J., & Shi, W. (2014). Multi resolution touch panel with built-in fingerprint sensing support. In Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014 (pp. 1–6). New Jersey: IEEE Conference Publications.

[130] Kunz, M., Kasper, K., Reininger, H., Möbius, M., & Ohms, J. (2011). Continuous Speaker Verification in Realtime. In Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, BIOSIG 2011 (pp. 79–88).

[131] Kurkovsky, S., & Syta, E. (2010). Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. In 2010 IEEE International Symposium on Technology and Society (pp. 441–449). IEEE.

[132] Kwang, G., Yap, R. H., Sim, T., & Ramnath, R. (2009). A usability study of continuous biometrics authentication. In M. Tistarelli & M. S. Nixon (Eds.), Proceedings of the Third International Conference on Advances in Biometrics (Vol. 5558, pp. 828–837). Berlin, Heidelberg: Springer Berlin Heidelberg.

[133] Ledermuller, T., & Clarke, N. L. (2011). Risk Assessment for Mobile Devices. In Proceedings of Privacy and Security in Digital Business – 8th International Conference, TrustBus 2011 (pp. 210–221). Toulouse, France: LNCS (LNCS6863).

[134] Leggett, J., & Williams, G. (1988). Verifying identity via keystroke characteristics. International Journal of Man-Machine Studies, 28(1), 67–76.

[135] Li, F. (2012). Behaviour Profiling for Mobile Devices. University of Plymouth.

[136] Li, F., Clarke, N., Papadaki, M., & Dowland, P. (2011). Behaviour Profiling for Transparent Authentication for Mobile Devices. In the 10th European Conference on Information Warfare and Security (ECIW 2011) (pp. 307–314). Tallinn, Estonia.

[137] Li, F., Wheeler, R., & Clarke, N. (2014). An Evaluation of Behavioural Profiling on Mobile Devices. In Proceedings of the Second International Conference HAS (Vol. 8533, pp. 330–339). Heraklion, Crete, Greece: Human Aspects of Information Security, Privacy, and Trust.

[138] Lin, C., Chang, C., & Liang, D. (2012). A New Non-intrusive Authentication Approach for Data Protection Based on Mouse Dynamics. In 2012 International Symposium on Biometrics and Security Technologies (pp. 9–14). IEEE.

[139] Liu, X., & Chen, T. (2003). Video-based face recognition using adaptive hidden markov models. In Proceedings of the 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'03). IEEE.

[140] Lloyds Bank. (2014). Lloyds Bank - Internet Banking - How to log on - Help logging on. Retrieved November 8, 2014, from http://www.lloydsbank.com/online-banking/logging-on.asp?WT.ac=SNOBLO1012

[141] Lu, H., Huang, J., Saha, T., & Nachman, L. (2014). Unobtrusive gait verification for mobile phones. In Proceedings of the 2014 ACM International Symposium on Wearable Computers - ISWC '14 (pp. 91–98). New York, New York, USA: ACM Press.

[142] Macworld. (2014). Take the pain out of two-factor authentication with an app. Retrieved January 8, 2015, from http://www.macworld.com/article/2840979/take-the-pain-out-of-two-factor-authentication-with-an-app.html

[143] Madsen, P., Koga, Y., & Takahashi, K. (2005). Federated identity management for protecting users from ID theft. In Proceedings of the 2005 workshop on Digital identity management - DIM '05 (pp. 77–83). New York, New York, USA: ACM Press.

[144] Mahar, D., Napier, R., Wagner, M., Laverty, W., Henderson, R., & Hiron, M. (1995). Optimizing digraph-latency based biometric typist verification systems: inter and intra typist differences in digraph latency distributions. International Journal of Human-Computer Studies, 43, 579–592.

[145] Mahbub, U., Sarkar, S., Patel, V. M., & Chellapa, R. (2016). Active User Authentication for Smartphones: A Challenge Data Set and Benchmark Results. In

8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS) (pp. 1–8). IEEE.

[146] Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2009). Handbook of fingerprint recognition (Second Edi). London, UK: Springer.

[147] Mäntyjärvi, J., Lindholm, M., Vildjiounaite, E., Mäkelä, S.-M., & Ailisto, H. (2005). Identifying users of portable devices from gait pattern with accelerometers. In Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005. (pp. 973–976). IEEE.

[148] Markets and Markets. (2014). Next Generation Biometric Market – By Technology, Function, Application, & Geography (2014-2020).

[149] Markets and Markets. (2016). Biometric System Market worth 32.73 Billion USD by 2022. Press Releases. Retrieved from http://www.marketsandmarkets.com/PressReleases/biometric-technologies.asp

[150] Marsters, J. (2009). Keystroke dynamics as a biometric. University of Southampton.

[151] Martucci, L. a., Zuccato, A., Smeets, B., Habib, S. M., Johansson, T., & Shahmehri, N. (2012). Privacy, Security and Trust in Cloud Computing: The Perspective of the Telecommunication Industry. In 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing (UIC/ATC), 2012 (pp. 627–632). IEEE.

[152] Matey, J. R., Naroditsky, O., Hanna, K., Kolczynski, R., LoIacono, D. J., Mangru, S., … Zhao, W. Y. (2006). Iris on the Move: Acquisition of Images for Iris Recognition in Less Constrained Environments. Proceedings of the IEEE, 94(11), 1936–1947.

[153] Mears, J. C. (2013). The Current and Future Applications of Biometric Technologies.

[154] Meeker, M., & Wu, L. (2013). 2013 Internet Trends. Retrieved June 18, 2013, from http://www.kpcb.com/insights/2013-internet-trends

[155] Messerman, A., Mustafic, T., Camtepe, S. A., & Albayrak, S. (2011). Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics. In 2011 International Joint Conference on Biometrics Compendium, IEEE Biometrics (IJCB) (pp. 1–8). IEEE.

[156] Microsoft. (2014). Features of Windows 8.1 - Microsoft Windows. Retrieved November 8, 2014, from http://windows.microsoft.com/en-gb/windows-8/features#personalize=startscreen

[157] Mock, K., Hoanca, B., Weaver, J., & Milton, M. (2012). Real-time continuous iris recognition for authentication using an eye tracker. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 1007–1009). ACM.

[158] Mogull, R. (2013, September). The iPhone 5s fingerprint reader: what you need to know. Retrieved June 13, 2014, from http://www.macworld.com/article/2048514/the-iphone-5s-fingerprint-reader-what-you-need-to-know.html

[159] Mondal, S., & Bours, P. (2013). Continuous authentication using mouse dynamics. In 2013 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1–12). IEEE.

[160] Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems, 16(4), 351–359.

[161] Moren, D. (2015). Face Recognition Security, Even With A "Blink Test," Is Easy To Trick. Retrieved February 16, 2017, from http://www.popsci.com/its-not-hard-trick-facial-recognition-security

[162] Morris, S. (2004). A shoe-integrated sensor system for wireless gait analysis and real-time therapeutic feedback. Massachusetts Institute of Technology. Retrieved from http://www.media.mit.edu/resenv/pubs/theses/sjmorrisSCDthesis.pdf

[163] Muaaz, M. (2013). A Transparent and Continuous Biometric Authentication Framework for User-Friendly Secure Mobile Environments. In The 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2013 Adjunct) (pp. 4–7). Zurich, Switzerland: ACM.

[164] Nanavati, S., Thieme, M., & Nanavati, R. (2002). Biometrics: Identity Verification in a Networked World. John Wiley & Sons, Inc.

[165] National Science and Technology Council. (2011). The National Biometrics Challenge 2011. Retrieved June 3, 2014, from http://biometrics.gov/Documents/BiometricsChallenge2011_protected.pdf

[166] NatWest. (2014). NatWest personal banking | Online banking. Retrieved November 8, 2014, from http://www.natwest.com/personal/online-banking/g1/banking-safely-online/card-reader.ashx

[167] Nelson, D., Reed, V., & Walling, J. (1976). Pictorial superiority effect. Journal of Experimental Psychology: Human Learning and Memory, 2(5), 523–528.

[168] Nickel, C., Wirtl, T., & Busch, C. (2012). Authentication of Smartphone Users Based on the Way They Walk Using k-NN Algorithm. In 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 16–20). IEEE.

[169] Niinuma, K., Park, U., & Jain, A. K. (2010). Soft Biometric Traits for Continuous User Authentication. IEEE Transactions on Information Forensics and Security, 5(4), 771–780.

[170] NIST. (2008). NIST/ITL Conformance Test Suite for Patron Format A Data Structures Specified in ANSI INCITS 398-2008, Common Biometric Exchange Formats Framework (CBEFF). Retrieved September 29, 2014, from http://www.nist.gov/itl/csd/biometrics/biocbeff_background.cfm

[171] NSTC. (2006a). Biometrics Overview. Subcommittee on Biometrics, National Science and Technology Council (NSTC), 1–10.

[172] NSTC. (2006b). Palm Print Recognition. Subcommittee on Biometrics, National Science and Technology Council (NSTC), 1–10.

[173] NSTC. (2006c). Speaker Recognition. Subcommittee on Biometrics, National Science and Technology Council (NSTC), 1–10.

[174] O'Boyle, B. (2014, April). How does the Samsung Galaxy S5 fingerprint scanner work? Retrieved June 13, 2014, from http://www.pocket-lint.com/news/127605-how-does-the-samsung-galaxy-s5-fingerprint-scanner-work

[175] O'Gorman, L. (2003). Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, 91(12), 2021–2040.

[176] Obaidat, M. S., & Sadoun, B. (1997). Verification of Computer Users Using Keystroke Dynamics. IEEE Transactions on Systems, Man, and Cybernetics. Part B, Cybernetics : A Publication of the IEEE Systems, Man, and Cybernetics Society, 27(2), 261–9.

[177] Office of National Statistics. (2013). Internet Access - Households and Individuals, 2013. Statistical Bulletin, (August). Retrieved from http://www.ons.gov.uk/ons/dcp171778_322713.pdf

[178] Ojala, S., Keinanen, J., & Skytta, J. (2008). Wearable Authentication Device for Transparent Login in Nomadic Applications Environment. In 2nd International Conference on Signals, Circuits and Systems (pp. 1–6).

[179] Onin. (2014). The History of Fingerprints. Retrieved September 25, 2014, from http://onin.com/fp/fphistory.html

[180] Oorschot, P. van, & Thorpe, J. (2011). Exploiting Predictability in Click-based Graphical Passwords. Journal of Computer Security, 19(4), 669–702.

[181] Passfaces. (2007). Passfaces Personal Version 1.0. Retrieved May 4, 2014, from http://www.passfaces.com/personal/support/helpmanual.htm

[182] Podio, F. (2011). Published International Biometric Standards Developed by ISO/IEC JTC 1/SC 37 – Biometrics and Adopted by INCITS as INCITS/ISO/IEC Standards.

[183] Proença, H., & Alexandre, L. (2006). Iris segmentation methodology for non-cooperative recognition. IEE Proceedings - Vision, Image and Signal Processing, 153(2), 199–205.

[184] Pusara, M. (2007). An Examination of User Behavior for User Re-authentication. ProQuest.

[185] Pusara, M., & Brodley, C. E. (2004). User re-authentication via mouse movements. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security - VizSEC/DMSEC '04 (pp. 1–8). New York, New York, USA: ACM Press.

[186] PwC. (2012). Consumer privacy: What are consumers willing to share? Retrieved from http://www.pwc.ru/en_RU/ru/retail-consumer/publications/assets/pwc-consumer-privacy-and-information-sharing.pdf

[187] PwC. (2013). Information Security Breaches Survey 2013.

[188] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011(1), 3. https://doi.org/10.1186/1687-417X-2011-3

[189] Riva, O., Qin, C., Strauss, K., & Lymberopoulos, D. (2012). Progressive

authentication: deciding when to authenticate on mobile phones. In The 21st USENIX Security Symposium.

[190] Rodwell, P. M. (2006). Non-Intrusive Subscriber Authentication for Next Generation Mobile Communication Systems. University of Plymouth.

[191] Ross, A. (2007). An Introduction to Multibiometrics. In the 15th European Signal Processing Conference (EUSIPCO) (pp. 20–24). Poznan, Poland.

[192] Ross, A. (2011). Advances in Ear Biometrics.

[193] Ross, A., Nandakumar, K., & Jain, A. (2006). Handbook of multibiometrics (1st ed., Vol. 6). New York, New York, USA: Springer.

[194] Roth, J., Liu, X., & Metaxas, D. (2014). On Continuous User Authentication via Typing Behavior. IEEE TRANSACTIONS ON IMAGE PROCESSING, 23(10), 4611–4624.

[195] Roy, S., & Biswas, A. (2011). A Personal Biometric Identification Technique based on Iris Recognition. (IJCSIT) International Journal of Computer Science and Information Technologies, 2(4), 1474–1477.

[196] Saevanee, H. (2014). Continuous User Authentication Using Multi-Modal Biometrics. Plymouth University.

[197] Saevanee, H., & Bhatarakosol, P. (2008). User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device. In 2008 International Conference on Computer and Electrical Engineering (pp. 82–86). IEEE.

[198] Saevanee, H., Clarke, N., & Furnell, S. (2011). SMS linguistic profiling authentication on mobile device. In 2011 5th International Conference on Network and System Security (pp. 224–228). IEEE.

[199] Saevanee, H., Clarke, N., Furnell, S., & Biscione, V. (2014). Text-Based Active Authentication for Mobile Devices. IFIP Advances in Information and Communication Technology, ICT Systems Security and Privacy Protection, 428(1), 99–112.

[200] Saevanee, H., Clarke, N. L., & Furnell, S. M. (2012). Multi-Modal Behavioural Biometric Authentication for Mobile Devices. In 27th IFIP International Information Security and Privacy Conference (SEC2012) (pp. 465–474).

[201] Salesforce. (2014). 2014 Mobile Behavior Report. Retrieved November 17, 2014, from https://www.exacttarget.com/sites/exacttarget/files/deliverables/etmc-2014mobilebehaviorreport.pdf

[202] Samba Financial Group. (2014). SambaOnline Banking – Ways To Bank. Retrieved November 8, 2014, from http://www.samba.com/en/personal-banking/ways-to-bank/samba-online.html

[203] Samsung. (2014). Samsung Galaxy S5 (Black) - Review, Specs & Features - Samsung UK. Retrieved November 8, 2014, from http://www.samsung.com/uk/consumer/mobile-devices/smartphones/android/SM-G900FZKABTU

[204] Sandhu, S. (2004). Single Sign On Concepts & Protocols. Retrieved March 26, 2014, from https://www.sans.org/reading-room/whitepapers/authentication/single-sign-concepts-protocols-1352

[205] Schouten, B., & Jacobs, B. (2009). Biometrics and their use in e-passports. Image and Vision Computing, 27(3), 305–312.

[206] Senk, C., Obergrusberger, F., & Bartmann, D. (2014). Toward Higher Flexibility of Federated Business Processes with Cloud-based Biometric Authentication Services. Journal of Internet Services and Applications.

[207] Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010). Google android: A comprehensive security assessment. IEEE Security and Privacy, 8(2), 35–44.

[208] Shankdhar, P. (2014). 10 Most Popular Password Cracking Tools. Retrieved December 30, 2014, from http://resources.infosecinstitute.com/10-popular-password-cracking-tools/

[209] Shen, C., Cai, Z., Guan, X., Huilan, I., & Du, J. (2009). Feature Analysis of Mouse Dynamics in Identity Authentication and Monitoring. In IEEE International Conference on Communications, 2009. ICC '09 (pp. 1–5).

[210] Shepherd, S. (1995). Continuous authentication by analysis of keyboard typing characteristics. In European Convention on Security and Detection, 1995 (pp. 111–114). Brighton: IET.

[211] Shrishak, K., Erkin, Z., & Schaar, R. (2016). Enhancing User Privacy in Federated eID Schemes. In 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2016. IEEE.

[212] Sim, T., Zhang, S., Janakiraman, R., & Kumar, S. (2007). Continuous Verification Using Multimodal Biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4), 687–700.

[213] Socolinsky, D., & Selinger, A. (2004). Thermal face recognition in an operational scenario. In the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04) (pp. 1012–1019). IEEE.

[214] Soltane, M., Doghmane, N., & Guersi, N. (2010). Face and Speech Based Multi-Modal Biometric Authentication. International Journal of Advanced Science and Technology, 21(6), 41–56.

[215] Spillane, R. (1975). Keyboard apparatus for personal identification. IBM Technical Disclosure Bulletin, 17(3346).

[216] Stanic, M. (2013). Continuous User Verification Based on Behavioral Biometrics Using Mouse Dynamics. In Proceedings of the ITI 2013 35th International Conference on Information Technology Interfaces (pp. 251–256). Cavtat, Croatia: IEEE.

[217] Statista. (2016). Smartphone users worldwide 2014-2020 | Statistic. Retrieved February 12, 2017, from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[218] Stihler, M., Santin, A. O., Marcon Jr., A. L., & Fraga, J. D. S. (2012). Integral

Federated Identity Management for Cloud Computing. In 2012 5th International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1–5). IEEE.

[219] Stolfo, S. J., Fan, W., Lee, W., Prodromidis, A., & Chan, P. K. (2000). Cost-based modeling for fraud and intrusion detection: Results from the JAM project. In Proceedings of DARPA Information Survivability Conference and Exposition, DISCEX '00. Hilton Head, SC: IEEE.

[220] Sui, Y., Zou, X., Du, E. Y., & Li, F. (2012). Secure and privacy-preserving biometrics based active authentication. In 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 1291–1296). IEEE.

[221] Symantec Corporation. (2013). Internet Security Threat Report 2013, 18(April), 58.

[222] Tanviruzzaman, M., & Ahamed, S. I. (2014). Your Phone Knows You: Almost Transparent Authentication for Smartphones. In 2014 IEEE 38th Annual Computer Software and Applications Conference (pp. 374–383). IEEE.

[223] Tanviruzzaman, M., Ahamed, S. I., Hasan, C. S., & Casey, O. (2009). ePet: When Cellular Phone Learns to Recognize Its Owner. In Proceedings of ACM workshop on assurable & usable security configuration (pp. 13–17).

[224] TeleSign. (2016). Beyond the Password: The Future of Account Security.

[225] Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A Risk Assessment Method for Smartphones. Information Security and Privacy Research, 376, 443–456.

[226] Traore, I., & Ahmed, A. A. E. (2012). Continuous Authentication Using Biometrics: Data, Models, and Metrics. IGI Global.

[227] Traore, I., Woungang, I., Obaidat, M. S., Nakkabi, Y., & Lai, I. (2012). Combining Mouse and Keystroke Dynamics Biometrics for Risk-Based Authentication in Web Environments. In 2012 Fourth International Conference on Digital Home (pp. 138–145). IEEE.

[228] Tsai, P., Khan, M. K., Pan, J., & Liao, B. (2014). Interactive Artificial Bee Colony Supported Passive Continuous Authentication System. IEEE SYSTEMS JOURNAL, IEEE Biometrics Compendium, 8(2), 395–405.

[229] Tsatsoulis, P. D., Jaech, A., Batie, R., & Savvides, M. (2012). Multimodal Biometric Hand-Off for Robust Unobtrusive Continuous Biometric Authentication. In I. Traore & A. A. E. Ahmed (Eds.), Continuous Authentication Using Biometrics: Data, Models, and Metrics (pp. 68–88). IGI Global.

[230] Umphress, D., & Williams, G. (1985). Identity verification through keyboard characteristics. International Journal of Man-Machine Studies, 23(3), 263–273.

[231] Vallabhu, H., & Satyanarayana, R. (2012). Biometric Authentication as a Service on Cloud: Novel Solution. International Journal of Soft Computing and Engineering (IJSCE), 2(4), 163–165.

[232] Vecchiato, D., Vieira, M., & Martins, E. (2016). Risk Assessment of User-Defined Security Configurations for Android Devices. In 2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE) (pp. 467–477). IEEE.

[233] Verizon. (2016). 2016 Data Breach Investigations Report. Verizon Business

Journal, (1), 1–65.

[234] Vildjiounaite, E., Mäkelä, S., Lindholm, M., & Riihimäki, R. (2006). Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices. In Proceedings of the 4th international conference on Pervasive Computing (pp. 187–201). Berlin, Heidelberg: Springer-Verlag.

[235] Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). Biometric Systems: Technology, Design and Performance Evaluation (Vol. 33). Springer-Verlag London Berlin Heidelberg.

[236] Weiss, R., & Luca, A. De. (2008). PassShapes: utilizing stroke based authentication to increase password memorability. In Proceedings of the 5th Nordic conference on n Human-Computer Interaction (pp. 18–22).

[237] White, C. (2013). Windows 8.1 will focus on biometrics for authentication. Retrieved March 24, 2014, from http://www.neowin.net/news/windows-81-will-focus-on-biometrics-for-authentication

[238] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. In Symposium On Usable Privacy and Security (SOUPS) 2005.

[239] Wildes, R. (1997). Iris recognition: an emerging biometric technology. Proceedings of the IEEE, 85(9), 1348–1363.

[240] Woo, R. H., Park, A., & Hazen, T. J. (2006). The MIT Mobile Device Speaker Verification Corpus: Data Collection and Preliminary Experiments. In IEEE Odyssey 2006: The Speaker and Language Recognition Workshop, 2006. (Vol. 0, pp. 1–6). IEEE.

[241] Wood, H. M. (1977). The use of passwords for controlling access to remote computer systems and services. In Proceedings of the June 13-16, 1977, national computer conference on (AFIPS '77) (pp. 27–33). New York, New York, USA: ACM Press.

[242] Woodward, J. D. J., Orlans, N. M., & Higgins, P. T. (2003). Biometrics: Identity Assurance in the Information Age. New York: McGraw Hill/Osborne.

[243] Wu, R. (2011). Ears: The New Fingerprints? Retrieved July 3, 2014, from http://www.yalescientific.org/2011/05/ears-the-new-fingerprints/

[244] Xiao, Q., & Yang, X.-D. (2010). Facial Recognition in Uncontrolled Conditions for Information Security. EURASIP Journal on Advances in Signal Processing, 2010, 1–10.

[245] Yang, K., & Du, E. (2011). A multi-stage approach for non-cooperative iris recognition. In 2011 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 3386–3391). IEEE.

[246] Yazji, S., Chen, X., Dick, R. P., & Scheuermann, P. (2009). Implicit User Re-Authentication for Mobile Devices. In Ubiquitous Intelligence and Computing (pp. 1–15). Springer-Verlag New York Inc.

[247] Zekri, L., & Furnell, S. (2006). Authentication based upon secret knowledge and its resilience to impostors. In Advances in Network & Communication Engineering

3 (pp. 30–38).

[248] Zheng, N., Paloski, A., & Wang, H. (2011). An efficient user verification system via mouse movements. In Proceedings of the 18th ACM conference on Computer and communications security (pp. 139–150). New York, NY, USA: ACM.

Appendices

Appendix A – Publications

1. Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2016). Continuous and transparent multimodal authentication: reviewing the state of the art. *Cluster Computing*, *19*(1), 455–474. https://doi.org/10.1007/s10586-015-0510-4

2. Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2015). Security, privacy and usability – a survey of users' perceptions and attitudes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 9264, pp. 153–168). https://doi.org/10.1007/978-3-319-22906-5_12

3. Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2015). A survey of continuous and transparent multibiometric authentication systems. In *European Conference on Information Warfare and Security, ECCWS* (pp. 1–10).

4. Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2015). The Current Use of Authentication Technologies: An Investigative Review. In *2015 International Conference on Cloud Computing, ICCC 2015*. https://doi.org/10.1109/CLOUDCOMP.2015.7149658

5. Al Abdulwahid, A., Clarke, N., Furnell, S., & Stengel, I. (2013). A Conceptual Model For Federated Authentication in the Cloud. In *Proceedings of the 11th Australian Information Security Management Conference, Edith Cowan University, (AISM2013)* (pp. 1–11). Perth, Western Australia. Retrieved from http://ro.ecu.edu.au/ism/151/

Appendix B – Ethical Approval (User Survey)

From: Paula Simson
Sent: 28 March 2014 09:35
To: Abdulwahid Al Abdulwahid <abdulwahid.alabdulwahid@plymouth.ac.uk>
Subject: RE: ETHICAL APPROVAL

Dear Abdulwahid

Thank you very much for confirming this and sending me your amended application.

I am pleased to confirm that your application has been approved.

Kind regards

Paula

Paula Simson l Secretary to Faculty Human Ethics Committee l Dean's Office l Faculty of Science and Environment l 009 Smeaton l Ext 84503 l email paula.simson@plymouth.ac.uk
Working hours: Monday – Thursday 09.30 – 17.00 Friday 09.30 – 16.30

From: Abdulwahid Al Abdulwahid
Sent: 14 March 2014 15:59
To: Paula Simson
Cc: SciEnv Human Ethics; Nathan Clarke; Gaseb Alotibi
Subject: ETHICAL APPROVAL
Importance: High

Dear Paula,

Please find attached a completed application for Ethical approval that is needed for our survey (a copy is attached) to be conducted this month.

Should you need any further information, please do not hesitate to contact me.

Best Regards,

Abdulwahid Al Abdulwahid

Centre for Security, Communications and Network Research (CSCAN)
School of Computing and Mathematics
Faculty of Science and Environment
University of Plymouth

Office#: A304, Portland Square Building
University of Plymouth, Drake Circus,
Plymouth, PL4 8AA, UK
Office Tel: +44 (0) 1752586287

Appendix C – User Survey Questions and Consent Form

Security, Privacy and Usability – A Survey of Users Perceptions and Attitudes

INFOSECURITY WITH PLYMOUTH UNIVERSITY

Centre for Security, Communications and Network Research (CSCAN)

Users are now in possession of an ever-growing number of advance digital devices (i.e. PCs, servers, laptops, tablets and smartphones) with a wide range of capabilities which are used for accessing, storing and processing personal, financial, medical and business information. Accordingly, each device has its own associated security requirements.

The survey aims to explore users' technology usage and security practices. The survey will also seek to understand the usability of these practices analyses users' awareness and attitude towards privacy.

There are 4 main sections organised as follows:

1. Demographic: Questions relating to age, gender, education and location.

2. Technology Usage (Services and Devices): Establishing an understanding of a person's technology usage.

3. Security Practices and Convenience: Investigating the role and usability of security.

4. Privacy: Analysing respondents' experience and acceptance level of privacy-related topics.

This survey is being conducted for PhD research at Plymouth University, United Kingdom.

Should you have any question about the study or you wish to receive a copy of the results, please contact the researchers via address or emails below:

Researcher's details:

Abdulwahid Al Abdulwahid

Centre for Security, Communications and Network Research (CSCAN)

School of Computing and Mathematics
Plymouth University, Plymouth, PL4 8AA, United Kingdom

E-mails: abdulwahid.alabdulwahid@plymouth.ac.uk

Project Supervisors:

Dr. Nathan Clarke

Prof. Steven Furnell

If you have any concern regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Environment Research Ethics Committee:

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Environment
Plymouth University, Plymouth, PL4 8AA, United Kingdom

Phone:+44 (0)1752584503
E-mail to: paula.simson@plymouth.ac.uk

A note on privacy

This survey is anonymous.

The record kept of your survey responses does not contain any identifying information about you unless a specific question in the survey has clearly asked for this.

All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data.

This survey is designed for adult participation. If you are UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY. Anyone 18 years old or above can take part in the survey and has the right to withdraw up until the final submission of their responses.

If you click 'Next', you confirm that you have read and understood the information given, understand that your are free to withdraw up until the point of submission of your responses, you are 18 years or above, and agree to take part in the study.

Demographic:

1- What is your gender?
   - Male
   - Female

2- What is your age group (in years)?
   - 18-29
   - 30-39
   - 40-49
   - 50-59
   - 60+

3- What is your current employment status:
   - Employed
   - Self-employed
   - Student
   - Other

4- What is your country of residence?

Technology Usage (Services and Devices):

5- How many Internet-enabled devices do you personally use?
   - 1
   - 2
   - 3
   - 4
   - 5
   - 6
   - 7
   - 8

- ○ 9
- ○ 10+

6- Select from the following list the digital devices that you usually use?

- ☐ Windows Desktop/Laptop
- ☐ Mac Desktop/Laptop
- ☐ Linux Desktop/Laptop
- ☐ IPad/ IPad mini/IPod Touch
- ☐ Android Tablet (e.g. Samsung Galaxy Tab/Note)
- ☐ Blackberry Tablet (e.g. BlackBerry PlayBook)
- ☐ Windows Tablet (e.g. Microsoft Surface)
- ☐ IPhone
- ☐ Android Smartphone (e.g. Samsung Galaxy, Sony Xperia, HTC, LG)
- ☐ Blackberry Smartphone
- ☐ Windows Smartphone (e.g. Nokia Lumia, HTC)
- ☐ Other Mobiles
- ☐ Games console (e.g. PlayStation, X-Box, Wii)
- ☐ Smart TV (e.g. LG Smart TV, Panasonic Smart Viera, Samsung Smart TV)
- ☐ Set-Top/IPTV Box (e.g. Apple TV, Samsung STB, Zaap, ATN TV)
- ☐ Other ____

7- Do you use any of the cloud services? (e.g. One/Sky drive, Google drive, Dropbox, iCloud)

- ○ Yes
- ○ No
- ○ Do not know what cloud services are
- ○ I am not sure

8- Which of the following network technologies do you have access to?

- ☐ WiFi (Home)
- ☐ WiFi (Public)
- ☐ Bluetooth
- ☐ 3G/4G
- ☐ Broadband/Fibre Optics
- ☐ Other

9- On average, how long do you spend online a day?

- ○ Never
- ○ 1-25%
- ○ 26-50%
- ○ 51-75%
- ○ 76-99%
- ○ Always connected

10- How frequent do you use the following services? (Select the most appropriate choice for each row) (1= hourly, 2= daily, 3= weekly, 4= monthly, 5= Rarely, N/A)

	1	2	3	4	5	N/A
News websites (e.g. BBC)	○	○	○	○	○	○
Email (e.g. Gmail)	○	○	○	○	○	○

Online banking (e.g. HSBC)	○	○	○	○	○	○
Utility online account (e.g. British Gas)	○	○	○	○	○	○
Online shopping (e.g. Sainsbury, Amazon)	○	○	○	○	○	○
Auction websites (e.g. eBay)	○	○	○	○	○	○
Messaging (e.g. iMessage, WhatsApp)	○	○	○	○	○	○
Social networking (e.g. Facebook, Google+)	○	○	○	○	○	○
Twitter	○	○	○	○	○	○
Internet Telephone (e.g. Skype)	○	○	○	○	○	○
Watching TV, Video (e.g. YouTube, Now TV)	○	○	○	○	○	○
Online Gaming (e.g. Minecraft, Happy Farm)	○	○	○	○	○	○
Mobile Apps (e.g. Apple store, Google Play)	○	○	○	○	○	○
Local Network Access	○	○	○	○	○	○
Corporate Network Access	○	○	○	○	○	○
Others [ ]	○	○	○	○	○	○

Security Practices and Convenience:

11- What kind of security tools or applications do you use in one or more of your digital devices? (Select all that apply)

- ☐ Anti-Virus
- ☐ Firewall
- ☐ Authentication
- ☐ Encryption
- ☐ Software Update
- ☐ Backup
- ☐ Other [ ]

12- What proportion of the services (e.g. email, online banking) and devices you use require you to authenticate (i.e. login)?

- ○ None
- ○ 1-25%
- ○ 26-50%
- ○ 51-75%
- ○ 76-100%

13- On a typical day, how many times do you need to authenticate (login)? (i.e. enter your login credentials to access a service and/or a digital device)

- ○ Never
- ○ Rarely (1-3 times a day)
- ○ Sometimes (4-10 times a day)
- ○ Frequently (11-15 times a day)
- ○ Very Frequent (16-20 times a day)
- ○ Too many to remember

14- Considering your most important account, how frequently do you typically change your password?

- ○ Never
- ○ Every 6 months or more
- ○ Quarterly (Every 3 months)
- ○ Monthly
- ○ Weekly

15- Amongst your accounts, what proportion of your passwords have you never changed?

- ○ None
- ○ 1-25%
- ○ 26-50%
- ○ 51-75%
- ○ 76-100%

16- Which of the following authentication methods would you use?
(Select one circle for each row) (1= Least, 5= Most)

	1	2	3	4	5
No authentication	○	○	○	○	○
PIN/Password/Pattern	○	○	○	○	○
Graphical Password	○	○	○	○	○
Cognitive Questions	○	○	○	○	○
Token	○	○	○	○	○
Physical Biometrics (e.g. Fingerprint, Facial Recognition, Iris/Retina scanning, Hand Geometry, Vein Pattern Recognition)	○	○	○	○	○
Behavioural Biometrics (e.g. Voice Recognition, Keystroke Analysis, Handwriting Recognition, Gait Recognition, Behavioural Profiling)	○	○	○	○	○

17- How frequently have you experienced authentication failure (i.e. failed to login)?
(e.g. forgotten the password, lost a token, or been falsely rejected by a biometrics)

- ○ Never
- ○ Very Rarely (less than once a week)
- ○ Rarely (once a week)
- ○ Sometimes (between 2 to 5 times a week)
- ○ Frequently (more than 5 times a week)

18- In which degree the login failure have bothered you? (Dependent upon the previous question; not never) (1= Least, 5= Most)

1	2	3	4	5
○	○	○	○	○

19- What was the cause of the failure? (Dependent upon the previous question; not never)

- ☐ Mismatched secret (PIN/password/pattern/graphical password)
- ☐ Forgotten secret (PIN/password/pattern/graphical password)
- ☐ Mismatched biometrics
- ☐ Absence of token/Mobile (lost/ forgotten/not available)
- ☐ Failure issues of token/token reader/software/biometrics reader
- ☐ Other ____

20- With respect to technology and Internet, how concerned are you about each of the following? (1= Least concerned, 5= Most concerned)

	1	2	3	4	5
Security (e.g., malicious programs)	○	○	○	○	○
Privacy (e.g., leakage of sensitive data)	○	○	○	○	○
Abuse (e.g., stolen, lost or borrowed device)	○	○	○	○	○
Convenience (i.e., usability and ease of use)	○	○	○	○	○

21- How usable do you feel the following authentication approaches are? (1= Least usable, 5= Most usable)

	1	2	3	4	5	N/A
iOS Touch ID (i.e. iPhone 5S fingerprint)	○	○	○	○	○	○
Android Face Unlock	○	○	○	○	○	○
Android Pattern Unlock (i.e. touching dots on specific sequence)	○	○	○	○	○	○
HSBC Secure Key (i.e. hardware token)	○	○	○	○	○	○
Amazon 1-Click	○	○	○	○	○	○
Windows 8.1 (i.e. picture password)	○	○	○	○	○	○
Google Authenticator (i.e. to access google account by 2FA)	○	○	○	○	○	○

Privacy:

22- How frequent do you read the End-User License/agreement/App permissions of the services/apps you use?

- ○ Never
- ○ Rarely (less than 25%)
- ○ Sometimes (26%-75%)
- ○ Frequently (76%-99%)
- ○ Always

23- How often have you decided not to use/install or uninstalled a service due to the End-User License/agreement/App permissions required?

- Never
- Rarely (1-3 times)
- Sometimes (4-10 times)
- Frequently (11-15 times)
- Very Frequent (16-20 times)
- Too many to remember

24- Would you be confident storing your biometrics with a Trusted Third Party (TTP)* so you can use them for authentication anywhere and with different devices and services?

- Very Confident
- Confident
- Neutral
- Un-confident
- Very Un-confident

* A Trusted Third Party (TTP), sometimes referred to as a Trusted Authority (e.g. PayPal, Verified by Visa), is an entity that is trusted and utilised by all parties (i.e. users, devices, and services) to facilitate interactions between them. This approach would reduce the burden on users to authenticate.

25- Where would you prefer to store your biometrics templates?

- ☐ On your own device(s)
- ☐ With your network operator (e.g. ISP, mobile operator)
- ☐ With Trusted Third Party (TTP)
- ☐ Do not know
- ☐ None

26- Would you accept the concept of monitoring* your usage behaviour to identify any potential misuse of your data, e.g. if your account was accessed from 2 different geographical locations simultaneously?

- Strongly Accept
- Accept
- Neutral
- Reject
- Strongly Reject

* The monitoring will be about the usage of your device normally that will help to identify any change of the behaviour in case of being stolen or misused and to protect your personal data from unauthorised or illegal action without collecting any of your private data throughout the monitoring. These types of technologies are extensively utilised in credit card and telephone companies to reduce possible fraud.

27- Would you be willing to pass the responsibility of managing authentication to TTP?

(1= Least, 5= Most)

1	2	3	4	5
○	○	○	○	○

Appendix D – Ethical Approval, Consent Form and Information Sheet (Data Collection)

RESEARCH WITH PLYMOUTH UNIVERSITY

22 February 2016

CONFIDENTIAL
Abdulwahid Al Abdulwahid
School of Computing, Electronics and Mathematics

Dear Abdulwahid

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

Transparent and Continuous Biometric Capturing

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Nathan Clarke
Prof Steven Furnell

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

T +44 (0) 1752 584 584
F +44 (0) 1752 584 540
W www.plymouth.ac.uk

Mrs Christine Mushens BA
Faculty Business Manager

SAMPLE SELF-CONSENT FORM

PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENGINEERING

Human Ethics Committee Sample Consent Form

CONSENT TO PARICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Abdulwahid Al Abdulwahid

Title of Research

Transparent and Continuous Biometric Capturing

Brief statement of purpose of work

Authentication is a key security control for any computing system, whether that is a PC, server, laptop, tablet, phablet or mobile phone. However, authentication is traditionally poorly served, with existing implementations falling foul of a variety of weaknesses, one of which is being merely at the point-of-entry. In order to secure sensitive services, it is imperative to increase the level of authentication beyond the standard point-of-entry technique, albeit without compromising the user convenience. Whilst a number of research has been undertaken exploring this, they were evaluated based upon simulated or semi-simulated off-line data and focus upon individual platforms rather than providing a universal and federated authentication approach.

This study seeks to investigate and specify the appropriate biometric modalities that need to be deployed and incorporated in the proposed solution to provide a more secure, user-friendly, universal and technology independent environment.

Therefore, this experiment seeks to capture and collect data of a set of biometric techniques from a real and live usage, in order to evaluate the appropriateness and effectiveness of utilising them for such universal authentication, with a view to identify the attributes required for a successful authentication mechanism.

As a participant, the application will be installed on your Android smartphones (and tablets where appropriate). Your biometric samples (i.e. face, voice, app usage, gait (walking pattern), location, and SMS linguistic) will be automatically, continuously and transparently collected and stored on your device(s)' local storage without any interference upon your normal activities (i.e. without the need for any additional actions from you and without interrupting you) for 2 weeks.

Upon completing the experiment duration, the captured biometric samples will be generated in a datasheet format files on your device(s)' SD card or local file/folder. The data will be shown to you – once you are happy with them, the files will be taken by the principal investigator and will be anonymous and stored in a secure location within the Centre for Security, Communications and Network Research (CSCAN) at Plymouth University.

At all stages of the study, confidentiality of the collected data and subsequent analysis will be maintained. At no time, will any identifying information about the participants be used in any publication or research output.

You have the right to withdraw at any stage upon until the completion of the data collection process. Should you wish to withdraw from the study, please contact Abdulwahid Al Abdulwahid.

For information regarding the study, please contact:

Abdulwahid Al Abdulwahid - abdulwahid.alabdulwahid@plymouth.ac.uk
For any questions concerning the ethical status of this study, please contact the secretary of the Human Ethics Committee – paula.simson@plymouth.ac.uk

---

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations).

Under these circumstances, I confirm that I am 18 years old or above and I agree to participate in the research.

Name: ……

Signature: …….. Date: ……..

SAMPLE INFORMATION SHEET FOR ADULT

PLYMOUTH UNIVERSITY
FACULTY OF SCIENCE AND ENGINEERING

RESEARCH INFORMATION SHEET

Name of Principal Investigator

Abdulwahid Al Abdulwahid

Title of Research

Transparent and Continuous Biometric Capturing

Aim of research

This experiment seeks to capture and collect data of a set of biometric techniques from a real and live usage, in order to evaluate the appropriateness and effectiveness of utilising them for such universal authentication with a view to identify the attributes required for a successful authentication mechanism.

Description of procedure

A biometric capturing software will be installed on users' Android smartphones (and tablets where appropriate). Participants will not need to do anything but merely continue using their device(s) in their normal fashion. The data will be collected over a 2 week period.

Description of risks

At no stage will any personally identifiable information be seen by any individual neither the researchers nor on any publication. The captured data will be stored after being converted to measurement features. All of the information will be treated confidentially and data will be anonymous during the collection, storage and publication of research material.

Benefits of proposed research

The ultimate aim of this research project is to build upon existing research on transparent and distributed authentication. An authentication system built upon this would provide a more secure, user-friendly, universal and technology independent environment.

Right to withdraw

You have the right to withdraw at any stage without giving a reason. Your biometrics and any recorded data will be removed and securely deleted.

Contact for Further Information

If you are dissatisfied with the way the research is conducted, please contact the principal investigator in the first instance: Abdulwahid Al Abdulwahid, A319, Portland Square Building, Plymouth University. Email: abdulwahid.alabdulwahid@plymouth.ac.uk, Telephone number *[*01752 586251*],* Mobile number *[07449250533].* If you feel the problem has not been resolved please contact the secretary to the Faculty of Science and Engineering Human Ethics Committee: Mrs Paula Simson 01752 584503.

Appendix E – Cloud Aura Software Code (Android)

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.app.cloudauraa"
    android:versionCode="10"
    android:versionName="1.9" >

    <uses-sdk
        android:minSdkVersion="14"
        android:targetSdkVersion="23" />

        <uses-permission android:name="android.permission.RECORD_AUDIO"/>


    <uses-feature android:name="android.hardware.camera" />
    <uses-feature android:name="android.hardware.camera.autofocus" />
    <uses-permission android:name="android.permission.CAMERA" />
    <uses-permission android:name="android.hardware.camera.autofocus" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.GET_TASKS" />
    <uses-permission android:name="android.permission.INTERNET"/>

    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"></uses-
permission>
   <uses-permission android:name="android.permission.READ_SMS" />
   <uses-permission android:name="android.permission.SEND_SMS"></uses-permission>
   <uses-permission android:name="android.permission.WAKE_LOCK"/>


    <application
        android:allowBackup="true"
        android:icon="@drawable/cloudicon"
        android:label="@string/app_name"
        android:theme="@android:style/Theme.Holo.Light">
        <activity
            android:name=".ui.SplashActivity"
            android:label="@string/app_name"
            android:noHistory="true" >
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <activity android:name="com.app.cloudauraa.ui.CamTestActivity"
            android:screenOrientation="landscape"/>
        <activity android:name="com.app.cloudauraa.ui.AppListActivity"
            android:noHistory="true"/>
        <activity android:name="com.app.cloudauraa.ui.DashBoardActivity"
            />
        <activity android:name="com.app.cloudauraa.ui.VoiceActivity"/>
        <activity android:name="com.app.cloudauraa.ui.FaceActivity"/>
        <activity android:name="com.app.cloudauraa.ui.FingerActivity"/>
        <activity android:name="com.app.cloudauraa.ui.RegisterActivity"/>
        <activity android:name="com.app.cloudauraa.ui.ShowBehaviourActivity"/>
        <activity android:name="com.app.cloudauraa.ui.SettingActivity"/>
        <activity android:name="com.app.cloudauraa.ui.DialogeActivity"/>

        <activity android:name="com.app.cloudauraa.changeui.ChangeFaceActivity"/>
        <activity android:name="com.app.cloudauraa.changeui.ChangeVoiceActivity"/>
        <activity android:name="com.app.cloudauraa.changeui.ChangeFingerActivity"/>
        <activity android:name="com.app.cloudauraa.changeui.ChangeAppActivity"/>
```

```
        <service android:name="com.app.cloudauraa.service.AppService"></service>
        <service
android:name="com.app.cloudauraa.service.LocationService"></service>
        <service android:name="com.app.cloudauraa.service.DemoService"></service>
        <service android:name="com.app.cloudauraa.service.MyService"></service>
        <service
android:name="com.app.cloudauraa.service.ImageCaptureService"></service>
        <service
android:name="com.app.cloudauraa.service.VoiceRecordService"></service>
        <service
android:name="com.app.cloudauraa.service.RetriveSentMessageService"></service>

        <service android:name="com.app.cloudauraa.steps.StepService"></service>

         <meta-data android:name="com.google.android.gms.version"
             android:value="@integer/google_play_services_version" />

          <receiver  android:name="com.app.cloudauraa.reciver.Receiver">
            <intent-filter android:priority="1000" >

                 <action android:name="android.intent.action.BOOT_COMPLETED" />
                 <category android:name="android.intent.category.HOME" />

            </intent-filter>
        </receiver>


    </application>

</manifest>


}
        }
```

```
package com.app.cloudauraa.async;

import java.util.ArrayList;
import java.util.List;

import org.apache.http.NameValuePair;
import org.apache.http.message.BasicNameValuePair;
import org.json.JSONObject;

import android.app.Activity;
import android.os.AsyncTask;
import android.util.Log;

import com.app.cloudauraa.helper.Attributes;
import com.app.cloudauraa.helper.ServiceHandler;
import com.app.cloudauraa.utils.CommanUtils;
import com.app.cloudauraa.utils.NetworkUtils;


public class FaceAsync extends AsyncTask<Void,Void,Void> {

   public static final String TAG="LoginAsync";
   Activity pcontext;
   String username,password,regId,latlong;
   boolean isConneted;
   String response,status;
   int res;


   public FaceAsync(Activity context,String username,String password,String
regId,String latlong) {
         // TODO Auto-generated constructor stub
         this.pcontext=context;
         this.username=username;
         this.password=password;
         this.regId=regId;
         this.latlong=latlong;
   }

   @Override
   protected void onPreExecute() {
      // TODO Auto-generated method stub
      super.onPreExecute();

   }

   @Override
    protected Void doInBackground(Void... arg0) {
     if(NetworkUtils.isConnectedToInternet(pcontext)){
       isConneted=true;
       List<NameValuePair> nameValuePair= new ArrayList<NameValuePair>(6);
        nameValuePair.add(new BasicNameValuePair("user_name",username));
        nameValuePair.add(new BasicNameValuePair("user_pass",password));
        nameValuePair.add(new BasicNameValuePair("gcm_reg_id",regId));
//        nameValuePair.add(new
BasicNameValuePair("user_imei",CommanUtils.getImeiNo(pcontext)));
        nameValuePair.add(new BasicNameValuePair("user_location",latlong));
        nameValuePair.add(new BasicNameValuePair("user_os","android"));

       ServiceHandler sh = new ServiceHandler();

//        response =
sh.makeServiceCall(Attributes.LOGIN_URL,ServiceHandler.POST,nameValuePair);
        Log.d(TAG,"Response: "+ response);

        if(response != null){
           try{
              JSONObject obj = new JSONObject(response);
```

```
                res = obj.optInt("user_id");
                status = obj.optString("status");
                Log.d("Response", "Response is "+res+","+status);
              }catch(Exception e){

              }
           }

        }else{
            isConneted=false;
         }
          return null;
     }

    @Override
    protected void onPostExecute(Void result) {
        // TODO Auto-generated method stub
        super.onPostExecute(result);

      }

}
```

```
package com.app.cloudauraa.async;

import java.util.ArrayList;
import java.util.List;

import org.apache.http.NameValuePair;
import org.apache.http.message.BasicNameValuePair;
import org.json.JSONObject;

import android.app.Activity;
import android.os.AsyncTask;
import android.util.Log;

import com.app.cloudauraa.helper.ServiceHandler;
import com.app.cloudauraa.utils.NetworkUtils;

public class VoiceAsync extends AsyncTask<Void,Void,Void> {

   public static final String TAG="LoginAsync";
   Activity pcontext;
   String username,password,regId,latlong;
   boolean isConneted;
   String response,status;
   int res;


   public VoiceAsync(Activity context,String username,String password,String
regId,String latlong) {
         // TODO Auto-generated constructor stub
         this.pcontext=context;
         this.username=username;
         this.password=password;
         this.regId=regId;
         this.latlong=latlong;
   }

   @Override
   protected void onPreExecute() {
      // TODO Auto-generated method stub
      super.onPreExecute();

   }

   @Override
    protected Void doInBackground(Void... arg0) {
     if(NetworkUtils.isConnectedToInternet(pcontext)){
       isConneted=true;
       List<NameValuePair> nameValuePair= new ArrayList<NameValuePair>(6);
        nameValuePair.add(new BasicNameValuePair("user_name",username));
        nameValuePair.add(new BasicNameValuePair("user_pass",password));
        nameValuePair.add(new BasicNameValuePair("gcm_reg_id",regId));
//        nameValuePair.add(new
BasicNameValuePair("user_imei",CommanUtils.getImeiNo(pcontext)));
        nameValuePair.add(new BasicNameValuePair("user_location",latlong));
        nameValuePair.add(new BasicNameValuePair("user_os","android"));

       ServiceHandler sh = new ServiceHandler();

//        response =
sh.makeServiceCall(Attributes.LOGIN_URL,ServiceHandler.POST,nameValuePair);
        Log.d(TAG,"Response: "+ response);

        if(response != null){
           try{
              JSONObject obj = new JSONObject(response);
              res = obj.optInt("user_id");
              status = obj.optString("status");
              Log.d("Response", "Response is "+res+","+status);
```

```
            }catch(Exception e){

            }
          }

       }else{
           isConneted=false;
        }
         return null;
     }

   @Override
   protected void onPostExecute(Void result) {
      // TODO Auto-generated method stub
      super.onPostExecute(result);

       }


}
```

```
package com.app.cloudauraa.service;

import java.io.File;
import java.io.IOException;

import android.app.Service;
import android.content.Intent;
import android.media.MediaRecorder;
import android.os.Build;
import android.os.Environment;
import android.os.Handler;
import android.os.IBinder;
import android.os.PowerManager;
import android.util.Log;
import android.widget.Toast;

import com.app.cloudauraa.db.DBAdapter;
import com.app.cloudauraa.utils.CommanUtils;
import com.app.cloudauraa.utils.PreferenceUtils;

public class VoiceRecordService extends Service {

   static PreferenceUtils pref;
   private static DBAdapter dbAdapter;
   private static final String AUDIO_RECORDER_FILE_EXT_3GP = ".3gp";
   private static final String AUDIO_RECORDER_FILE_EXT_MP4 = ".mp4";
   private static final String AUDIO_RECORDER_FOLDER = "AudioRecord";

   private MediaRecorder recorder = null;
   private int currentFormat = 0;
   private int output_formats[] = { MediaRecorder.OutputFormat.MPEG_4,
         MediaRecorder.OutputFormat.THREE_GPP };
   private String file_exts[] = { AUDIO_RECORDER_FILE_EXT_MP4,
         AUDIO_RECORDER_FILE_EXT_3GP };

   final static String TAG="CheckRunningApp";
   Handler handler ;
   Runnable runnable;


    @Override
    public IBinder onBind(Intent intent) {
        return null;
    }

    @Override
    public int onStartCommand(Intent intent, int flags, int startId) {
       // TODO Auto-generated method stub
       checking();
       return super.onStartCommand(intent, flags, startId);
    }

    public void checking(){

        PowerManager powerManager = (PowerManager) getSystemService(POWER_SERVICE);
         boolean isScreenOn = powerManager.isScreenOn();
         Log.e("TAG", "SCREEN ON OR OFF:============::"+isScreenOn);

       dbAdapter=new DBAdapter(this);
       pref=new PreferenceUtils(this);
       if(isScreenOn){
           startRecording();
             Log.d(TAG,"checking started ");
              //code run after when time will over
              handler = new Handler();
             runnable = new Runnable() {
                 public void run() {
```

```
                    Log.e(TAG, "Running");
                    stopRecording();
                    //handler.postDelayed(this, 7000);
                }
            };
            handler.postDelayed(runnable, 8000);
        }else{
            Log.e(TAG,"Screen Is OFF");
            save();
        }
    }

    @Override
    public void onDestroy() {
        // TODO Auto-generated method stub
        super.onDestroy();
        //handler.removeCallbacks(runnable);
        Log.i(TAG, ":Service is destroy:");
        SaveData();

//      MainActivity.GeneratedExelFile(CheckRunningApp.this);
//      CommanUtils.exportToExcel1(CheckRunningApp.this);
        //Toast.makeText(CheckRunningApp.this, "Task is Completed...",
Toast.LENGTH_LONG).show();
    }

    //Methods
   private String getFilename() {
      String filepath = Environment.getExternalStorageDirectory().getPath();
      File file = new File(filepath, AUDIO_RECORDER_FOLDER);
      if (!file.exists()) {
         file.mkdirs();
      }
      //String.format("sample-%d.jpg", System.currentTimeMillis());
      return (file.getAbsolutePath() + "/" + "Recording"+
file_exts[currentFormat]);
   }

   private void startRecording() {

      Log.d(TAG,"startRecording");
       recorder = new MediaRecorder();

      recorder.setAudioSource(MediaRecorder.AudioSource.VOICE_RECOGNITION);
      recorder.setOutputFormat(output_formats[currentFormat]);
      recorder.setAudioEncoder(MediaRecorder.AudioEncoder.AMR_NB);
      recorder.setOutputFile(getFilename());

      recorder.setOnErrorListener(errorListener);
      recorder.setOnInfoListener(infoListener);
      try {
         recorder.prepare();
         recorder.start();
      } catch (IllegalStateException e) {
         e.printStackTrace();
      } catch (IOException e) {
         e.printStackTrace();
      }
   }

   private void stopRecording() {
      Log.d("TAG", "STOP RECORDING");

      //Toast.makeText(this, "STOP RECORDING:"+getFilename(),
Toast.LENGTH_LONG).show();
      pref.setVoicePath(""+getFilename());

      if (null != recorder) {
```

```
//        recorder.stop();
          recorder.reset();
          recorder.release();
          recorder = null;
             pref.setVoicePath(getFilename());
             save();
             handler.removeCallbacks(runnable);
       }

   }

public void save(){

       String brand = Build.BRAND;
      Log.d("TAG", "Brand:"+brand);
      SaveData();
      if(brand.equals("samsung")){
         startService(new Intent(VoiceRecordService.this,FingureService.class));
      }else{

         Log.e("TAG", "Finger service is not supported in the device:");
         Toast.makeText(this, "Finger service is not supported in the device",
Toast.LENGTH_LONG).show();
         //stopService(new Intent(this,CheckRunningApp.class));
         //finish();
      }
   }


public static void SaveData(){

   dbAdapter.open();
   try {
   if(!pref.getVoicePath().equals("")){

         Log.e("TAG", "Voice.PATH:"+pref.getVoicePath());

         String voice=CommanUtils.ConvertVoiceToBase64(pref.getVoicePath());
         Log.e("TAG", "Voice.legnght:"+voice.length());
         dbAdapter.insertVoiceDetail(""+pref.getVoiceID(), ""+voice);
         int k=pref.getVoiceID();
         k++;
         pref.SetVoiceID(k);
         pref.setVoicePath("");

   }
   } catch (IOException e) {
      // TODO Auto-generated catch block
      e.printStackTrace();
   }
   dbAdapter.close();
}

private MediaRecorder.OnErrorListener errorListener = new
MediaRecorder.OnErrorListener() {
   @Override
   public void onError(MediaRecorder mr, int what, int extra) {
   }
};

private MediaRecorder.OnInfoListener infoListener = new
MediaRecorder.OnInfoListener() {
   @Override
   public void onInfo(MediaRecorder mr, int what, int extra) {
   }
};
}
```

```
package com.app.cloudauraa.service;

import java.io.File;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;

import android.app.Service;
import android.content.Context;
import android.content.Intent;
import android.graphics.Bitmap;
import android.graphics.BitmapFactory;
import android.graphics.Matrix;
import android.graphics.SurfaceTexture;
import android.hardware.Camera;
import android.hardware.Camera.Parameters;
import android.media.FaceDetector;
import android.net.Uri;
import android.os.AsyncTask;
import android.os.Environment;
import android.os.Handler;
import android.os.IBinder;
import android.util.Log;
import android.view.Display;
import android.view.SurfaceHolder;
import android.view.SurfaceView;
import android.view.WindowManager;
import android.widget.Toast;

import com.app.cloudauraa.db.DBAdapter;
import com.app.cloudauraa.utils.CommanUtils;
import com.app.cloudauraa.utils.PreferenceUtils;

@SuppressWarnings("deprecation")
public class ImageCaptureService extends Service
{

   //SOme Changes
   public static int imageWidth, imageHeight;
   public static int numberOfFace = 5;
   public static FaceDetector myFaceDetect;
   public static FaceDetector.Face[] myFace;
   public static float myEyesDistance;
   public static int numberOfFaceDetected;
   public static Bitmap myBitmap;

   private int midScreenWidth;
   private int midScreenHeight;
   DBAdapter  dbAdapter;
   Handler handler ;
   Runnable runnable;
   static int x=0;
         //Camera variables
         //a surface holder
         private SurfaceHolder sHolder;
         private SurfaceTexture sTexture;
         //a variable to control the camera
         public static Camera mCamera=null;
         //the camera parameters
         private Parameters parameters;
         File outFile;
      String fileName;
      FileOutputStream outStream = null;
      PreferenceUtils pref;

      @Override
       public int onStartCommand(Intent intent, int flags, int startId)
       {
```

```
           handler = new Handler();
          runnable = new Runnable() {
             public void run() {
                 checking();
                 handler.postDelayed(this, 180000);
             }
          };
          handler.postDelayed(runnable, 5000);
           return super.onStartCommand(intent, flags, startId);
       }

       private void checking() {
         Log.d("My Service", "Started");
          pref=new PreferenceUtils(this);
          dbAdapter=new DBAdapter(this);
          WindowManager window = (WindowManager)
getSystemService(Context.WINDOW_SERVICE);
           Display display = window.getDefaultDisplay();
            midScreenHeight = display.getHeight() / 2;
            midScreenWidth = display.getWidth() / 2;

            Camera.CameraInfo cameraInfo = new Camera.CameraInfo();
             int cameraId = 0;
             int camerasCount = Camera.getNumberOfCameras();
             for ( int camIndex = 0; camIndex < camerasCount; camIndex++ ) {
                 Camera.getCameraInfo(camIndex, cameraInfo );

                 if (cameraInfo.facing == Camera.CameraInfo.CAMERA_FACING_FRONT  )
{
                  cameraId = camIndex;
                  break;
                 }
             }
                    try {

                       mCamera = Camera.open(cameraId);
                     SurfaceView sv = new SurfaceView(getApplicationContext());
                     sTexture = new SurfaceTexture(0);

                    //Toast.makeText(this, "CAMERA
START...",Toast.LENGTH_LONG).show();

                       mCamera.setPreviewTexture(sTexture);
                      parameters = mCamera.getParameters();


                        //set camera parameters
                      mCamera.setParameters(parameters);
                      mCamera.startPreview();

                      mCamera.takePicture(null, null, mCall);

//                    mCamera.setFaceDetectionListener(faceDetectionListener);
//                  mCamera.startFaceDetection();

                      //Get a surface
                     sHolder = sv.getHolder();
                    //tells Android that this surface will have its data constantly
replaced
                     sHolder.setType(SurfaceHolder.SURFACE_TYPE_PUSH_BUFFERS);

                  } catch (IOException e) {
                       e.printStackTrace();
                  }

      }

      Camera.PictureCallback mCall = new Camera.PictureCallback()
```

```
        {
           public void onPictureTaken(byte[] data, Camera camera)
           {
               //decode the data obtained by the camera into a Bitmap
              Log.e("TAG", "DATA:"+data);

              new SaveImageTask().execute(data);
              camera.stopPreview();
              camera.release();
              Toast.makeText(getApplicationContext(), "Picture Captured.",
Toast.LENGTH_LONG).show();
           }
        };
          @Override
          public IBinder onBind(Intent intent) {
                return null;
          }

       @Override
        public void onDestroy() {
            //Toast.makeText(this, "Stopped", Toast.LENGTH_SHORT).show();
           handler.removeCallbacks(runnable);
            super.onDestroy();
        }

       private class SaveImageTask extends AsyncTask<byte[], Void, Void> {

          @Override
          protected Void doInBackground(byte[]... data) {
             FileOutputStream outStream = null;

             // Write to SD Card
             try {
                File sdCard = Environment.getExternalStorageDirectory();
                File dir = new File(sdCard.getAbsolutePath() + "/FaceImages");
                if(!dir.isDirectory()){
                   dir.mkdirs();
                }

                fileName =  String.format("sample-%d.jpg",
System.currentTimeMillis());
                      //CommanUtils.getCurrentDate()+".jpg";
                outFile = new File(dir, fileName);
                outStream = new FileOutputStream(outFile);
                outStream.write(data[0]);
                outStream.flush();
                outStream.close();

                refreshGallery(outFile);
                updateGallery(outFile,"front");
                pref.setImagePath(""+outFile.getPath());

             } catch (FileNotFoundException e) {
                e.printStackTrace();
             } catch (IOException e) {
                e.printStackTrace();
             } finally {
             }
             return null;
          }

          @Override
          protected void onPostExecute(Void result) {
             super.onPostExecute(result);
             Log.d("TAG", "ON POST");
             mCamera.release();
             dbAdapter.open();
             if(!pref.getImagePath().equals(""))
```

```
            {
               if(pref.getFaceDetetect()!=0)
               {
                  Log.d("TAG", "Image.PATH:"+pref.getImagePath());
                  File f=new File(pref.getImagePath());
                  File tempfile=CommanUtils.saveBitmapToFile(f);
                  Log.d("TAG", "f:"+f);
                  Log.d("TAG", "tempfile:"+tempfile);
                  String
image=CommanUtils.ConvertImageToBase64(tempfile.getPath());
                  Log.d("TAG", "Image.legnght:"+image.length());
                  dbAdapter.insertImageDetail(""+pref.getFaceID(), ""+image);
                  pref.setImagePath("");
                  int k=pref.getFaceID();
                  k++;
                  pref.SetFaceID(k);
                  pref.setFaceDetetect(0);
               }
               else{
                  File file= new File(""+pref.getImagePath());
                   if(file.exists())
                   {
                        file.delete();
                   }
               }
            }
            dbAdapter.close();

            startService(new
Intent(ImageCaptureService.this,VoiceRecordService.class));

            startService(new
Intent(ImageCaptureService.this,LocationService.class));
            startService(new Intent(ImageCaptureService.this,AppService.class));


         }

      }

      public void updateGallery(File outFile2, String cam) {
         Log.d("TAG", cam);

         Bitmap bitmap1;
         BitmapFactory.Options options = new BitmapFactory.Options();
         options.inPreferredConfig = Bitmap.Config.RGB_565;
               //ARGB_8888;
         Bitmap bitmap = BitmapFactory.decodeFile(outFile2.getPath(), options);

         if(cam.equals("back")){
            bitmap1 = rotateImage(bitmap, 90);
         }else{
            bitmap1 = rotateImage(bitmap, -90);
         }
         try {
                FileOutputStream out = new FileOutputStream(outFile2);
                bitmap1.compress(Bitmap.CompressFormat.JPEG, 90, out);
                   Log.e("TAG", "FACE FOUND UPDATE
GALLARY:"+CheckImageFace(bitmap1));
                   pref.setFaceDetetect(CheckImageFace(bitmap1));
                   out.flush();
                out.close();
         } catch (Exception e) {
                e.printStackTrace();
         }
      }
      private void refreshGallery(File file) {
         Intent mediaScanIntent = new Intent(
```

```
Intent.ACTION_MEDIA_SCANNER_SCAN_FILE);
         mediaScanIntent.setData(Uri.fromFile(file));
         sendBroadcast(mediaScanIntent);
      }

      public static Bitmap rotateImage(Bitmap src, float degree)
      {
               // create new matrix
               Matrix matrix = new Matrix();
               // setup rotation degree
               matrix.postRotate(degree);
               Bitmap bmp = Bitmap.createBitmap(src, 0, 0, src.getWidth(),
src.getHeight(), matrix, true);
               return bmp;
      }

      public static int CheckImageFace(Bitmap bitmap){

         myBitmap=bitmap;
               imageWidth = myBitmap.getWidth();
               imageHeight = myBitmap.getHeight();
               myFace = new FaceDetector.Face[numberOfFace];
               myFaceDetect = new FaceDetector(imageWidth, imageHeight,
                 numberOfFace);
               numberOfFaceDetected = myFaceDetect.findFaces(myBitmap, myFace);
               return numberOfFaceDetected;
      }
}
```

```
package com.app.cloudauraa.service;

import java.text.SimpleDateFormat;
import java.util.Calendar;
import java.util.Date;
import java.util.Locale;

import android.app.ActivityManager;
import android.app.AlertDialog;
import android.app.Service;
import android.content.Context;
import android.content.Intent;
import android.content.pm.PackageManager;
import android.content.pm.ResolveInfo;
import android.database.Cursor;
import android.os.Handler;
import android.os.IBinder;
import android.text.format.Time;
import android.util.Log;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;

import com.app.cloudauraa.db.DBAdapter;
import com.app.cloudauraa.helper.Attributes;
import com.app.cloudauraa.utils.PreferenceUtils;

public class AppService extends Service {

   Handler handler;
   Runnable runnable;
   static DBAdapter adp;
   PreferenceUtils pref;
   String p;
   AlertDialog.Builder mAlertDlgBuilder;
   AlertDialog mAlertDialog;
   View mDialogView = null;
   String app, weekDay, time, t1;
   Button btnGo, appuse;
   EditText edtDummy;
   String currentTimeString, newTimeString, minusTimeString, formattedTime,temp;
   java.sql.Time timeValue, lesstime, greatertime;
   int flage = 0;
   String lat, lng, latlng;

   @Override
   public IBinder onBind(Intent intent) {
      // TODO Auto-generated method stub
      return null;
   }

   @Override
   public int onStartCommand(Intent intent, int flags, int startId) {
      // TODO Auto-generated method stub

      adp = new DBAdapter(this);
      pref = new PreferenceUtils(this);
      checking();

      return super.onStartCommand(intent, flags, startId);
   }

   public void checking() {

      Log.e("TAG", "checking started ");
      // code run after when time will over
      handler = new Handler();
      runnable = new Runnable() {
```

```
        @SuppressWarnings("unused")
        public void run() {

           try {

              formattedTime="";
              Intent intent = new Intent(Intent.ACTION_MAIN);
              intent.addCategory(Intent.CATEGORY_HOME);
              ResolveInfo resolveInfo = getPackageManager()
                    .resolveActivity(intent,
                          PackageManager.MATCH_DEFAULT_ONLY);
              String currentHomePackage = resolveInfo.activityInfo.packageName;

              ActivityManager am = (ActivityManager)
getSystemService(Context.ACTIVITY_SERVICE);

//            if (Build.VERSION.SDK_INT > 20) {

                 String aTask = am.getRunningAppProcesses().get(0).processName;
//               Log.e("Lolipop", aTask + currentHomePackage);

                 // pref.setAppAllow(currentHomePackage);
                 if (aTask.toString().equals(currentHomePackage)) {
                    pref.setAppAllow(currentHomePackage);
                 }

                 if (!aTask.toString().equalsIgnoreCase(
                       currentHomePackage)
                       && !aTask.toString().equalsIgnoreCase(
                             pref.getAppAllow())
                       && !aTask.toString().equalsIgnoreCase(
                             "com.app.cloudauraa")) {
                    adp.open();
                    Cursor c = adp.getPriority(aTask);

                    if (c != null)
                       c.moveToFirst();
                    if (c.moveToFirst()) {
                       do {
                          p = c.getString(c
                                .getColumnIndex(Attributes.PRIORITY));
                          //Log.d("Priority", p);

                       } while (c.moveToNext());
                    }

                    lat = LocationService.getLat();
                    lng = LocationService.getLong();
                    Log.e("Lat Long", lat + " , " + lng);

                    app = adp.getAppNameTest(aTask.toString());

                    SimpleDateFormat dayFormat = new SimpleDateFormat(
                          "EEEE", Locale.US);
                    Calendar calendar = Calendar.getInstance();
                    weekDay = dayFormat.format(calendar.getTime());

//                  Log.d("weekda and pref day",
//                        weekDay + " , " + pref.getDay());

                    SimpleDateFormat dateFormat = new SimpleDateFormat(
                          "HH");
                    formattedTime = dateFormat.format(new Date())
                          .toString();
//                  System.out.println("24 hour format date "
//                        + formattedTime);

                    if (formattedTime.equals("01")) {
```

```
                formattedTime = "00-01";
            } else if (formattedTime.equals("02")) {
                formattedTime = "01-02";
            } else if (formattedTime.equals("03")) {
                formattedTime = "02-03";
            } else if (formattedTime.equals("04")) {
                formattedTime = "03-04";
            } else if (formattedTime.equals("05")) {
                formattedTime = "04-05";
            } else if (formattedTime.equals("06")) {
                formattedTime = "05-06";
            } else if (formattedTime.equals("07")) {
                formattedTime = "06-07";
            } else if (formattedTime.equals("08")) {
                formattedTime = "07-08";
            } else if (formattedTime.equals("09")) {
                formattedTime = "08-09";
            } else if (formattedTime.equals("10")) {
                formattedTime = "09-10";
            } else if (formattedTime.equals("11")) {
                formattedTime = "10-11";
            } else if (formattedTime.equals("12")) {
                formattedTime = "11-12";
            } else if (formattedTime.equals("13")) {
                formattedTime = "12-13";
            } else if (formattedTime.equals("14")) {
                formattedTime = "13-14";
            } else if (formattedTime.equals("15")) {
                formattedTime = "14-15";
            } else if (formattedTime.equals("16")) {
                formattedTime = "15-16";
            } else if (formattedTime.equals("17")) {
                formattedTime = "16-17";
            } else if (formattedTime.equals("18")) {
                formattedTime = "17-18";
            } else if (formattedTime.equals("19")) {
                formattedTime = "18-19";
            } else if (formattedTime.equals("20")) {
                formattedTime = "19-20";
            } else if (formattedTime.equals("21")) {
                formattedTime = "20-21";
            } else if (formattedTime.equals("22")) {
                formattedTime = "21-22";
            } else if (formattedTime.equals("23")) {
                formattedTime = "22-23";
            } else if (formattedTime.equals("24")) {
                formattedTime = "23-24";
            }

//              Log.d("weekda and pref day", formattedTime + " , "
//                    + pref.getTime());

            if (formattedTime.equals(pref.getTime())) {

                Log.e("Location Already Insert",
                      "AlreadyInsert");

                if (lat.equals("0.0") && lng.equals("0.0")) {
                    Log.d("Location not found", lat + "," + lng);
                } else {
                    latlng = lat + "," + lng;
                    // pref.setTime(formattedTime);
                }

            } else {

                if (lat.equals("0.0") && lng.equals("0.0")) {
                    Log.d("Location not found", lat + "," + lng);
```

```
                    } else {
                        latlng = lat + "," + lng;
                        // pref.setTime(formattedTime);
                    }
                }

                Time today = new Time(Time.getCurrentTimezone());
                today.setToNow();
                time = today.format("%k:%M:%S");

                adp.open();
                adp.insertAppsUse(weekDay, app, formattedTime);
                adp.insertCommonUse(weekDay, app, formattedTime);

                String LAT="";
//              if (flage == 0) {

                    if (!formattedTime.equals(pref.getTime())
                            && !weekDay.equals(pref.getDay())) {

                        Log.e("TAG","Time And Day Are Diffrent");

                        adp.insertLocation(weekDay, latlng,
                                formattedTime);
                        flage = 1;
                        pref.setTime(formattedTime);
                        pref.setDay(weekDay);

                    } else if (!formattedTime
                            .equals(pref.getTime())
                            && weekDay.equals(pref.getDay())) {

                        Log.d("TAG"," Time Is Diffrent And Day Is Same");

//                      String pre=PreviousLocation(formattedTime);
//                      Log.e("TAG","PRE:::"+pre);
//                      if(pre.equals("") || pre==null)
//                          LAT=latlng;
//                      else
//                          LAT=latlng+"~"+pre;
//
//
//                      Log.e("TAG","LAT:::"+LAT);

                        int u = adp.updateLocation(weekDay, LAT,
                                formattedTime);

                        Log.d("Update", "Row Update successfully "
                                + u);
                        flage = 1;
                        pref.setTime(formattedTime);
                        pref.setDay(weekDay);

                    } else if (formattedTime.equals(pref.getTime())
                            && !weekDay.equals(pref.getDay())) {

                        Log.e("TAG","Time is same And Day is Diffrent");

                        adp.insertLocation(weekDay, latlng,
                                formattedTime);
                        flage = 1;
                        pref.setTime(formattedTime);
                        pref.setDay(weekDay);

                    } else if (formattedTime.equals(pref.getTime())
                            && weekDay.equals(pref.getDay())) {

                        Log.e("TAG", "Time And Day Is Same");
```

```
                        String pre=PreviousLocation(formattedTime);
                        Log.e("TAG","PRE:::"+pre);
                        if(pre.equals("") || pre==null)
                           LAT=latlng;
                        else
                           LAT=latlng+"~"+pre;

                        Log.e("TAG","LAT:::"+LAT);

                        int u = adp.updateLocation(weekDay, LAT,
                              formattedTime);

                        Log.e("Update", "Row Update successfully"+ u);

                        flage = 1;
                        pref.setTime(formattedTime);
                        pref.setDay(weekDay);

                     }
//                   }
                     pref.setAppAllow(aTask.toString());
                     adp.close();
                  } else {
                     // Log.d("allowed", "allowed");
                  }


            } catch (Throwable t) {
//             Log.i("TAG", "Throwable caught:" + t.getMessage(), t);
               Log.i("TAG", "Throwable caught:");


            }
            handler.postDelayed(this, 2000);
         }
      };
      handler.postDelayed(runnable, 2000);
   }

   @Override
   public void onDestroy() {
      // Toast.makeText(this, "Stopped", Toast.LENGTH_SHORT).show();
      Log.e("TAG", "APPS SERVICE DESTROY:");
      handler.removeCallbacks(runnable);
      super.onDestroy();
   }

   public static String PreviousLocation(String time){

      Log.e("TAG", "PreviousLocation :LOCATION:"+time);

      String PreLocation="";
      Cursor loca = adp.getTestLocation();

      if (loca != null)
         loca.moveToFirst();
      if (loca.moveToFirst()) {
         do {

            if(time.equals("00-01")){

               PreLocation = loca.getString(loca
                     .getColumnIndex(Attributes.ONE_LOC));

            }else if(time.equals("01-02")){
               PreLocation = loca.getString(loca
                     .getColumnIndex(Attributes.TWO_LOC));
```

```
}else if(time.equals("02-03")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.THREE_LOC));

}else if(time.equals("03-04")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.FOUR_LOC));

}else if(time.equals("04-05")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.FIVE_LOC));

}else if(time.equals("05-06")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.SIX_LOC));

}else if(time.equals("06-07")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.SEVEN_LOC));

}else if(time.equals("07-08")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.EIGHT_LOC));

}else if(time.equals("08-09")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.NINE_LOC));

}else if(time.equals("09-10")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.TEN_LOC));

}else if(time.equals("10-11")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.ELEVEN_LOC));

}else if(time.equals("11-12")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.TWELVE_LOC));

}else if(time.equals("12-13")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.THIRTEEN_LOC));

   Log.e("Inside","Inside 13-14");
}else if(time.equals("13-14")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.FOURTEEN_LOC));

}else if(time.equals("14-15")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.FIFTEEN_LOC));

}else if(time.equals("15-16")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.SIXTEEN_LOC));

}else if(time.equals("16-17")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.SEVENTEEN_LOC));

}else if(time.equals("17-18")){
   PreLocation = loca.getString(loca
         .getColumnIndex(Attributes.EIGHTEEN_LOC));

}else if(time.equals("18-19")){
   PreLocation = loca.getString(loca
```

```
                        .getColumnIndex(Attributes.NINTEEN_LOC));

                }else if(time.equals("19-20")){
                   PreLocation = loca.getString(loca
                         .getColumnIndex(Attributes.TWENTY_LOC));

                }else if(time.equals("20-21")){
                   PreLocation = loca.getString(loca
                         .getColumnIndex(Attributes.TWENTYONE_LOC));

                }else if(time.equals("21-22")){
                   PreLocation = loca.getString(loca
                         .getColumnIndex(Attributes.TWENTYTWO_LOC));

                }else if(time.equals("22-23")){
                   PreLocation = loca.getString(loca
                         .getColumnIndex(Attributes.TWENTYTHREE_LOC));

                }else if(time.equals("23-24")){
                   PreLocation = loca.getString(loca
                         .getColumnIndex(Attributes.TWENTYFOUR_LOC));
                }

             } while (loca.moveToNext());
          }


          Log.e("TAG", "AFTER PreviousLocation :LOCATION:"+PreLocation);

          return PreLocation;



       }
}
```

```
package com.app.cloudauraa.db;

import java.util.ArrayList;

import android.content.ContentValues;
import android.content.Context;
import android.database.Cursor;
import android.database.sqlite.SQLiteDatabase;
import android.util.Log;

import com.app.cloudauraa.helper.Attributes;
import com.app.cloudauraa.utils.PreferenceUtils;

public class DBAdapter {

      DBHelper sqLiteHelper;
       SQLiteDatabase sqLiteDataBase;
      Context context;
      String TAG="DBAdapter";
      PreferenceUtils pref;

      public DBAdapter(Context context){
         this.context=context;
         pref=new PreferenceUtils(context);
      }

      public DBAdapter open(){
         sqLiteHelper=new DBHelper(context, Attributes.MLOCKALL_DATABASE,null,1);
         sqLiteDataBase=sqLiteHelper.getWritableDatabase();
         pref.setIsOpen(true);
         return this;
      }

      public void close(){
         if(sqLiteDataBase!=null && sqLiteDataBase.isOpen())
            sqLiteDataBase.close();
         if(sqLiteHelper!=null)
            sqLiteHelper.close();
         pref.setIsOpen(false);
      }


   //insert apps details
   public void insertApps(String name,String icon,String pack, String option,
String high, String medium, String low){ //, Boolean high, Boolean medium) {

            ContentValues contentValues=new ContentValues();
         try{

            contentValues.put(Attributes.NAME,name);
            contentValues.put(Attributes.ICON, icon);
            contentValues.put(Attributes.PACKAGE,pack);
            contentValues.put(Attributes.PRIORITY,option);
            contentValues.put(Attributes.HIGH,high);
            contentValues.put(Attributes.MEDIUM,medium);
            contentValues.put(Attributes.LOW,low);

         }catch(Exception e){
      }
         sqLiteDataBase.insert(Attributes.TABLE_APPS,null,contentValues);
   }

   public Cursor getCheckedOption() {
      // TODO Auto-generated method stub
       Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_APPS, null);
       return cursor;
```

```
    }

    public Cursor getNewCheckedOption() {
        // TODO Auto-generated method stub
         Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_APPS_NEW, null);
         return cursor;

    }
    public Cursor getPriority(String app) {
        // TODO Auto-generated method stub
        Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_APPS_NEW+" where "+Attributes.PACKAGE1+" = '" +app+ "'" , null);
         return cursor;
    }

    public void insertAppsNew(String name,String icon,String pack, String option) {
        // TODO Auto-generated method stub

        ContentValues contentValues=new ContentValues();
        try{

            contentValues.put(Attributes.NAME1,name);
            contentValues.put(Attributes.ICON1, icon);
            contentValues.put(Attributes.PACKAGE1,pack);
            contentValues.put(Attributes.PRIORITY1,option);

        }catch(Exception e){
    }
        sqLiteDataBase.insert(Attributes.TABLE_APPS_NEW,null,contentValues);

    }

    public void insertAppsUse(String day, String app, String time) {
        // TODO Auto-generated method stub


        ContentValues contentValues=new ContentValues();
        try{

            contentValues.put(Attributes.DAY, day);
            contentValues.put(Attributes.APP_NAME,app);
            contentValues.put(Attributes.TIME,time);

        }catch(Exception e){
    }
        sqLiteDataBase.insert(Attributes.TABLE_APPS_USE,null,contentValues);
        Log.d("Insert", "Insert App Successfull");

    }

    public Cursor getData(String app, String weekDay) {
        // TODO Auto-generated method stub
        Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_APPS_USE+" where "+Attributes.APP_NAME+" = '" +app+ "'"+" AND "+
Attributes.DAY+" = '" +weekDay+ "'", null);
        return cursor;
    }

    public Cursor getApp() {
        // TODO Auto-generated method stub
        Cursor cursor=sqLiteDataBase.rawQuery("select DISTINCT * from
"+Attributes.TABLE_APPS_USE, null);
        return cursor;
    }

    public Cursor getApp1() {
        // TODO Auto-generated method stub
```

```
      Cursor cursor=sqLiteDataBase.rawQuery("select DISTINCT * from
"+Attributes.TABLE_APPS_NEW, null);
      return cursor;
   }
   public Cursor getCommonApp() {
      // TODO Auto-generated method stub
      Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_COMMON, null);
      return cursor;
   }

   public Cursor getLocationData() {
      // TODO Auto-generated method stub
      Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION, null);
      return cursor;
   }

   public Cursor getAppTime() {
      // TODO Auto-generated method stub
      Cursor cursor=sqLiteDataBase.rawQuery("select "+Attributes.TIME+" from
"+Attributes.TABLE_APPS_USE/*+" where "+Attributes.APP_NAME+" = '" +name+ "'"*/,
null);
      return cursor;
   }

   public Cursor getAppName(String string) {
      // TODO Auto-generated method stub
      Cursor cursor=sqLiteDataBase.rawQuery("select DISTINCT "+Attributes.NAME1+"
from "+Attributes.TABLE_APPS_NEW+" where "+Attributes.PACKAGE1+" = '" +string+ "'",
null);
      return cursor;
   }

   public Cursor getDay() {
      // TODO Auto-generated method stub
      Cursor cursor=sqLiteDataBase.rawQuery("select DISTINCT "+Attributes.DAY+"
from "+Attributes.TABLE_APPS_USE, null);
      return cursor;
   }

   public Cursor getAppNameByTime(String time) {
      // TODO Auto-generated method stub
      Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_APPS_USE+" where "+Attributes.TIME+" = '" +time+ "'", null);
      return cursor;
   }

   public Cursor getAppTimeByName(String app) {
      // TODO Auto-generated method stub
      Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_APPS_USE+" where "+Attributes.APP_NAME+" = '" +app+ "'", null);
      return cursor;
   }


   //Saim created

   public String getAppNameTest(String app) {

      Log.d("package name", app);
      String temp="";
      // TODO Auto-generated method stub
      Cursor cursor=sqLiteDataBase.rawQuery("select "+Attributes.NAME1+" from
"+Attributes.TABLE_APPS_NEW+" where "+Attributes.PACKAGE1+" = '" +app+ "'", null);
      if(cursor!=null){
         cursor.moveToFirst();
      if(cursor.moveToFirst()){
```

```
            do{
               temp=(cursor.getString(cursor.getColumnIndex(Attributes.NAME1)));
            }while(cursor.moveToNext());
         }
         }
         Log.d("package temp", temp);

         return temp;

      }

      public String getAppNameTest1(String app) {

         Log.d("package name", app);
         String temp="";
         // TODO Auto-generated method stub
         Cursor cursor=sqLiteDataBase.rawQuery("select "+Attributes.NAME1+" from
"+Attributes.TABLE_APPS_NEW+" where "+Attributes.NAME+" = '" +app+ "'", null);
         if(cursor!=null){
            cursor.moveToFirst();
         if(cursor.moveToFirst()){
            do{
               temp=(cursor.getString(cursor.getColumnIndex(Attributes.NAME1)));
            }while(cursor.moveToNext());
         }
         }
         return temp;
      }

      public Cursor getCommonApp(String time, String days) {
         // TODO Auto-generated method stub
         Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_APPS_USE+" where "+Attributes.TIME+" = '" +time+ "'"+" AND "+
Attributes.DAY+" = '" +days+ "'", null);
         return cursor;
      }


      //From here new database design...

      public void insertCommonUse(String weekDay, String app, String formattedTime) {
         // TODO Auto-generated method stub

         Log.e("Inside","Inside Insert Function");
         ContentValues contentValues=new ContentValues();
         try{
            contentValues.put(Attributes.COMMONDAY,weekDay);
            if(formattedTime.equals("00-01")){
               contentValues.put(Attributes.ONE,app);
            }else if(formattedTime.equals("01-02")){
               contentValues.put(Attributes.TWO,app);
            }else if(formattedTime.equals("02-03")){
               contentValues.put(Attributes.THREE,app);
            }else if(formattedTime.equals("03-04")){
               contentValues.put(Attributes.FOUR,app);
            }else if(formattedTime.equals("04-05")){
               contentValues.put(Attributes.FIVE,app);
            }else if(formattedTime.equals("05-06")){
               contentValues.put(Attributes.SIX,app);
            }else if(formattedTime.equals("06-07")){
               contentValues.put(Attributes.SEVEN,app);
            }else if(formattedTime.equals("07-08")){
               contentValues.put(Attributes.EIGHT,app);
            }else if(formattedTime.equals("08-09")){
               contentValues.put(Attributes.NINE,app);
            }else if(formattedTime.equals("09-10")){
               contentValues.put(Attributes.TEN,app);
            }else if(formattedTime.equals("10-11")){
```

```
            contentValues.put(Attributes.ELEVEN,app);
         }else if(formattedTime.equals("11-12")){
            contentValues.put(Attributes.TWELVE,app);
         }else if(formattedTime.equals("12-13")){
            contentValues.put(Attributes.THIRTEEN,app);
         }else if(formattedTime.equals("13-14")){
            contentValues.put(Attributes.FOURTEEN,app);
         }else if(formattedTime.equals("14-15")){
            contentValues.put(Attributes.FIFTEEN,app);
         }else if(formattedTime.equals("15-16")){
            contentValues.put(Attributes.SIXTEEN,app);
         }else if(formattedTime.equals("16-17")){
            contentValues.put(Attributes.SEVENTEEN,app);
         }else if(formattedTime.equals("17-18")){
            contentValues.put(Attributes.EIGHTEEN,app);
         }else if(formattedTime.equals("18-19")){
            contentValues.put(Attributes.NINTEEN,app);
         }else if(formattedTime.equals("19-20")){
            contentValues.put(Attributes.TWENTY,app);
         }else if(formattedTime.equals("20-21")){
            contentValues.put(Attributes.TWENTYONE,app);
         }else if(formattedTime.equals("21-22")){
            contentValues.put(Attributes.TWENTYTWO,app);
         }else if(formattedTime.equals("22-23")){
            contentValues.put(Attributes.TWENTYTHREE,app);
         }else if(formattedTime.equals("23-24")){
            contentValues.put(Attributes.TWENTYFOUR,app);
         }

      }catch(Exception e){
   }
      sqLiteDataBase.insert(Attributes.TABLE_COMMON,null,contentValues);
      Log.e("Insert","Insert successfully");

   }

   public Cursor getCommonApp(String weekDay) {
      Cursor cursor = null;

      Log.e("Inside function","Inside Function");
      // TODO Auto-generated method stub

         cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON+"
where "+Attributes.COMMONDAY+" = '" +weekDay+ "'", null);
          return cursor;
   }

   public int updateCommonUse(String weekDay, String app, String formattedTime) {
      // TODO Auto-generated method stub

      ContentValues contentValues=new ContentValues();
      try{

         if(formattedTime.equals("00-01")){
            contentValues.put(Attributes.ONE,app);
         }else if(formattedTime.equals("01-02")){
            contentValues.put(Attributes.TWO,app);
         }else if(formattedTime.equals("02-03")){
            contentValues.put(Attributes.THREE,app);
         }else if(formattedTime.equals("03-04")){
            contentValues.put(Attributes.FOUR,app);
         }else if(formattedTime.equals("04-05")){
            contentValues.put(Attributes.FIVE,app);
         }else if(formattedTime.equals("05-06")){
            contentValues.put(Attributes.SIX,app);
         }else if(formattedTime.equals("06-07")){
            contentValues.put(Attributes.SEVEN,app);
         }else if(formattedTime.equals("07-08")){
```

```
            contentValues.put(Attributes.EIGHT,app);
         }else if(formattedTime.equals("08-09")){
            contentValues.put(Attributes.NINE,app);
         }else if(formattedTime.equals("09-10")){
            contentValues.put(Attributes.TEN,app);
         }else if(formattedTime.equals("10-11")){
            contentValues.put(Attributes.ELEVEN,app);
         }else if(formattedTime.equals("11-12")){
            contentValues.put(Attributes.TWELVE,app);
         }else if(formattedTime.equals("12-13")){
            Log.e("Inside","Inside 13-14");
            contentValues.put(Attributes.THIRTEEN,app);
         }else if(formattedTime.equals("13-14")){
            contentValues.put(Attributes.FOURTEEN,app);
         }else if(formattedTime.equals("14-15")){
            contentValues.put(Attributes.FIFTEEN,app);
         }else if(formattedTime.equals("15-16")){
            contentValues.put(Attributes.SIXTEEN,app);
         }else if(formattedTime.equals("16-17")){
            contentValues.put(Attributes.SEVENTEEN,app);
         }else if(formattedTime.equals("17-18")){
            contentValues.put(Attributes.EIGHTEEN,app);
         }else if(formattedTime.equals("18-19")){
            contentValues.put(Attributes.NINTEEN,app);
         }else if(formattedTime.equals("19-20")){
            contentValues.put(Attributes.TWENTY,app);
         }else if(formattedTime.equals("20-21")){
            contentValues.put(Attributes.TWENTYONE,app);
         }else if(formattedTime.equals("21-22")){
            contentValues.put(Attributes.TWENTYTWO,app);
         }else if(formattedTime.equals("22-23")){
            contentValues.put(Attributes.TWENTYTHREE,app);
         }else if(formattedTime.equals("23-24")){
            contentValues.put(Attributes.TWENTYFOUR,app);
         }

      }catch(Exception e){
   }

      int
id=sqLiteDataBase.update(Attributes.TABLE_COMMON,contentValues,Attributes.COMMONDAY
+" = '" +weekDay+ "'",null);
      return id;
   }

   public Cursor getCommon(String formattedTime) {
      // TODO Auto-generated method stub
      Cursor cursor = null;

      if(formattedTime.equals("00-01")){
         cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
      }else if(formattedTime.equals("01-02")){
         cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
      }else if(formattedTime.equals("02-03")){
         cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
      }else if(formattedTime.equals("03-04")){
         cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
      }else if(formattedTime.equals("04-05")){
         cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
      }else if(formattedTime.equals("05-06")){
         cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
      }else if(formattedTime.equals("06-07")){
```

```
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("07-08")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("08-09")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("09-10")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("10-11")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("11-12")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("12-13")){
            Log.e("Inside","Inside 13-14");
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("13-14")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("14-15")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("15-16")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("16-17")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("17-18")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("18-19")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("19-20")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("20-21")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("21-22")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("22-23")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }else if(formattedTime.equals("23-24")){
            cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_COMMON,
null);
         }

         return cursor;
      }

      public void insertLocation(String weekDay, String app, String formattedTime) {
         // TODO Auto-generated method stub

         Log.e("Inside","Inside Insert Function");
         ContentValues contentValues=new ContentValues();
         try{
            contentValues.put(Attributes.LOC_DAY,weekDay);
            if(formattedTime.equals("00-01")){
               contentValues.put(Attributes.ONE_LOC,app);
```

```
        }else if(formattedTime.equals("01-02")){
           contentValues.put(Attributes.TWO_LOC,app);
        }else if(formattedTime.equals("02-03")){
           contentValues.put(Attributes.THREE_LOC,app);
        }else if(formattedTime.equals("03-04")){
           contentValues.put(Attributes.FOUR_LOC,app);
        }else if(formattedTime.equals("04-05")){
           contentValues.put(Attributes.FIVE_LOC,app);
        }else if(formattedTime.equals("05-06")){
           contentValues.put(Attributes.SIX_LOC,app);
        }else if(formattedTime.equals("06-07")){
           contentValues.put(Attributes.SEVEN_LOC,app);
        }else if(formattedTime.equals("07-08")){
           contentValues.put(Attributes.EIGHT_LOC,app);
        }else if(formattedTime.equals("08-09")){
           contentValues.put(Attributes.NINE_LOC,app);
        }else if(formattedTime.equals("09-10")){
           contentValues.put(Attributes.TEN_LOC,app);
        }else if(formattedTime.equals("10-11")){
           contentValues.put(Attributes.ELEVEN_LOC,app);
        }else if(formattedTime.equals("11-12")){
           contentValues.put(Attributes.TWELVE_LOC,app);
        }else if(formattedTime.equals("12-13")){
           contentValues.put(Attributes.THIRTEEN_LOC,app);
        }else if(formattedTime.equals("13-14")){
           contentValues.put(Attributes.FOURTEEN_LOC,app);
        }else if(formattedTime.equals("14-15")){
           contentValues.put(Attributes.FIFTEEN_LOC,app);
        }else if(formattedTime.equals("15-16")){
           contentValues.put(Attributes.SIXTEEN_LOC,app);
        }else if(formattedTime.equals("16-17")){
           contentValues.put(Attributes.SEVENTEEN_LOC,app);
        }else if(formattedTime.equals("17-18")){
           contentValues.put(Attributes.EIGHTEEN_LOC,app);
        }else if(formattedTime.equals("18-19")){
           contentValues.put(Attributes.NINTEEN_LOC,app);
        }else if(formattedTime.equals("19-20")){
           contentValues.put(Attributes.TWENTY_LOC,app);
        }else if(formattedTime.equals("20-21")){
           contentValues.put(Attributes.TWENTYONE_LOC,app);
        }else if(formattedTime.equals("21-22")){
           contentValues.put(Attributes.TWENTYTWO_LOC,app);
        }else if(formattedTime.equals("22-23")){
           contentValues.put(Attributes.TWENTYTHREE_LOC,app);
        }else if(formattedTime.equals("23-24")){
           contentValues.put(Attributes.TWENTYFOUR_LOC,app);
        }

     }catch(Exception e){
}
     sqLiteDataBase.insert(Attributes.TABLE_LOCATION,null,contentValues);
     Log.e("Insert","Insert Location successfully");

}

public int updateLocation(String weekDay, String latlng,
        String formattedTime) {
     // TODO Auto-generated method stub

     ContentValues contentValues=new ContentValues();
     try{

        if(formattedTime.equals("00-01")){
           contentValues.put(Attributes.ONE_LOC,latlng);
        }else if(formattedTime.equals("01-02")){
           contentValues.put(Attributes.TWO_LOC,latlng);
        }else if(formattedTime.equals("02-03")){
           contentValues.put(Attributes.THREE_LOC,latlng);
```

```
            }else if(formattedTime.equals("03-04")){
               contentValues.put(Attributes.FOUR_LOC,latlng);
            }else if(formattedTime.equals("04-05")){
               contentValues.put(Attributes.FIVE_LOC,latlng);
            }else if(formattedTime.equals("05-06")){
               contentValues.put(Attributes.SIX_LOC,latlng);
            }else if(formattedTime.equals("06-07")){
               contentValues.put(Attributes.SEVEN_LOC,latlng);
            }else if(formattedTime.equals("07-08")){
               contentValues.put(Attributes.EIGHT_LOC,latlng);
            }else if(formattedTime.equals("08-09")){
               contentValues.put(Attributes.NINE_LOC,latlng);
            }else if(formattedTime.equals("09-10")){
               contentValues.put(Attributes.TEN_LOC,latlng);
            }else if(formattedTime.equals("10-11")){
               contentValues.put(Attributes.ELEVEN_LOC,latlng);
            }else if(formattedTime.equals("11-12")){
               contentValues.put(Attributes.TWELVE_LOC,latlng);
            }else if(formattedTime.equals("12-13")){
               Log.e("Inside","Inside 13-14");
               contentValues.put(Attributes.THIRTEEN_LOC,latlng);
            }else if(formattedTime.equals("13-14")){
               contentValues.put(Attributes.FOURTEEN_LOC,latlng);
            }else if(formattedTime.equals("14-15")){
               contentValues.put(Attributes.FIFTEEN_LOC,latlng);
            }else if(formattedTime.equals("15-16")){
               contentValues.put(Attributes.SIXTEEN_LOC,latlng);
            }else if(formattedTime.equals("16-17")){
               contentValues.put(Attributes.SEVENTEEN_LOC,latlng);
            }else if(formattedTime.equals("17-18")){
               contentValues.put(Attributes.EIGHTEEN_LOC,latlng);
            }else if(formattedTime.equals("18-19")){
               contentValues.put(Attributes.NINTEEN_LOC,latlng);
            }else if(formattedTime.equals("19-20")){
               contentValues.put(Attributes.TWENTY_LOC,latlng);
            }else if(formattedTime.equals("20-21")){
               contentValues.put(Attributes.TWENTYONE_LOC,latlng);
            }else if(formattedTime.equals("21-22")){
               contentValues.put(Attributes.TWENTYTWO_LOC,latlng);
            }else if(formattedTime.equals("22-23")){
               contentValues.put(Attributes.TWENTYTHREE_LOC,latlng);
            }else if(formattedTime.equals("23-24")){
               contentValues.put(Attributes.TWENTYFOUR_LOC,latlng);
            }

         }catch(Exception e){
      }

         Log.d("TAG", "WEEK DAY:"+formattedTime);
         Log.d("TAG", "WEEK DAY:"+weekDay);

         int
id=sqLiteDataBase.update(Attributes.TABLE_LOCATION,contentValues,Attributes.LOC_DAY
+" = '" +weekDay+ "'",null);
         return id;
      }

      public void updateSetepData(String weekDay, String caount,
            String formattedTime,String distance) {
         // TODO Auto-generated method stub
         Log.e("TAG", "FORMATED TIME:================="+formattedTime);

         ContentValues contentValues=new ContentValues();
         try{

            if(formattedTime.equals("00-01")){
               contentValues.put(Attributes.ONE_CAUNT,caount);
               contentValues.put(Attributes.ONE_DISTANCE,distance);
```

```
}else if(formattedTime.equals("01-02")){
   contentValues.put(Attributes.TWO_CAUNT,caount);
   contentValues.put(Attributes.TWO_DISTANCE,distance);
}else if(formattedTime.equals("02-03")){
   contentValues.put(Attributes.THREE_CAUNT,caount);
   contentValues.put(Attributes.THREE_DISTANCE,distance);
}else if(formattedTime.equals("03-04")){
   contentValues.put(Attributes.FOUR_CAUNT,caount);
   contentValues.put(Attributes.THREE_DISTANCE,distance);
}else if(formattedTime.equals("04-05")){
   contentValues.put(Attributes.FIVE_CAUNT,caount);
   contentValues.put(Attributes.FIVE_DISTANCE,distance);
}else if(formattedTime.equals("05-06")){
   contentValues.put(Attributes.SIX_CAUNT,caount);
   contentValues.put(Attributes.SIX_DISTANCE,distance);
}else if(formattedTime.equals("06-07")){
   contentValues.put(Attributes.SEVEN_CAUNT,caount);
   contentValues.put(Attributes.SEVEN_DISTANCE,distance);
}else if(formattedTime.equals("07-08")){
   contentValues.put(Attributes.EIGHT_CAUNT,caount);
   contentValues.put(Attributes.EIGHT_DISTANCE,distance);
}else if(formattedTime.equals("08-09")){
   contentValues.put(Attributes.NINE_CAUNT,caount);
   contentValues.put(Attributes.NINE_DISTANCE,distance);
}else if(formattedTime.equals("09-10")){
   contentValues.put(Attributes.TEN_CAUNT,caount);
   contentValues.put(Attributes.TEN_DISTANCE,distance);
}else if(formattedTime.equals("10-11")){
   contentValues.put(Attributes.ELEVEN_CAUNT,caount);
   contentValues.put(Attributes.ELEVEN_DISTANCE,distance);
}else if(formattedTime.equals("11-12")){
   contentValues.put(Attributes.TWELVE_CAUNT,caount);
   contentValues.put(Attributes.TWELVE_DISTANCE,distance);
}else if(formattedTime.equals("12-13")){
   Log.e("Inside","Inside 13-14");
   contentValues.put(Attributes.THIRTEEN_CAUNT,caount);
   contentValues.put(Attributes.THIRTEEN_DISTANCE,distance);
}else if(formattedTime.equals("13-14")){
   contentValues.put(Attributes.FOURTEEN_CAUNT,caount);
   contentValues.put(Attributes.FOURTEEN_DISTANCE,distance);
}else if(formattedTime.equals("14-15")){
   contentValues.put(Attributes.FIFTEEN_CAUNT,caount);
   contentValues.put(Attributes.FIFTEEN_DISTANCE,distance);
}else if(formattedTime.equals("15-16")){
   contentValues.put(Attributes.SIXTEEN_CAUNT,caount);
   contentValues.put(Attributes.SIXTEEN_DISTANCE,distance);
}else if(formattedTime.equals("16-17")){
   contentValues.put(Attributes.SEVENTEEN_CAUNT,caount);
   contentValues.put(Attributes.SEVENTEEN_DISTANCE,distance);
}else if(formattedTime.equals("17-18")){
   contentValues.put(Attributes.EIGHTEEN_CAUNT,caount);
   contentValues.put(Attributes.EIGHTEEN_DISTANCE,distance);
}else if(formattedTime.equals("18-19")){
   contentValues.put(Attributes.NINTEEN_CAUNT,caount);
   contentValues.put(Attributes.NINTEEN_DISTANCE,distance);
}else if(formattedTime.equals("19-20")){
   contentValues.put(Attributes.TWENTY_CAUNT,caount);
   contentValues.put(Attributes.TWENTY_DISTANCE,distance);
}else if(formattedTime.equals("20-21")){
   contentValues.put(Attributes.TWENTYONE_CAUNT,caount);
   contentValues.put(Attributes.TWENTYONE_DISTANCE,distance);
}else if(formattedTime.equals("21-22")){
   contentValues.put(Attributes.TWENTYTWO_CAUNT,caount);
   contentValues.put(Attributes.TWENTYTWO_DISTANCE,distance);
}else if(formattedTime.equals("22-23")){
   contentValues.put(Attributes.TWENTYTHREE_CAUNT,caount);
   contentValues.put(Attributes.TWENTYTHREE_DISTANCE,distance);
}else if(formattedTime.equals("23-24")){
```

```
            contentValues.put(Attributes.TWENTYFOUR_CAUNT,caount);
            contentValues.put(Attributes.TWENTYFOUR_DISTANCE,distance);
         }

      }catch(Exception e){
   }

      Log.d("TAG", "WEEK DAY:"+formattedTime);
      Log.d("TAG", "WEEK DAY:"+weekDay);
      Log.d("TAG", "UPDATED :");


sqLiteDataBase.update(Attributes.TABLE_WAKING,contentValues,Attributes.WAKING_DAY+"
= '" +weekDay+ "'",null);

   }

   public Cursor getLocation(String formattedTime) {
      // TODO Auto-generated method stub
      Cursor cursor = null;

      if(formattedTime.equals("00-01")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.ONE_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("01-02")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.TWO_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("02-03")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.THREE_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("03-04")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.FOUR_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("04-05")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.FIVE_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("05-06")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.SIX_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("06-07")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.SEVEN_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("07-08")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.EIGHT_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("08-09")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.NINE_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("09-10")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.TEN_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("10-11")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.ELEVEN_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("11-12")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.TWELVE_LOC+" = '" +formattedTime+
```

```
"'", null);
      }else if(formattedTime.equals("12-13")){
         Log.e("Inside","Inside 13-14");
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.THIRTEEN_LOC+" = '"
+formattedTime+ "'", null);
      }else if(formattedTime.equals("13-14")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.FOURTEEN_LOC+" = '"
+formattedTime+ "'", null);
      }else if(formattedTime.equals("14-15")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.FIFTEEN_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("15-16")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.SIXTEEN_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("16-17")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.SEVENTEEN_LOC+" = '"
+formattedTime+ "'", null);
      }else if(formattedTime.equals("17-18")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.EIGHTEEN_LOC+" = '"
+formattedTime+ "'", null);
      }else if(formattedTime.equals("18-19")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.NINTEEN_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("19-20")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.TWENTY_LOC+" = '" +formattedTime+
"'", null);
      }else if(formattedTime.equals("20-21")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.TWENTYONE_LOC+" = '"
+formattedTime+ "'", null);
      }else if(formattedTime.equals("21-22")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.TWENTYTWO_LOC+" = '"
+formattedTime+ "'", null);
      }else if(formattedTime.equals("22-23")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.TWENTYTHREE_LOC+" = '"
+formattedTime+ "'", null);
      }else if(formattedTime.equals("23-24")){
         cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION+" where "+Attributes.TWENTYFOUR_LOC+" = '"
+formattedTime+ "'", null);
      }
       return cursor;
   }

   public Cursor getTestLocation() {

      Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_LOCATION , null);
       return cursor;

   }

   public int updateApps(String name, String option) {
      // TODO Auto-generated method stub

      Log.e("Apps Updated", name);
      ContentValues contentValues=new ContentValues();
      try{
```

```
            contentValues.put(Attributes.PRIORITY1,option);
         }catch(Exception e){
      }

         int
id=sqLiteDataBase.update(Attributes.TABLE_APPS_NEW,contentValues,Attributes.NAME1+"
= '" +name+ "'",null);
         return id;
      }

      //saim code
      public void insertImageDetail(String id,String base64)
      {
            ContentValues contentValues=new ContentValues();
         try{
            contentValues.put(Attributes.IMGID,id);
            contentValues.put(Attributes.IMAGE_BASE64, base64);

         }catch(Exception e){
      }
         Log.d(TAG,"Data is Inserted");
          sqLiteDataBase.insert(Attributes.TABLE_IMAGE,null,contentValues);
      }

      public void insertVoiceDetail(String id,String voicebase64)
      {
            ContentValues contentValues=new ContentValues();
         try{
            contentValues.put(Attributes.VOICEID,id);
            contentValues.put(Attributes.VOICE_BASE64, voicebase64);

         }catch(Exception e){
      }
         Log.e(TAG,"VOICE Data is Inserted");
          sqLiteDataBase.insert(Attributes.TABLE_VOICE,null,contentValues);
      }

//===============get Methods================== //

//get all deta
      public Cursor getImageDetails(){
         Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_IMAGE+ " order by "+Attributes.IMGID+ " asc ", null);
         return cursor;
      }

      public Cursor getVoiceDetails(){
         Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_VOICE+ " order by "+Attributes.VOICEID+ " asc ", null);
         return cursor;
      }

      public void insertFingureDetail(String id,String urdutype) {
         ContentValues contentValues=new ContentValues();
         try{
            contentValues.put(Attributes.FACE_ID,id);
            contentValues.put(Attributes.FACE_INDEX, urdutype);
         }catch(Exception e){
      }
      Log.d(TAG,"Data is Inserted");
      sqLiteDataBase.insert(Attributes.TABLE_FINGURE,null,contentValues);

}

//===============get Methods================== //


      public Cursor getFingureDetails(){
```

```
      Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_FINGURE+ " order by "+Attributes.FACE_ID+ " desc ", null);
      return cursor;
   }


   //SMS Function Methoods

      public void inserttextsmsData(String id,String value,String text) {
            ContentValues contentValues=new ContentValues();
         try{
            contentValues.put(Attributes.TEXTSMS_ID,id);
            contentValues.put(Attributes.TEXTSMS_VALUE, value);
            contentValues.put(Attributes.TEXTSMS_TEXT, text);


         }catch(Exception e){
      }
         sqLiteDataBase.insert(Attributes.TABLE_TEXTSMS,null,contentValues);
   }

public Cursor gettextsmsData() {
   // TODO Auto-generated method stub
   Cursor cursor=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_TEXTSMS+" ORDER BY "+Attributes.TEXTSMS_ID+" DESC " , null);
   return cursor;

}

public void insertsentsmsData(String number,String content) {
    ContentValues contentValues=new ContentValues();
   try{
      contentValues.put(Attributes.SMS_NUMBER,number);
      contentValues.put(Attributes.SMS_CONTENT, content);

   }catch(Exception e){
}
   sqLiteDataBase.insert(Attributes.TABLE_SENTSMS,null,contentValues);
}

public Cursor getsentsmsData() {
// TODO Auto-generated method stub
Cursor cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_SENTSMS+"
ORDER BY "+Attributes.SMS_NUMBER+" DESC " , null);
return cursor;

}

public boolean getCheckTextSmsId(String text){

   boolean isvalid=false;
   ArrayList<String> textvalue=new ArrayList<String>();
   Cursor cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_TEXTSMS
, null);
   if(cursor!=null)
    cursor.moveToFirst();
   if(cursor.moveToFirst()){
    do{

textvalue.add(cursor.getString(cursor.getColumnIndex(Attributes.TEXTSMS_VALUE)));
       }while(cursor.moveToNext());
   }cursor.close();

   for(int i=0;i < textvalue.size();i++){
    if(text.equals(textvalue.get(i))){
     Log.d(TAG,"id is already exists");
     isvalid=true;
     break;
```

```
     }
    }
     return isvalid;
    }


public boolean getCheckSentSmsContent(String text){

   boolean isvalid=false;
   ArrayList<String> textvalue=new ArrayList<String>();
   Cursor cursor=sqLiteDataBase.rawQuery("select * from "+Attributes.TABLE_SENTSMS
, null);
   if(cursor!=null)
    cursor.moveToFirst();
   if(cursor.moveToFirst()){
    do{

textvalue.add(cursor.getString(cursor.getColumnIndex(Attributes.SMS_CONTENT)));
       }while(cursor.moveToNext());
   }cursor.close();

   for(int i=0;i < textvalue.size();i++){
    if(text.equals(textvalue.get(i))){
     Log.d(TAG,"id is already exists");
     isvalid=true;
     break;
    }
   }
    return isvalid;
   }

public String getallSMSNumber(String content){

   Log.e("TAG", "DB Contnt"+content);
// content=content.replaceAll("'","\'");

   String number="";
   Cursor cursor1=sqLiteDataBase.rawQuery("select * from
"+Attributes.TABLE_TEXTSMS+ " where "+Attributes.TEXTSMS_VALUE+" = '"+content+"'" ,
null);
   Log.d(TAG,"cursor1 caount == "+cursor1.getCount());
   if(cursor1!=null)
      cursor1.moveToFirst();
        if(cursor1.moveToFirst()){
         do{

         number=cursor1.getString(cursor1.getColumnIndex(Attributes.TEXTSMS_ID));

          }while(cursor1.moveToNext());
      }
    cursor1.close();
    Log.e("TAG", "DB number"+number);
   return number;
}

   public void insertWalkingStepCaunt(String caount,
         String distance,
//       String distance, String distanceperhour,
         String formattedTime,String formattedDay) {

      ContentValues contentValues = new ContentValues();
      try {

         contentValues.put(Attributes.WAKING_DAY, formattedDay);

         if(formattedTime.equals("00-01")){
            contentValues.put(Attributes.ONE_CAUNT,caount);
            contentValues.put(Attributes.ONE_DISTANCE,distance);
```

```
}else if(formattedTime.equals("01-02")){
   contentValues.put(Attributes.TWO_CAUNT,caount);
   contentValues.put(Attributes.TWO_DISTANCE,distance);

}else if(formattedTime.equals("02-03")){
   contentValues.put(Attributes.THREE_CAUNT,caount);
   contentValues.put(Attributes.THREE_DISTANCE,distance);
}else if(formattedTime.equals("03-04")){
   contentValues.put(Attributes.FOUR_CAUNT,caount);
   contentValues.put(Attributes.FOUR_DISTANCE,distance);
}else if(formattedTime.equals("04-05")){
   contentValues.put(Attributes.FIVE_CAUNT,caount);
   contentValues.put(Attributes.FIVE_DISTANCE,distance);
}else if(formattedTime.equals("05-06")){
   contentValues.put(Attributes.SIX_CAUNT,caount);
   contentValues.put(Attributes.SIX_DISTANCE,distance);
}else if(formattedTime.equals("06-07")){
   contentValues.put(Attributes.SEVEN_CAUNT,caount);
   contentValues.put(Attributes.SEVEN_DISTANCE,distance);
}else if(formattedTime.equals("07-08")){
   contentValues.put(Attributes.EIGHT_CAUNT,caount);
   contentValues.put(Attributes.EIGHT_DISTANCE,distance);
}else if(formattedTime.equals("08-09")){
   contentValues.put(Attributes.NINE_CAUNT,caount);
   contentValues.put(Attributes.NINE_DISTANCE,distance);
}else if(formattedTime.equals("09-10")){
   contentValues.put(Attributes.TEN_CAUNT,caount);
   contentValues.put(Attributes.TEN_DISTANCE,distance);
}else if(formattedTime.equals("10-11")){
   contentValues.put(Attributes.ELEVEN_CAUNT,caount);
   contentValues.put(Attributes.ELEVEN_DISTANCE,distance);
}else if(formattedTime.equals("11-12")){
   contentValues.put(Attributes.TWELVE_CAUNT,caount);
   contentValues.put(Attributes.TWELVE_DISTANCE,distance);
}else if(formattedTime.equals("12-13")){
   contentValues.put(Attributes.THIRTEEN_CAUNT,caount);
   contentValues.put(Attributes.THIRTEEN_DISTANCE,distance);
}else if(formattedTime.equals("13-14")){
   contentValues.put(Attributes.FOURTEEN_CAUNT,caount);
   contentValues.put(Attributes.FOURTEEN_DISTANCE,distance);
}else if(formattedTime.equals("14-15")){
   contentValues.put(Attributes.FIFTEEN_CAUNT,caount);
   contentValues.put(Attributes.FIFTEEN_DISTANCE,distance);
}else if(formattedTime.equals("15-16")){
   contentValues.put(Attributes.SIXTEEN_CAUNT,caount);
   contentValues.put(Attributes.SIXTEEN_DISTANCE,distance);
}else if(formattedTime.equals("16-17")){
   contentValues.put(Attributes.SEVENTEEN_CAUNT,caount);
   contentValues.put(Attributes.SEVENTEEN_DISTANCE,distance);
}else if(formattedTime.equals("17-18")){
   contentValues.put(Attributes.EIGHTEEN_CAUNT,caount);
   contentValues.put(Attributes.EIGHTEEN_DISTANCE,distance);
}else if(formattedTime.equals("18-19")){
   contentValues.put(Attributes.NINTEEN_CAUNT,caount);
   contentValues.put(Attributes.NINTEEN_DISTANCE,distance);
}else if(formattedTime.equals("19-20")){
   contentValues.put(Attributes.TWENTY_CAUNT,caount);
   contentValues.put(Attributes.TWENTY_DISTANCE,distance);
}else if(formattedTime.equals("20-21")){
   contentValues.put(Attributes.TWENTYONE_CAUNT,caount);
   contentValues.put(Attributes.TWENTYONE_DISTANCE,distance);
}else if(formattedTime.equals("21-22")){
   contentValues.put(Attributes.TWENTYTWO_CAUNT,caount);
   contentValues.put(Attributes.TWENTYTWO_DISTANCE,distance);
}else if(formattedTime.equals("22-23")){
   contentValues.put(Attributes.TWENTYTHREE_CAUNT,caount);
   contentValues.put(Attributes.TWENTYTHREE_DISTANCE,distance);
```

```
            }else if(formattedTime.equals("23-24")){
               contentValues.put(Attributes.TWENTYFOUR_CAUNT,caount);
               contentValues.put(Attributes.TWENTYFOUR_DISTANCE,distance);
            }

         } catch (Exception e) {
         }
         Log.e("TAG", "WAKING DATA IS INSERT");
         sqLiteDataBase.insert(Attributes.TABLE_WAKING, null, contentValues);
      }

      public Cursor getWalkingStepCaunt() {
         // TODO Auto-generated method stub
         Cursor cursor = sqLiteDataBase.rawQuery("select * from "
               + Attributes.TABLE_WAKING, null);
         return cursor;

      }


}
```

Appendix F – Experimental Analysis Scripts (MATLAB)

```
clear y;
% Enter the folder path below in colons that contains data
dirName = 'C:\Users\aalabdulwahid\OneDrive\OneDrive - University of
Plymouth\Cleaned BioData';              %# folder path
files=find_files(dirName,'.xls');

ctr=1;
ctr1=1;
ctr2=1;
appUsage=[];
stepDistance=[];
stepCount=[];
[y{1:2, 1:50}] = deal(zeros(1));

addressTAU={};
addressSD={};
addressSC={};
for file=files
    %file
    rawData=[];
    cell=strfind(file,'TotalAppsUsage');
    if ~isempty(cell{1,1})
      [~,~,rawData] = xlsread(fullfile(char(file)));
      addressTAU(ctr)=file;
      ctr=ctr+1;
      appUsage=[appUsage,rawData.'];
    end
    rawData=[];
    cell=strfind(file,'StepDetectCount');
    if ~isempty(cell{1,1})
      [~,~,rawData] = xlsread(fullfile(char(file)));
      addressSC(ctr1)=file;
      ctr1=ctr1+1;
      if (size(rawData)==[2,50])
          stepCount=[stepCount,rawData.'];
      else
          stepCount=[stepCount,y.'];
      end
    end
    rawData=[];
    cell=strfind(file,'StepDetectDistance');
    if ~isempty(cell{1,1})
      [~,~,rawData] = xlsread(fullfile(char(file)));
      addressSD(ctr2)=file;
      ctr2=ctr2+1;
      if (size(rawData)==[2,50])
          stepDistance=[stepDistance,rawData.'];
      else
          stepDistance=[stepDistance,y.'];
      end
    end
end


a=size(stepCount);
row=1;
col=1;
sc=[];
for i=2:2:a(2)
    for j=3:2:a(1)
        if isempty(stepCount{j,i}) || ~(ischar(stepCount{j,i}))
||isempty(str2num(stepCount{j,i}))
            sc(row,col)=0;
            row=row+1;
        else
```

```
            sc(row,col)=str2num(stepCount{j,i});
            row=row+1;
        end
    end
    col=col+1;
    row=1;
end

a=size(stepDistance);
row=1;
col=1;
sd=[];
for i=2:2:a(2)
    for j=3:2:a(1)
        if isempty(stepDistance{j,i}) || ~(ischar(stepDistance{j,i}))
||isempty(str2num(stepDistance{j,i}))
            sd(row,col)=0;
            row=row+1;
        else
            sd(row,col)=str2num(stepDistance{j,i});
            row=row+1;
        end
    end
    col=col+1;
    row=1;
end


addresstau=[];
for ad=addressTAU
    if ~isempty(regexp(char(ad),' (\d+) ','match'))
        temp=char(regexp(char(ad),' (\d+) ','match'));
        addresstau=[addresstau,str2num(temp(2:(length(temp)-1)))];
    else
        temp=(regexp(char(ad),' (\d+)\','match'));
        temp=char(temp(1));
        addresstau=[addresstau,str2num(temp(2:(length(temp)-1)))];
    end
end

addresssd=[];
for ad=addressSD
    if ~isempty(regexp(char(ad),' (\d+) ','match'))
        temp=char(regexp(char(ad),' (\d+) ','match'));
        addresssd=[addresssd,str2num(temp(2:(length(temp)-1)))];
    else
        temp=(regexp(char(ad),' (\d+)\','match'));
        temp=char(temp(1));
        addresssd=[addresssd,str2num(temp(2:(length(temp)-1)))];
    end
end

addresssc=[];
for ad=addressSC
    if ~isempty(regexp(char(ad),' (\d+) ','match'))
        temp=char(regexp(char(ad),' (\d+) ','match'));
        addresssc=[addresssc,str2num(temp(2:(length(temp)-1)))];
    else
        temp=(regexp(char(ad),' (\d+)\','match'));
        temp=char(temp(1));
        addresssc=[addresssc,str2num(temp(2:(length(temp)-1)))];
    end
end


s=size(sc);
[meanvectsc,meanusersc]=meanAll(sc,addresssc);
samplestdvectsc=stdAll(sc,addresssc);
```

```
farsc=FAR(meanusersc,meanvectsc,samplestdvectsc,s(2));
frrsc=FRR(sc,addresssc,meanvectsc,samplestdvectsc);
temp=abs(farsc-frrsc);
eersc=min(temp.');
%disp('the eer for step count =')'
%disp(eersc)

s=size(sd);
[meanvectsd,meanusersd]=meanAll(sd,addresssd);
samplestdvectsd=stdAll(sd,addresssd);
farsd=FAR(meanusersd,meanvectsd,samplestdvectsd,s(2));
frrsd=FRR(sd,addresssd,meanvectsd,samplestdvectsd);
temp=abs(farsd-frrsd);
eersd=min(temp.');
gaitPerUser=(abs(farsc-frrsc)+abs(farsd-frrsd))/2;
gaitPerUser=[gaitPerUser;meanusersc];

%App usage part
appusers=[];
s=size(appUsage);
ctr=1;
temp={};
user=addresstau(ctr);
appEER=[];
appUsage{6,1}=num2str(addresstau(ctr));
for i=2:s(2)
    if ~strcmp(appUsage{1,i},'APP Name')
        temp=[temp,appUsage(:,i)];
        appUsage{6,i}=num2str(addresstau(ctr));
    else
        ctr=ctr+1;
        appUsage{6,i}=num2str(addresstau(ctr));
        if user~=addresstau(ctr)
            appEER=[appEER,userappEER(temp)];
            temp={};
            appusers=[appusers,user];
            user=addresstau(ctr);
        end
    end
    if i==s(2)
        appUsage{6,i}=num2str(addresstau(ctr));
        appEER=[appEER,userappEER(temp)];
        appusers=[appusers,user];
    end
end
appEERperuser=appEER;
appEERperuser=[appEERperuser;appusers];
appEER=mean(appEER,2);


%location part

%dirName = 'D:\biometric analysis\Sample of BioData\Sample of
BioData';              %# folder path
files=find_files(dirName,'.xls');
Mat={};
locMat={};
ctr=1;
for file=files
    rawData=[];
    cell=strfind(file,'Location');
    if ~isempty(cell{1,1})
        try
          [~,~,rawData] = xlsread(fullfile(char(file)));
          s=size(rawData);
          for i=3:2:s(2)
              if ~isempty(rawData{2,i})
                  Mat(ctr)=rawData(2,i);
```

```
                else
                    Mat(ctr)={'0,0'};
                end
                ctr=ctr+1;
            end
            if ~isempty(regexp(char(file),' (\d+) ','match'))
                temp=char(regexp(char(file),' (\d+) ','match'));
                Mat(ctr)={(temp(2:(length(temp)-1)))};
            else
                temp=(regexp(char(file),' (\d+)\','match'));
                temp=char(temp(1));
                Mat(ctr)={(temp(2:(length(temp)-1)))};
            end
            ctr=1;
            locMat=[locMat,Mat.'];
            Mat={};
        catch
        end
    end
end

totalNonZero=0;
s=size(locMat);
for i=1:s(1)
    for j=1:s(2)
        temp=strsplit(locMat{i,j},'~');
        locMat(i,j)=temp(1);
    end
end

temp={};
user=locMat{25,1};
s=size(locMat);
locEERmatrix=[];
for i=1:s(2)
    if locMat{25,i}==user
        temp=[temp,locMat(:,i)];
    else
        try
            s1=size(temp);
            compare(1)=1;
            compare(2)=2;
            compare(3)=vectdist(temp(:,1),temp(:,2));
            for j=1:s1(2)
                for k=j+1:s1(2)
                    if vectdist(temp(:,j),temp(:,k)) < compare(3)
                        compare(1)=j;
                        compare(2)=k;
                        compare(3)=vectdist(temp(:,j),temp(:,k));
                    end
                end
            end

usereer=1/(nonZero(temp)/(nonZero(temp(:,compare(1)))+nonZero(temp(:,compare(2)))));
            locEERmatrix=[locEERmatrix,[usereer;str2num(user)]];
        catch
        end
            temp={};
            temp=[temp,locMat(:,i)];
            user=locMat{25,i};
    end
    if i==s(2)
        try
            s1=size(temp);
            compare(1)=1;
            compare(2)=2;
            compare(3)=vectdist(temp(:,1),temp(:,2));
            for j=1:s1(2)
```

```
                for k=j+1:s1(2)
                    if vectdist(temp(:,j),temp(:,k)) < compare(1)
                        compare(1)=j;
                        compare(2)=k;
                        compare(3)=vectdist(temp(:,j),temp(:,k));
                    end
                end
            end

usereer=1/(nonZero(temp)/(nonZero(temp(:,compare(1)))+nonZero(temp(:,compare(2)))));
            locEERmatrix=[locEERmatrix,[usereer;str2num(user)]];
        catch
        end
    end
end
locEERmatrixperuser=[];
s=size(locEERmatrix);
for i=1:s(2)
    locEERmatrixperuser(1:24,i)=locEERmatrix(1,i);
    locEERmatrixperuser(25,i)=locEERmatrix(2,i);
end
locEERmatrix=mean(locEERmatrix,2);
locEER(1:24)=locEERmatrix(1);


%Image Part.
imageEER=xlsread('imageEER.xls');
imageEERperuser=xlsread('imageEERperuser.xls');

%Gait
gaitEER=(eersc+eersd)/2;

%Fingerprint EER
fingerprintEER(1:24)=0.01;  %Assumed

%Voice EER
voiceEER(1:24)=0.15;%Assumed

%Face,Finger Print, GPS,Voice, App Usage, Gait. ! is for Yes and 0 is for No
availability=[1,1,1,1,1,1];  %Assumed
conditions=[1,1,1,1,1,1;1,1,0,1,1,1;1,0,1,1,1,1;1,0,0,1,1,1;0,1,1,1,1,1;0,1,0,1,1,1
;0,0,1,1,1,1;0,0,0,1,1,1];
weights=[20,25,10,15,15,15;25,25,0,15,20,15;30,0,10,20,20,20;30,0,0,30,20,20;0,35,1
0,25,15,15;0,35,0,30,20,15;0,0,15,35,30,20;0,0,0,40,30,30];

hour=0;

eer=[];

clear y;

%3D the overall fused authentication confidence, App usage timeline and
%their risk levels
%overall,individual,(Face,Finger Print, GPS,Voice, App Usage, Gait)*individual,
(")*overall.
s=size(appUsage);
temp={};
for i=2:s(2)
    if ~strcmp(appUsage{1,i},'APP Name')
        try
            temp=appUsage(:,i);
            z=temp{3};
            hour=strsplit(z,'-');
            hour=hour{1};
            hour=str2num(hour);
        catch
            hour=1;
        end
```

```
eer=([imageEER(hour),fingerprintEER(hour),locEER(hour),voiceEER(hour),appEER(hour),
gaitEER(hour)]).';
        eeroa=100*([1 1 1 1 1 1]-eer.');

        for j= 1:8
            if isequal(availability,conditions(j,:))
                fusedEER=weights(j,:)*eer;
            end
        end
        eer=zeros(1,6);
        ac=100-fusedEER;
        appUsage{7,i}=num2str(ac);
        user=str2num(appUsage{6,i});
        for j=imageEERperuser
            if user==j(25)
                eer(1)=j(hour);
            end
        end
        eer(2)=fingerprintEER(hour);
        for j=locEERmatrixperuser
            if user==j(25)
                eer(3)=j(hour);
            end
        end
        eer(4)=voiceEER(hour);
        for j=appEERperuser
            if user==j(25)
                eer(5)=j(hour);
            end
        end
        for j=gaitPerUser
            if user==j(25)
                eer(6)=j(hour);
            end
        end
        eer=eer.';
        for j= 1:8
            if isequal(availability,conditions(j,:))
                fusedEER=weights(j,:)*eer;
            end
        end
        ac=100-fusedEER;
        appUsage{8,i}=num2str(ac);
        eer=100*([1 1 1 1 1 1]-eer.');
        for j=9:14
            appUsage{j,i}=num2str(eer(j-8));
        end
        for j=15:20
            appUsage{j,i}=num2str(eeroa(j-14));
        end
    end
end
s=size(appUsage);
temp={};
matrix={};
j=1;
%overall,individual,(Face,Finger Print, GPS,Voice, App Usage, Gait)*individual,
(")*overall.
for i=2:s(2)
    if  ~strcmp(appUsage{1,i},'APP Name')
        matrix=[matrix,appUsage(:,i)];
        temp=[temp,appUsage(:,i)];
    elseif ~strcmp(appUsage{6,i-1},appUsage{6,i+1})
        [dat,used]=vis(temp,2);
        t=strcat('authentification confidence per app for user number:',temp{6,1});
        figure(j)
        boxplot(dat,used)
```

```
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,3);
        t=strcat('authentification confidence(face) per app for user
number:',temp{6,1});
        figure(j+1)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,4);
        t=strcat('authentification confidence(finger print) per app for user
number:',temp{6,1});
        figure(j+2)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,5);
        t=strcat('authentification confidence(gps) per app for user
number:',temp{6,1});
        figure(j+3)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,6);
        t=strcat('authentification confidence(voice) per app for user
number:',temp{6,1});
        figure(j+4)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,7);
        t=strcat('authentification confidence(app usage) per app for user
number:',temp{6,1});
        figure(j+5)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,8);
        t=strcat('authentification confidence(gait) per app for user
number:',temp{6,1});
        figure(j+6)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)
        j=j+7;
        temp={};
    end
    if i==s(2)
        [dat,used]=vis(temp,2);
        t=strcat('authentification confidence per app for user number:',temp{6,1});
        figure(j)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)
```

```
        [dat,used]=vis(temp,3);
        t=strcat('authentification confidence(face) per app for user
number:',temp{6,1});
        figure(j+1)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,4);
        t=strcat('authentification confidence(finger print) per app for user
number:',temp{6,1});
        figure(j+2)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,5);
        t=strcat('authentification confidence(gps) per app for user
number:',temp{6,1});
        figure(j+3)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,6);
        t=strcat('authentification confidence(voice) per app for user
number:',temp{6,1});
        figure(j+4)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,7);
        t=strcat('authentification confidence(app usage) per app for user
number:',temp{6,1});
        figure(j+5)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)

        [dat,used]=vis(temp,8);
        t=strcat('authentification confidence(gait) per app for user
number:',temp{6,1});
        figure(j+6)
        boxplot(dat,used)
        xlabel('App Name')
        ylabel('Authentification confidence')
        title(t)
        j=j+7;
    end
end

%overall,individual,(Face,Finger Print, GPS,Voice, App Usage, Gait)*individual,
(")*overall
[dat,used]=vis(matrix,1);
t='authentification confidence per app for all users';
figure(j)
boxplot(dat,used)
xlabel('App Name')
ylabel('Authentification confidence')
title(t)
```

```
[dat,used]=vis(matrix,9);
t='authentification confidence(face) per app for all users';
figure(j+1)
boxplot(dat,used)
xlabel('App Name')
ylabel('Authentification confidence')
title(t)

[dat,used]=vis(matrix,10);
t='authentification confidence(finger print) per app for all users';
figure(j+2)
boxplot(dat,used)
xlabel('App Name')
ylabel('Authentification confidence')
title(t)

[dat,used]=vis(matrix,11);
t='authentification confidence(GPS) per app for all users';
figure(j+3)
boxplot(dat,used)
xlabel('App Name')
ylabel('Authentification confidence')
title(t)

[dat,used]=vis(matrix,12);
t='authentification confidence(voice) per app for all users';
figure(j+4)
boxplot(dat,used)
xlabel('App Name')
ylabel('Authentification confidence')
title(t)

[dat,used]=vis(matrix,13);
t='authentification confidence(app usage) per app for all users';
figure(j+5)
boxplot(dat,used)
xlabel('App Name')
ylabel('Authentification confidence')
title(t)

[dat,used]=vis(matrix,14);
t='authentification confidence(gait) per app for all users';
figure(j+6)
boxplot(dat,used)
xlabel('App Name')
ylabel('Authentification confidence')
title(t)
j=j+7;

xlswrite('enterRiskLevelsInColumn2.xls',used.')
%xlswrite('appData.xlsx',appUsage)
save('appData','appUsage')
```

```
function [ used, dat ] = intrutionctr( mat,flag,level )
%Window type without degradation.
window=5;
totalCount=24*60/window;

s=size(mat);
used=[];
dat=[];
sum=0;
t=size(level);

temp={};
for count=1:totalCount
    used=[used,count];
    for l=1:s(2)
        z=strsplit(mat{5,l},' ');
        z=strsplit(z{5},':');
        z=str2num(z{1})+str2num(z{2})/60 + str2num(z{3})/360;
%         member(1)=z;
%         member(2)=day;
        if z<count*(window/60) && z>=(count-1)*(window/60)
            temp=[temp,mat(:,l)];
        end
    end

            for j=1:size(temp,2)
%                 if strcmp(mat{1,i},mat{1,j});
                for k=1:t(1)
                    if strcmp(level{k,1},temp{1,j}) &&
str2num(temp{6+flag,j})<level{k,2}
                        sum=sum+1;
                    end
                end
%                 end
            end
            dat=[dat,sum];
            sum=0;
            temp={};

end
end
```

```
% change the path at line 3 to destination saving folder.
clear
pwd='C:\Users\aalabdulwahid\Documents\MATLAB\intrution count plots\intrution count
with window\';

load('appData.mat')
[~,~,level]=xlsread(fullfile(char('enterRiskLevelsInColumn2.xls')));
%%%%%%%%%%%%%%%%
s=size(appUsage);
temp={};
matrix={};
j=1;
total=[];
allUserID={};
table={'User ID','Total Requests','Intrusive requests'};
%overall,individual,(Face,Finger Print, GPS,Voice, App Usage, Gait)*individual,
(")*overall.
for i=2:s(2)
    if  ~strcmp(appUsage{1,i},'APP Name')
        matrix=[matrix,appUsage(:,i)];
        temp=[temp,appUsage(:,i)];
    elseif ~strcmp(appUsage{6,i-1},appUsage{6,i})
        [window,count]=intrutionctr(temp,2,level);
        t=strcat('intrution attempts per app for user number-',num2str(temp{6,1}));
        a=figure;
        scatter(window,count)
        xlabel('Window')
        ylabel('no of intrusive authentication requests')
        title(t)
        saveas(a,strcat(pwd,t,'.fig'))
        close all

        allUserID=[allUserID,{num2str(temp{6,1})}];
%         total=[total,sum(window)];

table=[table;{num2str(temp{6,1}),num2str(size(temp,2)),num2str(sum(count))}];
        temp={};

    end
    if i==s(2)
        [window,count]=intrutionctr(temp,2,level);
        t=strcat('intrution attempts per app for user number-',num2str(temp{6,1}));
        a=figure;
        scatter(window,count)
        xlabel('Window')
        ylabel('no of intrusive authentication requests')
        title(t)
        saveas(a,strcat(pwd,t,'.fig'))
        close all
        allUserID=[allUserID,{num2str(temp{6,1})}];
%         total=[total,sum(window)];

table=[table;{num2str(temp{6,1}),num2str(size(temp,2)),num2str(sum(count))}];
        temp={};

    end
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

[window,count]=intrutionctr(matrix,1,level);
t='no of intrusive requests per app for all users';
a=figure;
scatter(window,count)
xlabel('Window')
ylabel('no of intrusive authentication requests')
title(t)
saveas(a,strcat(pwd,t,'.fig'))
```

```
close all

xlswrite(' Request Table.xls',table)

table={'Day','Total Requests','Intrusive requests'};
j=1;
total=[];
day=[];
%overall,individual,(Face,Finger Print, GPS,Voice, App Usage, Gait)*individual,
(")*overall.
for i=2:s(2)
    if  ~strcmp(appUsage{1,i},'APP Name')
        matrix=[matrix,appUsage(:,i)];
        temp=[temp,appUsage(:,i)];
    elseif strcmp(appUsage{6,i-1},appUsage{6,i})
        [window,dat]=intrutionctr(temp,2,level);
        %t=strcat('intrution attempts per app for user number-',num2str(temp{6,1}));
        %j=j+1;
        total=[total,sum(dat)];
        day=[day,j];
        table=[table;{num2str(j),num2str(size(temp,2)),num2str(sum(dat))}];
        j=j+1;
        temp={};

    elseif ~strcmp(appUsage{6,i-1},appUsage{6,i})
        [window,dat]=intrutionctr(temp,2,level);
        total=[total,sum(dat)];
        day=[day,j];
        table=[table;{num2str(j),num2str(size(temp,2)),num2str(sum(dat))}];
        temp={};
        t=strcat('intrution attempts per day for user number-',num2str(temp{6,1}));
        a=figure;
        scatter(day,total)
        xlabel('Day')
        ylabel('Count')
        title(t)
        saveas(a,strcat(pwd,t,'.fig'))
        close all
        xlswrite(strcat(t,'.xls'),table)
        total=[];
        day=[];
        table={'Day','Total Requests','Intrusive requests'};
        j=1;
    end

    if i==s(2)
        [window,dat]=intrutionctr(temp,2,level);
        total=[total,sum(dat)];
        day=[day,j];
        table=[table;{num2str(j),num2str(size(temp,2)),num2str(sum(dat))}];
        temp={};
        t=strcat('intrution attempts per day for user number-',num2str(temp{6,1}));
        a=figure;
        scatter(day,total)
        xlabel('Day')
        ylabel('Count')
        title(t)
        saveas(a,strcat(pwd,t,'.fig'))
        close all
        xlswrite(strcat(t,'.xls'),table)
        total=[];
        day=[];
        table={'Day','Total Requests','Intrusive requests'};
        j=1;

    end
end
function savefig(fname, varargin)
```

```
    op_dbg=     false;                                                  % Default value.

    % Compression
    compr=          [' -dUseFlateCompression=true -dLZWEncodePages=true -
dCompatibilityLevel=1.6' ...
                     ' -dAutoFilterColorImages=false -dAutoFilterGrayImages=false
' ...
                     ' -dColorImageFilter=%s -dGrayImageFilter=%s'];    %
Compression.
    lossless=       sprintf (compr, '/FlateEncode', '/FlateEncode');
    lossy=          sprintf (compr, '/DCTEncode',   '/DCTEncode'  );
    lossy=          [lossy ' -c ".setpdfwrite << /ColorImageDict << /QFactor %g
' ...
                     '/Blend 1 /HSample [%s] /VSample [%s] >> >>
setdistillerparams"'];

    % Create gs command.
    cmdEnd=         ' -sDEVICE=%s -sOutputFile="%s"';                    % Essential.
    epsCmd=         '';
    epsCmd= [epsCmd ' -dSubsetFonts=true -dNOPLATFONTS'];                % Future
support?
    epsCmd= [epsCmd ' -dUseCIEColor=true -
dColorConversionStrategy=/UseDeviceIndependentColor'];
    epsCmd= [epsCmd ' -dProcessColorModel=/%s'];                         % Color
conversion.
    pdfCmd= [epsCmd ' -dAntiAliasColorImages=false' cmdEnd];
    epsCmd= [epsCmd cmdEnd];

    % Get file name.
    if((nargin < 1) || isempty(fname) || ~ischar(fname))                 % Check
file name.
        error('No file name specified.');
    end
    [pathstr, namestr] = fileparts(fname);
    if(isempty(pathstr)), fname= fullfile(cd, namestr); end

    % Get handle.
    fighdl=     get(0, 'CurrentFigure'); % See gcf.                     % Get
figure handle.
    if((nargin >= 2) && (numel(varargin{1}) == 1) && isnumeric(varargin{1}))
        fighdl=     varargin{1};
        varargin=   {varargin{2:end}};
    end
    if(isempty(fighdl)), error('There is no figure to save!?'); end
    set(fighdl, 'Units', 'centimeters')                                  % Set paper
stuff.
    sz=         get(fighdl, 'Position');
    sz(1:2)=    0;
    set(fighdl, 'PaperUnits', 'centimeters', 'PaperSize', sz(3:4), 'PaperPosition',
sz);

    % Set up the various devices.
    % Those commented out are not yet supported by gs (nor by savefig).
    % pdf-cmyk works due to the Matlab '-cmyk' export being carried over from eps
to pdf.
    device.eps.rgb=     sprintf(epsCmd, 'DeviceRGB',    'epswrite', [fname '.eps']);
    device.jpeg.rgb=    sprintf(cmdEnd, 'jpeg',                     [fname
'.jpeg']);
%   device.jpeg.cmyk=   sprintf(cmdEnd, 'jpegcmyk',                 [fname
'.jpeg']);
    device.jpeg.gray=   sprintf(cmdEnd, 'jpeggray',                 [fname
'.jpeg']);
    device.pdf.rgb=     sprintf(pdfCmd, 'DeviceRGB',    'pdfwrite', [fname '.pdf']);
    device.pdf.cmyk=    sprintf(pdfCmd, 'DeviceCMYK',   'pdfwrite', [fname '.pdf']);
    device.pdf.gray=    sprintf(pdfCmd, 'DeviceGray',   'pdfwrite', [fname '.pdf']);
    device.png.rgb=     sprintf(cmdEnd, 'png16m',                   [fname '.png']);
```

```
%   device.png.cmyk=    sprintf(cmdEnd, 'png???',                   [fname '.png']);
    device.png.gray=    sprintf(cmdEnd, 'pnggray',                  [fname '.png']);
    device.tiff.rgb=    sprintf(cmdEnd, 'tiff24nc',                 [fname
'.tiff']);
    device.tiff.cmyk=   sprintf(cmdEnd, 'tiff32nc',                 [fname
'.tiff']);
    device.tiff.gray=   sprintf(cmdEnd, 'tiffgray',                 [fname
'.tiff']);

    % Get options.
    global savefig_defaults;                                        % Add
global defaults.
    if( iscellstr(savefig_defaults)), varargin= {savefig_defaults{:}, varargin{:}};
    elseif(ischar(savefig_defaults)), varargin= {savefig_defaults, varargin{:}};
    end
    varargin=   {'-r300', '-lossless', '-rgb', varargin{:}};        % Add
defaults.
    res=        '';
    types=      {};
    fonts=      'false';
    crop=       false;
    for n= 1:length(varargin)                                       % Read
options.
        if(ischar(varargin{n}))
            switch(lower(varargin{n}))
            case {'eps','jpeg','pdf','png','tiff'},     types{end+1}=
lower(varargin{n});
            case '-rgb',                color=  'rgb';  deps= {'-depsc2'};
            case '-cmyk',               color=  'cmyk'; deps= {'-depsc2', '-cmyk'};
            case '-gray',               color=  'gray'; deps= {'-deps2'};
            case '-fonts',              fonts=          'true';
            case '-lossless',           comp=           0;
            case '-crop',               crop=           true;
            case '-dbg',                op_dbg=         true;
            otherwise
                if(regexp(varargin{n}, '^\-r[0-9]+$')),      res=  varargin{n};
                elseif(regexp(varargin{n}, '^\-c[0-9.]+$')), comp=
str2double(varargin{n}(3:end));
                else    warning('pax:savefig:inputError', 'Unknown option in
argument: ''%s''.', varargin{n});
                end
            end
        else
            warning('pax:savefig:inputError', 'Wrong type of argument: ''%s''.',
class(varargin{n}));
        end
    end
    types=      unique(types);
    if(isempty(types)), error('No output format given.');   end

    if (comp == 0)                                                  % Lossless
compression
        gsCompr=        lossless;
    elseif (comp <= 0.1)                                            % High
quality lossy
        gsCompr=        sprintf(lossy, comp, '1 1 1 1', '1 1 1 1');
    else                                                            % Normal
lossy
        gsCompr=        sprintf(lossy, comp, '2 1 1 2', '2 1 1 2');
    end

    % Generate the gs command.
    switch(computer)                                                % Get gs
command.
        case {'MAC','MACI'},            gs= '/usr/local/bin/gs';
        case {'PCWIN','PCWIN64'},       gs= 'gswin32c.exe';
        otherwise,                      gs= 'gs';
    end
```

```
    gs=     [gs     ' -q -dNOPAUSE -dBATCH -dEPSCrop'];                 % Essential.
    gs=     [gs     ' -dPDFSETTINGS=/prepress -dEmbedAllFonts=' fonts]; % Must be
first?
    gs=     [gs     ' -dUseFlateCompression=true'];                     % Useful
stuff.
    gs=     [gs     ' -dAutoRotatePages=/None'];                        % Probably
good.
    gs=     [gs     ' -dHaveTrueTypes'];                                % Probably
good.
    gs=     [gs     ' ' res];                                           % Add
resolution to cmd.

    if(crop && ismember(types, {'eps', 'pdf'}))                         % Crop the
figure.
        fighdl= do_crop(fighdl);
    end

    % Output eps from Matlab.
    renderer=   ['-' lower(get(fighdl, 'Renderer'))];                   % Use same
as in figure.
    if(strcmpi(renderer, '-none')), renderer=   '-painters';    end     % We need a
valid renderer.
    print(fighdl, deps{:}, '-noui', renderer, res, [fname '-temp']);    % Output
the eps.

    % Convert to other formats.
    for n= 1:length(types)                                              % Output
them.
        if(isfield(device.(types{n}), color))
            cmd=        device.(types{n}).(color);                      % Colour
model exists.
        else
            cmd=        device.(types{n}).rgb;                          % Use
alternative.
            if(~strcmp(types{n}, 'eps'))    % It works anyways for eps (VERY
SHAKY!).
                warning('pax:savefig:deviceError', ...
                        'No device for %s using %s. Using rgb instead.', types{n},
color);
            end
        end
        cmp=    lossless;
        if (strcmp(types{n}, 'pdf')),   cmp= gsCompr;       end         % Lossy
compr only for pdf.
        if (strcmp(types{n}, 'eps')),   cmp= '';            end         % eps can't
use lossless.
        cmd=    sprintf('%s %s %s -f "%s-temp.eps"', gs, cmd, cmp, fname);% Add up.
            status= system(cmd);                                        % Run
Ghostscript.
            if (op_dbg || status),      display (cmd),      end
    end
    delete([fname '-temp.eps']);                                        % Clean up.
end


function fig= do_crop(fig)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%   Remove line segments that are outside the view.
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

    haxes=  findobj(fig, 'Type', 'axes', '-and', 'Tag', '');
    for n=1:length(haxes)
        xl=     get(haxes(n), 'XLim');
        yl=     get(haxes(n), 'YLim');
        lines=  findobj(haxes(n), 'Type', 'line');
        for m=1:length(lines)
            x=              get(lines(m), 'XData');
            y=              get(lines(m), 'YData');
```

```
            inx=            (xl(1) <= x) & (x <= xl(2));    % Within the x borders.
            iny=            (yl(1) <= y) & (y <= yl(2));    % Within the y borders.
            keep=           inx & iny;                      % Within the box.

            if(~strcmp(get(lines(m), 'LineStyle'), 'none'))
                crossx=     ((x(1:end-1) < xl(1)) & (xl(1) < x(2:end))) ... %
Crossing border x1.
                        |   ((x(1:end-1) < xl(2)) & (xl(2) < x(2:end))) ... %
Crossing border x2.
                        |   ((x(1:end-1) > xl(1)) & (xl(1) > x(2:end))) ... %
Crossing border x1.
                        |   ((x(1:end-1) > xl(2)) & (xl(2) > x(2:end)));    %
Crossing border x2.
                crossy=     ((y(1:end-1) < yl(1)) & (yl(1) < y(2:end))) ... %
Crossing border y1.
                        |   ((y(1:end-1) < yl(2)) & (yl(2) < y(2:end))) ... %
Crossing border y2.
                        |   ((y(1:end-1) > yl(1)) & (yl(1) > y(2:end))) ... %
Crossing border y1.
                        |   ((y(1:end-1) > yl(2)) & (yl(2) > y(2:end)));    %
Crossing border y2.
                crossp= [(  (crossx & iny(1:end-1) & iny(2:end)) ...    % Crossing
a x border within y limits.
                        |   (crossy & inx(1:end-1) & inx(2:end)) ...    % Crossing
a y border within x limits.
                        |   crossx & crossy ...                         % Crossing
a x and a y border (corner).
                         ), false ...
                        ];
                crossp(2:end)=  crossp(2:end) | crossp(1:end-1);        % Add line
segment's secont end point.

                keep=           keep | crossp;
            end
            set(lines(m), 'XData', x(keep))
            set(lines(m), 'YData', y(keep))
        end
    end
end



% Plot part 2

clear
load('appData.mat')
s=size(appUsage);
temp={};
matrix={};
path='C:\Users\aalabdulwahid\Documents\MATLAB\without window';
%overall,individual,(Face,Finger Print, GPS,Voice, App Usage, Gait)*individual,
(")*overall.
for i=2:s(2)
    if  ~strcmp(appUsage{1,i},'APP Name')
        matrix=[matrix,appUsage(:,i)];
    end
    if  ~strcmp(appUsage{1,i},'APP Name') && i~=s(2)
        temp=[temp,appUsage(:,i)];
    else
        confiMat=confiPerUserPerDay(temp);
        a=figure;
        scatter(confiMat(1,:),confiMat(4,:))
        xlabel('Time')
        ylabel('Authentication confidence')
        title(strcat('Authentication confidence for user ID:',temp{6,1},' on
',temp{2,1}))
```

```
        saveas(a,strcat(path,'Authentication confidence for user ID-',temp{6,1},'
on ',temp{2,1},'.fig'))
        xlswrite(strcat('Authentication confidence for user ID-',temp{6,1},' on
',temp{2,1},'.xlsx'),([confiMat(1,:);confiMat(4,:)]).')
        close all

        a=figure;
        scatter(confiMat(1,:),confiMat(5,:))
        xlabel('Time')
        ylabel('Authentication confidence')
        title(strcat('Authentication confidence(Face) for user ID:',temp{6,1},' on
',temp{2,1}))
        saveas(a,strcat(path,'Authentication confidence(Face) for user ID-
',temp{6,1},' on ',temp{2,1},'.fig'))
        xlswrite(strcat('Authentication confidence(Face) for user ID-',temp{6,1},'
on ',temp{2,1},'.xlsx'),([confiMat(1,:);confiMat(5,:)]).')
        close all
        a=figure;
        scatter(confiMat(1,:),confiMat(6,:))
        xlabel('Time')
        ylabel('Authentication confidence')
        title(strcat('Authentication confidence(Finger) for user ID:',temp{6,1},'
on ',temp{2,1}))
        saveas(a,strcat(path,'Authentication confidence(Finger) for user ID-
',temp{6,1},' on ',temp{2,1},'.fig'))
        xlswrite(strcat('Authentication confidence(Finger) for user ID-
',temp{6,1},' on ',temp{2,1},'.xlsx'),([confiMat(1,:);confiMat(6,:)]).')
        close all
        a=figure;
        scatter(confiMat(1,:),confiMat(7,:))
        xlabel('Time')
        ylabel('Authentication confidence')
        title(strcat('Authentication confidence(GPS) for user ID:',temp{6,1},' on
',temp{2,1}))
        saveas(a,strcat(path,'Authentication confidence(GPS) for user ID-
',temp{6,1},' on ',temp{2,1},'.fig'))
        xlswrite(strcat('Authentication confidence(GPS) for user ID-',temp{6,1},'
on ',temp{2,1},'.xlsx'),([confiMat(1,:);confiMat(7,:)]).')
        close all
        a=figure;
        scatter(confiMat(1,:),confiMat(8,:))
        xlabel('Time')
        ylabel('Authentication confidence')
        title(strcat('Authentication confidence(Voice) for user ID:',temp{6,1},' on
',temp{2,1}))
        saveas(a,strcat(path,'Authentication confidence(Voice) for user ID-
',temp{6,1},' on ',temp{2,1},'.fig'))
        xlswrite(strcat('Authentication confidence(Voice) for user ID-',temp{6,1},'
on ',temp{2,1},'.xlsx'),([confiMat(1,:);confiMat(8,:)]).')
        close all
        a=figure;
        scatter(confiMat(1,:),confiMat(9,:))
        xlabel('Time')
        ylabel('Authentication confidence')
        title(strcat('Authentication confidence(App  Usage) for user
ID:',temp{6,1},' on ',temp{2,1}))
        saveas(a,strcat(path,'Authentication confidence(App  Usage) for user ID-
',temp{6,1},' on ',temp{2,1},'.fig'))
        xlswrite(strcat('Authentication confidence(App Usage) for user ID-
',temp{6,1},' on ',temp{2,1},'.xlsx'),([confiMat(1,:);confiMat(9,:)]).')
        close all
        a=figure;
        scatter(confiMat(1,:),confiMat(10,:))
        xlabel('Time')
        ylabel('Authentication confidence')
        title(strcat('Authentication confidence(Gait) for user ID:',temp{6,1},' on
',temp{2,1}))
```

```
        saveas(a,strcat(path,'Authentication confidence(Gait) for user ID-
',temp{6,1},' on ',temp{2,1},'.fig'))
        xlswrite(strcat('Authentication confidence(Gait) for user ID-',temp{6,1},'
on ',temp{2,1},'.xlsx'),([confiMat(1,:);confiMat(10,:)]).')
        close all
        temp={};
    end
end

confiMat=confiPerUserPerDay(matrix);
a=figure;
scatter(confiMat(1,:),confiMat(3,:))
xlabel('Time')
ylabel('Authentication confidence')
title('Overall Authentication confidence')
saveas(a,strcat(path,'Overall Authentication confidence.fig'))
xlswrite(strcat('Overall Authentication
confidence','.xlsx'),([confiMat(1,:);confiMat(3,:)]).')
close all
a=figure;
scatter(confiMat(1,:),confiMat(11,:))
xlabel('Time')
ylabel('Authentication confidence')
title('Overall Authentication confidence(face)')
saveas(a,strcat(path,'Overall Authentication confidence(face).fig'))
xlswrite(strcat('Overall Authentication
confidence(face)','.xlsx'),([confiMat(1,:);confiMat(11,:)]).')
close all
a=figure;
scatter(confiMat(1,:),confiMat(12,:))
xlabel('Time')
ylabel('Authentication confidence')
title('Overall Authentication confidence(finger)')
saveas(a,strcat(path,'Overall Authentication confidence(finger).fig'))
xlswrite(strcat('Overall Authentication
confidence(finger)','.xlsx'),([confiMat(1,:);confiMat(12,:)]).')
close all
a=figure;
scatter(confiMat(1,:),confiMat(13,:))
xlabel('Time')
ylabel('Authentication confidence')
title('Overall Authentication confidence(GPS)')
saveas(a,strcat(path,'Overall Authentication confidence(gps).fig'))
xlswrite(strcat('Overall Authentication
confidence(GPS)','.xlsx'),([confiMat(1,:);confiMat(13,:)]).')
close all
a=figure;
scatter(confiMat(1,:),confiMat(14,:))
xlabel('Time')
ylabel('Authentication confidence')
title('Overall Authentication confidence(voice)')
saveas(a,strcat(path,'Overall Authentication confidence(voice).fig'))
xlswrite(strcat('Overall Authentication
confidence(voice)','.xlsx'),([confiMat(1,:);confiMat(14,:)]).')
close all
a=figure;
scatter(confiMat(1,:),confiMat(15,:))
xlabel('Time')
ylabel('Authentication confidence')
saveas(a,strcat(path,'Overall Authentication confidence(App Usage).fig'))
xlswrite(strcat('Overall Authentication confidence(App
Usage)','.xlsx'),([confiMat(1,:);confiMat(15,:)]).')
close all
a=figure;
scatter(confiMat(1,:),confiMat(16,:))
xlabel('Time')
ylabel('Authentication confidence')
title('Overall Authentication confidence(Gait)')
```

```
saveas(a,strcat(path,'Overall Authentication confidence(Gait).fig'))
xlswrite(strcat('Overall Authentication
confidence(Gait)','.xlsx'),([confiMat(1,:);confiMat(16,:)]).')
close all
```

```
%Image Part.

dirName = 'D:\biometric analysis\Sample of BioData\Sample of
BioData';              %# folder path
files=find_files(dirName,'.xls');
imageMat={};
ctr=1;
for file=files
    rawData=[];
    cell=strfind(file,'Image');
    if ~isempty(cell{1,1})
        try
          [~,~,rawData] = xlsread(fullfile(char(file)));
          s=size(rawData);
          for i=2:s(1)
              if ~isempty(rawData{i,2})&& ~isempty(rawData{i,3})
                  imageMat(1,ctr)=rawData(i,2);
                  imageMat(2,ctr)=rawData(i,3);
                  if ~isempty(regexp(char(file),' (\d+) ','match'))
                      temp=char(regexp(char(file),' (\d+) ','match'));
                      imageMat(3,ctr)={(temp(2:(length(temp)-1)))};
                  else
                      temp=(regexp(char(file),' (\d+)\','match'));
                      temp=char(temp(1));
                      imageMat(3,ctr)={(temp(2:(length(temp)-1)))};
                  end
                  ctr=ctr+1;
              end
          end
        catch
        end
    end
end
s=size(imageMat);
user=imageMat{3,1};
temp={};
ctr=1;
imatall=[];
for i=1:s(2)
    if imageMat{3,i}==user
        temp(ctr)=imageMat(1,i);
        ctr=ctr+1;
    else
        imat=[];
        t=size(temp);
        for j=1:t(2)
            for k=1:t(2)
                try
                    imat(j,k)=ssim(base64decode(temp{j}),base64decode(temp{k}));
                catch
                    imat(j,k)=0;
                end
            end
        end
        imat=mean(imat);
        imatall=[imatall,imat];
        temp={};
        ctr=1;
        temp(ctr)=imageMat(1,i);
        ctr=ctr+1;
        user=imageMat{3,i};
    end
    if i==s(2)
        imat=[];
        t=size(temp);
        for j=1:t(2)
            for k=1:t(2)
                try
```

```
                    imat(j,k)=ssim(base64decode(temp{j}),base64decode(temp{k}));
                catch
                    imat(j,k)=0;
                end
            end
        end
        imat=mean(imat);
        imatall=[imatall,imat];
    end
end
imageEER(1:2,1:24)=0;
s=size(imageMat);
for i=1:s(2)
    try
        z=strsplit(imageMat{2,i},' ');
        z=strsplit(z{5},':');
        y=str2num(z{1})+1;
        imageEER(1,y)=imageEER(1,y)+imatall(i);
        imageEER(2,y)=imageEER(2,y)+1;
    catch
    end
end
for i=1:24
    if imageEER(2,i)~=0
        imageEER(1,i)=imageEER(1,i)/imageEER(2,i);
    end
end
imageEER=imageEER(1,:);
user=imageMat{3,1};
temp={};
tempeer=[];
imageEERperuser=[];
for i=1:s(2)
    if strcmp(imageMat{3,i},user)
        temp=[temp,imageMat(:,i)];
        tempeer=[tempeer,imatall(i)];
    else

imageEERperuser=[imageEERperuser,imageIndividualEER(temp,tempeer,str2num(user))];
        temp={};
        tempeer=[];
        temp=[temp,imageMat(:,i)];
        tempeer=[tempeer,imatall(i)];
        user=imageMat{3,i};
    end
    if i==s(2)

imageEERperuser=[imageEERperuser,imageIndividualEER(temp,tempeer,str2num(user))];
    end
end

xlswrite('imageEER.xls',imageEER)
xlswrite('imageEERperuser.xls',imageEERperuser)
```