2016-03

Continuous and transparent multimodal authentication: reviewing the state of the art

AlAbdulwahid, A

10.1007/s10586-015-0510-4
Cluster Computing
Springer Science and Business Media LLC

Continuous and Transparent Multimodal Authentication: Reviewing the State of the Art

Abdulwahid Al Abdulwahid · Nathan Clarke ·

Ingo Stengel · Steven Furnell · Christoph Reich

Abstract 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 authorized user is granted access; however, it has historically suffered from a range of issues related to the security and usability of the approaches. They are also still mostly functioning at the point of entry and those performing sort of re-authentication executing it in an intrusive manner. Thus, it is apparent that a more innovative, convenient and secure user authentication solution is vital. This paper 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 high security and user satisfaction. This is followed by a literature review of the existing research on continuous and transparent multimodal authentication. It concludes that providing users with adequate protection and convenience requires innovative robust authentication mechanisms to be utilized in a universal level. Ultimately, a potential federated biometric authentication solution is presented; however it needs to be developed and extensively evaluated, thus operating in a transparent, continuous and user-friendly manner.

Keywords User authentication · Authentication technologies · Security · Usability · Transparent authentication · Biometrics · Continuous authentication

Abdulwahid Al Abdulwahid (✉)
Centre for Security, Communications and Network Research, Plymouth University, Plymouth, PL4 8RT, UK
Computer Science and Engineering Department, Jubail University College, Jubail Industrial City, KSA

e-mail: Abdulwahid.Alabdulwahid@plymouth.ac.uk

Nathan Clarke · Ingo Stengel · Steven Furnell
Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK

Christoph Reich

Cloud Research Lab, Furtwangen University, Furtwangen, Germany

1 Introduction

Protecting an IT system against unauthorized user activities is usually provided via user identification or authentication which enable successful authorization and subsequently accountability – these concepts together are referred to as AAA [1]. 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, authorization 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 tracks of them – usually through historical logs.

Therefore, managing appropriate authentication is the pivotal concept for implementing information security within an IT system. Achieving a high level of confidentiality, integrity, authorization, and accountability of an IT system would not be possible without carefully considering various aspects; a vital one of them is safeguarding sensible, robust and useable authentication. Authentication can be achieved by utilizing 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) [2].

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 utilized mainly by governments (e.g. forensics and borders), to becoming more available in the public domain (biometrics are now deployed in a wide range of applications that are fairly mainstream – passports, mobile phones, schools, police).

The authors aim at building an authentication system that would provide a more secure, user-friendly, universal, and technology independent environment. In order to achieve this, the following research objectives are established:

- To review the authentication methods including both the problems and available solutions.

- To investigate the state-of-the-practice of authentication technologies provided by various sectors.
- To develop a current state-of-the-art understanding of the biometric authentication techniques including its applications in the existing research on continuous, transparent and distributed authentication.

This paper is structured as follows: Section 2 reviews the conventional authentication approaches. Then Section 3 examines the current use of authentication technologies offered 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 are subsequently discussed in Section 4, in terms of the benefits they offer in balancing the trade-off between security and usability as well as their shortcomings. Furthermore, Section 5 undertakes a thorough review of the literature related to continuous and transparent authentication focusing upon those utilized multimodal biometrics, encompassing their open issues, users' perceptions, and desirable requirements, leading to an outline of the proposed solution alongside its limitations and future changes. Finally, the conclusion and sought features are presented in Section 6.

2 Conventional Authentication Approaches

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) [3]. 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 humans' memory and their 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 [4] as the so called secret is transferable, guessable and can be watched by others through shoulder surfing.

2.1.1 Personal Identification Number (PIN), Password and Passphrase

A PIN is considered the simplest knowledge-based authentication technique. It is apparently 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 due to 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 [5, 6]. For instance, 58% of the latter survey respondents never changed their PINs. Worse than that, it is also revealed in the former 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 their availability. Further more recent survey conducted by Crawford and Renaud [7] showed that 30% of participants do not enable any security 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 will be significant.

More recently, many digital services create password policies and guidelines to encourage good practice, which are adopted by many organizations to be utilized 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 password merely once a year or less [8]. Others are enforceable, such as the length of password, complexity and its lifetime. Accordingly, when users are faced with the need to memorize multiple passwords and change them periodically, they tend to forgetting passwords, writing them down, and selecting easily guessed ones [4]. Therefore, the problem is exacerbated as they would become susceptible to be stolen. Moreover, additional administrative costs would be posed by frequent passwords resetting [4]. 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 will be able to reuse the same cracked password to login to them.

Passphrases come as an alternative endeavor 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 sequence of words built to be used as credential secret. They are usually without spaces

but possibly with digits replacing letters or words; for example, "Going4al0n9journy". 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 alike.

Brute-force attack tools (attempting every possible combination automatically), such as Brutus and OphCrack, are notorious against most of knowledge-based authentication techniques [9]. 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 bothers the user due to its constant intrusiveness.

2.1.2 Cognitive Knowledge Question

Cognitive knowledge which comes in a form of question(s) seeks to alleviate the load of users memorizing desperate passwords thereby deploying associative question(s) [10]. These questions are typically about personal information, such as mother's maiden name and city of birth, or preferences, such as favorite color and movie. 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 utilizing it besides another authentication approach (as explained in 2.4 sub-section). 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 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.

2.1.3 Patterns and Graphical Passwords

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 memorize and remember multi complex passwords is not addressed by them. It is believed and has been proven that the human brain is more capable to store and remember pictorial information than textual [11]. As a result, pattern password authentication has emerged, with which a user is required to recognize and sequentially draw a pre-set outline on nine (3x3) dots grid that appear on a touch screen. Therefore, it is argued that it will be much more convenient to the user to recognize a pattern than an alphanumeric password. In addition, [12] 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 utilize 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, [13] extend this typical pattern password to allow skipping dots (as demonstrated in Fig. 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 [14].

To obtain the most from the advantages of human's ability to remember graphical over alphanumeric secrets, some 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 [15]. 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 screen. This leads to increase authentication failures that might bother the user. Moreover, poor selection of background images that have popular potential points yields to being easily predicted, for instance a study by [16] cracked an average of 7–10% of user passpoints (click-based) passwords within 3 guesses only.

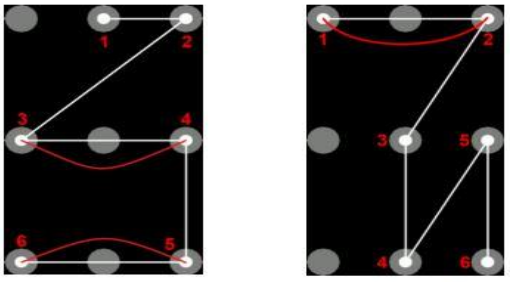

Fig.1 Pattern with the Possibility of Points to be Skipped [13]

Further to the work on click-based concept, proposals about choice-based or PassImages graphical authentication have risen [17, 18]; in addition to the recent application of the concept on Windows 8.1 Picture Password [19]. 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 randomized. Likewise, the product of [20] capitalizes on the psychological theory that human's brains recognize and recall faces better than any other picture or object [21]. Users are able to use familiar personal photos that are stored on the ones PC or on the web to form 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. Accordingly, the time taken to pass all the steps of graphical authentication could be an issue of inconvenience. Again, 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 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 categorized into two types: Hardware Tokens and Software Tokens [22]. With the former type, a separate token physical device is produced and provided, usually, by the service provider, such as bank smartcard and HSBC Secure Key OTP token [23]. On the other hand, with the latter type, there is utilization of an existing device as is, such as when sending OTP via short messaging service (SMS) to the user's registered mobile phone, or there is a need to install software (application) on the user's smartphone or PC [22], such as Google authenticator [24].

A typical authentication token either stores static but complex passwords or generates a OTP for each session [25]. The user is required to enter the generated password on the system or service he is authenticating to or it is synchronized 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 brain. However, reliance on human is still existent as it is assumed that the token is in the possession of the accredited user – they merely verify the presence of the token not the authorized user. Having said this, in recent tokens, 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.

Tokens provide compromise detection, for example if three failed attempts threshold is exceeded, as well as countermeasure denial-of-service attacks [4], albeit they are not fail-safe – the breach of RSA SecureID tokens in 2011 evidences this [26]. 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 sub-section 2.4.

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 additional cost over passwords. This is worsened if specialized 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 synchronization between the token and system might be difficult with those time-synchronous tokens [25], especially in out-of-coverage areas. Furthermore, user 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.

2.3 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. Regardless of whether the user has claimed an identity initially or not, the high level of uniqueness biometrics offers facilitates the process. It also removes the reliance upon the individual to either memorize and recall complex and various passwords or carry and secure tokens. However, whilst the resulting decision of other approaches is with complete accuracy (i.e. a Boolean decision), biometrics results in a confidence measure, with a pre-determined threshold deciding on whether this 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 the authorized user. Accordingly, the performance of a typical biometrics technique is measured based on its error rates, such as False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER).

Biometrics is dependent upon measurable and distinctive characteristics of an individual. They can be categorized based upon their underlying characteristics into: physiological and behavioral approaches [27, 28]. Physiological biometrics are those based upon a unique physical aspect of the body, such as a fingerprint, face, or iris, whereas behavioral biometrics utilizes the distinctive way in which humans behave, such as voice, keystroke and signature, to identify and/or verify a user. Both categories are non-transferable to others, unforgettable, believed to uniquely (with a varying level of accuracy) identify individuals, not easily lent or stolen, and difficult to reproduce, change or hide. As such, they offer a strong defense against repudiation [29]. However, biometric systems error rates and cost, together with usability have been hindering their widespread adoption [30]; notwithstanding, recent years have shown that this has been alleviated by significant enhancement in biometric systems capabilities [31, 32]. Nevertheless, stable uni-biometrics can be forged albeit some with difficulty [4]. For instance, traditional facial recognition can be fooled by a photo of the authorized 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 biometric sample is from a living legitimate user utilizing some biological indicators, such as blood flow and blinking for iris scan, and temperature and pulse for fingerprint systems [10, 25, 33]. 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 authorized person with two eye holes, stand behind it and blink in front of a facial recognition system. However, devising a biometrics system deploying a set of countermeasures makes it robust and difficult to compromise. Alternatively, multibiometrics would offer a more resilient authentication solution as can be seen in 5.1.

2.4 Multi-Layer and -Factor 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 that financial service providers should deploy "strong authentication" in all their online transactions [34]. 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 and latitude) [1], and/or the IP address.

The multi-layer method lack adherence to regulations of some sensitive sectors, such as banks where it is not compatible with the Federal Financial Institutions Examination Council regulations that emphasized clearly that these factors are required to be from two or more of the authentication categories [35]. Therefore, it can be inferred that multi-factor authentication is considered stronger than multi-layer one – thus banking sector has utilized 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 best knowledge no multi-factor authentication method has been utilized 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.

3 A Review 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 unauthorized access. Authentication technologies vary perhaps dependent on the data sensitivity involved and the users' requirements, and each have their 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 review some of these attempts with the current authentication technologies employed with/by a sample of service/device providers; namely:

- HSBC [23],
- NatWest [36],
- Lloyds [37],

- SAMBA (Saudi American Bank) [38],
- Windows 8.1 Laptop/PC [39, 19],
- Android (Samsung Galaxy S5 and above) [40, 41],
- iPhone 5S and above [42, 43] and
- Google Authenticator [24].

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 high 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 utilize such resilient protection tools. Thus, half of the selected list is banks in addition to the most dominant operating systems [44]. 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 [45].

Table 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.

Table 1 An Overview of Current Authentication Technologies

Service/Device Providers	Secret-based	Token-based	Biometrics-based	Point-of-entry	Re-Authentication
HSBC [23]	✓ User ID ✓ Cognitive question ✓ PIN	✓ Separate Hardware OTP	X	✓	(New OTP) ✓ New payee ✓ Transfer money
NatWest [36]	✓ User ID ✓ PIN ✓ Password	✓ Separate Hardware OTP (Card-Reader) ✓ Digital banking card	X	✓	(New OTP) ✓ New payee ✓ New standing order ✓ Change password ✓ Change phone
Lloyds [37]	✓ User ID ✓ Password ✓ Cognitive question	X	X	✓	(New OTP with Automated call to registered mobile) ✓ New payee ✓ Transfer money
SAMBA [38]	✓ User ID ✓ Password	✓ Separate Hardware OTP ***OR*** ✓ Mobile (SMS) OTP	X	✓	(New OTP) ***OR*** (ATM login) ✓ New payee ✓ Transfer money
Windows 8.1 [39, 19]	✓ User ID ✓ Password ✓ Picture password	X	X	✓	✓ Websites accounts
Android (Galaxy S5) [40, 41]	✓ PIN ✓ Pattern ✓ Password	X	✓ Face ✓ Fingerprint	✓	X
iPhone (5S) [42, 43]	✓ PIN ✓ Password	X	✓ Fingerprint	✓	✓ Access iTunes ✓ New purchase
Google Authenticator [24]	✓ User ID ✓ Password	✓ Mobile OTP	X	✓	X

Accessing all of the services mentioned in Table 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 memorized and recalled by users. All of these services except Lloyds bank augment their authentication process by offering the option of employing multi-factor authentication or imposing it. To be able to unlock an Android (Galaxy S5/6) 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 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 log in. 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 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 [24]. Once it is lost or stolen, the service is susceptible to be accessed by the unauthorized holder of the device.

On the other hand, there are some encouraging signs and endeavors 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 bothered.

A few other attempts to utilize biometrics appear with Windows 8.1, Galaxy S5 and iPhone 5S. For example, Microsoft declares that they will embed the functionality of fingerprints to access their apps in Windows 8.1, such as Windows Store, Xbox Music, and Xbox Video [39]. Similarly, Galaxy S5 and iPhone 5S employ the fingerprint scanner on their home button not only to login but also to access some apps, such as PayPal and iTunes. 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.

4 Featured Authentication Frameworks

A number of researches 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 the related two of these featured authentication frameworks, namely single sign-on and federated identity, in terms of the benefits they offer as well as their shortcomings.

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 organization after a single successful login [4, 46, 47]. 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 account with which the account holder is required to enter his/her 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 organizations. 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 authorized to access. Identity Access Management (IAM) system leverages 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 credential exchanging between services, such as Security Assertion Markup Language (SAML) [46].

Securing the authentication process in the first place is still crucial which if it is done by utilizing the aforementioned approaches, it would yield to keeping their downsides, such as the need to create a complex and lengthy unrepeated with other systems password as well as the burden of memorizing and recalling it. Additionally, SSO assumes that the authorized 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 organizations. As a consequence, the encumbrance of cognitive memory load and carrying tokens may persist.

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 organization to resources offered by other organizations seamlessly. To achieve this, inter-organizational trust relationship should be established [10, 48].

Thus, there is a dire 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 [48, 49]. 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 [50], 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 organizations. 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. However, Madsen et al. claimed that some of the mentioned standards offer mechanism to contain such a breach by de-federation [50]. 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 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.

5 Continuous and Transparent Authentication Systems

Further consideration has been given to continuous and transparent authentication in order to solve the point-of-entry issue. It seeks to verify whether the user is genuine in a periodic or constant manner utilizing biometrics without interrupting the user's normal interaction [7, 51]. Transparent Authentication Systems (TAS) have been studied by several researchers with varying approaches. 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, as demonstrated in Fig. 2.

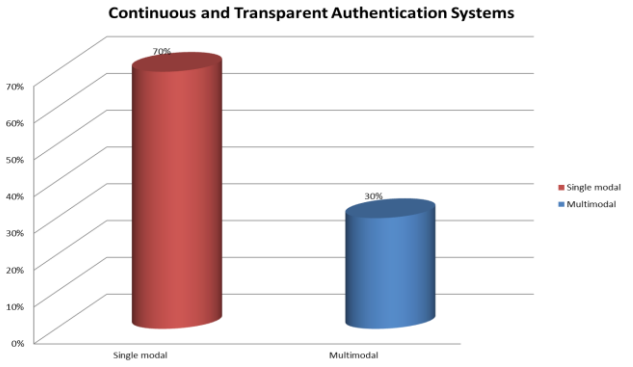

Fig.2 Continuous and Transparent Authentication Systems

As each of these models (shown in Table 2) utilizes 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 [117–119].

Table 2 Single biometric Transparent Authentication Systems

	Modality	Refs.
Behavioral	Keystroke	[52–66]
	Mouse	[67–77]
	Signature	[78]
	Gait	[79–87]
	Voice	[88–91]
	Behavioral Profiling	[92–96]
Physiological	Face	[97–101]
	Ear	[102–105]
	Finger	[106, 107]
	Palmprint	[108]
	Iris	[109–116]

5.1 Multimodal Authentication Systems

Based upon analyzing the prior art on continuous and transparent multimodal authentication systems, the 28 studies are categorized into: physiological multimodal systems; behavioral multimodal systems; hybrid multimodal systems; distributed multimodal systems; and web- and cloud-based multimodal systems. The first three categories are according to the nature of the utilized biometric modalities, whereas the last two ones are according to their operational deployments that distinguish them from the others.

5.1.1 Physiological Multimodal Systems

Table 3 demonstrates proposed frameworks in this domain deployed a set of two traits from face and fingerprint. [120] consolidated facial and fingerprint recognition systems and

integrated their resultant output with the lapsed time to act relevantly.

In evaluating their work, they proposed and used new performance measures, namely: Time to Correct Reject (TCR), Probability of Time to Correct Reject (PTCR), Usability, and Usability-Security Characteristic Curve (USC). However, it was undertaken with only 11 users without, even, any results.

Whilst [121] incorporated facial recognition and fingerprint in their model, the latter was applied intrusively when the confidence level went below the specified threshold, making it eventually unimodal. The accomplished matching score of 48.6% to 72.5% indicates undesirable performance especially with critical applications. Furthermore, it and the study of [122] were merely simulation.

Similarly, [123] investigated utilizing the face and iris modalities but again the latter in prompted in an intrusive manner and just at the entry point. With 61 participants, the verification rate was between 84-97% with a FAR was 3%.

The desirable performance of [124] (FRR of 1.0% with 90 users) notwithstanding, they introduced an extra processing overhead of 26-42%, raising usability (e.g. longer waiting time) and economic issues (e.g. power consumption).

Table 3 Physiological Transparent Multimodal Systems

Ref.	Platform	Biometrics			Performance (%)				Experiment Demographics	Mode	Limitations	Features
		F*	FP*	I*	Match	FAR	FRR	Verification				
[120]	PC	√	√						11 participants 30minutes	Real	New performance metrics	Holistic fusion Extendable
[121]	PC	√	√		48.6-72.5				300 minutes	Simulation	Intrusive login (FP)	
[124]	PC	√	√				1.0		90 participants	Prototype	26-42% added processing overhead	
[122]	PC	√	√						40 participants	Simulation	Intrusive login (secret)	Multibiometric security API
[123]	PC/Laptop	√		√		3.0		84-97	61 participants 5 minutes	Real	Intrusive login (I)	

* F is Face. FP is Fingerprint. I is Iris

5.1.2 Behavioral Multimodal Systems

The hindrance of transparently employing physiological biometrics has been evident; thus a shift to behavioral counterparts was sought (as shown in Table 4). [125–127] proposed the utilization of keystroke and mouse dynamics for this purpose. The last two studies were complemented by the inputs of the touch screen (touchalytics), albeit they achieved higher error rates (14.47 and 2.24 FAR and 1.78 and 2.10 FRR) compared to the first study (0.651 FAR and 1.312 FRR). They were, also, conducted under controlled environment with pre-specified tasks. Therefore, generalizing their results is questionable.

Another proposal used keystroke analysis whereas combining it with voice recognition of mobile phones was presented by [7, 130]. Unlike the previous frameworks, this experiment was with a blend of real and simulated data and achieved a keystroke EER of 10% and a voice EER of 25% (without an overall performance). Despite the attained 67% reduction of intrusive authentication, the recovery was designed to be secret PIN, hence carrying the weaknesses mentioned in section 2.1.

[128] fused voice and gait recognition within a mobile devices context and investigated its feasibility offline on the usage of 31 participants. In addition to being offline, the resultant performance occurred on a differing range from 2.0% to 12.0% EER, making it difficult to reflect on how it is in the actual live use.

The focus was then shifted to deploying various aspects of behavioral profiling as in [129, 131]. The former study accomplished an EER of 5.4%, 2.2% and 13.5% when utilized the usage of calling, text messaging, and general applications respectively with an overall of 7.03% EER. Likewise, the latter experiment consolidated texting linguistic profiling, keystroke dynamics and behavior profiling and obtained an EER of 12.8%, 20.8% and 9.2% respectively with an overall of 3.3% and a 91% decline in the explicit authentication requests. However, these two studies were conducted entirely or partly on old (2004/2005) and varying offline datasets which were joined assuming they are of the same group of users.

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 platform, extra care should be taken to their applicability and universality.

Table 4 Behavioral Transparent Multimodal Systems

Ref.	Platform	Biometrics						Performance (%)			Experiment Demographics	Mode	Limitations	Features
		V*	M*	K*	B*	G*	T*	FAR	FRR	EER				
[125]	PC		√	√				0.651	1.312		22 participants 9 weeks	Real		IDS Client-server
[128]	Mobile	√				√				2-12	31 participants	Offline experiment		
[126]	PC		√	√			√	14.47	1.78		61 participants 10 days	Real	Detection time 2.20 minutes	IDS
[129]	Mobile				√					7.03	76 participants	Simulation	Off-line dataset	Analyzed telephony, texting & apps services
[7, 130]	Mobile	√		√						(K) 10 (V) 25	30 participants 7 tasks	Real & Simulation		67% reduction of intrusive authentication
[131]	Mobile				√					9.2	30 participants	Simulation	Off-line dataset & Real	91% reduction of intrusive authentication
[127]	PC		√	√			√	2.24	2.10		31 participants 3 tasks	Real		

* V is Voice. M is Mouse. K is Keystroke. B is Behavioral profiling. G is Gait. T is Touchalytics

5.1.3 Hybrid Multimodal Systems

Researchers have recognized the operational complications of installing physiological biometrics only together with the instability of behavioral biometrics only in a continuous and transparent fashion. Therefore, various studies have been proposed deploying a mixture of physiological and behavioral or soft biometrics (e.g. color of face), as summarized in Table 5. The study of [132] was one of the initial endeavors which aimed to operate on and protect a flight deck. Despite the offered level of flexibility in terms of where the verification processing carried out (on-board or distributed), it was only conceptual with no implementation, the same as [133–135].

[136] investigated the plausibility of deploying voice verification, facial recognition, and fingerprint in a multimodal continuous authentication framework. It integrated them with the time at which they were acquired. The consequence of this integration would create a trust level on the user which fluctuates based upon the interval from the last successfully captured modalities samples. Accordingly, it and [137], alike, produced virtual data but they did not reveal any performance results. The latter, also, endured the problems of secret-knowledge approach as it utilized intrusive login using secret code. On the other hand, although the work of [140] was simulation also, they published results of fusing face and voice modalities of 30 simulated participants for 3 separate sessions. They accomplished a face EER of 0.449%, a voice EER of 0.003% and an overall EER of 0.087%.

[139] conducted one of the most comprehensive experiments in this domain. They proposed a mobile Non-Intrusive and Continuous Authentication (NICA) using those biometric techniques existing on the device to operate in both standalone and client-server modes – achieving favorable performance of 0.01% EER of 27 users with 60 biometric samples collected. Nevertheless, they loosened the threshold because they utilized in-house biometric algorithms which, in turn, perhaps affected the credibility of the result. An interesting feature of NICA is that it was designed to use the confidence level on the legitimate user (proposed earlier) in order to align it with the user privileges to access services that have varying risk levels.

Other studies investigated composite authentication systems of physiological and soft biometrics [141–143] on laptops. The first study experimented the fusion of the face trait along with its soft features, such as color, and claimed to subsequently succeed to have no FAR and an FRR of 4.17%. Similarly, using the same biometrics, the last two studies achieved a recognition score of 86.88% albeit with only 7 users. Furthermore, their experiment adopted an obtrusive login (password or face) and merely the soft biometrics were verified throughout, which might be affected by the surrounding environment, leading to convenience issues of increasing re-authentication requests.

Leveraging the advent of wearable technologies, [138] developed a wristband to be utilized as an initial login fingerprint sensor and then to constantly measure the user skin temperature and heart rate. However, the fingerprint was only presented at the login stage and the performance was quite low (matching score between 40-60%). Moreover, requiring an additional wristband to access a system, inherits the downsides of tokens.

Table 5 Hybrid Transparent Multimodal Systems

Ref.	Platform	Biometrics								Performance (%)					Experiment Demographics	Mode	Limitations	Features
		F*	FP*	V*	M*	K*	B*	G*	SB*	Match	FAR	FRR	EER	Recognition				
[132]	Flight Deck															Conceptual	No experiment	2 designs: on-board & distributed verification Several biometrics
[136]	PC	√	√	√											24 participants	Virtual data		Integration with time
[133]	Mobile										$2*10^{-4}$	0.4				Conceptual	Intrusive login (secret)	Several biometrics
[137]	PC	√					√									Simulation	Intrusive login (secret)	
[134]	PC		√		√											Conceptual	No experiment	e-Learning
[138]	Wearable & Laptop	√							√	40-60						Prototype	Intrusive login (F) Wristband	
[139]	Mobile	√		√		√							0.01		27 participants 45 minutes	Real		Extendable Standalone & client-server
[140]	PC	√		√									0.087		30 participants 3 sessions	Simulation		Adaptive Bayesian fusion
[141]	Laptop	√							√		0	4.17			20 participants	Real	Intrusive login (secret)	
[135]	Mobile	√		√				√								Conceptual	No experiment	Fuzzy Crypto
[142] [143]	Laptop	√							√					86.88	7 participants	Real		Swarm intelligence algorithms

* F is Face. FP is Fingerprint. V is Voice. M is Mouse. K is Keystroke. B is Behavioral. G is Gait. S is Soft biometrics.

5.1.4 Distributed Multimodal 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 6 have been conducted. [144] conceptually proposed deploying physiological signals (e.g. blood pressure and heart beat) and behavioral profiling.

In the one hand, [145] prototyped a progressive authentication model integrating the face, voice and behavior profiling traits, in conjunction with proximity to pre-defined logged-in device(s). In spite of the claimed decrease of intrusive verification prompts by 42%, it was investigated with 9 users only and no security measures revealed.

Table 6 Distributed Transparent Multimodal Systems

Ref.	Platform	Biometrics				Performance (%)			Experiment Demographics	Mode	Limitations	Features
		F*	V*	B*	PS*	FAR	FRR	EER				
[144]	PDA			√	√					Conceptual	No experiment	One user to Many devices
[145]	Mobile & PC	√	√	√					9 participants	Prototype		42% reduction of intrusive authentication
[146]	PDA & various devices			√					20 participants 14 days	Real & Simulation	Utilizes Secret & Token	74% reduction of intrusive authentication

* F is Face. V is Voice. B is Behavioral profiling. PS is Physiological Signals.

From the same standpoint, [146] developed their Authentication Aura system utilizing what authentication techniques exist on each device, i.e. secret, behavioral profiling, and even personal dumb objects, such as keys. Both the authentication status of and the user confidence level on each participating device are communicated between each other within a close proximity to form an overall confidence. Whilst it was carried out on a blend of real and simulated data of 20 participants, its focus was more on usability (74% less explicit authentication occurrences. Additionally, further examination on the processing overhead on each device is needed.

5.1.5 Web-based Multimodal Systems

[147, 148] proposed a solution to mitigate the processing burden on users' devices and make it occurs, instead, on a web server. In order to secure web services, [147] fused mouse and keystroke dynamics for continuous identity verification following a preliminary secret-knowledge login. They obtained a distinct EER for each modality (22.41 and 24.78 respectively) and an overall EER of 8.21. Apart from the persistence issues of intrusive login, their framework is not compatible when using a mobile device, with which there is no mouse inputs and the keystroke is likely to be limited.

[148] proposed an Internet protocol – Context Aware Security by Hierarchical Multilevel Architecture (CASHIMA) – capable to act as a multimodal biometric authentication system. It adopted the TAS user confidence (trust) notion that is fluctuating based on the captured biometrics' time and quality, upon which users privileges are authorized remotely. In assessing their prototype, they integrated facial and voice recognition, on a smartphone. Nonetheless, they did not reveal an overall performance but for individual trait; False Match Rate (FMR) of 2.58% and 10% respectively. Despite the promising universality features their framework offered, it needs to be extensively evaluated with real data not just as a prototype to examine various metrics, such as feasibility, scalability, and privacy-preserving.

Table 7 Web- and Cloud-based Transparent Multimodal Systems

Ref.	Platform	Biometrics				Performance (%)		Experiment Demographics	Mode	Limitations	Features
		F*	V*	K*	M*	FMR	EER				
[147]	Web			√	√		(M) 22.41 (K) 24.78 8.21	24 participants 8 weeks	Real	Intrusive login (secret)	Bayesian fusion
[148]	Web	√	√			(V) 10 (F)2.58			Prototype	Intrusive login (fingerprint)	

* F is Face. V is Voice. K is Keystroke. M is Mouse.

5.2 Users' Perceptions of Multimodal TAS

[7, 139] 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. The relative small samples of both 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 own smartphone and tablet would like to have seamless experience across all their devices [149].

5.3 Open Issues on Previous Studies

As the research revolving transparent authentication evolves, so do its evaluation and feasibility studies. It is apparent that a multimodal TAS approach outweighs its single modal counterpart due to proven security performance enhancement. However, the abovementioned reviewed studies suffer from one or more of the following open issues that need to be tackled in future research:

5.3.1 Lack of Transparency

It is found that a few frameworks are not, operationally, fully transparent as they integrated a form of intrusive login (i.e. secret, fingerprint or iris). This leads them to carry the limitations of secret-knowledge authentication approach, the single modality, and intrusive authentication.

5.3.2 Lack of Universality

The majority of them, also, are confined to work in a specific context and/or device, rendering them to lack the universality attribute that enables a seamless technology and service independent functioning.

5.3.3 Negligence of varying services risk levels

Some studies consider the fluctuation of user identity confidence/trust. Nevertheless, a little of them aligned it with the varying risk levels of conducted activities or accessed services, which is not the case with the real use.

5.3.4 Incomprehensive Evaluation

In terms of evaluation, those studies showed performance results carried out their experiments either on simulated/semi-simulated data or real but insufficient and offline data. In addition, some of them focused on usability solely whilst others on security only. Moreover, there were specific tasks for participants to perform, lending it not to

give a better insight about the system when they put in real live practice. Furthermore, some other related features would be difficult to measure, such as scalability, privacy, and subsequently user satisfaction.

5.4 Desirable Characteristics for an Effective Multimodal TAS

In order to offer an effective multimodal TAS, it should go through comprehensive stages, from the design to the appraisal, bearing in mind a number of critical factors. As a result of the thorough survey and analysis, the following desirable requirements are concluded in order to be in place to overcome the aforementioned open issues:

- no intrusive login,
- no additional device or sensor,
- flexibility to deploy mixture of biometrics,
- continuous user identity confidence,
- services risk levels aligned with user identity confidence,
- minimal processing overhead,
- high scalability,
- compatible with various platforms,
- real and adequate number of evaluation participants,
- task-free experiment,
- security measures to secure and manage biometric templates database and biometric samples in transient.

5.5 A Framework for Federated Authentication in the Cloud

Stemming from the abovementioned desirable characteristics, the authors have propounded a federated biometric authentication framework, shifting the burden of both the authentication processing and management responsibility to centralized Managed Authentication Service Provider (MASP) [150]. As shown in Fig. 3, this 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 within a close proximity. This accumulated identity confidence status is utilized in both device and service domain as MASP would verify the user identity continuously and transparently whilst they access services on the device or online depending upon their determined risk level. 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.

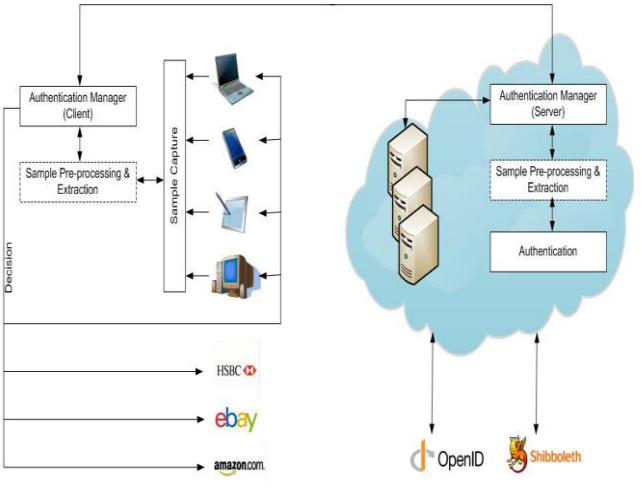

Fig. 3 A Framework of Federated Authentication in the Cloud

Even though this model is deemed to offer a potential solution for many issues of the aforementioned systems, it is still solely conceptual. Therefore, it lacks required tests to appraise acute issues, such as scalability, biometrics management, and battery consumption of portable digital devices. Thus, developing this proposed model and evaluating it with real and live data will perhaps give better insight about its feasibility and value in solving the technology and research problem.

5.5.1 Limitations and Future Challenges

Despite the fact that such a model would have the provisions of effective security and usability, it raises a number of limitations as future challenges that need to be addressed in order for it to function effectively.

- Trust: users and organizations are required to have a high level of trust in a third-party authentication provider;
- Scalability and response time: the time spent to make an authentication decision through the network may introduce a potential delay in transit and bottle-neck at the MASP;
- Privacy: From an end-user perspective, preserving their privacy thereby securing their biometrics information (during the transfer, processing and storage) is essential. Therefore, MASP architecture must be sensibly designed to ensure this and eliminate misuse.

6 Conclusion

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. Unfortunately these activities, services and information are the targets of

cybercrimes. Authentication is at the vanguard of ensuring that only the authorized user is given access; however, it has historically endured 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 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 utilized modality so they have issues regarding the universality and circumvention.

Therefore, a serious move towards employing two or more biometric modality 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. In order to provide users with adequate protection and convenience, innovative robust authentication mechanisms have to be utilized in a universal level, so they operate in a transparent, continuous and user-friendly fashion.

References

1. Conrad, E., Misenar, S., Feldman, J.: CISSP study guide. Elsevier Inc. (2012)
2. Wood, H.M.: 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. ACM Press, New York, New York, USA (1977)
3. Zekri, L., Furnell, S.: Authentication based upon secret knowledge and its resilience to impostors. In: Advances in Network & Communication Engineering 3. pp. 30–38 (2006)
4. O'Gorman, L.: Comparing Passwords, Tokens, and Biometrics for User Authentication. Proc. IEEE. 91, 2021–2040 (2003)
5. Kurkovsky, S., Syta, E.: 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 (2010)
6. Symes, J.E., Clarke, N.L.: Security on Mobile Devices: A Survey of Users' Attitudes and Opinions. Adv. Commun. Comput. Networks Secur. 9, 59–68 (2012)
7. Crawford, H., Renaud, K.: Understanding user perceptions of transparent authentication on a mobile device. J. Trust Manag. 1, 1–28 (2014)
8. CSID: Consumer Survey: Password Habits, A study among American consumers, http://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf. Accessed 18 June 2013
9. Shankdhar, P.: 10 Most Popular Password Cracking Tools, http://resources.infosecinstitute.com/10-popular-password-cracking-tools/. Accessed 30 December 2014
10. Clarke, N.: Transparent user authentication: biometrics, RFID and behavioural profiling. Springer London (2011)
11. Nelson, D., Reed, V., Walling, J.: Pictorial superiority effect. J. Exp. Psychol. Hum. Learn. Mem. 2, 523–528 (1976)
12. Weiss, R., Luca, A. De: PassShapes: utilizing stroke based authentication to increase password memorability. In: Proceedings of the 5th Nordic Conference on n Human-Computer Interaction. pp. 18–22 (2008)
13. De Luca, A., Hang, A., Brudy, F., Lindner, C., Hussmann, H.: 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 (2012)
14. Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M.: Smudge Attacks on Smartphone Touch Screens. In: Proceedings of the 4th USENIX Conference on Offensive technologies. WOOT'10 (2010)
15. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N.: Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. In: Symposium On Usable Privacy and Security (SOUPS) 2005 (2005)
16. Oorschot, P. van, Thorpe, J.: Exploiting Predictability in Click-based Graphical Passwords. J. Comput. Secur. 19, 669–702 (2011)
17. Charrau, D., Furnell, S., Dowland, P.: PassImages: An alternative method of user authentication. In: Proceedings of the f 4th Annual ISOneWorld Conference and Convention. , Las Vegas, USA (2005)
18. English, R., Poet, R.: Towards a metric for recognition-based graphical password security. In: 5th International Conference on Network and System Security (NSS), 2011. pp. 6–8 (2011)
19. Microsoft: Features of Windows 8.1 - Microsoft Windows, http://windows.microsoft.com/en-gb/windows-8/features#personalize=startscreen. Accessed 08 November 2014
20. Passfaces: Passfaces Personal Version 1.0, http://www.passfaces.com/personal/support/helpmanual.htm. Accessed 05 May 2014
21. Ellis, H., Shepherd, J., Davies, G.: Identification of familiar and unfamiliar faces from internal and external

features: Some implications for theories of face recognition. Perception. 8, 431–439 (1979)

22. Aloul, F., Zahidi, S., El-Hajj, W.: Two factor authentication using mobile phones. In: 2009 IEEE/ACS International Conference on Computer Systems and Applications. pp. 641–644. IEEE (2009)
23. HSBC Bank plc: Secure Key: two-factor authentication | HSBC UK, http://www.hsbc.co.uk/1/2/customer-support/online-banking-security/secure-key. Accessed 05 November 2014
24. Google: Install Google Authenticator, https://support.google.com/accounts/answer/1066447?hl=en. Accessed 05 November 2014
25. Furnell, S.M., Katsikas, S., Lopez, J., Patel, A.: Securing Information and Communications Systems: Principles, Technologies, and Applications. Artech House (2008)
26. BBC: Security firm RSA offers to replace SecurID tokens, http://www.bbc.co.uk/news/technology-13681566. Accessed 05 May 2014
27. Nanavati, S., Thieme, M., Nanavati, R.: Biometrics: Identity Verification in a Networked World. John Wiley & Sons, Inc (2002)
28. Jain, A.K., Flynn, P., Ross, A.A.: Handbook of Biometrics. Springer (2008)
29. Schouten, B., Jacobs, B.: Biometrics and their use in e-passports. Image Vis. Comput. 27, 305–312 (2009)
30. Clarke, N., Furnell, S.: Biometrics–The promise versus the practice. Comput. Fraud Secur. 12–16 (2005)
31. Goode Intelligence: Mobile Phone Biometric Security – Analysis and Forecasts 2011–2015. (2011)
32. FBI: Next Generation Identification, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi. Accessed 04 June 2014
33. NSTC: The National Biometrics Challenge 2011. (2011)
34. European Central Bank: Recommendations for the Security of Internet Payments - Final Version After Public Consultation. , Germany (2013)
35. FFIEC: Authentication in an Internet Banking Environment. (2005)
36. NatWest: NatWest personal banking | Online banking, http://www.natwest.com/personal/online-banking/g1/banking-safely-online/card-reader.ashx. Accessed 08 November 2014
37. Lloyds Bank: Lloyds Bank - Internet Banking - How to log on - Help logging on, http://www.lloydsbank.com/online-banking/logging-on.asp?WT.ac=SNOBLO1012. Accessed 08 November 2014
38. Samba Financial Group: SambaOnline Banking – Ways To Bank, http://www.samba.com/en/personal-banking/ways-to-bank/samba-online.html. Accessed 08 November 2014
39. White, C.: Windows 8.1 will focus on biometrics for authentication, http://www.neowin.net/news/windows-81-will-focus-on-biometrics-for-authentication. Accessed 24 March 2014
40. O'Boyle, B.: How does the Samsung Galaxy S5 fingerprint scanner work?, http://www.pocket-lint.com/news/127605-how-does-the-samsung-galaxy-s5-fingerprint-scanner-work. Accessed 13 June 2014
41. Samsung: Samsung Galaxy S5 (Black) - Review, Specs & Features - Samsung UK, http://www.samsung.com/uk/consumer/mobile-devices/smartphones/android/SM-G900FZKABTU. Accessed 08 November 2014
42. Mogull, R.: The iPhone 5s fingerprint reader: what you need to know, http://www.macworld.com/article/2048514/the-iphone-5s-fingerprint-reader-what-you-need-to-know.html. Accessed 13 June 2014
43. Apple: iPhone 5s - Technical Specifications, https://www.apple.com/uk/iphone-5s/specs/. Accessed 08 November 2014
44. IDC: Smartphone OS Market Share 2014, 2013, 2012, and 2011, http://www.idc.com/prodserv/smartphone-os-market-share.jsp. Accessed 08 January 2015
45. Macworld: Take the pain out of two-factor authentication with an app, http://www.macworld.com/article/2840979/take-the-pain-out-of-two-factor-authentication-with-an-app.html. Accessed 08 January 2015
46. Sandhu, S.: Single Sign On Concepts & Protocols. (2004)
47. Furnell, S.: Authenticating ourselves: will we ever escape the password? Netw. Secur. 2005, 8–13 (2005)
48. Stihler, M., Santin, A.O., Marcon Jr., A.L., Fraga, J.D.S.: Integral Federated Identity Management for Cloud Computing. In: 2012 5th International Conference on New Technologies, Mobility and Security (NTMS). pp. 1–5. IEEE (2012)
49. CSA: Identity and Access Management Implementation Guidance. (2012)
50. Madsen, P., Koga, Y., Takahashi, K.: Federated identity management for protecting users from ID theft. In: Proceedings of the 2005 workshop on Digital identity management - DIM '05. pp. 77–83. ACM Press, New York, New York, USA (2005)
51. Traore, I., Ahmed, A.A.E.: Continuous Authentication Using Biometrics: Data, Models, and Metrics. IGI Global (2012)

52. Umphress, D., Williams, G.: Identity verification through keyboard characteristics. Int. J. Man. Mach. Stud. 23, 263–273 (1985)
53. Leggett, J., Williams, G.: Verifying identity via keystroke characteristics. Int. J. Man. Mach. Stud. 28, 67–76 (1988)
54. Shepherd, S.: Continuous authentication by analysis of keyboard typing characteristics. In: European Convention on Security and Detection, 1995. pp. 111 – 114. IET, Brighton (1995)
55. Mahar, D., Napier, R., Wagner, M., Laverty, W., Henderson, R., Hiron, M.: Optimizing digraph-latency based biometric typist verification systems: inter and intra typist differences in digraph latency distributions. Int. J. Hum. Comput. Stud. 43, 579–592 (1995)
56. Furnell, S.M., Morrissey, J.P., Sanders, P.W., Stockel, C.T.: Applications of keystroke analysis for improved login security and continuous user authentication. In: Information systems security. pp. 283–294. Chapman & Hall, Ltd., London, UK (1996)
57. Monrose, F., Rubin, A.D.: Keystroke dynamics as a biometric for authentication. Futur. Gener. Comput. Syst. 16, 351–359 (2000)
58. Dowland, P.S., Singh, H., Furnell, S.M.: A Preliminary Investigation of User Authentication Using Continuous Keystroke Analysis. In: 8th IFIP Annual Working Conference on Information Security Management and Small System Security (2001)
59. Bergadano, F., Gunetti, D., Picardi, C.: User authentication through keystroke dynamics. ACM Trans. Inf. Syst. Secur. 5, 367–397 (2002)
60. Gunetti, D., Picardi, C.: Keystroke analysis of free text. ACM Trans. Inf. Syst. Secur. 8, 312–347 (2005)
61. Hempstalk, K.: Continuous typist verification using machine learning, (2009)
62. Hossain, M., Balagani, K.S., Phoha, V.V.: 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 (2012)
63. Marsters, J.: Keystroke dynamics as a biometric, University of Southampton, (2009)
64. Messerman, A., Mustafic, T., Camtepe, S.A., Albayrak, S.: 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 (2011)
65. Obaidat, M.S., Sadoun, B.: Verification of Computer Users Using Keystroke Dynamics. IEEE Trans. Syst. Man. Cybern. B. Cybern. 27, 261–9 (1997)
66. Roth, J., Liu, X., Metaxas, D.: On Continuous User Authentication via Typing Behavior. IEEE Trans. IMAGE Process. 23, 4611 – 4624 (2014)
67. Gamboa, H., Fred, A.: A behavioral biometric system based on human-computer interaction. In: Defense and Security, International Society for Optics and Photonics. pp. 381–392 (2004)
68. Pusara, M., Brodley, C.E.: 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. ACM Press, New York, New York, USA (2004)
69. Ahmed, A.A.E., Traore, I.: A New Biometric Technology Based on Mouse Dynamics. IEEE Trans. Dependable Secur. Comput. 4, 165–179 (2007)
70. Aksari, Y., Artuner, H.: Active authentication by mouse movements. In: ISCIS 2009. 24th International Symposium on Computer and Information Sciences, 2009. pp. 571 – 574. IEEE (2009)
71. Shen, C., Cai, Z., Guan, X., Huilan, I., Du, J.: Feature Analysis of Mouse Dynamics in Identity Authentication and Monitoring. In: IEEE International Conference on Communications, 2009. ICC '09. pp. 1–5 (2009)
72. Zheng, N., Paloski, A., Wang, H.: An efficient user verification system via mouse movements. In: Proceedings of the 18th ACM conference on Computer and communications security. pp. 139–150. ACM, New York, NY, USA (2011)
73. Jorgensen, Z., Yu, T.: 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. ACM, New York, NY, USA (2011)
74. Lin, C., Chang, C., Liang, D.: 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 (2012)
75. Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., Schclar, A.: User identity verification via mouse dynamics. Inf. Sci. (Ny). 201, 19–36 (2012)
76. Mondal, S., Bours, P.: Continuous authentication using mouse dynamics. In: 2013 International Conference of the Biometrics Special Interest Group (BIOSIG). pp. 1 – 12. IEEE (2013)
77. Stanic, M.: 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. IEEE, Cavtat, Croatia (2013)
78. Clarke, N.L., Mekala, a. R.: The application of signature recognition to transparent handwriting

verification for mobile devices. Inf. Manag. Comput. Secur. 15, 214–225 (2007)

79. Kale, A., Rajagopalan, A.N., Cuntoor, N., Kruger, V.: 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 (2002)
80. Morris, S.: A shoe-integrated sensor system for wireless gait analysis and real-time therapeutic feedback, University of Southampton, (2004)
81. Mäntyjärvi, J., Lindholm, M., Vildjiounaite, E., Mäkelä, S.-M., Ailisto, H.: 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 (2005)
82. Gafurov, D., Snekkenes, E.: Gait Recognition Using Wearable Motion Recording Sensors. EURASIP J. Adv. Signal Process. 2009, 415817 (2009)
83. Derawi, M.O., Gafurov, D., Bours, P.: Towards Continuous Authentication Based on Gait Using Wearable Motion Recording Sensors. In: Traore, I. and Ahmed, A.A.E. (eds.) Continuous Authentication Using Biometrics: Data, Models, and Metrics. pp. 170–192. IGI Global (2012)
84. Juefei-Xu, F., Bhagavatula, C., Jaech, A., Prasad, U., Savvides, M.: 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. IEEE, Arlington, VA (2012)
85. Nickel, C., Wirtl, T., Busch, C.: 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 (2012)
86. Lu, H., Huang, J., Saha, T., Nachman, L.: Unobtrusive gait verification for mobile phones. In: Proceedings of the 2014 ACM International Symposium on Wearable Computers - ISWC '14. pp. 91–98. ACM Press, New York, New York, USA (2014)
87. Tanviruzzaman, M., Ahamed, S.I.: Your Phone Knows You: Almost Transparent Authentication for Smartphones. In: 2014 IEEE 38th Annual Computer Software and Applications Conference. pp. 374–383. IEEE (2014)
88. Woo, R.H., Park, A., Hazen, T.J.: The MIT Mobile Device Speaker Verification Corpus: Data Collection and Preliminary Experiments. In: IEEE Odyssey 2006: The Speaker and Language Recognition Workshop, 2006. pp. 1–6. IEEE (2006)
89. Kunz, M., Kasper, K., Reininger, H., Möbius, M., Ohms, J.: Continuous Speaker Verification in Realtime. In: Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, BIOSIG 2011. pp. 79–88 (2011)
90. Martucci, L. a., Zuccato, A., Smeets, B., Habib, S.M., Johansson, T., Shahmehri, N.: 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 (2012)
91. Abdullah, M., Bashier, H., Sayeed, S., Yusof, I., Azman, A., Ibrahim, S.Z., Liew, T.H.: Answering Incoming Call for Implicit Authentication Using Smartphone. J. Theor. Appl. Inf. Technol. 61, 193–199 (2014)
92. Aupy, A., Clarke, N.: User Authentication by Service Utilisation Profiling. In: Proceedings of the ISOneWorld 2005. , Las Vegas, USA (2005)
93. Yazji, S., Chen, X., Dick, R.P., Scheuermann, P.: Implicit User Re-Authentication for Mobile Devices. In: Ubiquitous Intelligence and Computing. pp. 1–15. Springer-Verlag New York Inc (2009)
94. Jakobsson, M., Shi, E., Golle, P., Chow, R.: Implicit authentication for mobile devices. In: the 4th USENIX conference on Hot topics in security, HotSec'09 (2009)
95. Saevanee, H., Clarke, N., Furnell, S.: SMS linguistic profiling authentication on mobile device. In: 2011 5th International Conference on Network and System Security. pp. 224–228. IEEE (2011)
96. Li, F., Wheeler, R., Clarke, N.: An Evaluation of Behavioural Profiling on Mobile Devices. Proc. Second Int. Conf. HAS. 8533, 330–339 (2014)
97. Klosterman, A., Ganger, G.: Secure continuous biometric-enhanced authentication. In: Technical Report CMU-CS-00- 134, Carnegie Mellon University (2000)
98. Liu, X., Chen, T.: 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 (2003)
99. Janakiraman, R., Kumar, S., Sim, T.: 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 (2005)
100. Clarke, N., Karatzouni, S., Furnell, S.: Transparent facial recognition for mobile devices. In:

Proceedings of the 7th Security Conference. , Las Vegas, USA (2008)

101. Xiao, Q., Yang, X.-D.: Facial Recognition in Uncontrolled Conditions for Information Security. EURASIP J. Adv. Signal Process. 2010, 1–10 (2010)

102. Hurley, D., Nixon, M., Carter, J.: Automatic ear recognition by force field transformations. In: IEE Colloquium on Visual Biometrics. pp. 2–6. IET, London (2000)

103. Rodwell, P.M.: Non-Intrusive Subscriber Authentication for Next Generation Mobile Communication Systems, (2006)

104. Islam, S., Davies, R., Mian, A.S., Bennamoun, M.: A Fast and Fully Automatic Ear Recognition Approach Based on 3D Local Surface Features. Adv. Concepts Intell. Vis. Syst. Lect. Notes Comput. Sci. 5259, 1081–1092 (2008)

105. Fahmi, P.N.A., Kodirov, E., Choi, D.-J., Lee, G.-S., Mohd Fikri Azli, A., Sayeed, S.: 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 (2012)

106. Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunar, B., Jiang, Y., Nguyen, N.: Continuous mobile authentication using touchscreen gestures. In: 2012 IEEE Conference on Technologies for Homeland Security (HST). pp. 451–456. IEEE (2012)

107. Koundinya, P., Theril, S., Feng, T., Prakash, V., Bao, J., Shi, W.: Multi resolution touch panel with built-in fingerprint sensing support. In: Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014. pp. 1–6. IEEE Conference Publications, New Jersey (2014)

108. Kisku, D.R., Gupta, P., Sing, J.K., Tistarelli, M., Hwang, C.J.: Low Level Multispectral Palmprint Image Fusion for Large Scale Biometrics Authentication. In: Traore, I. and Ahmed, A.A.E. (eds.) Continuous Authentication Using Biometrics: Data, Models, and Metrics. pp. 89–104. IGI Global (2012)

109. Wildes, R.: Iris recognition: an emerging biometric technology. Proc. IEEE. 85, 1348 – 1363 (1997)

110. Matey, J.R., Naroditsky, O., Hanna, K., Kolczynski, R., LoIacono, D.J., Mangru, S., Tinker, M., Zappia, T.M., Zhao, W.Y.: Iris on the Move: Acquisition of Images for Iris Recognition in Less Constrained Environments. Proc. IEEE. 94, 1936–1947 (2006)

111. Proença, H., Alexandre, L.: Iris segmentation methodology for non-cooperative recognition. IEE Proc. - Vision, Image Signal Process. 153, 199–205 (2006)

112. Du, Y., Arslanturk, E., Zhou, Z., Belcher, C.: Video-Based Noncooperative Iris Image Segmentation. IEEE Trans. Syst. MAN, Cybern. B Cybern. 41, 64 – 74 (2011)

113. Yang, K., Du, E.: A multi-stage approach for non-cooperative iris recognition. In: 2011 IEEE International Conference on Systems, Man, and Cybernetics (SMC). pp. 3386 – 3391. IEEE (2011)

114. Chen, R., Lin, X., Ding, T.: Liveness detection for iris recognition using multispectral images. Pattern Recognit. Lett. 33, 1513–1519 (2012)

115. Mock, K., Hoanca, B., Weaver, J., Milton, M.: 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 (2012)

116. Sui, Y., Zou, X., Du, E.Y., Li, F.: Secure and privacy-preserving biometrics based active authentication. In: 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC). pp. 1291–1296. IEEE (2012)

117. Jain, A., Nandakumar, K., Ross, A.: Score normalization in multimodal biometric systems. Pattern Recognit. 38, 2270–2285 (2005)

118. Ross, A., Nandakumar, K., Jain, A.: Handbook of multibiometrics. Springer, New York, New York, USA (2006)

119. De Oliveira, A.E., Henrique Matos Bezerra Motta, G., Vidal Batista, L.: A multibiometric access control architecture for continuous authentication. In: 2010 IEEE International Conference on Intelligence and Security Informatics. pp. 171–171. IEEE (2010)

120. Sim, T., Zhang, S., Janakiraman, R., Kumar, S.: Continuous Verification Using Multimodal Biometrics. IEEE Trans. Pattern Anal. Mach. Intell. 29, 687–700 (2007)

121. Azzini, A., Marrara, S.: Impostor Users Discovery Using a Multimodal Biometric Continuous Authentication Fuzzy System. Knowledge-Based Intell. Inf. Eng. Syst. 5178, 371–378 (2008)

122. De Oliveira, A.E., Motta, G.H.M.B.: A Security API for Multimodal Multi-biometric Continuous Authentication. In: 2011 Seventh International Conference on Computational Intelligence and Security. pp. 988–992. IEEE (2011)

123. Tsatsoulis, P.D., Jaech, A., Batie, R., Savvides, M.: Multimodal Biometric Hand-Off for Robust Unobtrusive Continuous Biometric Authentication. In: Traore, I. and Ahmed, A.A.E. (eds.) Continuous

Authentication Using Biometrics: Data, Models, and Metrics. pp. 68–88. IGI Global (2012)

124. Kwang, G., Yap, R.H., Sim, T., Ramnath, R.: A usability study of continuous biometrics authentication. In: Tistarelli, M. and Nixon, M.S. (eds.) Proceedings of the Third International Conference on Advances in Biometrics. pp. 828–837. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)

125. Ahmed, A., Traore, I.: Anomaly intrusion detection based on biometrics. In: Proceedings of the 2005 IEEE Workshop on Information Assurance and Security. pp. 452 – 453. IEEE (2005)

126. Pusara, M.: An Examination of User Behavior for User Re-authentication, ProQuest, (2007)

127. Bailey, K.O., Okolica, J.S., Peterson, G.L.: User identification and authentication using multi-modal behavioral biometrics. Comput. Secur. 43, 77–89 (2014)

128. Vildjiounaite, E., Mäkelä, S., Lindholm, M., Riihimäki, R.: 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. Springer-Verlag, Berlin, Heidelberg (2006)

129. Li, F., Clarke, N., Papadaki, M., Dowland, P.: 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 (2011)

130. Crawford, H., Renaud, K., Storer, T.: A framework for continuous, transparent mobile device authentication. Comput. Secur. 39, 127–136 (2013)

131. Saevanee, H., Clarke, N., Furnell, S., Biscione, V.: Text-Based Active Authentication for Mobile Devices. IFIP Adv. Inf. Commun. Technol. ICT Syst. Secur. Priv. Prot. 428, 99–112 (2014)

132. Carrillo, C.: Continuous biometric authentication for authorized aircraft personnel: A proposed design, Naval Postgraduate School, Monterey, California, (2003)

133. Clarke, N., Furnell, S.: A composite user authentication architecture for mobile devices. J. Inf. Warf. 5, 11–29 (2006)

134. Asha, S., Chellappan, C.: Authentication of e-learners using multimodal biometric technology. In: International Symposium on Biometrics and Security Technologies, 2008. ISBAST 2008. pp. 1–6. IEEE (2008)

135. Muaaz, M.: 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. ACM, Zurich, Switzerland (2013)

136. Altinok, A., Turk, M.: Temporal Integration for Continuous Multimodal Biometrics. In: Multimodal User Authentication (2003)

137. Kang, H.-B., Ju, M.-H.: Multi-modal Feature Integration for Secure Authentication. In: Huang, D.-S., Li, K., and Irwin, G.W. (eds.) Proceedings of the 2006 international conference on Intelligent Computing. pp. 1191–1200. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)

138. Ojala, S., Keinanen, J., Skytta, J.: Wearable Authentication Device for Transparent Login in Nomadic Applications Environment. In: 2nd International Conference on Signals, Circuits and Systems. pp. 1–6 (2008)

139. Clarke, N., Karatzouni, S., Furnell, S.: 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. pp. 1–12. Springer, Pafos, Cyprus (2009)

140. Soltane, M., Doghmane, N., Guersi, N.: Face and Speech Based Multi-Modal Biometric Authentication. Int. J. Adv. Sci. Technol. 21, 41–56 (2010)

141. Niinuma, K., Park, U., Jain, A.K.: Soft Biometric Traits for Continuous User Authentication. IEEE Trans. Inf. Forensics Secur. 5, 771–780 (2010)

142. Tsai, P., Khan, M.K., Pan, J., Liao, B.: Interactive Artificial Bee Colony Supported Passive Continuous Authentication System. IEEE Syst. JOURNAL, IEEE Biometrics Compend. 8, 395–405 (2014)

143. Khan, M.K., Tsai, P.-W., Pan, J.-S., Liao, B.-Y.: Biometric Driven Initiative System for Passive Continuous Authentication. In: 7th International Conference on Information Assurance and Security (IAS), 2011. pp. 139–144. IEEE (2011)

144. Chowdhury, M., Light, J., McIver, W.: A Framework for Continuous Authentication in Ubiquitous Environments. In: Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), IEEE Press. pp. 1–6 (2010)

145. Riva, O., Qin, C., Strauss, K., Lymberopoulos, D.: Progressive authentication: deciding when to authenticate on mobile phones. In: The 21st USENIX Security Symposium (2012)

146. Hocking, C.G., Furnell, S.M., Clarke, N.L., Reynolds, P.L.: Co-operative user identity verification using an Authentication Aura. Comput. Secur. 39, 486–502 (2013)

147. Traore, I., Woungang, I., Obaidat, M.S., Nakkabi, Y., Lai, I.: 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 (2012)

148. Ceccarelli, A., Montecchi, L., Brancati, F., Lollini, P., Marguglio, A., Bondavalli, A.: Continuous and Transparent User Identity Verification for Secure Internet Services. IEEE Trans. Dependable Secur. Comput. PP, 1–14 (2014)

149. Salesforce: 2014 Mobile Behavior Report. (2014)

150. Al Abdulwahid, A., Clarke, N., Furnell, S., Stengel, I.: 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 (2013)