2016

The role of security and its antecedents in e-government adoption

Alharbi, Nawaf Sulaiman S

2016

The role of security and its antecedents in e-government adoption

Alharbi, Nawaf Sulaiman S

THE ROLE OF SECURITY AND ITS ANTECEDENTS IN E-GOVERNMENT ADOPTION

by

Nawaf Alharbi

A thesis submitted to Plymouth University
In partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics
Faculty of Science and Engineering

October 2016

Abstract

The role of security and its antecedents in e-government adoption

Nawaf Alharbi

The use of e-government has increased in recent years, and many countries now use it to provide high quality services to their citizens. As user acceptance is crucial for the success of any IT project, a number of studies have investigated the user acceptance of e-government via the use of adoption models, such as the Unified Theory of Acceptance and Use of Technology (UTAUT) model. However, these models do not pay sufficient attention to security. The lack of security is one of the key issues associated with the adoption of e-government. Thus, this study aims at investigating the role of security in the behaviour intention for using e-government services. In addition, this study seeks to determine the factors influencing end users' perceptions in e-government security. Therefore, in mind of achieving the aim, the research followed a mixed-methods approach, which divided the research into two phases. The first phase is a qualitative study aiming at exploring the factors influencing end users' perceptions in e-government security. The second phase is a quantitative study aiming at identifying the role of security and its antecedences in the behaviour intention for using e-government services. To achieve this goal, a research model was developed by integrating trust, security and privacy with the UTAUT2 and tested via Structural Equation Modelling (SEM). The findings show that user interface quality, security culture and cyber-security law positively affect security perception. These factors explain 54% of security perception variance and strongly influence trust in e-government services. The findings also show that trust is ranked as the third most critical factor affecting behaviour intention after performance expectance and habit. The results make a significant contribution to academic research as this research is the first that investigated the factors that influence the security perception in e-government services. This will provide opportunities for further research to investigate further contributing factors and validate the security antecedences explored in this study. This research has practical implications regarding understanding the role of security in e-government adoption and the factors affecting end users' perceptions of e-government security. This will help the decision makers in government to increase users' trust in e-government by focusing more on these factors.

Table of Contents

List of figures

List of table

Acknowledgements

First and foremost, I would like sincerely to extend my most sincere thanks to ALLAH, the most merciful and the most gracious who granted me the strength and power to undertake this study.

In addition, I also would like to express my deepest and most sincere thanks and appreciation to my parents, who have provided me with an abundance of love and support, and who have stood alongside me throughout the course of my life. In this same vein, special thank are extended to my wife, Amnah Alharbi, and my daughter, Wateen, both of whom have unfailingly given endless patience, love and support throughout the undertaking and completion of this PhD journey. This work is a token of my appreciation of you, and is a small gift for you.

I also would like to express my deep appreciation to my first supervisor, Dr Maria Papadaki, as well as to my second supervisor, Dr Paul Dowland, both of whom have afforded a wealth of help and support during my study. Without this support and guidance, and without the many instances of help offered, this work could not have been completed.

Plymouth University, as a whole, also has given me a wealth of help in the form of my PhD colleagues, specifically Mr Hussain Alsaiari, Mr Gomaa Agag and Dr Ahmed Alghamdi. Throughout this period, their support and help has been pivotal. So much thanks.

I also would like to thank Dr Faris Al-sobhi and Dr Mohammed Alshehri for their many different recommendations at the beginning of this PhD journey. Thanks are extended for their time and efforts in making the PhD journey easier and generally better.

I also would like to thank all of the individual participants involved in this work. I also would like to thank all of those who have helped me in the distribution of the questionnaire across social network websites. The abundance of cooperation has been highly appreciated.

And last but not least, I acknowledge King Abdulaziz City for Science and Technology (KACST) for sponsoring my undertaking of this PhD programme. I am so eternally grateful.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee. Work submitted for this research degree at the Plymouth University has not formed part of any other degree either at Plymouth University or at another establishment. Relevant scientific seminars and conferences were regularly attended at which work was often presented and several papers prepared for publication.

Publications:

Journal publication

[1] Alharbi, N., Papadaki, M., and Dowland, P. (2014). Security Factors Influencing End Users ' Adoption of E-Government. *Journal of Internet Technology and Secured Transactions (JITST)*, *3*(4), 320–328.

Conference publication

[1] Alharbi, N., Papadaki, M. and Dowland, P., 2014, December. Security challenges of E-government adoption based on end users' perspective. In *Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for* (pp. 78-82). IEEE.

[2] Alharbi, N., 2013. E-government Security Modeling: Explaining Main Factors and Analysing Existing Models. ICBG 2013: International Conference on e-Business and e-Government, Turkey, Istanbul September 19-20, Vol. 7, No. 9, pp675-678.

Word count of main body of thesis: 46,649 words

Signed: ……..

Date: …...……..

1. Introduction

1.1. Introduction

This chapter provides an introduction of the research and begins by highlighting the research problem this research seeks to solve. Subsequently, the aim of this research is provided, in addition to the objectives followed to achieve the research aim. Two main research questions are provided in this chapter that have been derived from the research aim. This chapter also shows how this thesis was structured and organised. In addition, it provides a conclusion for each chapter in the thesis.

1.2. Research Problem

Many countries around the world have tried to use Information Communication Technology (ICT) to provide high-quality services for their citizens. As the use of the Internet has recently increased, citizens are becoming more familiar with e-commerce, and are expecting their government to provide high quality services similar to those that they receive from the famous companies. There are a number of advantages to be gained from adopting e-government. For example, citizens are able to apply for government services from anywhere at anytime. In addition, its adoption decreases government expenditure due to the direct channel of communication between private and public sectors and other government entities resulting from combining a number of different agencies' systems into one individual web portal. Moreover, public expectations are increased through e-government, with a greater degree of transparency and services being more accessible to users, thereby establishing collaboration between the private and public sectors.

The implementation and provision of government services via the Internet is associated with several challenges, such as IT infrastructure, security issues associated with privacy and trust, availability, accessibility, computer literacy, management issues, website design and a lack of awareness. Several studies have been conducted to investigate these challenges.

The government is responsible for providing a high level of IT infrastructure and for encouraging citizens to use its e-government services. It is also responsible for protecting citizens' privacy. Users will not use these services if privacy is not guaranteed (Sang *et al.*, 2009). However, even if the government meets all these requirements, any e-government project will not be successful if citizens do not accept it. Users' acceptance is a main pre-condition for the success of any IT project (Alateyah *et al.*, 2013). For this reason, several models have been developed in order to investigate the factors affecting the acceptance of technology. A lack of security is recognised as one of the critical factors affecting citizens using e-government services (Alateyah *et al.*, 2012; Sang *et al.*, 2009). Alshehri et al. (2012a) conducted an empirical study in Saudi Arabia on the barriers to e-government adoption, and the results indicate that lack of security is the second most important barrier. Therefore, more research is needed to understand how security concerns influence the adoption of e-government and provide a theoretical and scientific investigation into its role in e-government adoption through the use of technology acceptance models. Previous technology acceptance models have not considered the role of security in e-government adoption. Thus, this study aims to investigate the role of security in e-government adoption by using an amended version of a recent acceptance model.

In addition, as security is important in e-services, such as in e-commerce and e-government, several studies have been conducted in order to investigate the factors influencing end users' perception of e-services security. In e-commerce studies, Kamoun and Halaweh (2012)

investigated the impact of the user interface design on security perceptions. In addition, Halaweh (2012) investigated the factors influencing end users' perception of e-commerce security; however, there is a lack of research investigating the factors influencing end users' perception of e-government security, and as e-government is situated in a different environment to e-commerce this results in a research gap. Thus, this research will investigate these factors and this will help both decision-makers in the government and researchers in e-government to understand how end users evaluate e-government security.

1.3. Aims and Objectives

This study aims at investigating the role of security and its antecedences in the behaviour intention for using e-government services; thus, the research begins by investigating the factors influencing end users' perceptions in e-government security. Subsequently, the research investigates the role of security in e-government adoption. Accordingly, based on the research aim, the following objectives of the research are outlined as follows:

1. Perform a literature review into the current state of the art in e-government adoption.
2. Review the models and theories of technology acceptance that have been used to investigate the adoption of e-government services.
3. Explore and investigate the security challenges that face end users in e-government adoption.
4. Conduct focus group sessions with general end users and security experts to investigate the factors that influence end users' perception of e-government security.
5. Develop the research model to investigate the role of security and its antecedents in e-government adoption.

6. Evaluate the research model and test the research hypotheses by using Structural Equation Modelling (SEM).

7. Discuss the findings from evaluating the research model and testing the research hypotheses in view of previous studies in this field.

1.4. Research Questions

As the aim of this study is investigating the role of security and its antecedences in behavioural intention for using e-government services, there are two main questions that this research seeks to answer. These questions are:

1- What are the factors influencing end users' perceptions in e-government security?

2- What is the role of security in e-government adoption?

1.5. Thesis Structure

This thesis has been divided into nine chapters in order to achieve the aim and objectives of this research and answer the research questions. These chapters are summarised as follows:

- Chapter 2 provides general information pertaining to e-government and the research background. It begins by providing information about the fundamentals of e-government; this includes providing the definition of e-government and explaining its types. The benefits of using e-government services and its stages are provided, as well as the e-government framework. E-government maturity models are provided and discussed. The challenges associated with e-government also are explained. As this study takes the e-government in Saudi Arabia as a case study, general information about Saudi Arabia and its e-government program will be provided; this information includes an overview of the YESSER program and the services it provides. The

relation between e-government and e-commerce will be discussed as both are e-services, and most of the studies investigating the adoption of e-services have focused on e-commerce.

- Chapter 3 provides the Literature Review for this research, as well as the theoretical background. There are two main sections. The first section focuses on the theories and models of technology acceptance, and provides an overview on these models and theories, whilst also discussing the limitations in these theories and models. At the end of this section, the empirical studies investigating the adoption of e-government are reviewed. In addition, studies applying the UTAUT and UTAUT2 are reviewed in particular. The second section focuses on security in e-services. It starts by explaining the security dimensions. Subsequently, studies investigating the security perceptions in e-services are reviewed. In addition, studies seeking to investigate the factors influencing end users' perceptions of e-services security also are reviewed.
- Chapter 4 provides a general overview on the research methodology. It begins by explaining the research paradigms and describing the research approaches. This study used a mixed-methods research approach that begins with the completion of a qualitative phase followed by a quantitative phase. The methodology for each phase is explained as well. The main data collection strategies in the research will be explained in this chapter, which are Literature Review, interview, focus groups and questionnaire. The justification for selecting the research paradigm and approach is provided. Moreover, the target population and how the sample size was determined also is described. At the end of the chapter, information related to the questionnaire translation and ethical considerations is provided.
- Chapter 5 focuses on the security challenges in e-government adoption based on end users' perceptions. An initial survey has been conducted to investigate the current

security challenges, with a more in-depth understanding for the phenomena at the beginning of the research. This initial survey helped the researcher to get more information and feedback from end users as the targeted population in this study are the end users of e-government services. This chapter focuses on the initial survey and begins by clarifying the surveys conducted in the research and the aim for each one. The survey methodology used for designing the survey was explained and described. The data obtained from 189 participants were analysed, with the findings described and discussed at the end of this chapter.

- Chapter 6 investigates the factors influencing end users' perceptions in e-government security. This is the first phase in the research that is a qualitative phase. The research adopts grounded theory for this phase. The analysis and procedures of this stage are detailed. The findings from the analysis stages determine the initial factors influencing end users' perceptions in e-government security.
- Chapter 7 focuses on the second phase, which is the qualitative phase. This phase begins by developing the research model and hypotheses. The base research model in this research is UTAUT2. There are three main parts included in the research model: the first part is the constructs related to the factors influencing end users' perceptions in e-government security, which have been obtained from the qualitative phase; the second part includes constructs of trust, security and privacy; and the third part includes the UTAUT2 constructs. After describing how the research model and hypotheses were developed, this chapter shows the methodology and the data collection, which is a questionnaire. This describes how the questionnaire was design and distributed. It also provides geographical information concerning the 625 participants who completed the questionnaire in full. The measurement items used in

the questionnaire to measure the research model constructs are provided at the end of the chapter, along with their sources.

- Chapter 8 focuses on the model assessment. This starts with providing general information about Structural Equation Modelling (SEM), which is used in the model assessment stage. An overview regarding the analysis process is provided. There are two main steps for the model assessment: the first step is the measurement model which was assessed by evaluating the reliability and validity of the model constructs; the second step is structural model assessment which has been done by testing the research hypotheses evaluating the model fit. The findings from analysing the research model are discussed at the end of this chapter.
- Chapter 9 provide a conclusion for this study. This starts by providing a summary of the research. Following, the answers to the two research questions are provided based on the findings in this research. The final model is provided, which is based on the accepted research hypotheses. Theoretical and practical contributions in research also are provided. Finally, the limitations in the research are addressed, with recommendations for future research provided.

2. E-government and Research Background

2.1. Introduction

This chapter will provide a general background on e-government, as well as general information pertaining to the case study considered in this research, which is that of e-government in Saudi Arabia. The chapter begins by providing a definition of e-government and accordingly clarifying the various types and stakeholders of e-government. In addition, the benefits associated with using e-government services for the government, business, government employees and citizens will be highlighted. This chapter will also make mention to the models used to evaluate e-government maturity overall. Furthermore, an e-government framework, complete with its four layers, will be explained. Moreover, general e-government challenges, as mentioned in previous studies, will be discussed. This chapter then will provide general information relating to e-government in the specific context of Saudi Arabia, beginning with an overview of Saudi Arabia characteristics. Subsequently, general details surrounding the e-government programme in Saudi Arabia (YESSER), as well as its various current projects and services, will be considered. Moreover, the current state of e-government in the KSA will be mentioned based on the latest United Nations report. The chapter will emphasises and discuss the relation between e-government and e-commerce by explaining the differences between them. A conclusion will be provided at the end of the chapter.

2.2. E-government Fundamentals

2.2.1. Definitions

When considering the term ‘electronic government’, it is essential to be clear exactly how this concept is to be defined, especially in a work such as this. The term ‘electronic

government', commonly referred to as 'e-government', is used widely in the literature; thus far, however, there is a lack of consensus as to its meaning. Importantly, the concept is relatively new and therefore is recognised as being in its infancy, having been first introduced in the 1990s, as noted by Caldow (1999). Since this time, however, it has become common to use the terms 'e-government' and 'e-Gov' (Faris, 2011).

Importantly, when seeking to define this new term, it is stated by Halchen (2004) that e-government is lacking a universally agreed upon definition. In this vein, it is further stated by Alsaif (2014) that a number of the literature defining e-government have done so from a narrow perspective of Internet-facilitated government implementations, with the concept considered by authors from a wider-angled lens, including with consideration to the application of ICT in the government surrounding process engineering and overall reform.

When considering definition, it is recognised by Isaac (2007) that e-government may be considered the use of technology by the government, specifically in mind of web-based Internet applications, concerned with improving not only the provision of government services and data but also access to them amongst citizens, agencies, business partners, staff and other government organisations.

As recognised by Hirst and Norton (1998), e-government may be defined in line with three individual categories: internal, external and relational. The first of this is seen to relate to the horizontal transactions completed by the government between the various government entities; the second concerns the vertical transactions between the government and users; whilst the last is centred on the way in which a government integrates both vertical and horizontal methods.

There are also additional definitions of e-government from different perspectives as shown in Table 2.1**Error! Reference source not found.**.

Definition	Reference
E-government is the application of modern information and communication technology which integrates management and service technologies through networks.	(Zhiming, 2009)
E-government is an administration system in which government offices fully use modern technologies, including information, network and office automation technologies to handle official affairs and provide public services for society.	(Liang, 2012)
The application of ICT to improve, transform and redefine any form of resource and information exchange (transacting and contracting) between involved actors such as companies and governmental organisations and their customers, suppliers or other partners, by developing and maintaining dedicated inter-organisational systems, virtual organisational arrangements and (inter)national institutional arrangements.	(Kurdi et al., 2011)
An institutional approach focuses on carrying out decisions related to service provisions. It uses information and communication technologies (ICTs) to transform the traditional public sector by making it accessible, transparent, effective and accountable.	(Rahim and Athmay, 2013)
The application of information and communications technology (ICT) to transform the efficiency, effectiveness, transparency and accountability of informational and transactional exchanges within government; between governments and government agencies at federal, municipal and local levels; and between citizens and businesses; also to empower citizens through access to and the use of information.	(AlAwadhi and Morris, 2008)
The intensive or generalised use of information technologies in government for the provision of public services, the improvement of managerial effectiveness, and the promotion of democratic values and mechanisms.	(Gil-García and Pardo, 2005)
The use by government agencies of information and communication technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or	(Khan et al., 2010)

more efficient government management.	
The use of ICT to promote more efficient and effective government that facilitates more accessible government services, allows greater public access to information, and makes government more accountable to citizens.	(Qaisar and Ghufran, 2010)
The use of technologies to improve access to and delivery of government services to citizens, businesses and employees. It presents the usage of Internet technologies both as a platform for information exchange, the provision of services, and for the transactions of citizens, businesses and other users.	(Milovanovic et al., 2010)
The initiatives of government agencies and departments to use ICT tools and applications, and Internet and mobile devices, to support good governance, strengthen existing relationships and build new partnerships within civil society.	(Nikkhahan et a.l, 2009)
The use of information and communication technologies (ICTs) in general and the utilisation of the Internet in particular to improve the efficiency, effectiveness, transparency, accountability and activities of a public sector organisation, with the goal of achieving better government.	(Sang et al., 2009)

Table 2.1: Different definitions of e-government

In consideration to the above, and also taking into account the fact that the current work falls under the external category through its emphasis on the behaviours of end users surrounding their intention to use e-government services, the decision is made to complete this work in line with the definition provided by Isaac (2007), as discussed above, where e-government is recognised as being concerned with the use of technology as demonstrated by the government, notably in regards web-based Internet applications, with the objective to improve the overall provision of its services and access to such.

2.2.2. Types of E-government

Various stakeholders are involved with e-government, whether organisations or individuals. Moreover, there is a well-recognised difference when considering whether they are parts of the government or external stakeholders. With this taken into consideration, e-government

may be broken down into four different main types. These four groupings as shown in Figure 2.1 are G2B (government to business), G2C (government to citizen), G2E (government to employee) and G2G (government-to-government).

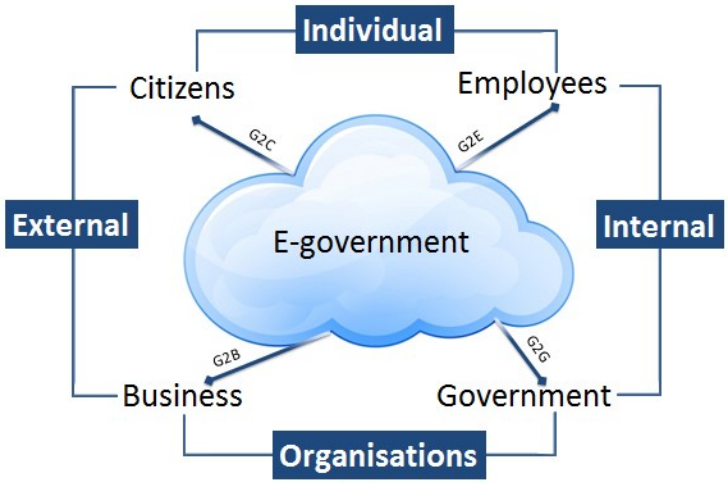

Figure 2.1: Types of e-government

2.2.2.1. Government-to-Citizen (G2C)

It is held by Ndou (2004) that most government services may be referred to as G2C in nature, and are seen to have the key aim of providing not only citizens but also other parties with comprehensive electronic resources adequate to respond to the routine concerns held by individuals as well as the ability to handle government transactions. Through the application of e-government, it is seen that citizens and the government will communicate, thereby facilitating and supporting democracy, accountability and public sector improvements overall.

There is a relationship centred on communication between government agencies and bodies, and their citizens (Huang and Bwoma, 2003). The intention is that e-government interactions between their associated bodies and stakeholders can be improved, with a greater degree of transparency and integrity ensured with citizens (Shahkooh *et al.*, 2008). Accordingly, e-

government could be pivotal in improving citizens' participation with the government and, thus, through greater efficiency and effectiveness in the provision of e-government services, can improve its overall democratic concept.

When considering the main aim of G2C e-government services, it is stated by Pina, Torres and Royo (2010) that this approach is centred on facilitating citizen interactions with the government and serving citizens through ensuring public information is made more accessible whilst also decreasing the time and costs associated with the completion of transactions. When implementing G2C, it is noted that individuals can benefit from both convenient and instantaneous access to government-provided services and information from all locations and at all times, thereby ensuring online interactions are reliable and efficiency is improved, as highlighted by Monga (2008). Moreover, as well as facilitating these transactions, G2C initiatives are well positioned to overcome the various obstacles associated with location and time, allowing citizens to be connected with one another and other organisations that, ordinarily, may not have been possible. This ensures citizen involvement in the government is facilitated and increased (Alshehri, 2012).

2.2.3. E-government Benefits

A number of the benefits associated with e-government are also detailed by Almarabeh and AbuAli (2010) as follows:

- Improved services through more in-depth understanding of user requirements, thereby seeking to achieve seamless online services.
- Providing citizens with government services at all times.
- Improves transparency, facilitates information-sharing and emphasises internal consistencies, thereby contributing to the reform of the government.

- Aids in the building of trust between governments and their citizens, which is fundamental to sound governance, through the adoption of Internet-based methods involving citizens in the policy process, highlighting government accountability and transparency.
- Increases equality between citizens and decreases levels of corruption.
- Provides all government services via online systems, enabling citizens to achieve access in any location.

The various advantages associated with e-government systems are detailed by Alsaif (2014) as centred on decreasing corruption in administration whilst similarly increasing transparency, which has the potential to enhance government services' overall effectiveness and efficiency. The scholar goes on to state that enhanced government service delivery is regarded as being one of the most fundamental factors in enhancing public services performance. In this same vein, the view is posed by Nkwe (2012) that e-government has the potential to empower citizens in such a way that they can overcome the digital divide, decrease costs and similarly reduce intermediaries. As stated by Ndou (2004), through decreasing costs and human errors, and also by applying streamlining in regard to internal processes, there could be a notable improvement in efficiency. Moreover, service delivery quality could be improved in terms of content, accessibility and wasted time by transactions that are considered to be both fast and convenient.

2.2.4. E-Government Maturity Models

Several stages should be followed in order to build fully integrated e-government services. Thus, several models have been developed in mind of measuring the maturity of e-government services. These models are discussed as follows.

- Layne and Lee's Model: This model, proposed by Layne and Lee (2001), details four different stages of e-government development. The first is the cataloguing stage, which means the website provides fundamental information. Such websites are intended to be static, and they enable users only to gain access to the website and download official forms. The second stage is the transactional stage, which focuses on transaction procedures, which users can undertake online. The third stage is the vertical integration stage, which focuses on the integration of government department systems and the transactions between these departments. The fourth stage, the horizontal integration stage, is centred on integrated services. This covers all levels and foundations that are provided for users.

- Chandler and Emanuel's Model: This model, developed by Chandler and Emanuels (2002), also has four stages. The first, the information stage, is basic since it provides only one-way communication between the government and users by allowing users to access the website and obtain the information provided there. The second stage is the interaction stage, which is more complex than the previous stage, providing two-way communications, such as sending and receiving emails and searching the site. Thirdly, the transaction stage centres on transactions between the government and its users. Such transactions include making payments, applying for a service and submitting a request. The fourth stage, the integration stage, is the last in this model, and covers both vertical and horizontal integrated services. Throughout this stage, users can access the portal to access different services in one place.

- Gartner's model: This model was developed by Baum C and Maio (2000) and also contains four stages. First, the web presence stage is a preliminary stage providing one-way communication. In this stage, the website only provides basic information to

users as the website is considered to be static. The second stage, the interaction stage, provides two-way communications between the government and the users. In this stage, users can send and receive emails, upload and download documents, and use the search engines. The third stage is the transaction stage. Here, users can apply for services and make payments through the website. The fourth and final stage, the transformation stage, focuses on integrating the services of all the government departments.

- United Nations Model: This model was proposed by the United Nations (2001), and includes five stages. The first stage is the emerging web presence, which provides initial information with limited options for users. The second stage is enhanced web presence, which is more advanced than the previous stage since the information is updated frequently; it also provides additional services to users, such as search engines and site maps. The third stage is the interactive web presence, which is better developed than the former stage since users can interact with the services easily with more options and facilities. The fourth stage is the transactional web presence which allows users to apply to services and submit requests. Users also can make a payment as it offers two-way communications. The fifth stage is the networked web presence, which is the integration stage, where services and systems are integrated, thereby allowing users to gain access to and accordingly use the facilities with ease.

- West's Model: This model, developed by West (2004), contains four stages. The first stage is the billboard, which allows users to access the website and obtain general published information. The second stage comprises the partial services delivery in which users have access to more facilities such as searching. The third stage is fully integrated service delivery, which simply is a government portal that integrates all

government services in one place. The fourth and last stage is the interactive democracy, which focuses on political transformation in online services.

- Hiller and Blanger's Model: This model has five stages. This first is information dissemination, which is a basic stage allowing users to find static information on the website. The second is a two-way communication stage, where users can interact with the website by, for example, sending and receiving emails, applying for a service, and downloading official forms. The third stage deals with financial and service transactions, and allows users to make a payment through the government website; this means that advanced technologies are used. The fourth stage is a vertical and horizontal integration, meaning means all services and government systems are integrated. The fifth stage is political participation, which allows citizens to be involved in political activities, such as voting (Moon, 2000).

- Moon's Model: This model, proposed by Moon (2002), is similar to that of Hiller and Blanger, since it has five stages. The only difference between them is that the first stage in Moon's model is named 'one-way communication' (Moon, 2000).

- Asia Pacific Model: The Asia Pacific model contains six stages, the first of which involves email and an internal network. This stage focuses on local processes and offers initial functions, such as email. The second is the accessibility stage, which allows local organisations and citizens to access the government website; it also manages the government's workflow. The third stage offers two-way communications and allows users to utilise Information Communication Technology with government departments. The fourth stage is the exchange of value stage, which enables citizens and internal organisations to conduct business with the government, whilst the fifth

stage, which focuses on digital democracy, encourages the democratic process such as voting and other political activities. The last stage is 'joined-up government', which offers vertical and horizontal integration (Wescott, 2001).

- Deloitte and Touche's Model: Deloitte and Touche's model (2001) has six stages. The first is information publishing. Here, the government provides a website that contains static general information for citizens; it offers only one-way communication. The second stage includes two-way transactions. This is a more developed stage where information can be transacted between the government and its citizens. The third stage is a multipurpose portal, which is a website that contains all the services provided by government departments in one place. The fourth stage is portal personalisation which allows users to customise the portal so that it is limited to their interests. The fifth stage is a clustering of common services, bringing together all government services to make the procedures easy for users to follow. The final stage is the integration and enterprise transaction stage, meaning that all services are integrated with advanced technologies to help make the services easily accessible to users.

- Howard's Model: This model was proposed by Howard (2005) and contains three stages. The first stage is publishing, which simply provides basic information on the government website. The second stage is interactive and allows users to interact with the online services, such as using email and sending requests. The last stage is transacting, which allows users to make a payment through the government website.

- World Bank Model: The World Bank model (2003) is similar to Howard's, and has three stages. The first stage is publishing, the initial stage, which provides important

information. The second stage is interactive, and allows users to interact with the government services by sending feedback forms and comments, whilst the final stage is transactions, which allows users to make a secure online payment.

- Organisation for Economic Co-operation and Development (OECD): This model was developed for OECD countries in 2003 to ensure that a good quality service is provided by e-government for users and front and back offices in the government. The OECD identified five areas that the government could improve, which are: user-focused e-government, multi-channel service delivery, identifying common business processes, the business case for e-government and e-government co-ordination. This model has four stages, which are: information, interaction, transaction and transformation (OECD, 2005).

- Interoperability Maturity Model (IMM): This model is used in EU countries to evaluate the maturity of public services and has five maturity stages: Ad Hoc, opportunistic, essential, sustainable and seamless. The evaluation covers four areas which are: service consumption, service choreography, service delivery and service provisioning (European Commission, 2016).

The summary of these models and their stages is shown in Table 2.2.

	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5	Stage 6
Layne and Lee	cataloguing	transactional	vertical integration	horizontal integration	-	-
Chandler and Emanuel	information	interaction	transaction	integration	-	-
Gartner	web presence	interaction	transaction	transformation	-	-
United Nation	emerging presence	enhanced presence	transactional presence	networked presence		-
West	billboard	partial services delivery	integrated service delivery	political transformation	-	-
Hiller and Blanger	information dissemination	two way communications	financial	vertical and horizontal integration	political participation	-
Moon	one way communication	two way communications	financial	vertical and horizontal integration	political participation	-
Asia Pacific	email and internal network	accessibility	two way communications	exchange of value	digital democracy	joined up government
Deloitte and Touche	information publishing	two way transactions	multipurpose portal	portal personalisation	clustering of common services	integration and enterprise transaction
Howard	publishing	interacting	transacting	-	-	-
World Bank	publishing	interactivity	transaction	-	-	-
OECD model	information	interaction	transaction	transformation	-	-
Interoperability model	Ad Hoc	opportunistic	essential	sustainable	seamless	-

Table 2.2: EGMMs and their stages

Karokola (2009) evaluated these models based on the ten principles of ISO 17799 security standards (Table 2.3 has been removed due to Copyright restrictions.

Table 2.3). The research critically analyses these models from a security point of view. A summary of the study is presented in Table 2.4.

Table 2.3 has been removed due to Copyright restrictions.

Table 2.3: ISO 17799 security standards: the ten principles (Karokola, 2009)

	Advantages	Disadvantages
Layne and Lee	-It covers technical issues	-It does not include political changes -Very little consideration of non- technical security issues such as cultural, ethical and economic aspects
Chandler and Emanuel	-Technical issues are covered in the transaction stage	-It does not include political change -It does not cover non-technical issues at all
Gartner	-It considers non-technical issues -It considers political changes	-Only a few technical security issues are covered
United Nation	-Technical issues are covered in the transaction stage	-It does not include political changes -It does not cover non-technical issues at all
West	-It considers some technical and non-technical issues	-It does not include political changes -It does not cover other technical and non-technical issues
Hiller and Blanger	-It considers political changes	-It only covers technical security issues in the financial transaction stage -It does not consider non-technical security issues
Moon	-It considers political changes	-It only covers technical security issues in the financial transaction stage -It does not consider non-technical security issues
Asia Pacific	-It considers political changes	-It only considers security issues in the value exchange stage
Deloitte and Touche	-It considers some technical and non-technical issues	-It does not include political changes very well -It does not cover other technical and non-technical issues
Howard	-It considers some technical security issues	-It does not include political changes -It does not cover both technical and non-security issues in all the stages
World Bank	-It considers some technical security issues	-It does not include political changes -The security in general is lacking except in the transaction stage
OECD model	-It considers political changes	-It does not cover both technical and non-security issues in all the stages
Interoperability model	-It considers some technical security issues	-Very little consideration of non- technical security issues

Table 2.4: Summary of reviews of EGMMs based on ISO 17799

The maturity models are used to evaluate e-government services in general. The majority of them were developed based on daily practice and experience. Thus, theoretical considerations were not a priority when these models were developed. In addition, most of them do not focus on the transition between the stages, as mentioned by Huijsman (2012). Several of these models, for example, Layne and Lee, Hiller and Blanger, Chandler and Emanuel, and West, only focus on two e-government types (G2C and G2B), while a few focus on G2G. As the main goal of these models is to evaluate e-government services in general, the dearth of consideration regarding security issues in these models may represent a concern. Karokola et al. (2011) identified this issue and developed a novel e-government maturity model to fill the gap. This model considers both technical and non-technical security issues at each stage, thus ensuring that all security issues are covered at every stage.

2.2.5. E-government Framework

The e-government framework has four main layers as shown in Figure 2.2. The first layer is the access layer, which contains the channels utilised by users. These channels may be smart phones, the Internet, computers, kiosks, digital TVs and call centres. This layer also includes government users, such as citizens, businesses, employees and government departments. In addition, the access layer is the simplest level of the e-government architecture.

The second layer is the e-government layer, which is connected directly to the access layer. When government users access e-government via a channel in the access layer, they are directed to the e-government portal, which is a single-sign website that has integrated the websites of government departments. This portal helps government users to utilise the government services of each department in one place. However, in some countries, the single-sign portal is still the first stage, meaning a portal is used for each government

department. In addition, a government without data centralisation will not be able to use a single-sign portal.

The third layer is the e-business layer, which is connected to the e-government layer. This layer contains all ICT applications and tools. In addition, it also contains government data resources, such as databases and data warehouses.

The final layer is the infrastructure layer, which includes the network infrastructure components, such as servers, LANs, the Internet, intranet and extranet. It also contains the foundation of government technologies.

Figure 2.2 has been removed due to Copyright restrictions.

Figure 2.2: Framework of e-government architecture (Ebrahim and Irani, 2005)

2.2.6. E-government Challenges

Several studies indicate the main challenges facing e-government (Alateyah *et al.*, 2012; Odat, 2012; Al-sobhi, 2011). Such challenges include IT infrastructure, security issues, such as privacy and trust, availability, accessibility, computer literacy, management issues, website design and a lack of awareness.

2.2.6.1. IT Infrastructure:

Information Technology infrastructure refers to technical components that are used in electronic services, such as hardware, software components and networks, which includes both LANs (Local Area Networks) and WANs (Wide Area Networks). The observed challenges are as discussed in the following paragraphs:

- Lack of hardware: Hardware components must be updated, with regular maintenance needing to be scheduled so as to make sure the hardware is working effectively. The cost of hardware can be an obstacle for some poor countries. Moreover, the low speed of the Internet network is another obstacle facing some countries. One of the main advantages of using e-government is that it saves users time; however, citizens will prefer traditional methods of saving time rather than applying online if the Internet speed is slow. Moreover, the Internet should be accessed easily, especially with mobiles, and significant coverage should be provided. This will help citizens to make applications with ease through their mobiles or smart devices.

- Lack of software: Software and databases that are used in e-government should be designed to cover large amounts of data, to accept a huge number of access requests, and to deal with different types of document. A limited database will not be able to provide high-quality services. It has been observed that some e-government services come to a halt when users apply at the same time, such as when they are applying for scholarships, enquiring for final results and applying for services that are based on a first-come first-served basis. In addition, the software must be updated and the database must be backed up regularly.

- Lack of system integration: The heads of department should work together as a team to avoid facing problems in the future; there must also be a clear plan for designing the systems. A lack of integration is one of the challenges facing e-government. Moreover, there should be strong communication systems so as to avoid delay in the services.

- Lack of data centralisation: Data centralisation plays an important role in efficiently delivering e-government services to citizens; it can also make integrating the systems of government departments easier. In addition, as long as citizens' data are saved in one place, each department will be able to use these data. Conversely, an absence of centralisation will lead each department to use its own database. In this case, citizens' data will be duplicated since their data will need to be provided for each department with which they are dealing. However, centralising data is subject to the political agenda of each country since, in some countries, this goes against human rights. Finally, however, the absence or complete lack of data centralisation will ultimately reduce the various benefits associated with the use of e-government.

2.2.6.2. Security Issues:

One of the main factors affecting the adoption of e-government is a lack of security (Al-Nuaimi *et al.*, 2011; Berdykhanova and Dehghantanha, 2010). In addition, whilst security problems can be either technical or non-technical, the effect of non-technical issues has been observed more in developing countries (Rehman and Esichaikul, 2011; Karokola *et al.*, 2013; Pokharel and Park, 2009). Security may be defined as the protection either of data or systems from unsanctioned intrusions or outflows. Security issues can be divided into four main categories, which are discussed below:

- Information security: The definition of information security is 'the subjective probability with which consumers believe that during information transit or storage their personal information will not be viewed, stored or manipulated by inappropriate parties, in a manner consistent with their confident expectations' (Chellappa and Pavlou, 2002). An information security strategy is based on confidentiality, integrity

and availability, which is referred to as the CIA security triangle (Syamsuddin and Hwang, 2010).

- Perceived risk: Received risk is defined as the negative consequences a customer is worried about when he/she carries out an action, such as making a wrong payment decision (Alateyah et al., 2012). Belanger et al. (2002) indicate that users are more concerned with the perceived risk of e-services, especially when they apply for a service or share their information. In addition, users with limited ICT skills will be more concerned about the perceived risks.

- Privacy: In e-government services, privacy is one of the most crucial concerns facing users (Syamsuddin and Hwang, 2010) who are sensitive about the recording of their personal information. This is likely to have a negative impact, which ultimately will affect their use of e-government services (Alateyah et al., 2012).

- Trust: The best way of encouraging users' trust is to reduce the risks in e-government services. Many research studies have indicated the importance of trust for users in their acceptance of new technologies (Al-sobhi, 2011). When their trust is low, users will pay more attention, time and effort when using e-government services. Thus, increasing the levels of trust will allow users to employ e-government services more easily since it will reduce their level of anxiety during the process of carrying out such a procedure. There are two main types of trust, which are:

    - Trust of the Internet (TOI): Trust of the Internet plays an important role in e-government as increasing trust in the Internet will lead to increases in the use of e-government. Users should feel that the Internet is a safe way of gaining access to government services. However, a lack of ICT skills and poor

computer literacy are pivotal in reducing the trust level of users, and they may not use e-government if they do not trust the Internet.

- Trust of Government (TOG): In some countries, such as developing countries, there is a lack of trust in the government. Some governments have made efforts towards increasing the level of trust by using intermediaries as a third party to encourage their citizens to use e-government services.

2.2.6.3. Availability:

Availability is one of the main benefits associated with e-government since it means that services will be available 24/7. However, sometimes, services are unavailable or users cannot access them easily. Many factors could have an effect on the availability of services, such as an inability to accept a lot of requests at the same time; this can lead to services working very slowly or even stopping altogether. Also, services can be halted owing to several types of attack, such as Denial of Service (DoS). As a result, a lack of security will lead to a lack of availability.

2.2.6.4. Accessibility:

E-government must be designed so as to allow all users to access services easily, which means taking into consideration people with disabilities. Users must also be encouraged to use the e-government services, and multi channels must be provided so as to allow users to access them: for example, the Government of Qatar provides free Internet wireless to their citizens, which helps them to gain access to and accordingly use e-government with facility (Alzahrani and Goodwin, 2012).

2.2.6.5. Lack of Awareness:

According to several studies, a lack of awareness is one of the barriers facing e-government. It has been shown that a lack of awareness plays an important role in accepting new technologies, meaning this inevitably influences potential users of e-government (Alawadhi and Morris, 2008). It is also considered to be one of the main factors that causes citizens to reject e-government in developing countries. Governments also are responsible for increasing their citizens' awareness by devising appropriate strategies and plans in this regard.

2.2.6.6. ICT Skills:

There are two types of skill that citizens commonly require: firstly, general skills in the use of computers, which is known as computer literacy; and secondly, information security skills, which are recognised as a necessity for anyone using e-government services.

- Computer literacy: Computer literacy is the ability and knowledge that people need to use computers and new technologies. In his study, Odat (2012) indicates that there is a lack of IT skills amongst leaders, employees, citizens and disabled people. This is considered to be one of the main barriers facing the adoption of e-government.

- Background in information security: Citizens who use e-government services should have at least a general background in information security. Increasing users' knowledge of information security will have an effect on their levels of confidence in their use of e-government services.

2.2.6.7. Website Design:

Suitable website design encourages citizens to use e-government services and certain important factors, such as usability, accessibility and perceived ease of use, need to be consider in the website design (Alateyah *et al*., 2012). Moreover, the website should contain

information and security instructions owing to the fact the citizens will not use e-government if security is not guaranteed.

2.2.6.8. Culture:

Culture plays a fundamental role in the adoption of e-government, with resistance to change recognised as one of the main cultural factors influencing any actions in this domain (Alshehri and Drew, 2010; Alzahrani and Goodwin, 2012). In addition, religion and the tribal system in some countries are significant factors in the adoption of e-government, as well as other cultural issues such as language and education.

A great many challenges face the adoption of e-government. This research focuses on the challenges that are related to security threats but other challenges, such as financial and managerial issues, also influence its adoption. However, these are not discussed in this research as they do not have a strong effect from a security perspective. Table 2.5 summarises the challenges facing the adoption of e-government.

Challenges	References
IT infrastructure	(Odat, 2012), Karokola *et al*. (2011), Ebrahim and Irani (2005), Alateyah *et al*. (2013)
Security issues	Al-azazi (2008), Alfawaz *et al*. (2007), Hadi and Muhaya (2011), Odat (2012), Alateyah *et al*. (2012), Zhang (2010)
Availability	Khan *et al*. (2010), Zulhuda and Ibrahim (2012), Smith and Jamieson (2005)
Accessibility	Odat (2012), Siddiqui and Singh (2012), Alotaibi (2012)
Lack of awareness	Liu (2010), Alateyah *et al*. (2013), Odat (2012)
ICT skills	Shareef (2012), Hwang *et al*. (2004), Odat (2012)
Website design	(Rehman and Esichaikul, 2011), (Al-sobhi, 2011)
Culture	(Alshehri and Drew, 2010), (Alzahrani and Goodwin, 2012), (Monga, 2008)

Table 2.5: Summary of challenges facing e-government adoption

2.3. Status of E-government adoption worldwide

The use of e-government services is increasing year after year. According to the United Nations e-government survey (UN, 2014), there is a huge difference between the percentage of citizens of developed and developing countries using e-government services. For example, more than 80% of citizens in the Nordic countries (Iceland, Denmark, Norway, Sweden and Finland) use e-government services. However, in developing countries, such as Chile, the percentage is much lower, less than 20%. In general, there is shortage in data that provides information regarding actual e-government usage in developing countries, as mentioned by the UN survey. However, the available data shows that only 11.3% of citizens in Egypt use e-government services. One of the main reasons for poor e-government adoption in developing countries is the low degree of e-government services maturity in those countries. For example, e-government services maturity in Egypt is 54% based on the UN maturity model, as shown in the UN e-government survey (UN, 2014). As a result, many citizens in Egypt do not use e-government services since they are not able to meet their requirements.

Maturity and acceptance are playing important role for making the e-government program succeed. Thus, e-government program for any country could be categorised into one of the following categories:

- High maturity, high acceptance.

- High maturity, low acceptance.

- Low maturity, high acceptance.

- Low maturity, low acceptance.

The acceptance of e-government in developing countries is low as mentioned above. Thus, investigating the factors that influence the adoption of e-government in developing countries

will be more successful when the degree of e-government services maturity is high and the services are widely available. The UN e-government survey (UN, 2014) ranks Saudi Arabia as one of the top 20 countries in online service delivery. This makes Saudi Arabia a good case for investigating the factors that influence the adoption of e-government in developing countries. The following section will provide a general overview of the e-government program in Saudi Arabia.

2.4. E-government in Saudi Arabia

2.4.1. Characteristics of Saudi Arabia: An Overview

The Kingdom of Saudi Arabia is the official name afforded to the country, although on an internal scale the country is most commonly referred to as Saudi Arabia. One of the key elements defining the KSA is the holy shrines, located at Makkah and Medina, and their overall importance as Islam's birthplace, which are known to contribute to the Muslim pilgrimage visits that equate to an approximate two million across the country every year, in addition to in times of prayer for Muslims globally. During such times, Muslims are known to turn towards the country's location five times daily, which is part of their tasks and activities for the Islamic faith.

Nonetheless, the importance of the country as Islam's key core necessitates that the agencies associated with the government implement and maintain sufficient control and management over various areas, including health services, accommodation and transportation, keeping in the mind the need to fulfil the large number of visitors to the location each and every year. Such logistical considerations have created the foremost justification for the application of the e-government initiative, meaning that a number of different government departments are

well positioned to align their services throughout the times of pilgrimage, as noted by Alsaif (2014).

In the KSA, the official language spoken is Arabic. Located in the Middle East, the KSA is known to have a total estimated population equating to around 30.8 million (STATS. 2016). The KSA's capital city is Al Riyadh, and in itself is known to have a population of 4 million. The country's economy is predominantly oil-based as a result of the KSA being home to the world's most significant oil ranks. There are a number of different elements that contribute to the characteristics of Saudi Arabian culture, including the tribal system and religion, amongst others.

2.4.2. E-government Programme (YESSER)

The KSA's government affords a great deal of emphasis and value to the change to the information society and its associated implementation of the various transactions associated with e-government and their individual concepts, all of which are known to provide the national economy with a multitude of advantageous. A number of governmental bodies are already implementing a vast number of projects for the application of e-government transactions.

The YESSER project, where the name may be translated to mean 'simplify', has become positioned as an initiative launched by the KSA with the objective to simplify the application of e-government schemes into the various departments of the government (Alsaif, 2014). The adoption of the programme was predominantly concerned with communications and Information Technology, where the application of the electronic transactions could be supported by governmental bodies. Importantly, the scheme acts as a facilitator/enabler of the application of the government within the public arena, carrying the aims of increasing the

overall effectiveness and efficiency of the public sector, ensuring the provision of faster and more improved government services, and ensuring the availability of the necessary information in a precise and timely way.

In mind of the programmes, a work plan was devised and implemented across two parallel methods: an urgent method was adopted first, through which the most basic of criteria for the programmes was to be provided, as well as the completion of various leading projects in the specific arena of governmental electronic transactions, which were carefully selected in an effort to garner tangible, quick and valuable results without significant costs. The second method was implemented with the beginning of the execution of the programmes. The plan was devised, as well as the determination of the various policies, priorities, procedure and regulations. There was a need for the governmental bodies to implementing the individual plans associated with e-government transactions. The programme comprises the application of various different projects, with some of them incorporated in the first approach, such as the more pressing aspect of the work plan. The other projects are included in the second method, with the below paragraphs discussing some of the present projects as they mentioned in YESSER website (www.yesser.gov.sa/en/nationalinitiatives).

Services Portal Project: The NIC (National Information Centre) of the Ministry of Interior is seen to be a creating a services portal, which is to be offered to individuals, centred on satisfying the objective to enable individuals to obtain information relating to these services, i.e. relevant e-forms and requirements, as well as the potential to provide a number of services on an electronic basis. The project further involves establishing approximately 100 electronic kiosks.

Smart Card Project: Smart Cards are one key aspect of modern technology, which have been provided on a worldwide scale with a number of different uses. Importantly, they have a notable processor and high-storage capacity, which facilitates each card in completing complicated operations. Moreover, their virtual lifespan is recognised as being a good length of time. Importantly, the Ministry of Interior has afforded much attention to this technology owing to the fact it is in its initial first few years of establishment. Notably, the Smart Card Project was adopted by the Ministry, which resulted in the traditional civil affairs ID being substituted for the smart ID approach. In subsequent stages, the project has sought to integrate into one card a number of the various government cards, including family cards and driving licenses, for example. In addition, there is the electronic passport application, which is recognised as a modern-day technological solution.

E-Payments Systems Project (SADAD): The SADAD was first devised by the Saudi Arabian Monetary Agency (SAMA) in mind of being the national Electronic Bill Presentment and Payment (EBPP) service provider for the KSA. Importantly, the SADAD's underpinning core mandate is concerned with enabling and streamlining the payment transactions of end consumers across all banks within the KSA. The launch took place at the beginning of October, 2004.

Saudi Electronic Data Interchange: The Public Investments Fund of the Ministry of Finance, at the present time, is responsible for implementing the Saudi Electronic Data Interchange (SaudiEDI) Project with the objective to incorporate transparency and speed into business transaction processes. Essentially, the objective in this regard is concerned with the international trade sector (import/export services e-Trade) in the KSA. Essentially, information concerned with the manifest, delivery notes, import and export statements is able to flow between the parties in question through the application of the project, with the

Customs Department, The General Organization of Ports, cargo agents, customs clearance agents, as well as various others associated with this process, able to benefit.

Social Insurance Management Information System (SIMIS): The General Organization for Social Insurance (GOSI) devised and adopted its innovative SIMIS (Social Insurance Management and Information System), and is recognised as a notable shift in the specific arena of Middle Eastern e-government applications. Importantly, SIMIS has been devised in mind of serving those concerned with the GOSI scheme. Through the application of SIMIS, various government agencies are able to exchange information and interact with GOSI, with the programme also allowing employers and organisations to carry out their business through its means. Importantly, they have the ability to register, change and exclude wages, and submit worker payment contributions. Establishment accounts with GOSI can also be reviewed and examined. As things stand at the present time, contributors also are able to make inquiries concerning their records, establish their services' sequences and establish that their GOSI-related contributions are correct, in addition to various other services commonly provided by GOSI. Importantly, SIMIS is recognised as a virtual field office for GOSI, where business is able to be carried out as a regular field office. Moreover, hospitals are also positioned to clarify and monitor injured persons and their coverage under the Occupational Hazards Branch so as to ensure they are provided with medical care services in a time-efficient manner, without any need to return to any field office. Furthermore, the development of SIMIS was carried out in mind of supporting B2B information between GOSI and establishments so as to ensure the direct transfer of data from the database of GOSI to the databases of establishments, and vice versa, which then can be processed without any degree of interference in the process.

The Internet Awareness Project: This was recognised as the first-fruit of Internet awareness projects, which notably has been envisioned in mind of developing skills and ensuring the application of the National Plan for IT and Sciences in mind of transforming Saudi society into one that is considered knowledge-based. Such an initiative has been directed across all community divisions through the application of audio-visual programmes and the distribution of relevant, interactive publications and digital materials across all areas. The Ministry of Culture and Information, in partnership with King Abdulaziz City for Sciences and Technology, is responsible for the implementation of the project, the aim of which is centred on creating various animated cartoons for both minors and adults, as well as various publications centred on the intact and suitable use of the Internet and the overall use of Information Technology. Moreover, efforts also will be directed towards the issuance of a magazine for children, as well as parties for both adults and minors to be shown in the future, with all project outcomes documented and published on the Internet.

Qawafel e-Training Initiative: Qawafel e-Training Initiative is one aspect of the involvement of the Ministry of Communications and Information Technology across various other initiatives adopted by the private sector and government in mind of facilitating society's various segments across all areas of the country in mind of addressing the issue of Communications and Information Technology and its effective management in filling the digital void and accordingly improving levels of ICT importance and awareness amongst through directing attention to the rural areas and low-income population and provision of basic and free training on using communications and information technology.

Omrah Project: This particular project is centred on the organisation of the process of issuing Omrah visas through electronic means. Such applications are required to be submitted via the Internet, which then will be sent to Omrah agents located internationally. Such applications

will be processed electronically, with processing carried out by the Ministries of Hajj, Foreign Affairs and Interior. Subsequently, there is the issuance of visas just 24 hours later. This particular system is in implementation on a global scale.

E-Government Project in Almadinah city: The Municipality of Almadinah is directing much attention towards the application of e-government. A special portal for Almadinah was devised in mind of introducing services to individuals and the business sector. Moreover, government entities are aiming at improving their overall eligibility for qualifying for e-government adoption across the greatest possible scope.

2.4.3. Status of e-government in the Kingdom of Saudi Arabia

In 2003, the United Nations (UN) ranked the Saudi e-government as number 103. Subsequently, in 2005, the KSA was positioned as 80th by the UN e-government reading report, with YESSER recognised as established during that particular time (YESSER website). In the Kingdom of Saudi Arabia, the e-government has made a number of improvements, with the last UN report ranking the KSA in position 36 worldwide and 18 in Asia. Moreover, as can be seen detailed in Table 2.6, Saudi Arabia has been positioned as 3rd in Gulf Cooperation Council (GCC) (UN, 2014). The report further details that the KSA is one of top 20 countries in online services delivery. In line with the maturity framework devised by the UN, the Kingdom of Saudi Arabia has been seen to achieve 94% emerging presence (stage 1), 68% enhanced presence (Stage 2), 63% transactional presence (Stage 3) and 53% networked presence (Stage 4), with 69% in total. Furthermore, the e-government Development Index (EGDI) assigns countries to one of four different categories, as follows: very high EGDI (more than 0.75), High EGDI (between 0.75 and 0.50), middle EGDI

(between 0.50 and 0.25) and low EGDI (less than 0.25). Importantly, the KSA has been categorised in the high EGDI category owing to the fact its EGDI is seen to total 0.69.

Table 2.6 has been removed due to Copyright restrictions.

Table 2.6: E-government development of Gulf Cooperation Council (GCC)

2.5. Conclusion

This chapter has provided fundamental information pertaining to e-government in general, such as its types and the challenges that face countries in the adoption of e-government. One of these challenges is a lack of security, as mentioned previously in this chapter. Thus, in order to investigate the role of security in e-government adoption, there is a need to investigate its impact among the other key factors influencing citizens' adoption of e-government services. For this reason, several models have been developed in order to investigate these factors further. The next chapter will provide some theoretical background on these models, referring to empirical studies that have focused on investigating the factors that influence end users to use e-government services. In addition, the next chapter will also review the previous studies that sought to investigate and examine the role of security in e-services.

3. Theoretical Background

3.1. Introduction

This chapter provides a theoretical background related to both technology acceptance and information security. It begins by reviewing the theories and models associated with technology acceptance by describing each of them and accordingly highlighting their limitations. The chapter further reviews studies that applied these models in the e-government context overall. Furthermore, this chapter provides additional information relating to UTAUT and UTAUT2 in particular, and subsequently reviews the empirical studies applying UTAUT and UTAUT2 in e-government studies.

This chapter further delivers a theoretical background pertaining to security perception in e-services in general and in e-government specifically. This includes explaining the security dimensions and reviewing those studies that investigate the impacts of security perceptions in e-services. In addition, it investigates the factors influencing end users' security perceptions in e-services.

3.2. Theories and Models of Technology Acceptance

3.2.1. Theory of Reasoned Action (TRA)

This is one of the first and most valuable of technology acceptance models, with a great deal of attention and support having been proffered through both empirical works and literature. The Theory of Reasoned Action is a theory that has been devised by Ajzen and Fishbein (1980), the fundamental focus of which is concerned with establishing the elements impacting the intended behaviours of users. The framework is centred on motivation at its core, with the model stating that the behaviours of people have two individual motivational

elements: the attitude of the individual towards their own behaviour, and the concern about the thoughts of people they consider important in relation to their behaviours as shown in Figure 3.1. It has been stated by Ajzen and Fishbein (1980) that, following their observations, attitude, in addition to subject norms, were found to establish the behavioural intention amongst individuals, with three critical components of the model established as attitude, behavioural intention and subjective norms.

Figure 3.1 has been removed due to Copyright restrictions.

Figure 3.1: Theory of Reasoned Action Model (TRA) (Ajzen and Fishbein, 1980)

In the TRA model, the key variables are identified as follows:

Attitude towards behaviour: this considers the extent to which behaviour performance may be valued, either positively or negatively. It has been stated by Ajzen and Fishbein (1980) that an individual's attitude in relation to a particular objective might be estimated with a particular degree of accuracy when considering the knowledge of the individual surrounding beliefs the attitude object and such beliefs' assessment. In particular, the attitude is recognised as being a sum of the beliefs, multiplied by their own assessment aspect.

Subjective norms: such norms consider the social environment's influence on behaviour, which may be described as the perception of the individual in regards to those who are close to them and whether they believe they should perform those behaviours. As stated by the TRA, the perceived expectations of a particular referent group or individual may go some way to determining the general subjective norms, with the person's motivation to adhere to such expectations also recognised as important (Al-Qeisi, 2009).

Various works have established a number of limitations in the use of the TRA for estimating behaviours, with the work of Sheppard *et al.* (1988), for example, making the statement that the TRA can be used to predict behaviours when the intention and attitude are aligned with action, context, target and time. Moreover, it is noted by Ajzen (1985) that the theory is somewhat limited by what is referred to as correspondence. So as to ensure the theory is able to predict particular behaviours, intentions and attitudes need to be aligned with actions, context, target, timeframe and specificity (Sheppard *et al.*, 1988). When considering this particular context, the TRA is not able to provide the necessary theoretical basis for the analysis of government application, as highlighted by Faris (2011).

3.2.2. Theory of Planned Behaviour (TPB)

Owing to the various limitations associated with the TRA, the proposition of the Theory of Planned Behaviour was made by Ajzen (1985), where this theory provides a further extension of the TRA, where the core is the individual's own intention to carry out a particular action.

In an effort to estimate and accordingly describe behaviour, TPB centres on the antecedents of attitude, perceived behavioural control and subjective norms as shown in Figure 3.2. The suggestion of the TPB centres on the view that behaviour is a function of the outstanding beliefs associated with that behaviour.

Figure 3.2 has been removed due to Copyright restrictions.

Figure 3.2: Theory of Planned Behaviour (TPB) (Ajzen, 1985)

When describing such antecedents, the following summary was provided by Al-Qeisi (2009).

Behavioural beliefs: Such beliefs are held as influencing attitude towards behaviour, where a behavioural belief is the subjective likelihood that a particular outcome will follow a certain action. Despite the fact that an individual might hold a number of beliefs in regard to specific actions, it remains that only a small number of accessible at any particular moment.

Normative beliefs: It is held that normative beliefs, in addition to the motivation of a person to adhere to various referents, are pivotal in establishing the prevailing subjective norm. Otherwise stated, the desire to comply with each referent contributes to the subjective norm in direct proportion to the subjective likelihood of a person that the referent believes the behaviour in question should or should not be carried out.

Control beliefs: Such beliefs are associated with the recognised presence of factors that could either enable or restrict performance-related behaviour, where all control factors are afforded a particular power, where such perceived power is seen to be valuable to the perceived behavioural control in line with the various elements identified in a specific situation, encouraging the behaviour.

3.2.3. Technology Acceptance Model (TAM)

TAM is a theoretical framework that has been considered widely in empirical works. The TAM was devised by scholars Davis *et al.* (1989) in consideration to the TRA, the fundamental focus of which was concerned with providing insight into the acceptance and application of behaviours, by users, across a number of different computer technologies. When compared with various other technology acceptance models, the TAM is recognised as one that is most commonly applied by IS researchers owing to the fact it is viewed as being IS-specific and cost-effective (Venkatesh *et al.*, 2003).

The proposition is made by TAM that the behavioural intentions of users establish their acceptance and subsequent use of new technologies. In turn, users' perceptions of the technology are believed to be fundamental in establishing behavioural intention, such as in terms of perceived ease of use and usefulness as shown in Figure 3.3. Importantly, perceived usefulness is recognised as the degree to which a particular technology is considered by the individual as having the ability to improve their productivity and the outcomes associated with use. In contrast, perceived ease of use centres on the extent to which individuals hold the belief that the use of a technology will require only minimal effort (Venkatesh *et al*., 2003).

Figure 3.3 has been removed due to Copyright restrictions.

Figure 3.3: Technology Acceptance Model (TAM) (Davis et al, 1989)

TAM is viewed as a valuable framework, which is seen to be practical and as able to provide sound understanding into behaviours surrounding acceptance. The overall suitability of the TAM to this specific research further is grounded by the wide acceptance of the framework amongst professionals in the information systems arena, as well as their general capacity to be adopted in various contexts. Notably, the model has been implemented in various cultures, and has demonstrated validity beyond its original organisational and geographical contexts.

The TAM's most commonly discussed limitation centres on its reliance on self-reporting and the assumption that measuring the self-reporting of a user may estimate actual usage. Furthermore, the issue of generalisation is inherent in the TAM owing to the fact the framework originated in organisational and student environments, which thus causes issues in generalising the outcomes derived by the TAM to beyond and into other contexts (Legris *et al*., 2003). Moreover, the TAM is recognised as lacking the ability to enable the IS system

usage changes to be measured throughout the various steps of application (Venkatesh *et al.*, 2003).

3.2.4. Extension of the Technology Acceptance Model (TAM2)

The original TAM was further developed by Venkatesh and Davis (2000) with the inclusion of new estimations surrounding the intention to use and usefulness constructs. The core objective of the extended model was concerned with examining the way in which the growing experience of users with an IS system cause changes in the effects of the two constructs over time. Additional constructs were added by the authors, lending factors from the Diffusion of Innovation Theory (DOI) and TRA. The completion of the study was witnessed in mandatory and voluntary use settings across four IS systems and in three different times: before system application, one month post-application and three months post-application. The new constructs were explained by the authors as theoretical variables associated with cognitive instrumental methods, seeking to draw comparisons between what systems provide with what is required by users. These included ease of use, quality of output and job relevance, in addition to a construct representative of the result demonstrability. Furthermore, those constructs representing the commonly referred to 'social influence processes' were also included due to their capacity to enable innovation acceptance, namely image, subjective norms and voluntariness as shown in Figure 3.4.

Figure 3.4 has been removed due to Copyright restrictions.

Figure 3.4: Technology Acceptance Model 2 (TAM2) (Venkatesh and Davis, 2000)

In the TAM2, the cognitive instrumental process makes the assertion that individuals draw comparisons between system usage outcomes with their job objectives in an effort to ensure

usefulness perceptions. Efficient result demonstrability and output quality constructs result in usefulness being perceived as positive. Nonetheless, the relationship in this regard is not influenced by user experience. Accordingly, it should be noted that TAM2 adopts longitudinal methods in examination of the different systems (Venkatesh and Davis, 2000).

3.2.5. Diffusion of Innovation Theory (DOI)

Another valuable framework for assessing the acceptance of new technologies amongst users is the DOI, which was developed by Rogers (1995) with the aim of describing how innovations diffuse through social systems. The DOI explains how innovation-related information reaches the public through social system networks over a particular duration.

Importantly, the innovation decision process comprises five different stages, namely knowledge, persuasion, decision, implementation and confirmation. Al-Qeisi (2009) noted that innovation adoption rates can be described by innovation attributes, where the majority of the variance in this rate (49–87%) can be explained in consideration to the five perceived attributes of innovation. These attributes are relative advantage, compatibility, complexity, observability, and trialability. Importantly, users are different from one to the next, as can be seen when reviewing their adoption trends. They may be categorised in line with the time they first began to use the new innovation.

There are five categories of adopter as follows:

1. Innovators (2.5%): Innovators are recognised as venturesome, which is one of their most striking features. They have an ability to apply and understand complicated technology knowledge, enjoy financial resources, and are able to manage a significant degree of uncertainty surrounding the innovation when first making use of it. They are

seen to play a critical role in the launch of new, innovative ideas within a social framework, and therefore may be considered as gatekeepers when there is a new idea.

2. Early adopters (13.5%): Early adopters are well recognised for their respect, where the local social system affords them much esteem. In this category, the individuals are opinionated leaders who are the first port of call when advice and information is sought relating to new ideas. These people essentially are viewed as role models for different individuals in the social system, which provides one explanation as to why they are sought out by change agents owing to their ability to encourage and attract the masses when implementing an innovation.

3. Early majority (34%): Such individuals apply the new ideas before the average member, with their most prominent characteristic that of acting in a deliberate fashion; they are seen to take time before applying a new idea but are deliberate in the time they take and the actions they apply. They follow with intended inclination but rarely adopt the role of a leader. Essentially, they are pivotal in the diffusion process owing to the fact they act as an intermediary between early adopters and late majority members.

4. Late majority (34%): In contrast to the category above, those who adopt new ideas in the late majority category are seen to do so as a result of economic necessity or peer pressure (for the sake of following norms). As a result of their limited resources, they prioritise the need to feel more certain and stay safe prior to applying any new innovation. Accordingly, their most striking characteristic is scepticism.

5. Laggards (16%): This group comprises those individuals who are amongst the last to utilise a new innovation, with the group almost entirely lacking leaders; instead, their

attention is directed towards what has been done in past times, which is a key consideration in their decision-making. Importantly, they interact only with like-minded individuals and call change agents into question. Such resistance to change might be logical from their own perspective but, owing to their restricted resources, they are unable to afford to implement innovations that might not be successful (Al-Qeisi, 2009).

The various DOI theory-related limitations are numerous, with the DOI criticised owing to its apparent inability to provide evidence on how users' rejection and acceptance decisions are affected by innovation and their attitudes towards such. There has also been criticism centred on failure to explain how innovation and its various characteristics play a role in the final decision-making process (Chen *et al.*, 2002).

3.2.6. Unified Theory of Acceptance and Use of Technology (UTAUT)

The Unified Theory of Acceptance and Use of Technology (UTAUT) is the framework in the field of information systems literature that has been most recently developed, and seeks to describe and estimate the acceptance of new technologies amongst users. This framework was devised and synthesised by Venkatesh *et al.* (2003) in consideration to various IS models. Consideration is directed towards a number of different models, including Technology Acceptance Models (TAM), Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TPB), the Motivational Model (MM), Innovation Diffusion Theory (IDT), the Model of PC Utilisation (MPCU), Social Cognitive Theory (SCT), and the model that combines TAM and TPB (C-TAM-TPB). Essentially, the UTAUT framework has the objective to provide a wide-ranging explanation and estimation of the behaviours of users that otherwise have not been achievable when applying other models (Venkatesh *et al.*,

2003). Importantly, all of the aforementioned theories and models have sought to describe the behaviours and usage of new technology as demonstrated by users, with attention directed towards various users. In actuality, the UTAUT framework suggestion is centred on the various similarities between such independent variables from all of the models mentioned above (Faris, 2011).

In consideration to the prior model comparisons and tests, the authors detailed five limitations, all of which are discussed in their works. These include the following as mentioned by Al-Qeisi, (2009):

- The technologies under examination were not complex or sophisticated, but rather were simple and individual-centred.
- The majority of subjects in such works were students, with the exception of a small number of researches.
- Measurement time was general, with such measurement carried out following the rejection or acceptance of usage, meaning the thoughts of individuals were retrospective.
- Measurement was generally seen to be cross-sectional in nature.
- The majority of the works were carried out in the context of voluntary usage, meaning the results could not be easily generalised to mandatory environments.

The eight frameworks then underwent empirical comparison in longitudinal field works carried out across four different businesses amongst individuals that had been introduced to an innovative technology in the work setting. Three different points of time were outlined for measurement completion, namely post-training, one month following application, and three months following application. A six-month post-training mark was utilised in mind of actual usage behaviour measurement. Importantly, data were divided into two samples for the eight

models, in line with the voluntary and mandatory settings. Moreover, the various effects of various moderating variables were examined by the authors, as highlighted in previous works as potentially influencing usage decision, namely age, experience, gender and voluntariness (Al-Qeisi, 2009).

In the UTAUT model (Figure 3.5), there was the defining and relating of the constructs in line with comparable variables in the eight frameworks, as discussed below:

Figure 3.5 has been removed due to Copyright restrictions.

Figure 3.5: Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al, 2003)

Performance Expectancy (PE): The extent to which an individual holds the view that the system will be pivotal and valuable in assisting them in their own job performance. In the other models, the constructs that relate to performance expectancy are recognised as extrinsic motivation (MM), job fit (MPCU), outcome expectancy (SCT), relative advantage (DOI) and perceived usefulness (TAM and combined TAM-TPB).

Effort Expectancy (EE): The extent to which there is an ease associated with system utilisation. Across the various models, the constructs that are able to capture the same concept are complexity (DOI and MPCU) and perceived ease of use (TAM).

Social Influence (SI): The extent to which an individual recognises that people they themselves consider to be important hold the view that system utilisation would be best. Comparable constructs are identified in existing models, such as image (DOI), social factors (MPCU) and subjective norms (TRA, TAM2, TPB/DTPB, and combined TAM-TPB).

Facilitating Conditions (FC): The extent to which an individual holds the view that a technical or organisational infrastructure is able to provide system utilisation support, where such a definition captures three individual constructs in present frameworks: compatibility (DOI), facilitating conditions (MPCU) and perceived behavioural control (TPB/DTPB and combined TAM-TPB).

The original data garnered from the four different organisations underwent empirical testing and subsequent cross-validation with the use of new data, notably that garnered by two additional organisations, with the UTAUT model receiving much support. The new framework was found to be able to account for as much as 70% of the variance in intention of utilisation, which his recognised as a significant improvement in measurement when contrasted with other models, which generally were seen to achieve 40%. The authors recognised there was a content validity limitation as a result of the measurement processes, and accordingly made the suggestion that subsequent studies should be focused on validating and fully developing suitable scales for all of the constructs, whilst ensuring emphasis on the revalidation or the extension of the UTAUT model, as well as on content validity, with the new measures (Al-Qeisi, 2009).

3.2.7. Extending the Unified Theory of Acceptance and Use of Technology (UTAUT2)

The UTAUT model is extended in the work of Venkatesh *et al*. (2012), with the three key contributions made as follows: first, hedonic motivation, habit and price value integration induces a number of new mechanisms linked to the new constructs into the predominantly intention and cognition-based UTAUT as shown in Figure 3.6; second, through altering and developing UTAUT in mind of modifying existing links and including new constructs, this work further extends the generalisability associated with UTAUT in line with a different

context (i.e., consumer IT), which is recognised as fundamental in the field of theory advancement; and last, from a more practical perspective, more in-depth understanding can be pivotal in assisting business in the consumer technology field to implement improvement in market technologies and design in a number of different demographic categories and across different stages of the use curve.

Figure 3.6 has been removed due to Copyright restrictions.

Figure 3.6: UTAUT2 (Venkatesh et al, 2012)

3.2.7.1. Hedonic Motivation:

Hedonic motivation is a term that may be explained as the pleasure or fun experienced when utilising a technology, and it acknowledged as fundamental in achieving technology use and acceptance. In consideration to the consumer context specifically, hedonic motivation also has been recognised as a fundamental determinant concerning the use and acceptance of technology. Accordingly, hedonic motivation is included as an additional estimator in consumers' behavioural intention in technology use.

3.2.7.2. Price Value:

One of the most essential differences when drawing a contrast between the organisational use setting and the consumer use setting, where there is the development of the UTAUT, is seen when considering that it is common for consumers to shoulder the monetary costs associated with use, with employees not required to do so. The pricing and costing structure could have a notable effect on the technology use demonstrated by consumers.

3.2.7.3. Habit:

Past studies centred on the use of technology have presented two associated yet separate constructs, namely habit and experience; the latter, as has been defined in past works (Venkatesh *et al.*, 2003), emphasises the change to use a target technology and is commonly operationalised as the passage of time from the initial use of a technology by an individual; habit, on the other hand, has been explained as the degree to which people are likely to carry out behaviours in an automatic way owing to their learning. Habit has been operationalised first as a prior behaviour and also as the degree to which a person holds the view that the behaviour is automatic. As a result, two key differences are apparent when comparing habit and experience: firstly, experience is an essential but not adequate condition for creating habit; and secondly, the passing of time may mean different levels of habit are established depending on the degree of familiarity and interaction developed within a target technology. Importantly, in relation to technology use, predictions are seen to be more accurate when context habit is considered as opposed to initial acceptance.

3.2.8. Reviewing Empirical Studies of e-government Acceptance

Several studies were conducted in e-government context that applied original or amended acceptance models and reviewed previous studies (Alshehri, 2012; Elsheikh, 2012; Alsaif, 2014). The following paragraphs review and summarise the previous empirical studies in this field.

When considering the theoretical salient factors that have an effect on the application of electronic government in the USA, by citizens, one of the initial works in the field was that by Carter and Belanger (2004). The diffusion of innovation theory was applied by the researchers, utilising a sample comprising 40 students in mind of examining factors that affect the adoption of e-government by citizens, which highlighted the various benefits,

compatibility and image seen to notably impact the intentions of citizens to utilise e-government services.

In a further work, the TAM framework was combined with the DOI and trust in order to devise a comprehensive framework comprising the various factors of relevance that are seen to affect the adoption of e-government by citizens (Carter and Belanger, 2005). In total, the study sample comprised 140 undergraduate students, which highlighted the fact that users' intentions in this regard are influenced by a number of factors, including compatibility, perceived usefulness and relative advantage. However, undergraduate students' efficacy in the assessment of technology acceptance is somewhat called into question when considering the ability of the research to be generalised is limited.

The study by Choudrie and Dwivedi (2005) examined the UK government gateway in regards citizens' awareness and their general utilisation of such services by considering demographic variables. A self-administered questionnaire and postal survey were applied in the study. The total responses received were 358. It was found that the age, education, gender and social class, as demographic variables, have a fundamental effect on citizens' awareness and their subsequent application of e-government services.

Factors believed to be essential in achieving success in the adoption of e-government services in Canada were analysed in the work of Kumar *et al.* (2007), who suggested a framework comprising various influence variables, where the factors affecting incorporation were categorised into users' characteristics and website design variables. Users' characteristics were included, such as experience of the Internet, perceived control and perceived risk, in mind of evaluating ease of use and perceived usefulness as aspects affecting e-government adoption. Users' satisfaction of services was found to be positive affected by service quality.

In the development of a framework comprising factors that are believed to have an effect on citizens' use of e-government services in the context of Malaysia, the study of Lean *et al.* (2009) asked 195 participants to complete a structured questionnaire. TAM, DOI and Trust models were combined with five dimensions, namely perception of authentication, perception of confidentiality, perception of data integrity, perception of non-repudiation and perception of privacy. The conclusion was drawn that perceived image, perceived relative advantage, perceived usefulness, and trust were found to have a positive and significant effect on the intention to use such services; on the other hand, a negative effect was witnessed in regards perceived complexity. This study further highlighted that perceived strength of online privacy and perceived strength of non-repudiation have a positive effect on the trust of citizens when utilising e-government services.

A sample of 206 citizens was taken in the work of Doong *et al.* (2010) in mind of analysing their psychological traits through directing consideration to how the innovative cognitive style of the individuals, as well as their overall involvement, affected their loyalty intention in the use of e-government services in Taiwan. The conclusions drawn by the study emphasised that a combination of both involved citizens and innovators positively affect the use of services in the long-term, with strong loyalty intention witnessed amongst such citizens. In future research, however, there is the suggestion that random sampling be utilised in an effort to ensure an improved degree of generalisability.

Lin *et al.* (2011) validated the TAM in the specific context of Gambia. A structured questionnaire was designed and disseminated amongst the subjects with the aim of identifying the intentions of the individuals to utilise such e-government services. The TAM was found, throughout the course of the study, to have a strong core construct effect in estimating the intentions of citizens to use e-government services. Importantly, the work

emphasised that both information quality (IQ) and perceived ease of use (PEOU) were seen to positively affect perceived usefulness (PU) amongst the Gambian citizens in the use of e-government services, with PEOU found to have a fundamental link with the attitudes of the subjects in the use of such services. Regardless, however, PU was found to have no fundamental link to the behaviours and attitudes of citizens in the use of e-government services.

3.2.9. UTAUT and UTAUT2 in e-government Acceptance Studies

This section reviewed the empirical studies that applied UTAUT or UTAUT2 in e-government context. The following paragraphs summarise these empirical studies.

Alawadhi and Morris (2008) have applied UTAUT to investigate the factors affecting e-government services in Kuwait. The target sample in their study comprised undergraduate and postgraduate university students as the e-government in Kuwait was not widely used, and university students might be the main users for e-government services in the future as the majority of citizens fall into the youth age bracket. A questionnaire was distributed to 1,013 students, 880 of whom completely answered the questionnaire. The research used four dependent variables, namely performance expectancy, effort expectance, facilitating conditions and peer influence. The social influence was replaced with peer influence to ensure its suitability for the sample and their culture. The research also used gender, academic course and Internet experience as moderators. Age and voluntariness of use, as suggested by the original UTAUT, were eliminated in their proposed model. The research findings showed that performance expectancy and peer influence have a significant influence on behaviour intention; however, the reliability of peer influence is just 0.13, which might have affected their findings. Effort expectancy has a significant effect in line with behaviour

intention. Facilitating conditions and behaviour intention also have significant effects on the use of e-government services. The research suggests that culture and trust should be considered in future work. This study considers one of the first studies known to have validated UTAUT in an e-government context.

As the digital divide is one of challenges facing e-government adoption, Wang and Shih (2009) investigated the factors affecting the use of information kiosks, which are seen to be helpful for reducing the impact of the digital divide. The research validated the UTAUT in the use of information kiosks in Taiwan. The data were collected from 244 participants from different demographic backgrounds in Taiwan. The original UTAUT model was applied, the only change being the exclusion of both the experience and voluntariness of use as moderators. The research findings showed that performance expectance, effort expectancy and social influence have a positive influence on behaviour intention. Moreover, facilitating conditions and behavioural intention were found to influence use behaviour in a positive way. The reliability of their model constructs was very high; the findings were consistent with those garnered by the original UTAUT model.

Yahya *et al*. (2012) conducted a research centred on investigating the factors that affect end users e-Syairah portal for intention to use the online services. The research model was based on UTAUT, with the inclusion of two additional constructs, namely the information quality and system quality. The research used only a pilot study as the total participants who fully completed the survey equated to 35 participants in Malaysia. The facilitating conditions and moderators variables were eliminated from their research model. The research findings showed that performance expectancy, effort expectancy, social influence, information quality and system quality have a significant influence on the intention of using e-Syariah portal.

Alshehri *et al.* (2012) investigated the factors known to influence end users for using e-government in Saudi Arabia. Trust was added to the research model, besides the original four constructs of the UTAUT model. Moreover, age, gender and Internet experience were used as moderators while voluntariness of use was eliminated. The questionnaire was distributed amongst 900 Saudi citizens during a three-month period. The total participants who completed the questionnaire totalled 618, meaning there was a response rate of 68.6%. The findings indicated that performance expectancy, effort and trust have a positive influence on behaviour intention in the use of e-government services. However, the findings showed that social influence did not affect behaviour intention. The findings also showed that facilitating conditions and behaviour intention influenced the use of e-government services.

Weerakkodya *et al.* (2013) also integrated the trust with UTAUT to investigate the role of intermediaries in e-government adoption in Madinah City. The trust also has been investigated as two constructs, which are trust of the Internet and trust of intermediary. Data from 502 participants were analysed in mind of the suggested model, where the findings showed that performance expectancy, effort expectancy and trust of intermediary have a significant influence on behaviour intention. The findings also showed that social influence and trust of the Internet have an insignificant influence on behaviour intention. The findings also indicate that both facilitating conditions and behaviour intention have a significant influence on usage behaviour. One of the limitations in this research is that the research was based on only one city in Saudi Arabia.

Few studied have applied UTAUT2 in the e-government context. Krishnaraju *et al.* (2015) applied UTAUT2 in mind of investigating the impact of web personalisation in the intention to use e-government services. The experiment was carried out in the Indian Institute of Management Ahmedabad (IIM-A); a total of 143 students were involved in this experiment.

The participants were divided into two groups: the first group used a simulation government website that includes personalised content, whilst the other website did not have any. The findings showed that social influence, price value and habit are the only factors to influence their intention to use this service; however, the main purpose of this research is centred on investigating the role of web personalisation as a moderator and how it influences the relation between the independent variable of UTAUT2 and behaviour intention. The findings showed that web personalisation did not have a positive influence as a moderator on performance expectancy, facilitating conditions and habit. Thus, only effort expectancy, hedonic motivation and price value were affected by web personalisation as a moderator between the behaviour intention and these three constructs. There were several limitations to this study: for example, the data have been collected from undergraduate and postgraduate students, which may cause this study to fail when they are generalised to citizens showing differences in age, education level and experience. In addition, the sample size in this research was small, meaning it would be difficult for generalisations to be applied to the findings.

Critical factors influencing the citizens for using e-government services in Pakistan have been investigated by the application of the UTAUT model (Ovis, 2013). Data from 115 Pakistani citizens were used to analyse the model, with the findings showing that performance expectance, effort expectance, facilitating conditions and social influence affect the Pakistani citizens in the use of e-government services. The moderators of the UTAUT model were not considered in the research model. The research sample targeted the university students, where the results can be affected once the model applied to other citizens with different demographical characteristics. Besides this, the sample size was too small to generalise the results to all Pakistani citizens. In addition, this model did not measure other important factors seen to affect the adoption of e-government in Pakistan, as the original UTAUT

model was applied, which gave a general perception of the adoption of e-government services. However, this research provided significant information pertaining to the adoption of e-government services in developing countries in general, as well as in south Asia specifically.

Sociocultural values have been investigated in the adoption of e-government services by Alsaif (2014). The research model was based on the amended UTAUT model. Three independent variables from UTAUT were used: performance expectancy, effort expectancy and social influence. In addition, gender, age and experience were proposed in the research model, as based on the UTAUT as moderators. However, voluntariness of use was eliminated, and the research proposed education level as an additional moderator. The research model also proposed that the awareness of e-government and compatibility were independent variables known to have affected the intention behaviour of using e-government services. Trust also was considered in the research, and was used as two separate constructs, namely trust of the government and trust of the Internet. Facilitating conditions was divided into four constructs: computer self-efficacy, availability of resources, information quality and system quality. These four factors were proposed to affect usage behaviour directly as the facilitating conditions construct was proposed to be affecting the usage behaviour directly in the UTAUT model. The data were collected via a questionnaire, which was distributed via social network websites during a six-week period. The total responses amounted to 723 Saudi citizens, who fully answered the questionnaire. The findings of the research showed that only performance expectancy, from the original UTAUT independent variables, had a significant influence on behaviour intention, whilst social influence and effort expectancy had an insignificant influence. In addition, both awareness of the system and compatibility were found to have insignificant influence on behaviour intention. The findings also showed that

trust in the Internet only has a significant influence on behaviour intention as the trust of the government has insignificant influence. The usage behaviour was affected in this research by behaviour intention, computer self-efficacy and the availability of resources, whilst only service quality was found to have an insignificant influence on usage behaviour. The main theoretical implication in this research was the dividing of the facilitating conditions into four constructs. Moreover, the variance explained by this model accounted for 60%. However, there are two main limitations in this research: firstly, the study had a cross-sectional nature, whilst the original UTAUT was based on a longitudinal study, which would provide better understanding for the phenomena throughout changes in the environment; and secondly, the sample population comprised young citizens, in the main, who are educated and familiar with using the Internet.

Lian (2015) applied the UTAUT2 in mind of investigating the critical factors affecting the adoption of cloud-based e-invoice services in the e-government of Taiwan. Only the original four constructs of UTAUT, namely performance expectancy, effort expectancy, social influence and facilitating conditions, were included, with three new constructs that were added to the UTAUT2 eliminated in this research. Hedonic motivation was eliminated as the e-invoice service was not for entertainment. The price value was not an important factor as the service was free of charge. Habit was excluded as the service was new in Taiwan, meaning there was no habituated use of the service by citizens. Three additional constructs were added to the research model; these constructs included perceived risk, trust in e-government and security concerns. Perceived risk was proposed as affecting behaviour intention directly, with trust in e-government and security concerns acting as antecedents. Trust in e-government was investigated as one of the constructs, and was proposed as affecting both perceived risk and behaviour intention. The security concerns were proposed

as directing affecting the trust of e-government, perceived risk and behaviour intention. Age and gender also were used as moderators in the research model, whilst experience moderator was excluded. The data were collected from 251 citizens in Taiwan, which subsequently were used for analysing the research model. The findings showed that only effort expectancy and social influence had a positive influence on behaviour intention whilst performance expectancy and facilitating conditions had an insignificant influence. Moreover, the findings showed that perceived risk affected behaviour intention in a negative way. Trust in e-government was found to have a positive influence on behaviour intention; however, it was found to have an insignificant influence on perceived risk. The findings also showed that security concerns have an insignificant, direct impact on behaviour intention. However, security concerns negatively affect trust in e-government and positively affect perceived risk. One of the main limitations in this research is the fact that is focused on cloud-based e-invoice service. The model needs to be applied to different e-government services so as to provide a better understanding of the impacts of these factors on e-government adoption. In addition, the variance explained in trust was only 0.09%; thus, the trust antecedents need to be investigated to a greater degree so as to provide better understanding of the factors affecting trust in e-government. Table 3.1 summaries the empirical studies that have applied UTAUT and UTAUT2 in e-government adoption.

	Research	Country	Model used	Constructs	Sample
1	Alawadhi and Morris (2008)	Kuwait	UTAUT	Performance expectancy	880 students
				Effort expectance	
				Peer influence	
				Facilitating conditions	
2	Wang and Shih (2009)	Taiwan	UTAUT	Performance expectancy	244 citizens
				Effort expectance	
				Social influence	
				Facilitating conditions	
3	Yahya *et al*.	Malaysia	UTAUT	Performance expectancy	35 citizens

	(2012)			Effort expectance	
				Social influence	
				Information quality	
				System quality	
4	Alshehri *et al*. (2012)	Saudi Arabia	UTAUT	Performance expectancy	618 citizens
				Effort expectance	
				Social influence	
				Facilitating conditions	
				Trust	
5	Weerakkodya *et al*. (2013)	Saudi Arabia	UTAUT	Performance expectancy	502 citizens
				Effort expectance	
				Social influence	
				Facilitating conditions	
				Trust of Internet	
				Trust of intermediary	
6	Krishnaraju *et al*. (2015)	India	UTAUT2	Performance expectancy	143 students
				Effort expectance	
				Social influence	
				Facilitating conditions	
				Hedonic motivation	
				Price value	
				Habit	
				Web personalization	
7	Amhed *et al*. (2013)	Pakistan	UTAUT	Performance expectancy	115 citizens
				Effort expectance	
				Social influence	
				Facilitating conditions	
8	Alsaif (2014)	Saudi Arabia	UTAUT	Performance expectancy	723 citizens
				Effort expectance	
				Social influence	
				trust in the Internet	
				Trust in of the government	
				Awareness of e-government	
				compatibility	
				computer self-efficacy	
				availability of resources	
				Information quality	
				System quality	
9	Lian (2015)	Taiwan	UTAUT2	Performance expectancy	251 citizens
				Effort expectance	
				Social influence	
				Facilitating conditions	
				Perceived risk	
				Trust in e-government	
				Security concerns	

Table 3.1: Summary of empirical studies applied UTAUT and UTAUT2 in e-government adoption

3.3. Security Perception in e-services

Security has been discussed widely in e-services studies, as it is known to play an important role in the acceptance of these e-services; however, such studies use a different dimension of security; thus, Hartono *et al*. (2014) reviewed the studies defining the dimensions of security and mentioned previous studies known to have investigated the role of security in e-services. This section mentions the security dimensions and accordingly reviews prior works that have investigated the role of security in e-services.

3.3.1. Security Dimensions

Several studies mention Confidentiality, Integrity and Availability (CIA triad) as the key concepts and dimensions associated with information security (Hartono *et al*., 2014): Confidentiality infers that the online user believes that the information submitted by the user will not be disclosed to any unauthorised party; Integrity means that the online user believes that his/her information, as garnered throughout the course of the transaction, will not be altered by any unauthorised party; and Availability means the online user believes that the service provider is able and willing to make the information available to authorised users when required (Hartono *et al*., 2014). Besides these three dimensions, Siponen and Kukkonen (2007) add Non-repudiation as a fourth dimension, which means online users believe that the service provider cannot deny receiving a transaction. Furthermore, Cegielski (2008) added both Non-repudiation and Authentication, in addition to the CIA triad. Moreover, Access Control has been added as a security dimension (Parent, 2007). Finally, Gurbani and McGee

(2007) determine eight different dimensions of security, namely Confidentiality, Integrity, Availability, Authentication, Access control, Non-repudiation, Communications security, and Privacy.

3.3.2. Studies Investigated Security Perception in e-services

One of first studies known to have investigated the role of security in e-services was carried out by Salisbury *et al.* (2001), who completed an empirical longitudinal study centred on investigating the critical factors affecting users in making purchases online. The first phase targeted 119 undergraduate students from south-eastern US University, who were studying a course based on an introduction to computing. The second phase was carried out later and targeted 253 undergraduate students from the same university. The data from both of these two phases were used to analyse the research model; the findings show security as being the greatest factor influencing their intention to purchase from the Internet.

Cheung and Lee (2001) investigated the factors influencing Consumer trust in Internet shopping. Their research model investigated the role of four antecedents of trust, which are Perceived security, Perceived privacy, Perceived competence and Perceived integrity. Data from 278 participants showed that all of these constructs influence Trust with the exception of Perceived privacy. This model explained 84% of the variance of consumer trust in Internet shopping. This percentage is very high as this study is only focused on Trust.

Chellappa and Pavlou (2002) conducted an empirical study to investigate the factors influencing the consumer trust in e-commerce transactions. Data from 128 graduate students and 51 undergraduate students, all of whom were studying at business school, were used in the analysis stage. The findings showed that Perceived security strongly influences Consumer trust in e-commerce transactions. In addition, the findings showed that Encryption, Protection

and Authentication have a significant influence on Perceived security, whilst Verification has an insignificant influence. This study measured Perceived security based on three components, which are Authentication, Authorisation and Non-repudiation. Moreover, Authentication has been considered as a factor influencing Perceived security. Thus, measuring a construct that exists in other second-order constructs may have had an effect on the results of their study, which can be considered a limitation.

O'Cass and Fenech (2003) applied an amended TAM model in mind of investigating the factors affecting Internet users on the adoption of web retailing usage. Three constructs were added to the TAM model, which are Personality, Web experiences and Shopping orientation. Web experiences was a second order involving four elements, which are Internet self-efficacy, Perceived web security, Satisfaction with web sites and Web shopping compatibility. Data from Australian citizens were collected; the total response was 392. The results showed that Web experiences positively affect both Perceived usefulness and Perceived ease of use. This study is considered as one of the first to have investigated the role of security in technology acceptance models.

Yensisey *et al.* (2005) conducted an experiment to determine the factors positively influencing perceived security in e-commerce amongst Tuskish university students. Their experiment contains three groups, each of which comprised ten students. All of those students were from the School of Engineering at the Technical University of Istanbul. This study was based on Virtual Shopping Security Questionnaire (VSSQ), as designed by the authors. The participants had previous experience in online shopping. They were involved in this experiment and asked to fill the questionnaire after using simulated e-commerce sites. The findings of the study categorised the factors into two main groups, which are Perceived

operational factors and Perceived policy-related factors. Each of these categories has different factors, as follows:

- Perceived operational factors:
    - Blocking of Unauthorised Access
    - Emphasis on Login Name and Password Authentication
    - Funding and Budget Spent on Security
    - Monitoring of User Compliance with Security Procedures
    - Integration of State-of-the-Art Systems
    - Distribution of Security Items within the Site
    - Web Site's Encryption Strategy
    - Consolidation with Network Security Vendors.

- Perceived policy-related factors Emphasis
    - Emphasis on Network Security
    - Top Management Commitment
    - Effort to Make Users Aware of Security Procedures
    - Web Site's Keeping Up-to-Date with Product Standards
    - Web Site's Emphasis on Security in File Transfers
    - Issues Concerning the Web Browser.

These factors were suggested by the authors and accordingly were validated by 30 Turkish students. One of the main goals of the study was to investigate whether the price value influenced users in regard to the perceived security, as the authors divided participants into three groups, namely shopping for cheap, mid-range, and expensive products. The findings showed that there were no significant differences between these three groups.

TAM also was extended by Fang *et al.* (2005) in regards mobile commerce acceptance. Perceived security was added as an independent factor that influences the intention to use mobile commerce. The experiment contained 12 tasks, some of which involved transactions, such as online banking, purchasing books and purchasing books. The participants in the study totalled 101, where the majority of them were working adults. The findings showed Perceived security as having a significant influence on their intention if the task contained a transition. One of the main limitations in the study was that Perceived security was measured by only one item, which therefore influenced the reliability of the construct.

Cheng *et al.* (2006) also integrated Perceived web security into the original TAM model in an effort to investigate the adoption of Internet banking in Hong Kong. The data were obtained from 203 individuals, all of whom were Internet banking users. Perceived security was measured with the use of four items in their questionnaire; the results showed that Perceived security directly influences the intention to use Internet banking. One of the limitations, as mentioned in the study, was that they did not consider the privacy issue, and suggested that security and privacy need to be investigated separately.

Flavián and Guinalíu (2006) conducted an empirical study in mind of investigating the relationship between trust in a website and loyalty. Trust was extended to cover both security and privacy; security and privacy should be considered as two separate constructs. However, they suggested that both security and privacy could be combined into one construct. This construct was referred to as Perceived Security in the Handling of Private Data (SHPD). They suggested this as they believe the consumer, company and legislator view both security and privacy as having a close relationship. In terms of analysing the research model, data from 354 participants were used. The results showed that the security and privacy construct influenced both loyalty and trust directly. Thus, they suggested, as based on the results, that

security, privacy and trust are the three basic elements for website loyalty. However, the variance of the loyalty in their model was only 21%.

Lain and Lin (2008) investigated the impact of consumer characteristics on online shopping acceptance, using different product types. Five critical consumer characteristic variables were investigated, namely Personal Innovativeness of Information Technology (PIIT), Internet self-efficacy, Perceived web security, Privacy concerns and Product involvement. The study targeted undergraduate students in Taiwan, all of whom were found to have prior experience with online shopping. The total number of valid responses equated to 123. One of the main findings showed that Perceived security positively influences user attitudes towards purchasing expensive products or services.

Laio and Wong (2009) investigated the factors known to influence customer interactions with Internet banking by extending the TAM to cover Perceived security, Responsiveness and Convenience. Perceived security was measured by three items covering three aspects, namely Unauthorised access, Customer private data and Security control. The data have been collected from 320 Internet banking customers in Singapore. The findings showed that all five independent constructs had an influence on customer interactions with Internet banking. TAM constructs were found to be the factors most greatly affecting customer interactions amongst the five factors.

Another study on online banking was conducted by Vatanasombut *et al*. (2008) in order to investigate the factors influencing users' Continuance intention to use online banking. The model was developed by integrating and extending the Commitment Trust Theory, an expectation confirmation model and Technology Acceptance Theory. Perceived security, in their study, comprised two components, namely Perceived security in using the technology

and Perceived security in interacting with the service provider, which involved computer crime, privacy violation and transaction errors. Their model suggested that Perceived security influences Continuance intention via Trust construct. The data were collected from one of the twenty largest banking and financial institutions in the United States. The survey was randomly sent to 4,667 customers; valid responses equated to 1,004, with the surveys in these instances answered fully, making the response rate 21.5%. The findings showed that Perceived security has a significant influence on Trust. In addition, Trust has a significant influence on Continuance intention. One of the main limitations in the model is the fact that this model explains only 22% of the Continuance intention variance.

Yousafzai *et al.* (2009) investigated the role of Trust in Internet banking adoption. Their research model investigated the impact of Trust on Behaviour intention, both directly and indirectly, via Perceived risk. The model also contains three antecedences of trust, which are Perceived security, Perceived privacy and Perceived trustworthiness. All of these constructs were first-order constructs with the exception of Trustworthiness, which was a second-order construct and which contains Perceived ability, Perceived integrity and Perceived benevolence. The questionnaire was distributed amongst 2,000 Internet banking users of Halifax Bank of Scotland. The total valid responses totalled 441, therefore equating to a 22.05% responses rate. The findings showed that Trust influences both Perceived risk and Behavioural intention. In addition, Perceived security, Perceived privacy and Perceived trustworthiness influence Trust.

Chang and Chen (2009) investigated the role of Interface quality and Security perception in the loyalty of electronic commerce websites. Their research model suggested that Interface quality and Perceived security influence Customer loyalty via both Customer satisfaction and Switching costs. A web-based survey was distributed amongst adults in Taiwan, who had at

least one year's experience in online shopping. The valid responses obtained amounted to 314, where the majority were university students. The findings showed that Perceived security had a significant influence on both Customer satisfaction and Switching costs.

The importance of Perceived trust, Security and Privacy has been investigated in relation to online trading systems in the work by Roca *et al*. (2009), whose research model was developed by integrating Trust, Security and Privacy with the TAM model. The data were collected from 180 undergraduate students at a university in south-western Spain. The total valid responses equated to 103, which were used for the analysis stage. The majority of these students had more than six years' experience on Internet use. The findings showed that only Perceived security had a significant influence on Perceived trust, whereas Perceived privacy had an insignificant influence.

Kim *et al*. (2010) conducted an empirical study aimed at investigating the effects of Perceived security and Trust on using e-payment systems. The survey was sent to 1260 participants in South Korea, where only 291 responses were valid for the purposes of analysis. The findings showed that Perceived security has a significant and direct influence on both Trust and Actual usage. More specifically, Perceived security influences Trust more so than Actual usage. In addition, Trust influences Actual usage in a direct manner.

Hartono *et al*. (2014) completed a study focused on measuring Perceived security specifically in e-commerce. In this study, Perceived security was measured as a formative second-order construct covering four different security dimensions, namely Confidentiality, Integrity, Availability and Non- repudiation. Confidentiality was integrated with Integrity in this study. The data were been collected from three anonymous organisations, namely a university, a private company and a government office. The participants were well-educated and known to

have good knowledge about online security. The total number of questionnaires received amounted to 489; only 436 were used for analysing the model. The research model was based on TAM and the findings emphasised Perceived security as having a direct influence on Behaviour intention at the 0.05 level of significance.

Ponte *et al*. (2015) investigated the impact of Trust and Perceived value on online purchasing. Their model extended Trust to cover Perceived security, Perceived privacy and Information quality. Data from 451 participants indicated that Perceived security and Perceived information quality have a significant influence on Trust, whilst Perceived privacy has an insignificant influence. In addition, the findings showed Trust as having a significant influence on behavioural intention.

3.3.3. Factors Influencing Security Perception in e-services

As security is important in e-services, such as in e-commerce and e-government, several studies have been carried out in mind of investigating the factors known to influence end users' security perceptions. In relation to e-commerce, Kamoun and Halaweh (2012) investigated the impacts of User interface design on Security perceptions. Their study was based on the top-five out of seven design elements of the customer interface (7Cs), namely context, content, communication, connection and commerce. A total of 18 elements covered these fives constructs: for example, in relation to the Connection construct, the findings show that non-working links in the website are ranked as the first element influencing the security perceptions of end users. The findings also reveal that all of these five constructs have a positive impact on end users' perceptions of e-commerce security. In e-commerce also, Chang and Chen (2009) investigated the role of Consumer perception of interface quality and

Security in website loyalty. The findings showed that Interface quality of the website influenced the security perceptions of consumers. Their research model explained 20% variance of Perceived security. As their model suggests, Interface quality is the only variable known to affect Perceived security; this means that Interface quality is explained as fifth in the explained variance of Perceived security. Another study conducted by Halaweh (2012) investigated the factors known to influence end users' perceptions of e-commerce security. This research began with a qualitative study to determine the factors based on end users' perceptions. The outcome of the study was the classification of the factors into five categories, namely Perception of intangible security features (e.g. well known, international), Perception of tangible security features (e.g. padlock, security certificate), User characteristics (e.g. experience, knowledge), Cooperative responsibility (government, e-commerce website) and Psychological aspects of security (e.g. fear). A quantitative study then was conducted to test the impact of these factors (Halaweh, 2012). Data from 61 students reveals that only User characteristics, Intangible security features and Psychological aspects of security have a positive impact on Perceptions of e-commerce security.

3.4. Discussion

The technology acceptance models that have been described in this chapter focus on the general factors that influence end users to adopt new technology in general. These models can be applied to any new technology and provide a general overview of the factors that influence its adoption. Different factors play an important role in the adoption of technology. TAM, TAM2, and TRA provide partial view of the problem, as they tend to focus on a limited set of influencing factors. TAM focuses on two factors only, usefulness and ease of use, whereas it ignores important factors, such as social influence. The TRA model covers the social influence factor and could be suitable for investigating these types of technologies.

However, it only focuses on social influence and beliefs, and so it can only give an initial overview of the adoption factors. The TAM2 attempts to fill the gap in the original TAM by considering the social influence factor. However, the TAM2 does not cover the facilitating conditions factor, which is considered in the TPB model.

Thus, the UTAUT model attempts to provide a wider view and fill the gap by covering four factors, which are performance expectancy (perceived usefulness in TAM and TAM2), effort expectancy (perceived ease of use in TAM and TAM2), social influence (subjective norm in TRA and TAM2) and facilitation conditions (perceived behavioural control in TPB). Unfortunately though, the UTAUT model does not pay attention to the factors of trust and risk. However, it should be mentioned that these models were developed for employees using the new technology provided by their companies and organisations and trust may not be an issue in this case. In addition, transactions and the Internet may not be required when using several technologies.

Technology acceptance models have since been used to investigate the factors that influence the consumer. As such, UTAUT has been amended to consider additional factors that could influence consumers. The UTAUT2 model focuses on consumer studies in particular and included three additional factors, price value, hedonic motivation and habit. However, trust is not addressed in this model either. However, as mentioned previously, several technologies may not use the Internet. Thus, trust and risk may not be important issues as the risk is increased if the service is provided via the Internet (Pavlou, 2001). This could be the reason that trust and risk were not included in the UTAUT2 model. The aim of the UTAUT2 model and other popular technology acceptance models is to be used as a standard model to investigate the adoption of any new technology. However, price value and hedonic motivation may not be issues in several technologies, such as e-government services. Trust

could be more important than these factors and need to be considered, especially as most new technologies are now online based.

This chapter provided several studies that investigated the factors that influence the adoption of e-government services. The common factors need to be considered in the research model and this will also be helpful for selecting one of popular acceptance model to be the base model for this research. In terms to investigate the role of security in e-government adoption there is a need to identify the other factors that influence the adoption of e-government services. This is necessary to determine the impact of security in e-government adoption among other factors.

As the factors that influence the end users' perception in e-government security never been investigated; this chapter tried to review the factors that influence the end users' perception in e-services security in general. Most of studies that investigate the security factors in e-services were conducted in e-commerce. Both of e-government and e-commerce are e-services and one of the main different between them that the services provider in e-government is government while in e-commerce is company. Thus, both of them are providing e-services to the end users and there could be common factors that influence the end users to use them. Thus, the reason for reviewing the factors that influence the end users' perception in e-services security is that they can be discussed during the focus group sessions and they might be helpful for discovering more influenced factors.

The factors that influence e-services security perceptions mentioned in this chapter may not be the same as those influencing e-government security perceptions. For example, in the e-commerce area, a study conducted by Halaweh (2012) shows that intangible indicators of security influence end users' security perceptions. An example of such an indicator is a shop

having an offline store and providing its local address and contact details or a shop having a good reputation. However, these indicators would not be relevant when investigating security perceptions in the e-government environment. Thus, there is a need to investigate the factors that influence end users' e-government security perceptions in particular. This can be done by conducting a qualitative study and considering the factors that have been speculated to influence such security perceptions.

3.5. Conclusion

The technology acceptance models that have been used to investigate the factors that influence the adoption of e-government were explained in this chapter. One of the most popular acceptance models is the UTAUT model, which combines eight other adoption models. For this reason, a recent version of the UTAUT model was used in this research to investigate the role of security in e-government adoption. In addition, the factors that influence the end users' perceptions of e-services security that were mentioned in this chapter were considered in order to determine the security antecedents to e-government adoption. The next chapter will present more information on the methodology used in this research to achieve the research aim and objectives.

4. Research Methodology

4.1. Introduction

This chapter provides an initial background concerning the research methodology applied in this research. It begins by explaining three of the main research paradigms, which are positivist, interpretive and critical. Subsequently, qualitative and quantitative approaches will be described in greater detail. Moreover, the combination of qualitative and quantitative approaches will be described, which is referred to as the mixed-methods approach. The types of mixed-method approach will be discussed, in addition to the chosen research approach. The justification for selecting the research approach and paradigms will be explained. This chapter also will highlight the main data collection strategies used, namely literature review, interview, focus group and questionnaire. As this study is following a mixed-methods approach, which comprises two phases (qualitative phase and quantitative phase), the data collection strategies for each phase will be explained. Furthermore, the methodology and justification for designing the research model will be explained as well. This chapter also discusses how the sample size has been determined, and goes on to explain how the questionnaire was translated, which is the main data collection strategy in this study. In addition, the chapter will explain how the ethical issues in the study were taken into account. Lastly, a conclusion for the research methodology will be provided at the end of this chapter.

4.2. Research Paradigms

From a practical point of view, such assumptions provide philosophical assumptions surrounding the basic views held about the world in which we live, what constitutes the social levels, the various approaches and techniques applied in the completing the research, and general guidelines on how such researches should be carried out on a technical level.

The ways in which knowledge are garnered and accordingly perceived is how epistemological assumptions can be described (Bryman, 2015). In the specific case of positivist paradigms, knowledge is centred on how the social world can be examined as one of the natural sciences, with empirical methods applied in order to test hypotheses. The subsequent results need to be objective through the application of social methods. Although interpretive paradigms' knowledge is concerned with examining the phenomena in a variety of different ways, when considering that the social context differs to that of natural sciences, social phenomena investigations need to consider various explanations. In the context of critical theory paradigms, knowledge may be recognised as a practical result. Such frameworks have a tendency to change particular conditions by directing criticism towards policy, practice and society-centred issues. As a result, the outcomes may be subjective (Elsheikh, 2012).

The methods of analysis applied for data acquisition may be referred to as methodological assumptions (Cohen *et al*., 2013). In the case of positivist paradigms, quantitative methods are applied in order to observe objects. This applies mathematical calculations in an effort to test theory and accordingly generalise results. Although interpretive paradigms are centred on field work and observations in their examination of the object in question and the garnering of knowledge, there is a tendency for interpretative models to utilise a qualitative method in order to acquire and examine knowledge. Accordingly, the results may be open to interpretations. In the context of critical theory models, qualitative and quantitative approaches are applied in order to acquire and observe knowledge. Notably, as Elsheikh (2012) mentioned that quantitative methods are centred on ensuring the social arena is controlled when carrying out specific actions, whereas qualitative methods are geared towards observing the changes that arise following such actions.

The majority of studies conducted in the fields of natural science of social science are reliant on one of the philosophical paradigms: critical, interpretive and positivist (Oates, 2005). Such a classification method is commonly acknowledged in modern-day IS research as each individual method characterised various ways of viewing the world in various attempts to measure, observe and understand social reality.

4.2.1. The Positivist Paradigm

The positivism approach is centred on epistemological views that make the assumption of reality as objectively provided and therefore able to be explained through measurable elements that are not dependent on the researcher and their chosen methods of application (Myers and Avison, 2002). A study is recognised as positivist if there is some proof in relation to hypothesis-testing, formal propositions, establishing meaning pertaining to a phenomenon and quantifiable measures of variables from the sample in relation to a particular group. The potential that people and their behaviours and entities may be examined as objectively as the natural world is the view adopted by positivism (Fisher, 2004).

4.2.2. The Interpretive Paradigm

It is noted by Lee (1991) that the interpretive approach necessitates that social scientists need to garner data and facts that explain not only the aspects of human behaviour that are objective but also the subjective meaning for the people themselves. In actuality, the interpretations of the social environment and people's understanding of such is the focus of an interpretative paradigm (May, 2011). This makes the suggestion that, within such a framework, the meaning as opposed to the measuring of social phenomena is what necessitates focus. In this vein, the observation is made by Lee (1991) that the positivist and interpretive approaches would seem to be contrasting and opposing, where the positivist

approach adopts the view that its approaches are the only ones that can be seen as scientific, whereas those that are interpretive suggest that the examination of people and their institutions calls for approaches that are alien to those adopted in the natural sciences domain. Furthermore, a qualitative data collection method is applied in the case of interpretivist epistemology.

4.2.3. The Critical Paradigm

Critical researchers widely make the assumption that social reality has been historically established, and is created and recreated by people. Critical realists pose the same view as positivists, suggesting that there are a huge number of phenomena that are independent of human awareness and are observable, with the view held that this world's knowledge is merely a social construct (Denzin and Lincoln, 2005). More specifically, critical research places emphasis on the various conflicts, contradictions and oppositions modern-day society, and further aims at being emancipatory (Myers and Avison, 2002).

In the view of Bryman and Bell (2015), critical realism expresses two opinions: primarily, the conceptualisation of scientists is a simple way of establishing that specific reality; and secondarily, critical realists are happy to acknowledge their rationalisations in theoretical terms that are not directly in line with observations. Accordingly, it is perfectly acceptable for hypothetical entities to explain away natural or social order regularities, as in the case of realists but not positivists.

4.3. Research Approaches

It is common for research approaches to be categorised as being either qualitative or quantitative in nature (Creswell, 2013). In the view of Hughes (2006), the quantitative

approach is recognised as the scientific empirical conventional methods, whereas the qualitative method, on the other hand, is viewed as being the naturalistic phenomenological approach. When considering the variation in focus and emphasis, the decision as to which to apply depends, to a significant degree, on the study framework, the researcher's own underlying assumptions, and the general nature of the phenomenon under examination (Yauch and Steudel, 2003). As highlighted by Elsheikh (2012), the positivist paradigm is commonly through the use of a quantitative approach, whereas the interpretive paradigm utilises a qualitative method. The approach applies is one specific technique or a set of techniques aimed towards garnering and examining data. Conventionally, the data utilised in the quantitative approach seems to adopt a numerical form, whilst data utilised in the completion of a qualitative method comprises text and words in an effort to highlight subjects' emotions and intended meaning behind carrying out a particular behaviour.

Qualitative and quantitative approaches in combination is recognised as the most valuable method behind examining IS phenomena, as noted by Fidock and Carroll (2009). Otherwise stated, the qualitative approach commonly aims at establishing the researcher's scope, developing a corresponding tool for measurement and accordingly devising associated hypothesis; the quantitative approach, on the other hand, aims at testing the hypotheses. Nonetheless, the various pros and cons associated with these methods will be discussed in greater depth in the following sections.

4.3.1. Qualitative Research

The gathering and analysis of non-numerical data is the focus of qualitative methods; nonetheless, this approach's strength can be seen in its subjective and open nature, particularly throughout the analysis process (Lancaster, 2007). In other words, as stated by

Elsheikh (2012), such a method aims at creating and accordingly developing more in-depth understanding of the experiences, perceptions and views of groups and individuals that could potentially affect being involved in particular behaviours within the natural context in which it occurs.

Throughout the 20th Century, social science professionals and researchers have come to acknowledge the various restrictions associated with quantitative research in terms of comprehending situations seen to involve the complicated interactions of cultural traditions, economics, human behaviours, interpersonal relationships and politics. As a result, throughout recent years, qualitative research has been more widely adopted, particularly in the arena of social sciences (Denzin and Lincoln, 2002). Qualitative studies defines as an inquiry process centred on garnering insight into and knowledge concerning a human social or human issue, as based on a complicated, holistic picture, created with words and discussed in a natural setting (Al-shehri, 2012).

The qualitative approach is commonly recognised by the following: (1) it is focused on providing understanding of the phenomena in its natural contexts; (2) it adopts a number of realities; (3) it presents data through rich verbal explanations; (4) it enables the researcher to be immersed and in direct communication throughout the data collection process; (5) it further facilitates the interactive collection of data; (6) it facilitates the application of a data collection that is evolving and flexible—notably a dynamic and tentative approach to the methodology; (7) it directs focus to the holistic perspective, ensuring attention is directed towards interrelationship complexity and dynamics in the world surrounding the phenomenon; (8) it is context-sensitive; (9) it highlights daily life invisibility and repositions the familiar as something strange; (10) it creates meaning from the viewpoint of the subject as an informant as opposed to just a participant to be studied; (11) it examines open questions

as opposed to testing hypotheses; (12) and it implements purposive sampling (Elsheikh, 2012).

4.3.1.1. Grounded Theory

Originally, the Grounded Theory concept was devised by Glaser and Strauss, two sociologists, who were not satisfied with how present theories were seen to dominate sociological studies. The two researchers posed the view that an approach that would enable them to move to theory from data was necessary, which would, in turn, allow other theories to be introduced. These theories were recognised as specific to the context in which they had been developed; they would be 'grounded' in the data from which they had emerged as opposed to directing emphasis to analytical constructs, categories or variables from other theories (Willing, 2013).

Two critical schools for Grounded Theory include the Straussian School and the Glaserian School as noted by Willing (2013). When comparing the two schools, there is an abundance of differences, although some are relatively minor. The key differences are recognised as having a fundamental effect on how primary research is both directed and applied. For instance, the position is adopted by Glaser that academics need to progress into a field with an open, clear mind, whereas Strauss, on the other hand, encourages the view that a general idea of the area under study is essential. In this vein, Glaser considers that theory needs to emerge, whereas Strauss, in contrast, devises and accordingly works in line with structured questions in an effort to lead to a more forced emergence of theory (Willing, 2013).

4.3.1.2. Concepts of Grounded Theory

Rose *et al*. (2014) mentioned that Grounded Theory is known to comprise four key concepts, as discussed as follows:

- Theoretical Sampling: One aspect involved in Grounded Theory is its approach to sampling, referred to as theoretical sampling, which is aimed at facilitating and supporting the development of theory. Sampling undergoes change and adjustment in line with the theory that emerges. Moreover, there may be the collection of additional data so as to facilitate the investigation of a specific concept.
- Data Collection: A number of different data collection approaches may be applied in Grounded Theory, including in-depth observations and interviews, in addition to the analysis of documentation, thus providing the potential to take sources and complete triangulation, aimed at garnering rich data that can explore far more than simply the subjective and social arena. In this regard, Grounded Theory is recognised as predominantly linked with qualitative data.
- Data Analysis: A coding approach to the analysis of data is adopted by Grounded Theory, which is a process during which the data is taken by the researcher and concepts are derived at and developed. Throughout the approach, activities, events and occurrences in the raw data are treated as indicators of various phenomena, which then are afforded a code, otherwise referred to as a conceptual label. With the continuation of the analysis, the researcher examines various other instances of data that appear to be examples of this same phenomenon, which are then labelled as appropriate. The various coded concepts are seen to form the emerging theory's building blocks, and throughout analysis become ever more abstract and numerous.

- Theoretical Saturation: Data collection and subsequent analysis are repeated until no additional dimensions, categories or insights can be identified. This is a stage referred to as theoretical saturation.

4.3.1.3. Advantages and Disadvantages of Grounded Theory

A number of limitations are recognised as apparent with Grounded Theory, including the fact it is a very complicated and time-consuming method, with in-depth coding and iterative processes involved. An additional issue with the theory, as highlighted by Elsheikh (2012), is the fact it does not depend on particular guidance concerning the intellectual process of identifying patterns in the data, thus meaning it is a very subjective process with much dependence on the capacity and ability of the researcher.

A number of advantages and disadvantages have been highlighted by El Hussein *et al.* (2014) as inherent in the Grounded Theory:

Advantages:

- Data depth
- Data richness
- Intuitive appeal
- Potential to conceptualise
- Systematic approach to data analysis.

Disadvantages:

- Exhaustive process.
- Limited capacity of generalisability.
- Much possibility for methodological error to occur.

- The need to complete a Literature Review without assumptions.
- Various approaches to Grounded Theory.

As highlighted by Elsheikh (2012), one of the key issues established is that there is a need for the identification of one central category as representative of the key underlying research theme. Nonetheless, when seeking to combine all categories into one main category, the process is problematic. Axial coding output can mean a number of different category clusters, resulting in the issue of how all clusters can be combined into one large cluster, with one key theme in the data then identified. For example, the majority of sampling is viewed as purposive and therefore is defined prior to the onset of data collection. Nonetheless, in the context of Grounded Theory, sampling is first initiated as a rational process of discussion with subjects who are well positioned to provide early data. Such information, upon examination, can be pivotal in establishing provisional explanatory concepts and then can lead the researcher to establish further respondents, locations and forms of data, at least from a theoretical standpoint.

4.3.1.4. Coding

Coding, as devised by Punch (2009), is the initial stage to be carried out in the case of qualitative analysis, the foundation for which is established at a later stage. For those analyses centred on identifying regularities in the data, coding is pivotal.

For the sake of clarity, a code may be a label, name or tag, where coding therefore involves assigning labels, names or tags to different segments of data. Each segment might be individual words, or larger or smaller chunks of data. The objective underpinning the assignment of codes is to provide meaning to the data, with such codes adopting a number of functions; they index data and provide a basis for both storing and retrieving the data.

When seeking to establish a Grounded Theory, the main aim is concerned with identifying a core category, at a high level of abstraction but grounded in the data, where this is seen to account for what is deemed pivotal in the data. This is achieved through three stages, which are individual but not always consecutive. The first is to identify the conceptual categories evident in the data, notably at the first level of abstraction; the second is to establish links between categories; and the third is to complete the conceptualisation of the categories within the data, where there is a link between theoretical codes and categories, and the core code, which is the highest-order conceptualisation of the theoretical coding, providing a foundation for the theory.

Central to the analysis of the Grounded Theory is coding, whether axial coding, open coding or selective coding: axial applies theoretical codes in an effort to interlink the key substantive codes; open coding establishes substantive codes; and selective coding isolates and further enhances the higher order core category. Punch (2009) described these three types of coding as follows.

4.3.1.4.1.Open Coding:

The first step in coding is called open coding which aims to generate conceptual labels and categories to be used in theory building. Successful open coding generates many provisional labels quickly from even a small amount of data, but this sort of coding does not go on indefinitely. The objective of open coding is not the endless generation of conceptual labels throughout the data. This process of labelling therefore needs to be balanced by two other processes. One is to keep an overview of the data in mind, and to keep looking broadly across the data, rather than only to do the intensive coding.

The outcome of open coding is a set of conceptual categories generated from the data. There will also be some ordering and classification of these categories, and some sense of what is central in the data. There may be some initial views of possible core categories, but whether this has happened or not at this stage, a small number of important categories will have emerged.

4.3.1.4.2.Axial Coding:

The second function involved in the analysis of the Grounded Theory is that of axial coding, which involves the main categories identified in the data's open-coding process to be interconnected with one another. In this context, Strauss and Corbin use the term 'axial' in an effort to communicate the idea of incorporating an axis within the data, where the axis links the categories recognised throughout the open-coding process. A more general term of 'theoretical coding' is used by Glaser in describing this stage, the meaning of which is discussed as follows.

Should the open-coding mean the data is broken apart or otherwise allowed to highlight their theoretical categories and possibilities, axial coding repositions the categories but in conceptually different ways. Accordingly, axial coding is centred on interrelating the key categories developed throughout the open coding process.

4.3.1.4.3.Selective Coding:

In the Grounded Theory analysis, the third operation is selective coding, where the term 'selective' is assigned owing to the fact that, throughout this stage, the analyst is focused on choosing one fundamental element of the data as a key category, which then receives attention. Upon selection, the theoretical analysis and subsequent development is delimited to

those areas of the data that are associated with this key category, with open coding then eradicated. The analysis then begins centred on the core category, which becomes the main foundation of the Grounded Theory.

Accordingly, in specific regards selective coding, the aim is centred on combining and pulling together the developing analysis. There must be a key focus inherent in the theory to be developed, around which it is combined. This will act as the theory's key category, and therefore is positioned as the data's central theme. In an effort to combine all data categories, the core category will need to be at a higher level of abstraction. Possible core categories are recognised at the onset of the analysis, although the core category is decided further on in the analysis.

The emphasis is centred on establishing a higher order concept at the second level of abstraction. Essentially, the emphasis of selective coding is directed towards what is considered central in the data from an analytical perspective not only descriptively. All elements of the analysis of Grounded Theory centre on ensuring the conceptualisation and explanation of data, not on data description.

4.3.2. Quantitative Research

Unlike the qualitative approach, the quantitative method is scientific in nature, and is concerned with the gathering and analysis of data in a numerical form. Assumptions, both objectivist and positivist, form the foundation for researchers who utilise such an approach. The quantitative approach is defined as predominantly aimed at gathering and analysing data that is either numerical or objective in nature, and which is commonly detailed through the use of charts, graphs or tables. Nonetheless, these data may be analysed using statistical methods. Moreover, these approaches necessitate large samples in order to ensure

generalisation of the population as a whole, which means the results can be used in a comparative manner and can be replicated (Black, 1999).

Quantitative research also is viewed as valuable when seeking to provide quantification for behaviours, opinions and personal beliefs in an effort to establish the views and perceptions of populations concerning specific phenomenon. Quantitative studies and the outcome of such commonly adopt the form of charts, graphics and tables, and are beneficial in highlighting the link between variables (dependent and independent) through the application of suitable tool and appropriate measurement scale. Quantitative methodology is recognised as valuable in testing hypotheses and theories (Bryman, 2015).

Nonetheless, quantitative research approaches are reviewed as having various disadvantages, as with any approach, such as the fact it is limiting in explaining and understanding particular phenomena, and is not able to observe gesture. Moreover, the data collection process lacks environmental control and also fails to provide situational context, providing only specific and limited data as a result of the closed nature of the approach and the posing of only structured questions (Alsaif, 2014).

From a practical perspective, this method is centred on garnering quantitative descriptions of the various in the study, with the researcher establishing the links between variables of interest in the study, and accordingly devising and subsequently testing hypotheses garnered from theories, which may be evaluated, and thus accepted or rejected in line with the completion of statistical and comparative analyses. This particular approach may be adopted across various methods, including surveys to population that is either a random or a stratified sample. It is common for such surveys to be administered in person, via the Internet or

through mail. Moreover, laboratory experiments, formal methods and numerical approaches are amongst those methods applied in the quantitative approach (Elsheikh, 2012).

4.3.2.1. Survey Research

Such research delivers numerical or quantitative descriptions pertaining to attitudes, opinions and trends of a population through examining a selective sample of the population. In the view of Creswell (2013), this involves longitudinal and cross-sectional works through the adoption of structured interviews and/or questionnaires for the purpose of data gathering, with the aim of generalising from a sample to a population.

4.3.3. Mixed-Methods Research

Strengths and weaknesses are inherent in all researches, whether qualitative or quantitative in nature. Accordingly, a mixed-methods approach is sometimes preferable as a way of counterbalancing the various drawbacks associated with each (Creswell, 2013).

4.3.3.1. Mixed Methods Strategies:

A number of professionals and scholars in the field have considered a number of possible approaches for combining qualitative and quantitative methods. In this vein, for example, Creswell (2013) stated three main different methods for combining quantitative and qualitative methods that can be extended to be six methods as discussed below.

4.3.3.1.1. Sequential Mixed-Methods:

Sequential mixed methods procedures may be explained as those applied by a researcher in mind of expanding on and further developing the findings garnered through one method with the use of another method. This might involve, for example, applying an interview approach

that is qualitative in nature and subsequently completing a quantitative survey with a large sample so that the results can be generalised to a specific population. This is referred to as sequential exploratory strategy. The application of quantitative methods suggests that results of qualitative approaches can be tested and generalised to different samples of the study population. In contrast, however, a quantitative method may be applied first, involving a concept of theory being tested, with a qualitative method adopted involving the in-depth examination of a select few individuals. This is referred to as sequential explanatory strategy. In this vein, Creswell (2013) further states that qualitative approach application is valuable in analysing the results garnered through a quantitative approach, especially unexpected results, in greater depth.

4.3.3.1.2. Concurrent Mixed-Methods:

Concurrent mixed-methods procedures are known to involve the researcher merging qualitative and quantitative data in an effort to deliver an in-depth analysis of the study problem. Through such a design, the researcher gathers both types of data and subsequently combines the data so as to interpret the results. Moreover, throughout the design approach, one smaller data form may be embedded by the researcher with another larger one in an effort to examine different types of question, as highlighted by Creswell (2013).

4.3.3.1.3. Transformative Mixed-Methods:

Transformative mixed methods procedures involve a researcher applying a theoretical lens as an all-encompassing perspective within a particular design, which comprises both types of data, i.e. qualitative and quantitative. Such a lens provides a model for methods of data collection, topics of interest, and changes or outcomes expected and predicted by the study.

Within such a lens, data collection might involve a concurrent or sequential approach (Creswell, 2013).

4.4. Data Collection Strategies

Both qualitative and quantitative approaches have several methods and strategies for data collection: For example, focus groups, semi or unstructured interviews, direct observations, documents analysis are methods used in qualitative approach, whilst structured interviews and questionnaire, on the other hand, are methods used in quantitative approach. This section focuses on the data collections methods applied in this study, as follows:

4.4.1. Literature Review

Reviewing the previous studies, works and documents was one of the main tasks in this study. Journals and specialists conferences associated to the research topic have been checked regularly, with such documents classified into three main categories: the first category is related to the documents linked to e-government, which include official documents and reports pertaining to e-government, as well as prior studies and works that are related to e-government in general; the second category is associated with the previous studies that mention the security challenges in e-services in general and in e-government specifically; and finally, the third category is related to previous studies and articles that were focused on technology acceptance and adoption, which include the main articles discussing the theories and models of technology acceptance, as well as the previous empirical studies applying such models in e-services in general and e-government in particular. Mendeley software was adopted for organising these categories, and other files and documents related to the PhD thesis. This software is valuable for reading and making notes on documents. It is also used for organising the references used in this research.

4.4.2. Interviews

Interviews can be unstructured, semi-structured or structured. In this study, there were two unstructured interviews with two experts, both of whom hold a PhD degree; their PhD these were about e-government adoption in Saudi Arabia. These interviews were conducted separately at the beginning of the PhD programme. The aim of the interview was centred on garnering more understanding concerning the current issues in e-government adoption in Saudi Arabia and accordingly discussing with them the research aim and objectives. Both of the researchers used UTAUT in their models, which were helpful in extending the discussion to cover the issues related associated with applying the UTAUT model, gathering the data and analysing the model. These two researchers were contacted by the researcher after designing the research model in order to discuss this with them and get feedback.

4.4.3. Focus Groups

Focus groups are able to provide more in-depth insight into subjects' views, beliefs, opinions, suggestions, perceptions and problems in the research topic (Creswell, 2013). In the view of Neuman (2006), focus groups are aimed towards facilitating the exchange and communication of experiences, ideas and opinions, thus resulting in greater knowledge and understanding of the research topic.

In this study, the focus group method was the main data collection strategy for the first phase. The aim of the focus group is centred on identifying the factors influencing end users' perceptions on e-government security. There were two focus groups conducted in this study.

4.4.4. Questionnaire

In this study, two questionnaires were conducted: the first was an initial questionnaire for investigating the general issues related to e-government security, as described in the previous chapter; the second questionnaire was the main questionnaire and directed consideration to the main data collection strategy in the study. The aim of the second questionnaire was to test and validate the research model. More details about the main questionnaire will be provided in Chapter 7. Both of these questionnaires targeted end users, and the data obtained were hosted securely at the Centre for Security, Communications and Network Research (CSCAN).

4.5. Selection and Justification of Research Paradigm and Approach

After reviewing the research paradigms and approaches, the main research methodology considered most suitable for this study was identified as the sequential exploratory strategy, which is one of the mixed-methodology approaches beginning with the completion of a qualitative study, followed by a quantitative study (Creswell, 2013). Thus, the interpretative paradigm is best suited to achieving the first phase of this research as the security antecedents of e-government had not been investigated before. For this reason, the research started with a qualitative study aimed at establishing these antecedents based on end users' perspectives. In this phase, an initial survey has been conducted to investigate the security challenges in e-government services based on end users' perspectives. After that, the findings from the initial survey were discussed during two focus groups that have been conducted to deeply investigate the factors that influence end users' perception in e-government security. The results of the qualitative study will be used to build the research hypothesis, which will be

tested in the second phase, which is a quantitative study. Thus, the positivist paradigm is best suited to achieving the second phase of this research.

4.6. Research model

The research developed the research model based on the UTAUT2 model. This model is the extended version of UTAUT, and was developed for consumers in particular as the UTAUT was originally developed for employees (Venkatesh *et al.*, 2012). In addition, as the UTAUT integrated eight of the adoption models and theory, this allows the UTAUT to increase the percentage of explained variances and accordingly fill the gap in other adoption models, such as TAM and TRA, which presented low explanatory power. Lian (2015) indicates that the major theoretical basis in e-government adoption is UTAUT; this can be observed clearly in the literature review of e-government adoption, as shown in Section 2.2.9. Several studies applied the original UTAUT model in e-government studies (AlAwadhi and Morris, 2008; Ovais Ahmad *et al.*, 2013; Wang and Shih, 2009; Yahya *et al.*, 2012). Other studies have applied an amended UTAUT model by integrating additional factors. One of these factors is trust in e-government (Alsaif, 2014; Alshehri et al., 2012a; Lian, 2015; Weerakkody et al., 2013). Security perception is considered to be one of the trust antecedences in e-services (Pavlou, 2001; Roca *et al.*, 2009; Shin, 2010). Thus, the researcher believes that UTAUT is the best model for investigating the role of security in e-government services as the role of trust was investigated in e-government studies.

4.7. Sample Size

This study targets Saudi citizens who use e-government services. Thus, data should represent the targeted population. As there is no statistical data showing the total number of citizens who use e-government services, the sample size has been determined based on Internet users

in Saudi Arabia. In 2015, the Communication and Information Technology Commission indicated in its report that the total number of Internet users in Saudi Arabia amounted to 21 million (MCIT, 2016). The total population in Saudi Arabia is 30.8 million, as shown in the last report of the central department of statistics and information in 2015 (STATS, 2016). Thus, the following equation is used to determine the minimum sample size, as based on the information above:

$$n = \frac{t^2 \times p \times (1-p)}{m^2}$$

Where:

- n = Minimum sample size
- t = Confidence level at 95% (standard value of 1.96)
- p = Estimated fractional population of subgroup
- m = Margin of error at 4% (standard value of 0.05)
- Population of Saudi Arabia = 30.8 million
- Internet users in Saudi Arabia = 21 million
- P = 21/30.8 = 0.68

$$n = \frac{1.96^2 \times 0.68 \times (1-0.68)}{0.04^2} = 522$$

In addition, a useful tool provided by Creative Research Systems (www.surveysystem.com) for calculating the sample size required also has been used, as shown in **Error! Reference source not found.**. Based on this tool, the sample size required is 600 as shown in Figure 4.1.

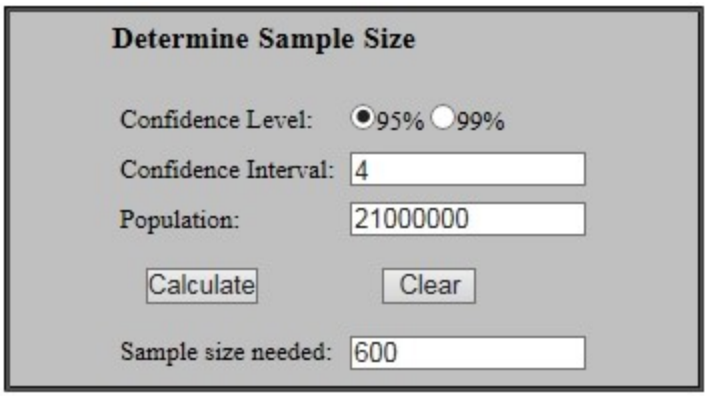

Figure 4.1: Sample size required

In addition, Alshehri (2012), who completed a study in mind of investigating the critical factors for e-government adoption in Saudi Arabia, suggests that the minimum sample required is 500 participants. Moreover, Alsaif (2014) carried out a study investigating the effects of socio-culture value in e-government adoption in Saudi Arabia, and further suggested that the sample should be between 500 and 1000 participants. Thus, based on the previous information, this study will target a minimum of 500 participants who use e-government services in Saudi Arabia.

This sample size was determined for the quantitative study to test the research model and hypotheses. However, as the initial survey was conducted to get an overview of the security challenges in e-government adoption and to support the focus group session, the confidence interval was set at 8, which made the required sample size 150 participants, as shown in Figure 4.2.

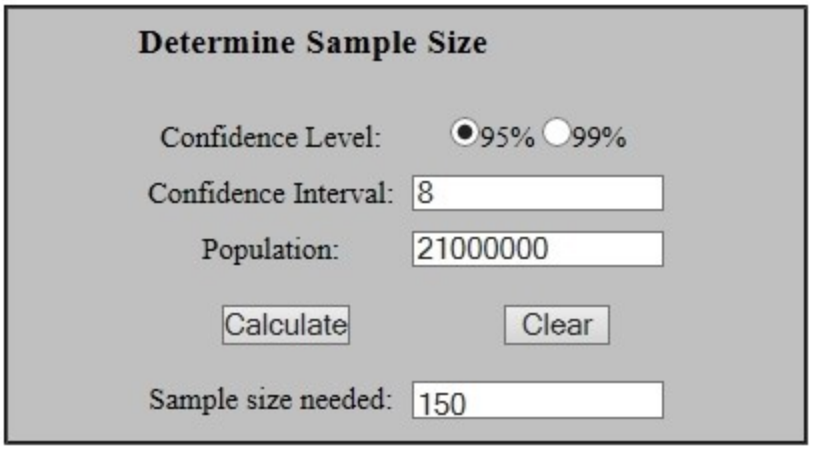

Figure 4.2: Sample size required for the initial survey

This study did not follow a specific methodology for determining the required sample size for the focus group sessions, which is considered to be one of the research limitations. However, the focus group sessions were supported by data from 189 participants from the initial survey. Thus, both the focus group sessions and the initial survey were used together in the qualitative study to determine the factors influencing end users' perceptions of e-government security.

4.8. Translation of the Questionnaire

The main research questionnaire was devised in English and subsequently was translated into Arabic, which is the native language spoken by the intended respondents of the questionnaire. It is considered that this will help to ensure more in-depth understanding amongst the participants and thus achieve a greater response rate. Subjects were chosen randomly from the general population, with individuals seen to have different backgrounds and qualifications.

Three Saudi linguistic teachers were sent the questionnaire and accordingly were asked for feedback. The subsequent version of the questionnaire included their suggestions, which then

was piloted. The participants' comments were considered when devising the final version of the questionnaire, which subsequently was distributed amongst the population of the target sample.

4.9. Ethical Considerations

When studies are seeking to examine human behaviours, it is paramount that ethical considerations are made prior to beginning, as well as throughout and following the completion of data collection (Zikmund *et al.,* 2012). Failing to direct attention to this area could result in subjects' failure to cooperate and comply, which causes problems in the collection of data. Adhering to ethical standards and ensuring the gaining of consent from the subjects are the critical factors in completing studies. Ethical considerations need to ensure compliance in order to ensure human rights are not violated. This also should guarantee that respondents' information is kept completely confidential. Moreover, personal information should not be required, nor should information be misused or changed. The research aims and objectives should be clearly communicated to the sample, with respondents made aware of their freedom to remove themselves from the research process at any time.

In actuality, this study adheres to the guidelines set forth by Plymouth University's Ethical Principles for Research Involving Human Participants, which monitors data collection processes. As outlined, the researcher needs to ensure they garner the right permission at the outset, when subjects have been advised that they are not obliged to participate in the study and have the right to withdraw at any stage should they choose to do so.

The issue of confidentiality was explained and the subjects were given assurance that all data would be protected and used only for the purposes identified by the researcher. Furthermore, it was made clear that the data would not be distributed to any other individual and/or group.

The data collection process warranted consent prior to being initiated; the university research ethical committee issued consent, as detailed in Appendix A.

4.10. Conclusion

This chapter presented the methodology that was used in this research, which adopted a mixed methods approach. This approach starts with a qualitative phase that is followed by a quantitative phase. The aim of the first phase was to explore the initial security antecedents to e-government adoption, while the second phase aimed to investigate the role of security in e-government adoption. The second phase was used to confirm the security antecedents to e-government adoption. The main data sources in the first phase were the initial survey and the focus group, while the second phase used a questionnaire to collect the required data.

The next two chapters will focus on the first phase, with the results from this phase will be used in the second phase.

5. Security challenges in e-government adoption: initial survey

5.1. Introduction

This chapter seeks to provide a general overview concerning the current status of e-government security based on end users' perspectives. The aim of this survey is centred on understanding the phenomena and garnering more information about current security challenges that need to be considered in developing the research model. The survey is targeting Saudi citizens as the e-government in Saudi Arabia is the case study in this research..

This chapter begins by providing a general overview about the research surveys completed in this study. Subsequently, the survey methodology followed in completing the survey will be explained. The findings of this survey will be described and discussed. Finally, the conclusion of this chapter will be provided.

5.2. Research Surveys

In total, two surveys will be carried out in the PhD research. The first survey, which is aimed at evaluating e-government security based on end users' perspectives, investigates current general security threats facing the end users of e-government, whether technical or non-technical. The survey also investigates whether or not a lack of security is the main reason behind participants not using e-government services. The findings of this survey are analysed in this report. The second survey, the main purpose of which is to test and evaluate the model, will be conducted after the novel model has been designed. This survey will contain specific questions in order to represent specific variables in the model.

5.3. Survey Methodology

This survey comprises 17 questions, the majority of which are based on multiple choices. A Likert scale (ranging 1–5) is also used, spanning 'strongly agree' to 'strongly disagree'. The survey, which has been designed in both Arabic and English languages, was distributed via the Internet and hosted online by the Centre for Security, Communications and Network Research (CSCAN) at Plymouth University. There are three main sections included in this survey: the first section (questions 1–6) seeks to garner general information about respondents, such as age, gender, educational background, employment status, information security background and nationality; the second section (questions 7–10) covers participants' e-government usage, including the analysis of their experience in using e-government services and determining the current challenges; the third section (questions 11–17) look at participants' experience of e-government security, and is considered to be the most important section in the survey as it covers the security issues in e-government and accordingly analyses respondents' experience of e-government security.

The survey begins by posing a consent question to confirm that the age of the participant is 18 or above, and to ensure he/she understands the conditions and accepts taking part in the survey. At the end of the survey, the participants were asked to provide comments and feedback in relation to e-government security, such as security challenges or suggestions. The participants were informed that their comments would be highly considered. The survey has been written in a simple way, to the greatest possible extent, as it is for the public and so should be clear and easy to understand. The survey has been tested and reviewed by both academic staff and some members of the public in an effort to ensure that it has been written so that it is understandable; it also has been approved by the faculty ethics committee.

5.4. Survey Findings

The total number of participants who fully answered the survey totalled 228. The majority of the participants were male whilst females accounted for only 33.8%. Based on Saudi culture, men are more likely to be responsible for applying for different government services. As this survey was distributed via a social network on the Internet, only 6 participants were 50 years old or older, whilst 97.4% of the participants were aged between 18 and 39 years. With regards educational level, more than half of the participants held a Diploma or a Bachelor's degree, whilst 16.2% of the participants held either a Master's or a PhD degree. In total, 39.9% of the participants were government-employed whilst approximately quarter of the participants was students. Finally, most of the participants had only a basic background in information security, whereas one-quarter of the participants had an intermediate background in this area. Table 5.1 below presents details regarding the general information of the participants.

Demographic Variable	Categories	Response Frequency	Percent
Gender	Male	151	66.2
	Female	77	33.8
Age (years)	18-29	126	55.3
	30-39	78	34.7
	40-49	18	7.9
	50-59	6	2.6
	60+	0	0
Educational Level	Secondary School	46	20.2
	Diploma/ Bachelor	142	62.3
	Master/ Doctorate	37	16.2
	Other	3	1.3
Employment Status	Student	61	26.8
	Government employed	91	39.9
	Private sector employed	39	17.1
	Self-employed	35	15.4
	Other	2	0.9
Information Security Awareness	Basic	156	68.4
	Intermediate	59	25.9
	Advanced	13	5.7

Table 5.1: General information about the participants

In total, 82.9% of the participants had used e-government services before, whereas the percentage of participants who had not used e-government services was 17.1%, as shown in Table 5.2. This survey was distributed over the Internet, meaning that the participants had at least a basic level of skill in this area.

	Frequency	Percent
Participants who used e-government	189	82.9
Participants who did not use e-government	39	17.1
Total	228	100.0

Table 5.2: Participants' experience of using e-government services

Altogether, 38.5% of the participants had not used e-government because most government services are not available online, whereas 12.8% had not used e-government services because they did not trust the level of e-government security. Another factor also seen to affect the

use of e-government services is resistance to change and a preference for traditional methods. One participant stated the following:

> '*I have good experience in computer skills. However, I used to apply for government services though a branch only. It does not mean that I prefer it, I just got used to it.*'

There are also other factors, such as a lack of skills that need to be taken into account, as mentioned by some of the participants, in addition to the complexity of e-government services, as noted by 25.6% of the participants. In general, the majority of the participants preferred to use government services through the Internet, either by laptop or desktop, whereas 39.7% preferred applying for services through their mobiles. Table 5.3 presents more details regarding the methods of applying for government services.

Preferred method	Frequency	Percent
Face-to-face (traditional way)	16	8.5
Via phone	10	5.3
Via the Internet using a laptop or desktop	158	83.6
Via a mobile application	75	39.7
Via ATM machines	32	16.9

Table 5.3: Preferred methods of applying for government services

In seven statements in the survey, participants were asked to provide their opinion using a Likert scale that offered the following alternatives: strongly agree, agree, neutral, disagree and strongly disagree. The statements are listed below:

- I'm worried about my privacy when using e-government services
- I do not trust the e-government security
- The website design of e-government services has influenced me in determining the level of e-government security

- Culture and social relationships play an important role in e-government security (e.g., obtaining personal information from the users by using social relationships)
- Users' awareness is one of the main factors affecting e-government security
- The security advice provided to users via the media and e-government websites is very limited
- Most current security issues are basically non-technical, such as lack of users' awareness and lack of trust.

The first statement concerns privacy in e-government. Figure 5.1 and Table 5.4 shows that 23.5% of participants strongly agreed that they were concerned about privacy when using e-government services; only 5.1% of participants strongly disagreed with this statement.

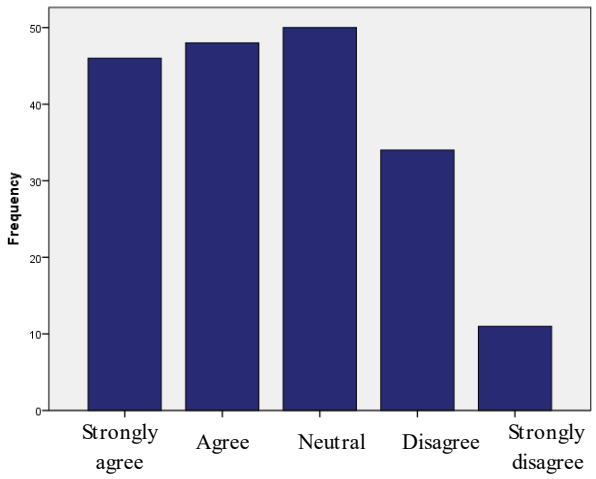

Figure 5.1: Privacy statement (all participants who used e-government services)

	Frequency	Percent
Strongly agree	46	24.3
Agree	48	25.4
Neutral	50	26.5
Disagree	34	18.0
Strongly disagree	11	5.8
Total	189	100.0

Table 5.4: Privacy statement (all participants who used e-government services)

Furthermore, 61.5% of the participants who had advanced information security backgrounds agreed with this statement, whereas only 23.1% disagreed, as shown in Figure 5.2 and Table 5.5.

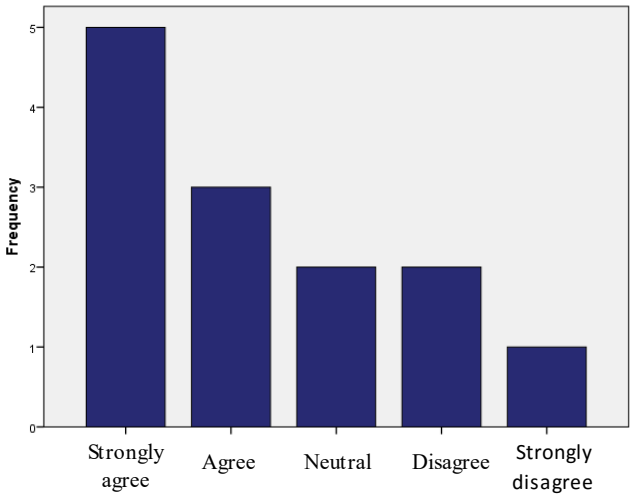

Figure 5.2: Privacy statement (participants who have advance Information security background)

	Frequency	Percent
Strongly agree	8	36.4
Agree	5	22.7
Neutral	5	22.7
Disagree	3	13.6
Strongly disagree	1	4.5
Total	22	100

Table 5.5: Privacy statement (all participants who used e-government services)

It is clear from the statistics and participants' comments that e-government users show a higher level of concern in relation to privacy. One participant mentioned that his government was focused on providing e-services to its citizens to the greatest possible extent without considering the protection of citizens' privacy. Another participant stated the following:

> *'The thing that I'm most worried about is protecting my personal data from being observed by unauthorised persons as there are no polices that protect my privacy in e-government.'*

It was also observed that some personal information can be obtained by knowing someone's national ID number. This number can be found on the Internet or in a newspaper, and subsequently may be used in some e-government services to obtain personal information about a user. In addition, it is easy to obtain personal information about any user if a government employee with access to an e-service database is known, as mentioned by one of the participants. This participant also suggested that there should be an organisation monitoring access to the database in an effort to protect the privacy of users and to set policies to track unauthorised access.

With regards the second statement, relating to trust in e-government security, 53.8% of the participants with advanced information security backgrounds agreed that they did not trust e-government security (Figure 5.3 and Table 5.6). On the other hand, 28.6% of the participants with basic information security backgrounds selected neutral. The percentage of those in agreement and disagreement was the same at 29.4%. However, the participants who strongly agreed were more numerous than those who strongly disagreed (Figure 5.4 and Table 5.7).

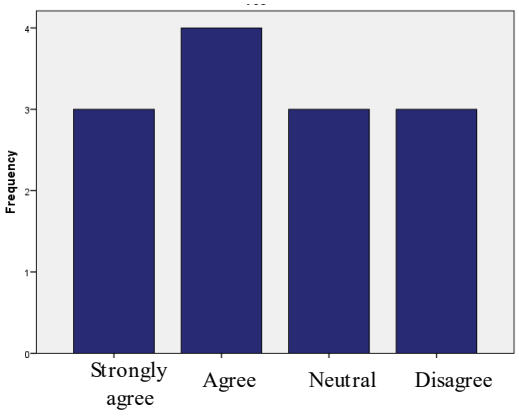

Figure 5.3: Trust statement, (participants with advanced security background)

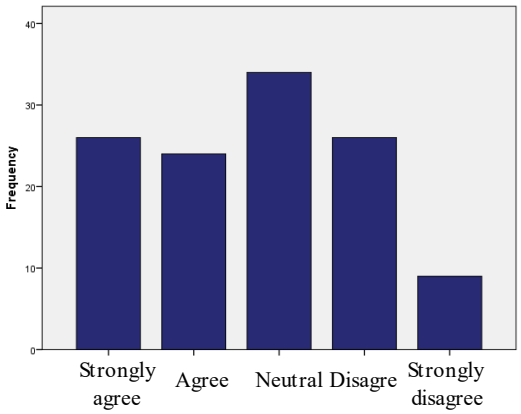

Figure 5.4: Trust statement, (participants with basic security background)

	Freq.	%
Strongly agree	3	23.1
Agree	4	30.8
Neutral	3	23.1
Disagree	3	23.1
Strongly disa□ree	0	0
Total	13	100.0

Table 5.6: Trust statement, (participants with advanced security background)

	Freq.	%
Strongly agree	26	21.8
Agree	24	20.2
Neutral	34	28.6
Disagree	26	21.8
Strongly disagree	9	7.6
Total	119	100.0

Table 5.7: Trust statement, (participants with basic security background)

Several participants provided comments regarding trust. Some of these comments related to the trust of the Internet and the others related to trust of the government itself. One participant said:

> *'I'm sure that my information and details in the e-government will be used against me when I face problems with the government since there is no protection for citizens' rights.'*

Another participant said:

> *'...One point which needs to be considered is that the government provides the service. I trust e-government that my information is secure 90% when I apply for e-services in Australia. However, I only trust the e-government 30% when I use e-services in Saudi Arabia.'*

Another participant evaluated the security of e-government in line with the number of successful attacks the e-government services had faced:

> *The security in e-government is very weak and the large number of successful attacks is strong evidence.''*

Another participant who did not trust G2G services said:

> *'...We have an internal system in our department and the head of department deleted all his digital signatures for the last year before he left the department which puts me in trouble. I'm using now the normal signature as I will never trust the e-services.'*

Other, similar comments to those above also were made. However, a participant mentioned that he did not trust the security of e-government not because of a lack of security but

because he was confident that hackers could break into any system, which led him to avoid carrying out any financial transactions over the Internet.

The third statement related to the relation between website design and security. Figure 5.5 and Table 5.8 show that 62.9% of the participants agreed that website design influenced them in determining the security level of any government website. When participants' responses were analysed based on their information security background, the results were found to be almost the same as those shown in Table 5.9.

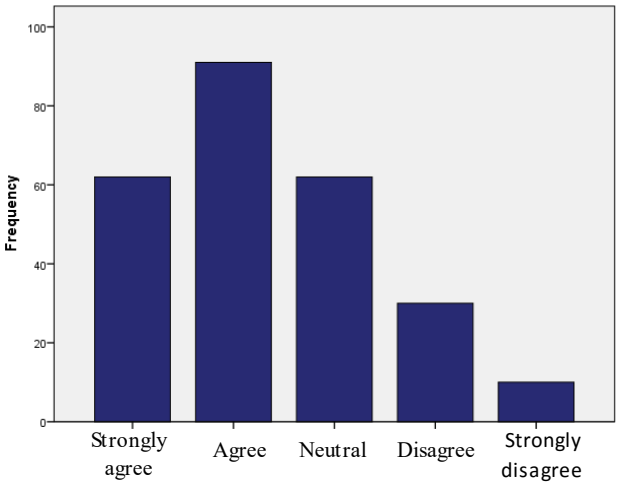

Figure 5.5: Website design statement (all participants who used e-government)

	Frequency	Percent
Strongly agree	45	23.8
Agree	70	37.0
Neutral	46	24.3
Disagree	20	10.6
Strongly disagree	8	4.2
Total	189	100.0

Table 5.8: Website design statement (all participants who used e-government)

		Basic		Intermediate		Advanced	
		Freq.	%	Freq.	%	Freq.	%
1	Strongly agree	33	27.7	10	17.5	2	15.4
2	Agree	43	36.1	21	36.8	6	46.2
3	Neutral	26	21.8	18	31.6	2	15.4
4	Disagree	11	9.2	7	12.3	2	15.4
5	Strongly disagree	6	5.0	1	1.8	1	7.7
Total		119	100.0	57	100.0	13	100.0

Table 5.9: Website design statement (based on participants' security background)

The fourth statement related to culture and social relationships and their impacts on e-government security. It is clear from the responses that culture and social relationships strongly influence e-government security. A total of 38.8% of participants strongly agreed that culture and social relationships played an important role in e-government security, as can be seen in Figure 5.6 and Table 5.10.

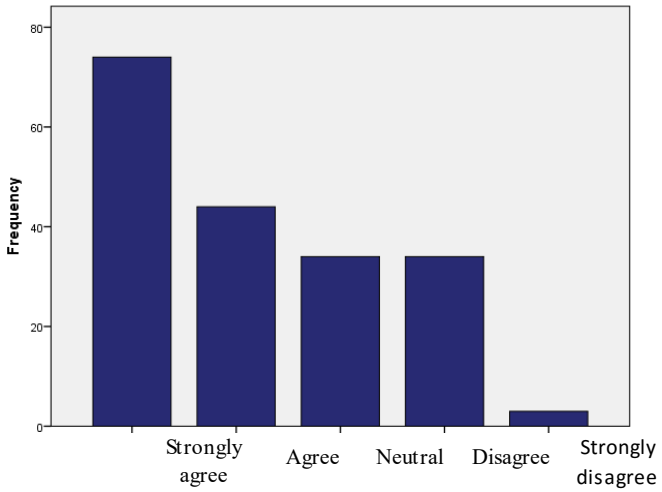

Figure 5.6: Culture statement (all participants who used e-government)

	Frequency	Percent
Strongly agree	74	39.2
Agree	44	23.3
Neutral	34	18.0
Disag□ee	34	18.0
Strongly disagree	3	1.6
Total	189	100.0

Table 5.10: Culture statement (all participants who used e-government)

One of the participants mentioned that information about users can be obtained from a friend or relative who works on the e-government programme; this can threaten users' privacy.

The fifth statement related to users' awareness, and it is clear from participants' responses that the majority agreed that users' awareness was one of the main factors affecting the security of e-government. Figure 5.7 and Table 5.11 show that 57.7% of participants who had used e-government strongly agreed and 26.5% agreed with the statement, whilst only 2.1% disagreed.

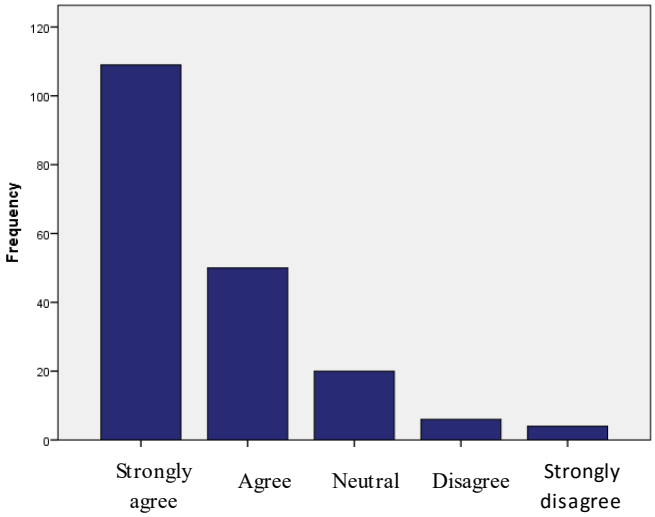

Figure 5.7: Users' awareness statement (all participants who used e-government)

	Frequency	Percent
Strongly agree	109	57.7
Agree	50	26.5
Neutral	20	10.6
Disagree	6	3.2
Strongly disa□ree	4	2.1
Total	189	100.0

Table 5.11: Users' awareness statement (all participants who used e-government)

Users' awareness was mentioned a number of times in participants' comments, and other comments were made in relation to the awareness of government employees and decision-makers in the e-government programme. One participant stated that most of the current security problems stemmed from users' lack of awareness. Another participant made the following statement:

> *'There is a lack of awareness, not only with users, but also with employees and managers who work in e-government. Awareness needs to be increased for both of them.'*

Another participant also said:

> *'...There is a lack of information security skills with the programmers who develop the government websites. An information security course must be given for those programmers. Also, a course on information security must be given to university students...'*

Another participant mentioned that the awareness of both public and government employees needs to be increased. Both need to be more careful about the privacy of citizens.

The sixth statement relates to the security advice provided in the media and on government websites. A total of 58.2% of the participants who used e-government strongly agreed that the advice provided on the government websites and the media was scant. In addition, 28% of participants agreed, whilst 1.6% disagreed, and only 0.5% strongly disagreed, as is shown in Figure 5.8 and Table 5.12.

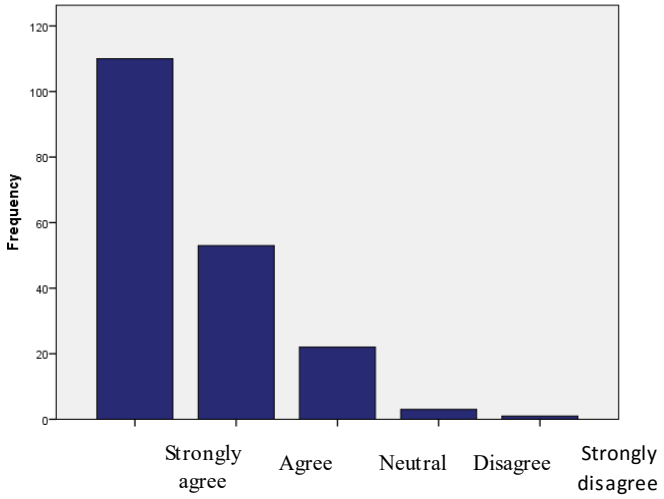

Figure 5.8: Security advice statement (all participants who used e-government)

	Frequency	Perce□t
Strongly agree	110	58.2
Agree	53	28.0
Neutral	22	11.6
Disagree	3	1.6
Strongly disagree	1	0.5
Total	189	100.0

Table 5.12: Security advice statement (all participants who used e-government)

A participant mentioned that most e-government websites do not provide enough security advice, whereas some of them provide very extensive information regarding information security. This participant suggested that the advice should be increased but provided in a simple way. In addition, the participant mentioned that some government websites provide information to protect their rights and to make the user responsible for using this service, which might lead the user to avoid using the service.

The seventh statement investigated whether the most current security threats came from the non-technical side. The participants' responses, as detailed in Figure 5.9 and Table 5.13,

show that 72% agreed that most of the current security threats come from the non-technical side, whereas only 6.4% of participants disagreed.

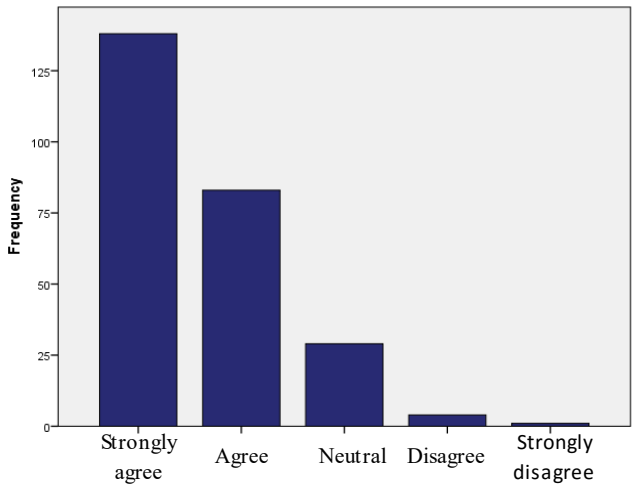

Figure 5.9: Non-technical threats statement (all participants who used e-government)

	Frequency	Percent
Strongly agree	69	36.5
Agree	67	35.4
Neutral	41	21.7
Disagree	10	5.3
Strongly disagree	2	1.1
Total	189	100.0

Table 5.13: Non-technical threats statement (all participants who used e-government)

This statement summarised the other six statements and proved that most of the current security issues stem from the non-technical side. These include a lack of awareness, privacy, trust, culture and website design.

5.5. Discussion

This survey investigates the current security threats facing end-users of e-government. These factors will be considered in the development of the research model. There is a need for

increasing the security awareness of the citizens via the media or through government websites. However, 86.2% of the participants who had used e-government programs agreed that the security advices provided to users either through the media or e-government websites is very limited. In addition, some of this advice is not presented in the most appropriate way as much of it is very long and complex. Such advice should be simple and short so as to allow users to understand it easily. Furthermore, this survey shows that 84.1% participants agreed that most of the current security issues are non-technical. Moreover, the participants gave some examples that clarified how culture and social relationships have an impact on the security levels in e-government. Another factor that only a few research studies on e-government have mentioned is website design and its impact on end-users in regards determining the level of security. A total of 60.8% of the participants agreed that the website design of e-government services influenced them in deciding on the level of e-government security. The survey results show that half of participants were worried about their privacy when using e-government services, and many comments were made by participants regarding this issue. One of the participants suggested that the government must increase the knowledge of both its citizens and employees. Finally, the survey shows that 42.3% of the participants agreed that they do not trust e-government security. Moreover, there is a 7.4% difference between the trust and privacy statements, which shows that the participants were more concerned about privacy. Table 5.14 shows the ranking for each statement and the percentage of participants' agreement.

Rank	Statement	Frequency	Percentage of agreement
1	Security advice provided to users via the media and e-government websites is very limited	163	86.2
2	Users' awareness is one of the main factors that affects e-government security	159	84.1
3	Most of the current security issues are non-technical such as lack of users' awareness and lack of trust	136	72.0
4	Culture and social relationships play an important role in e-government security	118	62.4
5	The website design of e-government services influenced me in determining the level of e-government security	115	60.8
6	I'm worried about my privacy when using e-government services	94	49.7
7	I do not trust the e-government security	80	42.3

Table 5.14: Ranking of statements

5.6. Conclusion

This chapter has provided details on the current security challenges and e-government security status from the perspective of end users. The main findings show that information security awareness, website design, security advice and culture all play an important role in e-government security. These findings will be considered when investigating the factors that influence end users' perceptions of e-government security. Thus, these findings will be discussed during the focus group sessions in order to determine the initial security antecedences in e-government adoption. The following chapter will focus on determining these initial security antecedents.

6. Security antecedents in e-government adoption

6.1. Introduction

This chapter focuses on the first phase of this study, which is centred on identifying the factors that influence end users' perceptions in the field of e-government security. As the factors influencing end users perceptions in e-government security have not been investigated before, the study applied the Grounded Theory that allows the researcher to identify these factors and built hypotheses that can be texted in the second phase. The justification of its use in this study is explained in section 6.2. Subsequently, the process of applying Grounded Theory is provided. As the initial survey focused on the security challenges that face end users in general, there was a need to conduct focus groups to investigate the factors that influence end users' perceptions of e-government security in particular. The analysis of the data and the procedures were then explained. Finally, the results from the analysis stage were presented and discussed. The results provide the identified initial factors seen to influence end users' perceptions in e-government security.

6.2. Justification of using Grounded Theory

Based on the literature review, it is clear that there is a lack of existing theories investigating the factors influencing end users' perceptions of e-government security. As the main concept of Grounded Theory for investigating actualities from the real world, this study applied Grounded Theory in an effort to develop a theory that identifies these factors.

Grounded Theory is applied with the aim of identifying a theory where there is only a little recognised in relation to the phenomenon under examination. As stated by Goulding (2002), the overall value associated with Grounded Theory application becomes apparent when the

literature is lacking integrated theory. Furthermore, insight, understanding and a meaningful guide to action can be provided by Grounded Theory, as derived from data. In this vein, the statement is made by Creswell (2013) that the overarching objective of the Grounded Theory approach is to create or otherwise identify a theory that is grounded in data that is both gathered and accordingly analysed in a systematic way.

Furthermore, when drawing a contrast with other qualitative analysis methods, a systematic method of analysis is provided by Grounded Theory, which involves the inclusion of axial, open and selecting coding, which is pivotal in developing a theory grounded in data. This is in line with the indication made by Charmaz (2006) that Grounded Theory enables analysis processes, including particular steps for developing categories, concepts and theory.

The Grounded Theory will prove helpful and valuable in the generating of hypotheses. These hypotheses will be tested in the second phase, which is the quantitative approach.

6.3. Grounded Theory Research Process

6.3.1. Data Sources

The data utilised in the current work was garnered across three different stages using a number of different sources, including focus groups, literature review and survey. Practically, multiple sources should be used for data collection, which is one of the key factors affecting such a work, especially those centred on the generation of theories. This provides a number of different perspectives relating to the phenomenon to be examined and supported through the provision of more knowledge relating to the emerging categories and concepts, thereby enabling their more precise analysis so as to ensure the provision of strong evidence to validate the emerging constructs (Elsheikh, 2012).

6.3.1.1. Literature Review:

The researcher starts with reviewing the previous studies related to the factors influencing end users' perceptions in e-services. The aim of the literature review is focused on gathering more information about the phenomena, which could prove helpful during the focus group sessions. In addition, it would be valuable to link the output of the focus groups with the literature review and accordingly discuss the findings with previous studies.

As stated by Elsheikh (2012), it is common for there to be the view that the researcher is expected to work in the arena without considering any past literature or theory linked to the phenomenon under examination, and to wait for theory to emerge merely through gathering data. All theory known before beginning a research cannot be eradicated from the mind. In this vein, Glaser and Strauss (1967) encourage academics completing research papers to include the works and contributions of others in an effort to form a foundation of knowledge, which can be recognised as literature sensitivity. It was further stated by Glaser (2002) that the literature review is a further data source and adopts a key role in the emergence of Grounded Theory,

6.3.1.2. Initial Survey:

Following the completion of the initial survey, the findings are recognised by the researcher as valuable for consideration throughout the focus group sessions. A number of different feedback was garnered from the participants in the initial survey, which underwent review and consideration in the focus group sessions. The participants were able to provide the researcher with an abundance of information concerning present security issues that were not covered by the survey questions through the inclusion of open-end questions. Owing to the fact that the sample of participants who answered the initial survey amounted to 189, the

researcher was well-positioned to garner different viewpoints concerning the present situation of security in the e-government field.

6.3.1.3. Focus Groups:

Two focus groups were conducted in this study. The first group was of participants, all of whom were Saudi citizens and familiar with e-government services in Saudi Arabia. The participants were from different age groups and had different levels of education. The second group comprised six participants, all of whom were specialists in computer and network security and had a Master's degree and at least five years' experience. The participants' demographic details were kept anonymous in order to ensure their privacy was safeguarded. The aim of researching the first focus group was to examine the factors influencing public citizens' perceptions of e-government security. The following questions have been asked during the focus group session:

- Have you used e-government services? If not, why?

- In your opinion, is using e-government services secure? Why /why not?

- How do you measure the level of security in e-government services?

- What are the factors that influence your perception in e-government security?

- What does security on e-government websites mean to you?

The findings from the initial survey were discussed, in addition to establishing the critical factors influencing their perceptions in e-government security. The second group was carried out later on in an effort to discuss the factors influencing their perceptions in e-government

security. Moreover, the outcomes of the research on the first group were discussed based on the perspectives of security specialists.

6.3.2. Analysis and Procedures

This study uses Straus's approach, which is considering the literature review any other source before and during the study itself. Thus, in previous studies, as discussed in Section 3.3.3, the factors influencing end users' perception in e-services were considered in the data collection. This gives the researcher a background about the phenomena in other e-services that are similar to e-government services. Previous studies were helpful in establishing the data collection sample. In addition, several studies provided different types of question deemed suitable for during the focus group sessions, which can allow participants to provide more details about the phenomena.

Besides the literature review, the findings from the initial survey were considered, in addition to the focus group sessions. This rich data from 189 participants were helpful in determining critical security issues based on end users' perspective. The initial survey was mainly focused on the security challenges in e-government services. The findings from the initial survey, especially qualitative data related to the perceptions in e-government security, were reviewed before focus group sessions.

After the completion of the two focus group sessions, they were transcribed by the researcher and the analysis begun by converting the recoded files of the sessions into Arabic, which is the language adopted during both of the focus groups sessions. Each focus group session's materials were stored separately, including participant forms and recoding files. The research subsequently translated the Arabic transcripts to the English version. The research used QSR NVivo software for the purpose of analysis. Following, when both the focus groups sessions

were transcribed, the researcher then started with the coding process. The first stage of coding was open coding. The researcher read the text on a line-by-line basis, highlighting and labelling the key points and significant words: for example, the padlock icon was mentioned during the focus group session and then was highlighted and labelled, as will be shown in the Results section.

The experience and knowledge of the researcher plays an important role in determining the significant words and terms. The second stage of coding is axial coding, which aims at identifying the relations between categories from open coding. However, in this study, the main focus was centred on identifying those factors influencing end users' perceptions in e-government services; thus, the relations between these categories were not considered in this study, where the only relation was considered is the relation between the identified categories and security perceptions. Relation could be either positive or negative. The researcher, during the axial coding process, can determine whether a particular category influences the security perception either positively or negatively. The final stage of coding is selective coding, which aims at selecting the core category that is at the centre of the phenomenon, based on the results from the axial coding. Thus, as the only relation considered in the axial coding is the relation between the identified categories and security perception, the core category stage was security perception.

6.4. Results

After completing the analysis of the two focus group data by applying the Grounded Theory, the findings from the analysis stage were seen to show five categories that affect end users' perceptions in e-government services. This section explains each category and further shows

how the categories were identified. The main results obtained from the analysis stage are summarised in Table 6.1.

Code		Category	Description
1	Padlock icon	Tangible security features	Technological security features provided on certain website that are visible and can be checked by users (Kamoun and Halaweh 2012).
2	http(s)		
3	Complex password		
4	Two factor authentication		
5	Knowledge	General information security awareness	Users' overall knowledge about information security and the negative consequences of potential security threats (Bulgurcu et al. 2010).
6	Security background		
7	Experience		
8	Security threats		
9	Looks organized	User interface quality	The usability of the website and how it is organised and presented to the users.
10	Looks secure		
11	Easy navigation		
12	Cybersecurity law	Cybersecurity law	The rules and regulations that are used by the government in case of a cybersecurity incident.
13	Security policy violation		
14	Internet activity monitoring	Security culture	How the government creates a security culture among its citizens.
15	Government interest		
16	Security advices provided		

Table 6.1: Extracted codes and themes from the qualitative study

6.4.1. Tangible Security Features

The participants indicated that several security features provided on e-government websites affected their perception of security. These factors are the padlock icon and the presence of 's' in the http(s). Participant A6 said, 'When I see the padlock icon in the browser, I know that this website is what I'm looking for'. This feature allows users to be sure that their communication with the e-government website is secure. In addition, participant A5 indicated the significance of asking users to create a complex password, saying, 'I feel that the security level of the e-government website is high when it requires me to create a complex password and does not accept easy passwords'. Complex passwords help prevent others guessing the user's password and carrying out brute-force attacks. A complex password can be created by following specific rules, such as through adhering to the minimum length of the password as

8 characters, for example, or that the password must contain lowercase and uppercase alphabetic characters, as well as a number and a symbol, or it should not be your name or username. Another security feature was mentioned by participant A5, who said, 'Also, when an e-government website uses a password and SMS message (two way authentication), this give me the impression the website is secure'. This feature is used when dealing with sensitive information or when making a payment. Security features seem to be important in general e-services, such as e-commerce, as mentioned in section 3.3.3.

6.4.2. General Information Security Awareness

Information security awareness was talked about extensively in the focus group discussion. Participant A6 said, 'We still have a shortage of people using e-services in general. Usually, persons who have good information security awareness are more confident buying from the Internet'. General information security awareness can be gained in different ways; it can come from users' experiences of using the Internet or their knowledge, practice and learning. Bulgurcu *et al.* (2010) measured general information security awareness by investigating users' general awareness of security threats and their negative impacts, as well as users' knowledge of the costs associated with security threats.

6.4.3. User Interface Quality

One of the main factors affecting security perceptions is the quality of the user interface. Participant A7 clearly stated that, 'The high quality of the user interface on e-government websites has a strong impact on the security level of those websites'. Participant A6 interrupted, stating, 'Technically, this might not be true, but it gives a strong impression that this website is secure'. Participant 7 then said, 'If there are problems with website quality and usability, this absolutely means that there are problems with the website's security because it

is more complex'. As mentioned in Section 3.3.3, the quality of the interface design plays a significant role in the perceptions of security. The results from the focus group discussion indicate that users evaluate the e-government website based on the quality of the user interface.

6.4.4. Cybersecurity Law

The participants mentioned cybersecurity law as one of the important factors affecting perceptions of security. Participant A1 said, 'I think when an e-government website indicates that it is linked with the Ministry of the Interior, this makes citizens feel the website is secure. It may not be secure, but linking the e-government website with the Ministry of the Interior indicates that there is a security system monitoring the services'. Participant A2 also mentioned the importance of cybersecurity law, stating, 'Without cybersecurity law, some employees and hackers may be able to access citizens' sensitive information and share it with non-authorised parties'. Cybersecurity law can be helpful when dealing with hackers and citizens who violate information security, and also might prevent hackers from getting unauthorised access to citizens' data. Cybersecurity law differs from one country to another, as Participant B2 in the second focus group (security specialists) session pointed out when saying, 'In some developed countries, making a port scan is illegal whether the attack has been successful or not. However, in other countries, it is legal as long as the attack is unsuccessful. The port scan is the key to the attack and must be prevented'. Participant B3 commented on current cybersecurity law, saying, 'Current cybersecurity law needs to be altered and improved. There is a lack of clarity regarding the suitable punishment for each information security violation'. At the end of the discussion, participant B1 said, 'Effective cybersecurity law positively affects the perceptions of e-government websites' security'.

6.4.5. Security Culture

The impact of security culture recently has been investigated in businesses and organisations (D'Arcy and Greene 2014; Singh *et al*., 2014; Williams et *al*., 2009). D'Arcy and Greene (2014) indicate that security culture comprises three dimensions: firstly, top management commitment to security, which refers to the extent top management considers security as an important organisational priority; secondly, security communication, which refers to how the organisation or the company makes its employees aware of its security policies; and thirdly, computer monitoring, which refers to the extent to which users or employees believe that their computing and Internet activities are monitored by their organisation.

In this study, this theme was generated by adapting these three dimensions for application to the e-government environment, based on the outcome of the focus group discussion: the first dimension centres on the extent to which the government is interested in information security and considers it to be an important priority from the perspective of its citizens; the second dimension concerns the extent to which the government seeks to make citizens aware of security policies and accordingly provides them with advice on security; the third dimension is concerned with the extent to which citizens believe their Internet activities are monitored by the government.

Participant A7 stated that, 'The government should take more interest in information security. Also, it should make clear that it will help citizens when they face a security problem. This will make them feel that their applications for e-government services will be secure'. This participant also said, 'I suggest that the government mentions that the e-government websites are secure and protected to increase the trust levels of those who are worried about the security of the services. Failing to mention these things may make citizens feel that the

government is not interested in security, and therefore, they feel the e-government website is not secure'. Participant B1 confirmed the role of government interest, pointing out that, 'In a neighbouring country, the government makes e-government security a high priority. If I was a citizen in that country, I would feel confident using their services whenever I needed them'. Furthermore, Participant A1 mentioned that, 'The government is interested in information security, and it is monitoring the activities of citizens using the Internet'. Participant A6 interrupted, saying, 'The monitoring definitely exists, but it is based on priority'. Participant B4 pointed out the advantages of monitoring Internet activities, and said, 'Identity theft will be reduced if citizens know that the government is monitoring their Internet activities'. Participant A5 brought up security advice from the government, saying, 'The security advice on the e-government websites is very low when compared with that available even in the street and the media'.

6.5. Discussion

Several factors that influence end users' perception of e-government security were discussed in this chapter. The participants stated that tangible security features influence their perception of e-government security. For example, one participant mentioned that he checked for the presence of a padlock icon when he was using e-government services. However, such behaviour depends on the users' security awareness and knowledge about the purpose of these features. Users who do not know the goal of these features will not pay attention to them, whether they exist or not. Generalisation of this result might then depend on public awareness, which could be different in developed and developing countries. Thus, the important role an awareness of information security could play in the use of e-government services is mentioned in this chapter.

One important factor that influences end users is the quality of the user interface. The participants mentioned that they make an initial assessment of e-government security based on the usability and quality of the user interface. Websites that are not well designed in these respects give end users the impression that they may also not be well designed in terms of security. Thus, government websites should be designed so they are easy to use and operate smoothly to make users feel that they are well designed in relation to security. It was observed that several government websites try to provide many services but do not pay enough intention to the user interface design and service delivery, which may affect users' adoption of these services in general and their perception of the website's security level in particular.

The government plays a very important role in increasing citizens' trust in the level of e-government security. As mentioned above, if the government takes an interest in the security of e-government services, this will increase citizens' trust and positively influence their perception regarding the level of e-government security. Governments can show their citizens how interested they are in making e-services secure in several ways, such as by providing security tips in the media, on the street and on government websites. Also, governments should monitor Internet activities to protect the information of their citizens from any person attempting to violate the information security policy.

Cybersecurity law plays an important role in end users' perceptions of e-government security. However, this may depend on the efficiency of the cybersecurity law in a specific country as it varies from one country to another. Cybersecurity law may help reduce the number of attacks as hackers knowing that they will be punished for criminal behaviour may act as a deterrent. Also, cybersecurity law should help protect citizens' privacy. In Saudi Arabia, there might be an issue in future with the national identity number as the e-government

services provided to Saudi citizens are linked with this number. Thus, when e-government reaches the final stage and all the services are linked with the e-government portal, the privacy of Saudi citizens may be threatened as hackers might be able to access all the services linked with their national identity numbers. Thus, the level of security might need to be improved when the e-government program reaches an advanced level of maturity.

It can be observed from the above findings that the government is more responsible for making the end users feel secure when using e-government services as the three identified factors are offered by the government which are cybersecurity law, security culture and user interface design. The rest factors are based on the knowledge and experience of the end users in information security which are tangible security features and general information security awareness and these factors did not have positive impact.

6.6. Conclusion

This chapter provided insight into how the factors influencing end users' perceptions of e-government security were identified. This was done by applying the Grounded Theory procedure. Two focus groups were used for data collection. The factors that influence end users' perception of e-government security were identified and then put into five categories: tangible security features, general information security awareness, user interface quality, cybersecurity law and security culture. The next chapter considers these five categories when developing research hypotheses. These categories will represent the initial security antecedences in the research model. The results from this chapter will be validated by conducting a quantitative study, as will be shown in the next chapter.

7. The role of security in e-government adoption

7.1. Introduction

This chapter focuses on developing the research model and hypotheses for investigating the role of security in e-government adoption. The constructs of the research model will be explained. These constructs can be divided into three groups: the first group is the security antecedents; the second group is security, privacy and trust constructs; and the third group is UTAUT2 constructs. In addition, the development of the research hypotheses that explain the relation between the constructs will be described. As this phase is a quantitative study, the methodology used for collecting the data will be explained, which is a questionnaire method. This includes how the questionnaire was designed, and further provides more information pertaining to the participants involved in this study. Moreover, the questionnaire used to measure the research model constructs have been provided in this chapter, along with their sources. Finally, a conclusion of this chapter will be provided at the end.

7.2. Research Model: Constructs and Hypotheses

After investigating and determining the initial security antecedents in previous chapter, the research investigated the impact of security and its antecedents in e-government adoption. Thus, the research model used in this study was based on the UTAUT2. However, two constructs from UTAUT2 were excluded: firstly, price value as the use of e-government services is free of charge in Saudi Arabia; and secondly, hedonic motivations as e-government services are not used for entertainment purposes. Moreover, the influence of demographical variables is not included in this study as these variables are used for initial adoption research. Recent studies in e-government and e-services showed a tendency to exclude these variables (Krishnaraju *et al.*, 2015; Ovais Ahmad *et al.*, 2013; Venkatesh *et al.*,

2011; Zhou, 2011). The actual usage also was not included in this study as the current work focuses on behaviour intention only. Furthermore, recent studies in e-government adoption have centred on behaviour intention only, therefore excluding actual usage (Hung *et al*., 2013; Krishnaraju *et al*., 2013; Lian, 2015). Security construct, trust and privacy were added to the research model as trust is influenced by security and privacy. The total constructs and hypotheses are described as follows:

7.2.1. Security Antecedents

The results from the first phase showed that five initial security antecedents influence end users' perceptions of e-government security. Thus, the following research hypotheses were derived from these antecedents:

Hypothesis 1: Tangible security features have a positive influence on the perception of e-government services security.

Hypothesis 2: General information security awareness has a positive influence on the perception of e-government services security.

Hypothesis 3: User interface quality has a positive influence on the perception of e-government services security.

Hypothesis 4: Cyber-security law has a positive influence on the perception of e-government services security.

Hypothesis 5: Security culture has a positive influence on the perception of e-government services security.

7.2.2. Security, Privacy and Trust

The impact of trust on the adoption of e-government has been investigated widely. Trust in e-government has two components, namely trust in government (services provider) and trust in the Internet (enabling technology) (Carter and Bélanger, 2005). A number of studies have investigated these two components as separate constructs (Carter and Bélanger, 2005; Navarrete, 2010; Wang and Lo, 2013; Weerakkody *et al*., 2013), whilst other studies have investigated them as one construct in e-government adoption (Alshehri *et al*., 2012b; Shareef *et al*., 2011). Security and privacy both have been widely investigated as antecedents of trust in e-services research (Carter and Bélanger, 2005; Escobar-Rodríguez and Carvajal-Trujillo, 2014; Pavlou, 2001; Riquelme and Román, 2014; Shin, 2010). Security and privacy have been investigated in e-government as separate constructs (Belanche-Gracia *et al*., 2015) and also as one construct (Abu-Shanab, 2014; Sarabdeen *et al*., 2014). This research investigated the role of trust, security and privacy in the UTAUT2, examining trust as one construct and security and privacy as separate constructs. In e-commerce studies, Hartono *et al*. (2014) measured perceived security in Business to Citizens (B2C), e-commerce as a second-order construct that involved four first-order formative security dimensions, which are: confidentiality, integrity, availability and non-repudiation. Our research measured perceived security as a first-order construct that covers the original triad of information security, which is confidentiality, integrity and availability (CIA triad). As a result, the following hypotheses were developed:

Hypothesis 6: Security perception has a positive influence on trust in e-government services.

Hypothesis 7: Privacy perception has a positive influence on trust in e-government services.

Hypothesis 8: Trust has a positive influence on behaviour intention to use e-government services.

7.2.3. UTAUT2 Constructs

In this research, five independent variables from UTAUT2 were used, namely performance expectancy, effort expectancy, social influence, facilitating conditions and habit. In addition, one dependent variable, behavioural intention, was used. These five independent variables are explained as follows:

Performance expectancy: defined as 'the degree to which using a technology will provide benefits to consumers in performing certain activities' (Venkatesh *et al*., 2012). Performance expectancy was measured in this study as the degree of usefulness that end users perceived from using e-government services. This usefulness can be achieved by applying e-government servicers faster and accordingly saving the time of end users' when applying online. Performance expectancy has been recognised as positively influencing behaviour intention positively in e-government services (Alsaif, 2014; Alshehri and Drew, 2012; Ovais Ahmad et al., 2013; Weerakkody et al., 2013; Yahya et al., 2012). As a result, the following hypothesis has been proposed:

Hypothesis 9: Performance expectancy has a positive influence on behaviour intention to use e-government services

Effort expectancy: is defined as 'the degree of ease associated with consumers' use of technology' (Venkatesh *et al*., 2012). In this study, effort expectancy was measured as how end users perceived the ease of use of e-government services. This includes how it is easy for them to learn how to apply and how it is easy for them to be skilful in the use of e-

government services. Effort expectancy has been found to positively influence behaviour intention in e-government services (AlAwadhi and Morris, 2008; Alshehri *et al.*, 2012a; Lian, 2015; Ovais Ahmad *et al.*, 2013; Weerakkody *et al.*, 2013; Yahya *et al.*, 2012). Thus, the following hypothesis has proposed:

Hypothesis 10: Effort expectancy has a positive influence on behaviour intention to use e-government services.

Habit: defined as 'the extent to which people tend to perform behaviours automatically because of learning' (Venkatesh *et al.*, 2012). In this study, habit was measured as how habit obtained from using e-government services influences end users in their continuance intention of using the services. Venkatesh *et al.* (2012), in UTAUT2, suggests that habit plays an important role in influencing end users in relation to continence intention to use the new technology. Thus, several studies have been conducted in mind of investigating the role of habit in the behaviour intention of using e-services; the results show that habit positively influences behaviour intention (Escobar-Rodríguez and Carvajal-Trujillo, 2014, 2013). Thus, the following hypothesis has proposed:

Hypothesis 11: Habit has a positive influence on behaviour intention to use e-government services.

Social influence: is defined as 'the extent to which consumers perceive that important others (e.g., family and friends) believe they should use a particular technology' (Venkatesh *et al.*, 2012). In this study, social influence is measured concerning the extent to which end users are influenced by their family, friends and others in the use of e-government services. Social influence has been found to positively influence behaviour intention in e-government services

(Alsaif, 2014; Lian, 2015; Ovais Ahmad et al., 2013; Weerakkody et al., 2013; Yahya et al., 2012). As a result, the following hypothesis has proposed:

Hypothesis 12: Social influence has a positive influence on behaviour intention to use e-government services.

Facilitating conditions: refers to 'consumers' perceptions of the resources and support available to perform a behaviour' (Venkatesh *et al.*, 2012). In this study, facilitating conditions were measured as the availability of resources necessary in the use of e-government services. These include the basic knowledge for using e-government services and in getting help from others when facing difficulties in the use of e-government services. Alsaif (2014) divides facilitating conditions into four constructs, namely computer self-efficacy, availability of resources, information quality and system quality, whilst other studies in e-government use the original construct of facilitating conditions in UTAUT. The role of facilitating conditions has been investigated in e-government services; it was found to positively influence behaviour intention (AlAwadhi and Morris, 2008; Alshehri *et al.*, 2012a; Ovais Ahmad *et al.*, 2013; Yahya *et al.*, 2012). As a result, the following hypothesis has proposed:

Hypothesis 13: Facilitating conditions have a positive influence on behaviour intention to use e-government services.

In the study, behaviour intention is defined as the degree to which end users intend to continue using e-government services. This construct was measured by three items, adapted from Venkatesh *et al.* (2012); these three items also have been used to investigate continuance intention (Venkatesh *et al.*, 2011).

Based on the hypotheses above, the research model has been designed and the relations between the constructs that represent the research hypotheses described. Thus, Figure 7.1 shows the research model and hypotheses in this research.

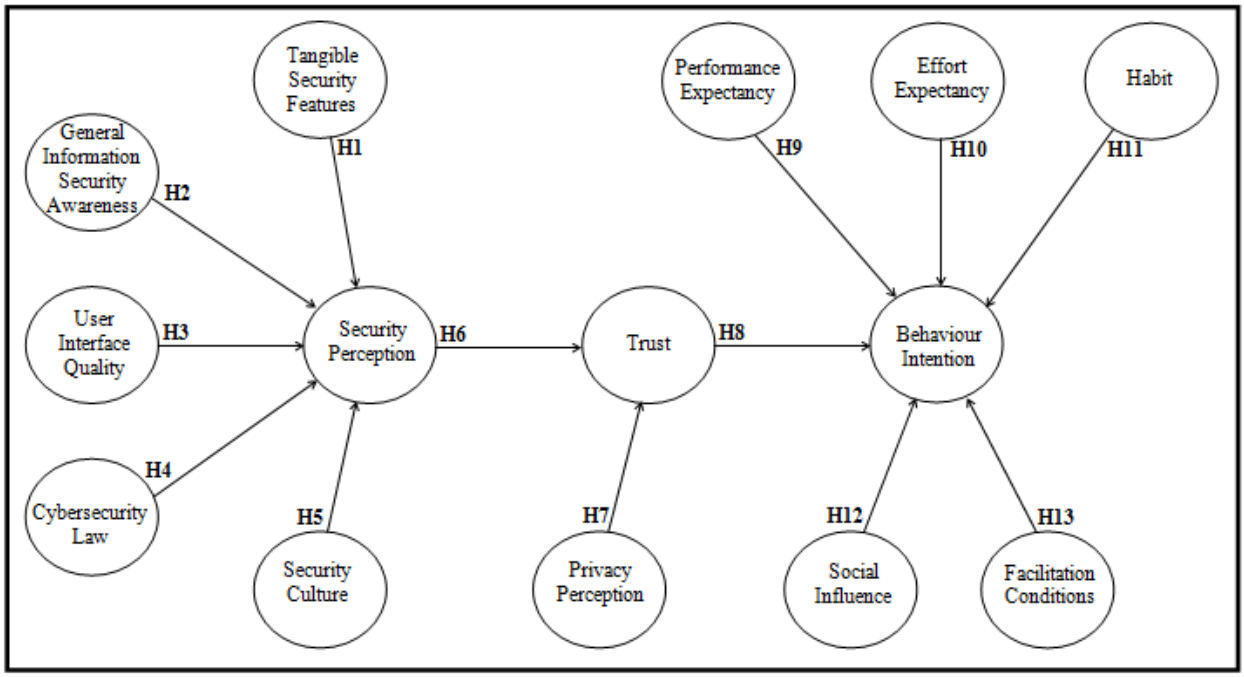

Figure 7.1: Research model

7.3. Questionnaire Methodology

7.3.1. Questionnaire Design

The questionnaire consisted of 46 items on a Likert scale (1–5) that ranged from 'strongly disagree' to 'strongly agree'. The questionnaire, which was designed in both the Arabic and English languages, was distributed on the Internet via email, social networks and mobile apps. The questionnaire was hosted online by the Centre for Security, Communications and Network Research (CSCAN) at Plymouth University. There were three main sections in the survey: The first section consisted of six questions asking for general information pertaining to the respondents in relation to age, gender, educational background, employment status, Internet usage and e-government usage. The second section consisted of 16 items, which

covered the security antecedents obtained from the qualitative study. The third section comprised 30 items covering security, privacy and trust (12 items). It also covered the UTAUT2 constructs (18 items). This section covered the factors influencing behaviour intention to use e-government service, and highlighted the role of security in behaviour intention. The survey began with a consent question to confirm that the age of the participant was 18 or above and also to ensure he/she understood the conditions and agreed to taking part in the survey. The survey was written in as simple a way as possible as it was for the general public and so needed to be clear and easy to understand. The survey was tested and reviewed by both academic staff and members of the public to ensure that it was written in the right way. It also was approved by the faculty ethics committee.

7.3.2. Participants

The total number of participants from Saudi Arabia who answered the survey in full totalled 635. However, ten of the participants were eliminated as they had not used e-government services before; behaviour intention in UTAUT2 is based on continuance intention, and thus previous use of e-government services was a mandatory requirement. The majority of the participants were male, whilst females accounted for only 19.8%. In addition, 71.8% of the participants were between 25 and 40 years old. A total of 89.6% of the participants had at least a diploma degree. 66.7% of the participants were government employees, and 72.2% of the total participants had ten or more years' experience in the use of the Internet. Table 7.1 shows the full demographic information of the participants.

Demographic Variable	Categories	Response Frequency	Percent
Gender	Male	501	80.2
	Female	124	19.8
Age (years)	18 - 24	83	13.3
	25 – 30	189	30.2
	31 – 40	260	41.6
	41 – 50	81	13.0
	50+	12	1.9
Education level	High School	62	9.9
	Diploma/ Bachelor	362	57.9
	Master/ Doctorate	198	31.7
	Other	3	0.5
Occupation	Student	92	14.7
	Government employed	417	66.7
	Self-employed	58	9.3
	Other	58	9.3
Internet experience	Less than 1 year	2	0.3
	1 - 3	4	0.6
	4 - 10	168	26.9
	10+	451	72.2
E-government usage	Rarely	47	7.5
	Sometimes	207	33.1
	Often	213	34.1
	Always	158	25.3

Table 7.1: Participant demographics

7.3.3. Measurement

All of the questionnaire items, with the exception of three, were adapted from previous studies. Some of the adapted items were modified to be suitable for the purpose of this research.

For measuring the security antecedences, the researcher used four items to measure the Tangible Security Features (TSF). Two of these factors were adapted from the study of Halaweh (2012), as the study measured TSF in e-commerce. The third item was adapted from the study of Ma and Pearson (2005), who used this measurement for their study, focusing on the ISO 17799 best practices in Information Security Management (ISM). The fourth item

was developed for this study to represent the use of two-factor authentications, as the participants mentioned in the focus group sessions. The researcher measured the General Information Security Awareness (GISA) by three items adapted from Bulgurcu *et al*. (2010); an empirical study was completed to investigate the information security policy compliance based on beliefs and Information Security Awareness (ISA). ISA was measured as a second-order construct, which involved GISA and Information Security Policy (ISP). In this study, GSIA was considered based on the results of the qualitative study only. User Interface Quality (UIQ) was measured by three items; two of them were adapted from the study of Alshehri and Drew (2012), whose study sought to investigate the impact of website quality on e-government adoption, whilst the third item was adapted from the study of Kamoun and Halaweh (2012), which focused on the impact of UIQ in e-commerce security. The researcher used three items to measure the Cybersecurity Law (CL); two of these items were developed for this study to be suitable to the findings of the qualitative study, whereas the third item was adapted from the study of Ma and Pearson (2005). Security Culture (SC) was measured in this study with three items that have been adapted from the study of D'Arcy and Greene (2014). They measured security culture in organisations as a second-order construct. This construct has three sub-constructs, which are top management commitment, security communication and computer monitoring. In this study, security culture was measured as a first-order construct containing an item from each of three sub-constructs, as utilised by D'Arcy and Greene (2014) in the measurement of security culture.

Security perception was measured by five items that have been adapted from the study of Shin (2010) and Flavián and Guinalíu (2006). Shin (2010) investigated the effects of security, privacy and trust in the adoption of social networking, whereas Flavián and Guinalíu (2006) conducted a study to confirm that security, privacy and trust are the three basic elements of

loyalty to a website. In this study, the researcher measured security perception as a first-order construct that covers the original triad of information security, which is confidentiality, integrity and availability (CIA triad). Privacy perception has been measured in this study as a first-order construct containing three items. There items also were adapted from the studies of both Shin (2010) and Flavián and Guinalíu (2006). Trust has been measured in this study with four items that were adapted from the study of Alshehri *et al*. (2012), whose work investigated the effect of trust in e-government adoption in Saudi Arabia. Thus, the research adapted these four items exactly in an effort to measure the trust variable as in this study, which can be considered an extension of the study by Alshehri *et al*. (2012). Using the same items in both studies is helpful for validating the results.

UTAUT2 constructs items were adapted from Venkatesh *et al*. (2003) and Venkatesh *et al*. (2012) with the exception of one item, which was adapted from Alshehri *et al*. (2012) to measure the performance expectancy. Each of the UTAUT2 constructs has three items. The difference between UTAUT and UTAUT2 is that the habit construct exists in only UTAUT2, whilst the behaviour intention in UTAUT2 is focused on the continuance intention as it is mainly for post-adoption research. Table 7.2 shows the questionnaire items and their sources.

Code	Items	Source
Tangible Security Features (TSF)		**4 items**
TSF1	I check the presences of http(s) in the URL when I use e-government services.	(Halaweh, 2012)
TSF2	I check the small padlock icon on e-government websites.	(Halaweh, 2012)
TSF3	Government websites require users to follow security practices in the selection and use of passwords.	(Ma and Pearson, 2005)
TSF4	Government websites has useful mechanisms to verify my identity (such as password + SMS).	Developed for this study
General Information Security Awareness (GISA)		**3 items**
GISA1	Overall, I am aware of the potential security threats and their negative consequences.	(Bulgurcu *et al*., 2010)
GISA2	I have sufficient knowledge about the cost of potential security problems.	(Bulgurcu *et al*., 2010)
GISA3	I understand the concerns regarding information security and the risks they pose in general.	(Bulgurcu *et al*., 2010)

User Interface Quality (UIQ)		**3 items**
UIQ1	Government websites looks organised.	(Alshehri and Drew, 2012)
UIQ2	Government websites look secure and safe for carrying out transactions.	(Alshehri and Drew, 2012)
UIQ3	Website navigation in government websites is easy.	(Kamoun and Halaweh, 2012)
Cybersecurity Law (CL)		**3 items**
CL1	The government has disciplinary procedures for dealing with citizens who violate information security policy.	(Ma and Pearson, 2005)
CL2	Anti-cyber-crimes law is helpful for reducing cybercrimes.	Developed for this study
CL3	Anti-cyber-crimes law is helpful for protecting citizens' private information.	Developed for this study
Security Culture (SC)		**3 items**
SC1	I believe that citizens' Internet activities are monitored by the government.	(D'Arcy and Greene, 2014)
SC2	The government considers information security an important priority	(D'Arcy and Greene, 2014)
SC3	The government provides useful security tips to increase the citizens' security awareness.	(D'Arcy and Greene, 2014)
Security Perception (SP)		**5 items**
SP1	In general, I feel secure using e-government services.	(Shin, 2010)
SP2	I believe the information I provide with government websites will not be manipulated by inappropriate parties	(Shin, 2010)
SP3	I am confident that the private information I provide with government websites will be secured.	(Shin, 2010)
SP4	I think government websites have sufficient technical capacity to ensure that the data I send will not be intercepted by hackers.	(Flavián and Guinalíu, 2006)
SP5	I think government websites have sufficient technical capacity to ensure that the data I send cannot be modified by a third party.	(Flavián and Guinalíu, 2006)
Privacy Perception (PP)		**3 items**
PP1	I think e-government shows concern for the privacy of its users.	(Flavián and Guinalíu, 2006)
PP2	I feel safe when I send personal information to e-government.	(Flavián and Guinalíu, 2006)
PP3	I am not concerned that the information I submitted on e-government could be misused.	(Shin, 2010)
Trust (TR)		**4 items**
TR1	The Internet is trustworthy	(Alshehri *et al*., 2012b)
TR2	I have confidence in the technology used by government agencies to operate the e-government services	(Alshehri *et al*., 2012b)
TR3	Government agencies can be trusted to carry out online transactions faithfully	(Alshehri *et al*., 2012b)
TR4	I believe that e-government services are trustworthy	(Alshehri *et al*., 2012b)
Behaviour Intention (BI)		**3 items**
BI1	I intend to continue using e-government services in the future.	(Venkatesh *et al*., 2012)
BI2	I will always try to use e-government services in my daily life.	(Venkatesh *et al*., 2012)
BI3	I plan to continue to use e-government services frequently.	(Venkatesh *et al*., 2012)
Performance Expectancy (PE)		**3 items**

PE1	I find e-government services useful in my daily life	(Venkatesh *et al*., 2003)
PE2	Using e-government services help me accomplish things more quickly.	(Venkatesh *et al*., 2003)
PE3	Using e-government services would save citizens' time	(Alshehri *et al*., 2012b)
Effort Expectancy (EE)		**3 items**
EE1	It is easy for me to become skilful at using e-government services.	(Venkatesh *et al*., 2003)
EE2	I find e-government services easy to use.	(Venkatesh *et al*., 2003)
EE3	Learning how to use e-government services is easy for me.	(Venkatesh *et al*., 2003)
Habit (HT)		**3 items**
HT1	The use of e-government has become a habit for me.	(Venkatesh *et al*., 2012)
HT2	I must use e-government services.	(Venkatesh *et al*., 2012)
HT3	Using e-government has become natural to me.	(Venkatesh *et al*., 2012)
Facilitating Conditions (FC)		**3 items**
FC1	I have the resources necessary to use e-government services.	(Venkatesh *et al*., 2003)
FC2	I have the knowledge necessary to use e-government services	(Venkatesh *et al*., 2003)
FC3	I can get help from others when I have difficulties using e-government services.	(Venkatesh *et al*., 2003)
Social Influence (SI)		**3 items**
SI1	People who influence my behaviour think that I should use e-government services.	(Venkatesh *et al*., 2003)
SI2	People who are important to me think that I should use e-government services.	(Venkatesh *et al*., 2003)
SI3	People whose opinions that I value prefer that I use e-government services.	(Venkatesh *et al*., 2003)

Table 7.2: Questionnaire items and their sources

7.4. Conclusion

This chapter focused on the second phase, that is, the quantitative study. An amended UTAUT2 model was developed in view of investigating the role of security in e-government adoption. This model was developed by integrating security, privacy and trust with the constructs of the UTAUT2 model. In addition, the initial antecedences of security perception that were obtained from phase one were considered. Data from 625 participants were collected via a questionnaire. Moreover, the items used to measure the research model constructs were provided in this chapter with their sources. This chapter mainly focused on how the research model was designed and the research hypotheses developed. Thus, the next chapter shows how the research model was tested using the collected data, as mentioned in this chapter.

8. Model Assessment and Discussion

8.1. Introduction

After developing the research model in the previous chapter, this chapter shows how the research model will be assessed. The research model will be assessed using Structural Equation Modelling (SEM); thus, this chapter starts by providing an overview on SEM. Subsequently, an overview on the analysis process will be provided. The model assessment is based on two main parts. The first part involves the measurement model, with emphasis on the reliability and validity of the research model constructs and their items, meaning each construct will be analysed and the reliability, validity and other tests will be provided. The reliability is measured by Cronbach's alpha and composite reliability. The validity is measured by convergent and discriminant validity. The second part of model assessment is structural model. This part is focused on the relation between research model constructs and testing the research hypotheses. It also focuses on how the research model is fit. This chapter will also discuss the research hypotheses by dividing them into three groups: firstly, hypotheses related to the security antecedents, which are the factors influencing end users' perceptions of e-government security; secondly, hypotheses related to trust, security and privacy; and thirdly, hypotheses related to the constructs of the UTAUT2 model. The findings from testing each of the research hypotheses will be compared with the findings from previous studies.. At the end, the findings from testing the research model will be discussed

8.2. Structural Equation Modelling (SEM)

As has been highlighted by Hox and Bechger (1998), Structural Equation Modelling is recognised as an overall statistical modelling approach, commonly applied in the behavioural

sciences domain. It may be considered as path analysis or as a mix of factor analysis and regression. SEM emphasis commonly is placed on theoretical constructs; these are represented through latent factors. The links between the various constructs are detailed through the path or regression coefficients between factors.

Importantly, SEM is known to adopt a number of different types of model in depicting relationships between the variables observed, adopting the key objective to delivering a quantitative test of a theoretical model hypothesised by the researcher. In particular, a number of different theoretical models may undergo testing in SEM, hypothesising the way in which sets of variables define constructs, and how such constructs can be linked with one another (Schumacker and Lomax, 2004). Moreover, as stated by Schumacker and Lomax (2004), SEM analysis is focused on establishing the degree to which the theoretical model can be supported through the use of sample data.

A very generalised and simple framework focused on statistical analysis is provided through SEM, and is known to comprise a number of different traditional multivariate approaches, including regression analysis, factor analysis and discriminant analysis. SEMs commonly are viewed through a graphical path diagram. In this vein, the statistical model commonly is represented through a number of different matrix equations, as highlighted by Hox and Bechger (1998).

The majority of criticism centred on the use of SEM has focused on two main issues, as mentioned by Hox and Bechger (1998). The first issue is concerned with the sample size requires and the statistical assumptions made. Importantly, there has been much study focused on the importance of sample sizes in order to ensure strength in the results, as well as the need of normality assumption. Secondly, also as recognised by the scholars, the issue of

casual interpretation is highlighted when applying the SEM in a casual way. Notably, non-experimental data has been the focus of most SEM uses, with the final model interpreted as a casual one. This might be valid, but of course SEM lacks any capability to transform correlational data into casual conclusions.

The wide use of SEM is recognised as owing to four key factors, as detailed by Schumacker and Lomax (2004), namely the greater awareness of researchers in regard to the need to apply multiple observed variables in an effort to ensure more in-depth insight into their field of study. Basic statistical approaches only make use of a limited number of variables; these do not have the capacity to manage the more sophisticated theories being designed.

A second factor centres on the more wide-ranging acknowledgement afforded to the overall reliability and validity associated with measurement instrument scores. In particular, measurement error has become recognised as a key issue across a number of areas, whilst statistical analysis and measurement error in data have commonly been handled separately. As noted by Schumacker and Lomax (2004), SEM methods clearly take into account measurement error when completing the statistical analysis of data.

As the third factor, focus centres on the maturation of the SEM the past thirty years, specifically the capacity to analyse more advanced theoretical SEM frameworks.

The fourth factor is owing to the increased user-friendly nature of SEM software programs, with the majority of them Windows-based and able to generate program syntax internally. Accordingly, such programs are now easier to use than before and provide features comparable to other Windows-based software packages.

There are several SEM software, such as AMOS, SmartPLS, Mplus and WarpPLS. In this study, WarpPLS version 5.0 is used in order to assess the research model.

8.3. Analysis Process: An Overview

As has been stated by Ullman (2007), SEM is recognised as suitable owing to the fact it enables the answering of questions that engage the multiple regression analysis of factors of one evaluated dependent variable, in addition to a number of measured independent variables. SEM seeks to test theoretical models. It is common for two types of model to be involved. The first is a measurement model through which the theory is represented, with the measured variables assimilated with the aim of represent latent factors. The second is structural model which enables theory to be followed in establishing the links between model constructs.

Accordingly, the measurement model will begin with the analysis stage. This study applies the CFA (Confirmatory Factor Analysis) as its first method in mind of evaluating the measurement items for all constructs owing to the factors having been established previously. CFA is applied in order to validate and support not only the research model constructs' reliability but also the validity. This study assessed the reliability by both of Cronbach's alpha and composite reliability. It also evaluated the validity through examining both discriminant and convergent validity.

The second step is analysing the structure model. This has been assessed by testing the research hypotheses which represent the theoretical relations between the research model constructs. Also, the model fit has been assessed by interpreting Average path coefficient (APC), Average R-squared (ARS), Average block VIF (AVIF) and Goodness of Fit (GoF).

Figure 8.1 shows the steps of the research model assessment.

Model Assessment	Measurement model	Reliability	Cronbach's alpha
			Composite reliability
		Validity	Discriminant validity
			Convergent validity
	Structure model	Hypothesis testing	P Value
			β
			R^2
		Model fit	Average path coefficient (APC)
			Average R-squared (ARS)
			Average block VIF (AVIF)
			Goodness of Fit (GoF)

Figure 8.1: Steps of the research model assessment

8.4. Measurements Model Assessment

The measurement framework is the aspect linking measured variables to latent variables. Through the completion of the CFA, the measurement model undergoes testing. Following acceptable outcomes from the measurement model tests, there then can be the completion of structural model tests, in line with the theoretical hypotheses, structural model tests than can be completed.

CFA is acknowledged as a statistical approach applied in mind of testing a pre-specified link relationship of observed measures as stated by Elsheikh (2012). Moreover, CFA further enables the researcher to test whether the measures applied for a particular factor are consistent and measure the same factor. In the view of Klein (2007), CFA may be applied in order to validate the hypothesised theoretical constructs. Moreover, as noted by Hair *et al*., (2006), combining the CFA results with construct validity tests would further enable researcher to garner a more in-depth insight into the measures and their quality.

Hair *et al.* (2006) suggested that the factor loading for each item should be 0.5 or above. Thus, three items were deleted, as shown in Table 8.1. In this study, CFA were used to assess both of reliability and validity of research model constructs.

Item	Factor loading	Item	Factor loading	Item	Factor loading
TSF1	(0.894)	TR1	(0.686)	HT1	(0.871)
TSF2	(0.905)	TR2	(0.883)	HT2	(0.786)
TSF3	(0.347)*	TR3	(0.888)	HT3	(0.913)
TSF4	0.149)*	TR4	(0.880)	-	-
GISA1	(0.848)	PP1	(0.825)	SC1	0.423)*
GISA2	(0.860)	PP2	(0.886)	SC2	(0.864)
GISA3	(0.869)	PP3	(0.831)	SC3	(0.815)
UIQ1	(0.868)	BI1	(0.865)	EE1	(0.826)
UIQ2	(0.834)	BI2	(0.913)	EE2	(0.784)
UIQ3	(0.752)	BI3	(0.913)	EE3	(0.872)
CL1	(0.887)	PE1	(0.789)	FC1	(0.851)
CL2	(0.901)	PE2	(0.881)	FC2	(0.866)
CL3	(0.606)	PE3	(0.718)	FC3	(0.502)
SP1	(0.774)	SI1	(0.886)	-	-
SP2	(0.840)	SI2	(0.918)	-	-
SP3	(0.880)	SI3	(0.842)	-	-
SP4	(0.834)	-	-	-	-
SP5	(0.832)	-	-	-	-
* Item deleted					

Table 8.1: Factor loading

8.4.1. Reliability

In the view of Kline (2015), reliability is recognised as the extent to which scores in a specific sample are seen to be free from random measurement error, and is predicted as being one minus the proportion of total observed variance as a result of random error.

As shown in the majority of the literature, coefficient alpha is the most commonly reported reliability type. This statistic measures the internal consistency reliability, the extent to which there is consistency across the response items in a measure. Should there be low internal

consistency, the items' contents then also might be so heterogeneous that the complete score is not the best possible analysis unit for measurement.

Cronbach's alpha coefficient was used to investigate the reliability of constructs used in this research. Hair *et al.* (2006) suggest that Cronbach's alpha should be 0.70 or above; however, it has been mentioned that, should the items in the construct be six or less, Cronbach's alpha can be acceptable if it is 0.6 or above (Petrick and Backman, 2002). Thus, as the number of items in each construct is equal to less than six, a Cronbach's alpha value of 0.6 and higher was accepted in the research. This is consistent with various previous studies (Antony and Fergusson, 2004; Ha *et al.*, 2007; Petrick and Backman, 2002). In addition, Black and Porter (1996) indicated that a Cronbach's alpha of 0.6 or greater is adequate for constructs reliability. Four degrees of reliability were suggested by Hinton *et al.* (2014), namely excellent (0.90 and above), high (0.70 to 0.90), high-moderate (0.50 to 0.70) and low (0.50 and below). In this research, a Cronbach's alpha value for all constructs was above 0.6, as detailed in Table 8.2. Moreover, reliability may be tested through the application of composite reliability. Across all of the research model's constructs, the composite reliability should be more than 0.70 in order to be an acceptable value, as highlighted by Bagozzi and Yi (1988). Notably, Table 8.2 details the composite reliability results.

Construct	No. of Items	Cronbach's Alpha (α)	Comments
Tangible Security Features (TSF)	2	0.828	High Reliability
General Information Security Awareness (GISA)	3	0.822	High Reliability
User Interface Quality (UIQ)	3	0.754	High Reliability
Cybersecurity Law (CL)	3	0.724	High Reliability
Security Culture (SC)	2	0.681	High moderate Reliability
Security Perception (SP)	5	0.889	High Reliability
Privacy Perception (PP)	3	0.804	High Reliability
Trust (TR)	4	0.856	High Reliability
Behaviour Intention (BI)	3	0.879	High Reliability
Performance Expectancy (PE)	3	0.712	High Reliability

Effort Expectancy (EE)	3	0.770	High Reliability
Habit (HT)	3	0.819	High Reliability
Social Influence (SI)	3	0.609	High moderate Reliability
Facilitating Conditions (FC)	3	0.857	High Reliability

Table 8.2: Cronbach's alpha results

8.4.2. Validity

As defined by Kline (2015), validity centres on the accuracy and value of the inferences based on the scores, with information pertaining to score validity communicating to the researcher whether or not the test is able to achieve particular objectives. CFA was used for construct validity assessment, which was based on assessing both discriminant validity and convergent validity. In this research, discriminant validity was assessed by measuring the square root of the average variance extracted (AVE) of each construct, which is greater than other correlations (Fornell and Larcker, 1981). Table 8.3 shows that discriminant validity was satisfied. Composite reliability (CR) and AVEs were used to assess the convergent validity of the constructs. The construct has convergent validity if the AVE is 0.5 or higher and the CR is 0.7 or higher (Fornell and Larcker, 1981; Hair *et al.* 2006). Table 8.4 shows that the convergent validity across all constructs was accepted.

		1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	**TSF**	0.924													
2	**GISA**	0.457	0.859												
3	**UIQ**	-0.002	-0.037	0.819											
4	**CL**	0.079	0.102	0.304	0.810										
5	**SC**	0.024	0.022	0.521	0.432	0.871									
6	**SP**	-0.078	-0.061	0.660	0.415	0.564	0.832								
7	**PP**	-0.024	-0.036	0.596	0.417	0.509	0.796	0.848							
8	**TR**	-0.047	-0.095	0.634	0.441	0.567	0.785	0.758	0.839						
9	**BI**	0.086	0.163	0.291	0.270	0.225	0.330	0.331	0.338	0.897					
10	**PE**	0.119	0.197	0.207	0.318	0.209	0.295	0.274	0.290	0.656	0.799				
11	**EE**	0.133	0.211	0.247	0.234	0.112	0.208	0.181	0.202	0.452	0.500	0.828			
12	**HA**	0.157	0.220	0.255	0.251	0.132	0.238	0.221	0.193	0.616	0.593	0.610	0.858		
13	**SI**	0.205	0.280	0.229	0.229	0.149	0.231	0.220	0.207	0.532	0.492	0.593	0.659	0.758	
14	**FC**	0.131	0.202	0.236	0.246	0.208	0.235	0.247	0.258	0.408	0.394	0.278	0.411	0.406	0.882

Table 8.3: Discriminant Validity Results for the Measurement Model

Construct	AVE	CR	Comments
Tangible Security Features (TSF)	0.854	0.921	Accepted
General Information Security Awareness (GISA)	0.738	0.894	Accepted
User Interface Quality (UIQ)	0.672	0.859	Accepted
Cybersecurity Law (CL)	0.656	0.847	Accepted
Security Culture (SC)	0.758	0.862	Accepted
Security Perception (SP)	0.693	0.918	Accepted
Privacy Perception (PP)	0.719	0.884	Accepted
Trust (TR)	0.703	0.904	Accepted
Behaviour Intention (BI)	0.805	0.925	Accepted
Performance Expectancy (PE)	0.638	0.840	Accepted
Effort Expectancy (EE)	0.686	0.868	Accepted
Habit (HA)	0.737	0.893	Accepted
Social Influence (SI)	0.575	0.794	Accepted
Facilitating Conditions (FC)	0.779	0.913	Accepted
*** Accepted if the AVE ≥ 0.5 and CR ≥ 0.7**			

Table 8.4: Convergent Validity for the Constructs

8.5. Analysis of Research Model Constructs

This section provides further details of the analysis for each construct in the research model. It starts by providing statistical information about the correlation between the items of constructs.

Generally, between the items, the correlation coefficients are more than 0.3, which suggests their suitability for factor analysis (Coakes, 2005). In the view of Pallant (2013), a value of the corrected item-total correlation of less than 0.30 suggests that the variable is not measuring what is intended from the construct overall.

The factor loading for each item also is provided. As mentioned in Section 8.4, the factor loading for each item should be 0.5 or above. The average variance extracted (AVE) of each construct is provided, which is used for validity purpose. In addition, the Cronbach's alpha and composite reliability are described. In this study, the Cronbach's alpha is acceptable over

0.6 and composite reliability is acceptable at 0.7. Convergent validity also is provided, which is acceptable if AVE is greater than 0.5 and composite reliability is greater than 0.7 for each construct.

Furthermore, there is the provision of the KMO (Kaiser-Meyer-Olkin) measure, which represents the square correlation ratio between variables to the square partial correlation between variables (Kaiser, 1970). Moreover, Kaiser (1970) recommends an acceptance value should be no less than 0.5.

8.5.1. Tangible Security Features (TSF)

TSF was measured by four items. However, as the factor loadings for TSF3 and TSF4 were less than 0.5, they were eliminated and not considered in the analysis stage. The first two items are suitable for factor analysis as the correlation coefficients between these items is greater than 0.3. The factor loading for TSF1 was 0.894 and 0.905 for TSF2. The composite reliability for TSF construct was 0.921. Moreover, Cronbach's alpha was 0.828; this means that this construct has a high reliability, as mentioned by Hinton *et al.* (2004). The convergent validity is accepted as the AVE is 0.854 (more than 0.5) whilst the composite reliability is 0.921 (over 0.7). The KMO value for this construct is 0.5, which is the minimum acceptance value, as suggested by Kaiser (1970).

		TSF1	**TSF2**
Correlation	**TSF1**	**1.000**	0.707
	TSF2	0.707	**1.000**
Factor loading		0.894	0.905
Average Variance Extracted (AVE)		0.854	
Cronbach's alpha		0.828	
Composite reliability		0.921	
Convergent Validity		Accepted	
KMO test		0.500	

Table 8.5: Analysis of Tangible Security Features (TSF)

8.5.2. General Information Security Awareness (GISA)

GISA was measured by three items. The factor loadings for these three items were 0.848, 0.860 and 0.869. The correlation coefficients between these three items are greater than 0.3, which made them suitable for factor analysis. This construct has a high reliability as the Cronbach's alpha was 0.822 (over 0.6) and the composite reliability was 0.894 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is over 0.7 and the AVE is 0.738 (over 0.5). The KMO value for this construct is 0.71, which is greater than the minimum acceptance value (0.5).

		GISA1	**GISA2**	**GISA3**
Correlation	**GISA1**	**1.000**	0.585	0.605
	GISA2	0.585	**1.000**	0.630
	GISA3	0.605	0.630	**1.000**
Factor loading		0.848	0.860	0.869
Average Variance Extracted (AVE)		0.738		
Cronbach's alpha		0.822		
Composite reliability		0.894		
Convergent Validity		Accepted		
KMO test		0.719		

Table 8.6: Analysis of General Information Security Awareness (GISA)

8.5.3. User Interface Quality (UIQ)

UIQ was measured by three items. These items are suitable for factor analysis as the correlation coefficients between these items is greater than 0.3. The factor loadings for these items are 0.868, 0.834 and 0.752. The reliability for these constructs is high as the composite reliability is 0.859. The Cronbach's alpha is 0.754 (over 0.6). The convergent validity for this construct has met as the AVE is 0.672 (over 0.5) and the composite reliability is over 0.7. The KMO test value for this construct is acceptable (0.659) as it is more than 0.5.

		UIQ1	UIQ2	UIQ3
Correlation	**UIQ1**	**1.000**	0.619	0.485
	UIQ2	0.619	**1.000**	0.410
	UIQ3	0.485	0.410	**1.000**
Factor loading		0.868	0.834	0.752
Average Variance Extracted (AVE)		0.672		
Cronbach's alpha		0.754		
Composite reliability		0.859		
Convergent Validity		Accepted		
KMO test		0.659		

Table 8.7: Analysis of User Interface Quality (UIQ)

8.5.4. Cybersecurity Law (CL)

The CL construct was measured by three items; these three items are suitable for factor analysis as the correlation coefficients between them is greater than 0.3. The factor loading for these items were 0.887, 0.901 and 0.606. This construct has a high reliability as the Cronbach's alpha was 0.724 (over 0.6) and the composite reliability was 0.847 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is more than 0.7 and the AVE is 0.656 (over 0.5). The KMO value for this construct is 0.582 which is greater than the minimum acceptance value (0.5).

		CL1	CL2	CL3
Correlation	**CL1**	**1.000**	0.745	0.307
	CL2	0.745	**1.000**	0.348
	CL3	0.307	0.348	**1.000**
Factor loading		0.887	0.901	0.606
Average Variance Extracted (AVE)		0.656		
Cronbach's alpha		0.724		
Composite reliability		0.847		
Convergent Validity		Accepted		
KMO test		0.582		

Table 8.8: Analysis of Cybersecurity Law (CL)

8.5.5. Security Culture (SC)

SC was measured by three items; however, Item SC1 was eliminated as the factor loading was less than 0.5 (0.423). The correlation coefficients between these three items are greater than 0.3, which makes them suitable for factor analysis. The factor loadings for the remaining two items were 0.864 and 0.815. This construct has a high moderate reliability as the Cronbach's alpha was 0.681 (over 0.6) and the composite reliability was 0.862 (over 0.7). The KMO test value for this construct is 0.5, which is the minimum acceptance value.

		SC2	**SC3**
Correlation	**SC2**	**1.000**	0.516
	SC3	0.516	**1.000**
Factor loading		0.864	0.815
Average Variance Extracted (AVE)		0.758	
Cronbach's alpha		0.681	
Composite reliability		0.862	
Convergent Validity		Accepted	
KMO test		0.500	

Table 8.9: Analysis of Security Culture (SC)

8.5.6. Security Perception (SP)

The SP construct was measured by five items. The correlation coefficients between these five items are greater than 0.3, which makes them suitable for factor analysis. The factor loadings for these items are 0.774, 0.840, 0.880, 0.834 and 0.832. This construct has a high reliability as the Cronbach's alpha was 0.889 (over 0.6) and the composite reliability was 0.918 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is over 0.7 and the AVE is 0.693 (over 0.5). The KMO value for this construct is 0.819 which is greater than the minimum acceptance value (0.5).

		SP1	SP2	SP3	SP4	SP5
Correlation	**SP1**	**1.000**	0.615	0.623	0.514	0.497
	SP2	0.615	**1.000**	0.760	0.567	0.544
	SP3	0.623	0.760	**1.000**	0.615	0.645
	SP4	0.514	0.567	0.615	**1.000**	0.770
	SP5	0.497	0.544	0.645	0.770	**1.000**
Factor loading		0.774	0.840	0.880	0.834	0.832
Average Variance Extracted (AVE)		0.693				
Cronbach's alpha		0.889				
Composite reliability		0.918				
Convergent Validity		Accepted				
KMO test		0.819				

Table 8.10: Analysis of Security Perception (SP)

8.5.7. Privacy Perception (PP)

The PP construct was measured by three items. These three items are suitable for factor analysis as the correlation coefficients between these items is greater than 0.3. The factor loadings for these three items were 0.825, 0.886 and 0.831. This construct has a high reliability as the Cronbach's alpha was 0.804 (over 0.6) and the composite reliability was 0.884 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is over 0.7 and the AVE is 0.719 (over 0.5). The KMO value for this construct is 0.691, which is greater than the minimum acceptance value (0.5).

		PP1	PP2	PP3
Correlation	**PP1**	**1.000**	0.612	0.494
	PP2	0.612	**1.000**	0.624
	PP3	0.494	0.624	**1.000**
Factor loading		0.825	0.886	0.831
Average Variance Extracted (AVE)		0.719		
Cronbach's alpha		0.804		
Composite reliability		0.884		
Convergent Validity		Accepted		
KMO test		0.691		

Table 8.11: Analysis of Privacy Perception (PP)

8.5.8. Trust (TR)

TR was measured by four items. These items are suitable for factor analysis as the correlation coefficients between these items is greater than 0.3. The factor loadings for these items are 0.686, 0.883, 0.888 and 0.880. The reliability for this constructs is high as the composite reliability is 0.904. The Cronbach's alpha is 0.856 (over 0.6). The convergent validity for this construct has met as the AVE is 0.703 (over 0.5) and the composite reliability is over 0.7. The KMO test value for this construct is acceptable (0.799) as it is over than 0.5.

		TR1	**TR2**	**TR3**	**TR4**
Correlation	**TR1**	**1.000**	0.508	0.450	0.450
	TR2	0.508	**1.000**	0.721	0.696
	TR3	0.450	0.721	**1.000**	0.757
	TR4	0.450	0.696	0.757	**1.000**
Factor loading		0.686	0.883	0.888	0.880
Average Variance Extracted (AVE)		0.703			
Cronbach's alpha		0.856			
Composite reliability		0.904			
Convergent Validity		Accepted			
KMO test		0.799			

Table 8.12: Analysis of Trust (TR)

8.5.9. Behaviour Intention (BI)

BI construct was measured by three items. These three items are suitable for factor analysis as the correlation coefficients between these items is greater than 0.3. The factor loadings for these items were 0.865, 0.913 and 0.913. This construct has a high reliability as the Cronbach's alpha was 0.879 (over 0.6) and the composite reliability was 0.925 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is more than 0.7 and the AVE is 0.805 (over 0.5). The KMO value for this construct is 0.729 which is greater than the minimum acceptance value (0.5).

		BI1	BI2	BI3
Correlation	**BI1**	**1.000**	0.671	0.670
	BI2	0.671	**1.000**	0.779
	BI3	0.670	0.779	**1.000**
Factor loading		0.865	0.913	0.913
Average Variance Extracted (AVE)		0.805		
Cronbach's alpha		0.879		
Composite reliability		0.925		
Convergent Validity		Accepted		
KMO test		0.729		

Table 8.13: Analysis of Behaviour Intention (BI)

8.5.10. Performance Expectancy (PE)

PE construct was measured by three items. There is an issue with correlation coefficients between PE1 and PE3 as it 0.291, which should be greater than 0.3. However, PE3 was kept as it is close to 0.3. In addition, this item was validated in previous studies for measuring the PE construct. The factor loadings for these three items were 0.789, 0.881 and 0.718. This construct has a high reliability as the Cronbach's alpha was 0.712 (over 0.6) and the composite reliability was 0.840 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is over 0.7 and the AVE is 0.638 (over 0.5). The KMO value for this construct is 0.599, which is greater than the minimum acceptance value (0.5).

		PE1	PE2	PE3
Correlation	**PE1**	**1.000**	0.581	0.291
	PE2	0.581	**1.000**	0.483
	PE3	0.291	0.483	**1.000**
Factor loading		0.789	0.881	0.718
Average Variance Extracted (AVE)		0.638		
Cronbach's alpha		0.712		
Composite reliability		0.840		
Convergent Validity		Accepted		
KMO test		0.599		

Table 8.14: Analysis of Performance Expectancy (PE)

8.5.11. Effort Expectancy (EE)

EE construct was measured by three items. These three items are suitable for factor analysis as the correlation coefficients between these items is greater than 0.3. The factor loading for these items were 0.826, 0.784 and 0.872. This construct has a high reliability as the Cronbach's alpha was 0.770 (over 0.6) and the composite reliability was 0.868 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is over 0.7 and the AVE is 0.686 (over 0.5). The KMO value for this construct is 0.673, which is greater than the minimum acceptance value (0.5).

		EE1	**EE2**	**EE3**
Correlation	**EE1**	**1.000**	0.439	0.608
	EE2	0.439	**1.000**	0.536
	EE3	0.608	0.536	**1.000**
Factor loading		0.826	0.784	0.872
Average Variance Extracted (AVE)		0.686		
Cronbach's alpha		0.770		
Composite reliability		0.868		
Convergent Validity		Accepted		
KMO test		0.673		

Table 8.15: Analysis of Effort Expectancy (EE)

8.5.12. Habit (HT)

HT construct was measured by three items. These three items are suitable for factor analysis as the correlation coefficients between these items is greater than 0.3. The factor loadings for these three items were 0.871, 0.786 and 0.913. This construct has a high reliability as the Cronbach's alpha was 0.819 (over 0.6) and the composite reliability was 0.893 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is over 0.7 and the AVE is 0.737 (over 0.5). The KMO value for this construct is 0.660, which is greater than the minimum acceptance value (0.5).

		HT1	HT2	HT3
Correlation	**HT1**	**1.000**	0.480	0.741
	HT2	0.480	**1.000**	0.584
	HT3	0.741	0.584	**1.000**
Factor loading		0.871	0.786	0.913
Average Variance Extracted (AVE)		0.737		
Cronbach's alpha		0.819		
Composite reliability		0.893		
Convergent Validity		Accepted		
KMO test		0.660		

Table 8.16: Analysis of Habit (HT)

8.5.13. Social Influence (SI)

SI construct was measured by three items. These items are suitable for factor analysis as the correlation coefficients between these items is greater than 0.3. The factor loading for these items were 0.886, 0.918 and 0.842. This construct has a high moderate reliability as the Cronbach's alpha was 0.609 (over 0.6) and the composite reliability was 0.794 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is over 0.7 and the AVE is 0.575 (over 0.5). The KMO value for this construct is 0.703, which is greater than the minimum acceptance value (0.5).

		SI1	SI2	SI3
Correlation	**SI1**	**1.000**	0.755	0.584
	SI2	0.755	**1.000**	0.662
	SI3	0.584	0.662	**1.000**
Factor loading		0.886	0.918	0.842
Average Variance Extracted (AVE)		0.575		
Cronbach's alpha		0.609		
Composite reliability		0.794		
Convergent Validity		Accepted		
KMO test		0.703		

Table 8.17: Analysis of Social Influence (SI)

8.5.14. Facilitating Conditions (FC)

FC construct was measured by three items. There is an issue with correlation coefficients between SI1 and SI3 as it 0.193 which it should be great than 0.3. Also, the correlation between SI2 and SI3 as it is 0.231. Thus, is it clear that there is issue with item FC3. However, all three items were kept as they were adapted from the original UTAUT model. The factor loadings for these three items were 0.851, 0.866 and 0.502. This construct has a high reliability as the Cronbach's alpha was 0.857 (over 0.6) and the composite reliability was 0.913 (over 0.7). The convergent validity for this construct is satisfied as the composite reliability is over 0.7 and the AVE is 0.779 (over 0.5). The KMO value for this construct is 0.552, which is greater than the minimum acceptance value (0.5).

		FC1	**FC2**	**FC3**
Correlation	**FC1**	**1.000**	0.602	0.193
	FC2	0.602	**1.000**	0.231
	FC3	0.193	0.231	**1.000**
Factor loading		0.851	0.866	0.502
Average Variance Extracted (AVE)		0.779		
Cronbach's alpha		0.857		
Composite reliability		0.913		
Convergent Validity		Accepted		
KMO test		0.552		

Table 8.18: Analysis of Facilitating Conditions (FC)

8.5.15. Discussion

Two methods, Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA), can be used to analyse the latent variables in quantitative studies. EFA is usually applied if the factors have not been identified, and it helps the researcher to identify the constructs of the developed model. On the other hand, CFA is usually applied to test and confirm these constructs by assessing both the validity and reliability of each construct (Hair *et al.*, 2006).

This study mainly used CFA as the constructs of the research model had been identified. However, EFA was used as additional analysis to show that these constructs had been well developed. The results from analysis of the security antecedents showed that all five constructs had been well developed, as shown by the results from analysis of the EFA for each construct. In addition, the security, privacy and trust constructs had also been well developed, and the findings from analysis of the EFA for these constructs showed that they were suitable for use in CFA. With regard to the constructs of the UAUT2 model, the findings showed a correlation coefficient of 0.291 between PE1 and PE3. However, the PE3 item was kept in the constructs as it was still close to 0.3 and because it had been used and validated in a previous study on e-government adoption. Similarly, there was an issue with item FC3 as the correlation coefficient between FC3 and other items was less than 0.3. However, this item was also kept as it is an original item in the UTAUT model..

8.6. Structural Model Assessment

The structural model was analysed by testing the research hypotheses and the model fit. This step was performed after successfully completing the analysis of the measurement model and finding that the items and constructs were valid for evaluating the research model and testing the hypotheses. Figure 8.2 shows the result of analysing the research model and Table 5.13 summarises the research hypotheses.

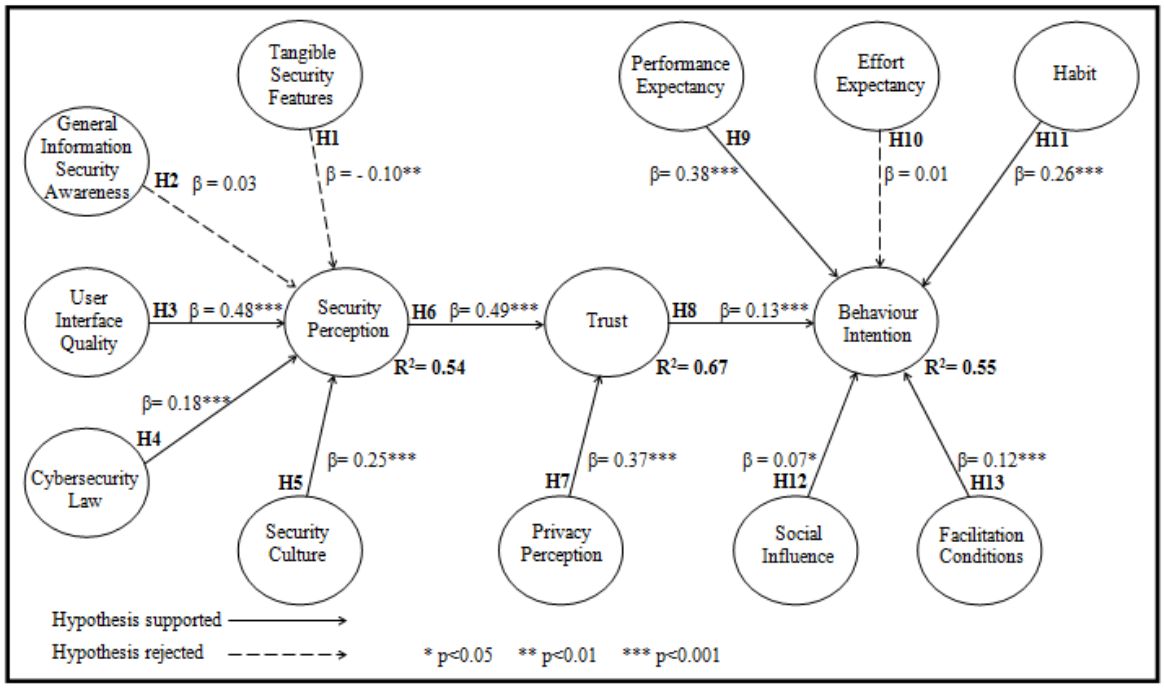

Figure 8.2: The results of analysing the research model

	Research hypotheses	Supported?
H1	Tangible security features have a positive influence on the perception of e-government services security.	No
H2	General information security awareness has a positive influence on the perception of e-government services security.	No
H3	User interface quality has a positive influence on the perception of e-government services security.	Yes
H4	Cyber-security law has a positive influence on the perception of e-government services security.	Yes
H5	Security culture has a positive influence on the perception of e-government services security.	Yes
H6	Security perception has positive influence on trust in e-government services.	Yes
H7	Privacy perception has positive influence on trust in e-government services.	Yes
H8	Trust has a positive influence on behaviour intention to use e-government services.	Yes
H9	Performance expectancy has a positive influence on behaviour intention to use e-government services	Yes
H10	Effort expectancy has a positive influence on behaviour intention to use e-government services.	No
H11	Habit has a positive influence on behaviour intention to use e-government services.	Yes
H12	Social influence has a positive influence on behaviour intention to use e-government services.	Yes
H13	Facilitating conditions have a positive influence on behaviour intention to use e-government services.	Yes

Table 8.19: Research hypotheses results

Model fit was assessed through the following measures: average path coefficient (APC), average R-squared (ARS) and average variance inflation factor (AVIF). It is recommended that the values for both the APC and ARS be significant at least at the 0.05 level, whilst the AVIF should be lower than 5. Table 5.14 shows that the model meets the requirements.

Indices	Value	Comments
Average path coefficient (APC)	0.220	P<0.001
Average R-squared (ARS)	0.586	P<0.001
Average adjusted R-squared (AARS)	0.583	P<0.001
Average block VIF (AVIF)	1.730	acceptable if <= 5, ideally <= 3.3
Average full collinearity VIF (AFVIF)	2.197	acceptable if <= 5, ideally <= 3.3
Tenenhaus GoF (GoF)	0.648	small >= 0.1, medium >= 0.25, large >= 0.36
Sympson's paradox ratio (SPR)	1.000	acceptable if >= 0.7, ideally = 1
R-squared contribution ratio (RSCR)	1.000	acceptable if >= 0.9, ideally = 1
Statistical suppression ratio (SSR)	1.000	acceptable if >= 0.7
Nonlinear bivariate causality direction ratio (NLBCDR)	0.885	acceptable if >= 0.7

Table 8.20: Model fit indices

8.7. Discussion

The results of the WarpPLS structural analysis are summarised in Figure 8.2. The overall results from this study show that user interface design, security culture and cyber-security law have a positive effect on security perception. In addition, security perception and privacy perception have a positive effect on trust. Moreover, performance expectancy, social influence, facilitation conditions, trust and habit have a positive effect on behaviour intention. In this section, the factors are discussed within three groups: firstly, hypotheses related to security perception; secondly, hypotheses related to trust; and thirdly, hypotheses related to UTAUT2 constructs.

8.7.1. Security Antecedents Constructs

The first group is hypotheses related to security perception, as investigated by H1 through to H5. With regarding to H1, the study shows that tangible security features do not have a positive effect on security perception, consist to the findings of Halaweh (2012). Furthermore, the findings show that tangible security features actually have a negative impact on security perception. This means that users who do not check these features still feel that e-government is secure, meaning they assessed security based on other factors. Also, this means that users who have checked these security features believe that e-government is not secure.

The findings also led to Hypothesis 2 being rejected; general information security awareness does not have a positive effect on security perception. Halaweh (2012) shows that a user's character is based on the security awareness gained from their experience and knowledge, which affects their security perception positively; however, the results in this study show that general information relating to security awareness does not have an effect on security perception. Such information might help users to understand security features and other security factors; however, it does not affect their security perception directly.

H3 tested the influence of user interface quality on security perception; the findings show that user interface quality has a strong positive effect on security perception. These findings are consistent with those of Kamoun and Halaweh (2012). The results show that user interface quality is the highest factor affecting security perception. Based on the results from this study, as well as from that of Kamoun and Halaweh (2012), it can be said that user interface plays an important role in security perception for both e-government and e-commerce.

The findings also show that cyber-security law has a positive effect on security perception, which supports H4. These findings are consistent with the qualitative findings in the first phase as the participants clearly indicated the importance of cyber-security law, which they believe reduces cyber-security crimes and protects citizens' data from being misused. This factor could be considered in future works focused on investigating privacy and its antecedents.

It was also found that security culture positively affects security perception, which supports H5. Thus, governments should create a security culture amongst their citizens by making it clear that they are interested in information security, providing more security advice to their citizens and monitoring the Internet activities of users. These three steps will make citizens feel secure when applying for e-government services. In this study, security culture was investigated as a first-order construct, whilst D'Arcy and Greene (2014) investigated the consideration as a second-order construct containing three different dimensions.

The findings from testing the research hypotheses related to the security antecedents in e-government show that only three factors, user interface design, security culture and cybersecurity law, positively influence end users' perception in e-government security, while tangible security features and general information security awareness do not have a positive influence. This means that the government is responsible for making citizens feel secure when using e-government services as the three influential factors depend on government support. The government should pay attention to the user interface design as it can make citizens feel that the service operates smoothly and is secure. In addition, the government should focus on improving the security culture by taking the following three steps. Firstly, the government should show citizens that it is interested in information security and make citizens' privacy and the security of their data a high priority. Secondly, the government

should provide citizens with security tips via the media, on the street and on government websites. This will increase citizens' awareness of information security and show them that the government is interested in making e-government services secure. Thirdly, the government should monitor citizens' Internet activities since this can be helpful when investigating cyber-crimes. It is not enough for the government to try to provide a high level of security for its e-services; it must also take action to make citizens feel that it is interested in information security in order to increase their confidence in using e-government services. Cybersecurity law also plays an important role in end users' perceptions of e-government security. The government should continuously improve the law to combat each newly identified cyber-crime, and there should be a clear punishment for each crime, as suggested by one of the security expert participants in the qualitative study.

8.7.2. Security, Privacy and Trust Constructs

The second group comprises the hypotheses related to trust. In this study, trust has two antecedents, namely security and privacy perceptions. The findings from this study show that trust has a positive effect on behaviour intention, which supports H8. The majority of studies in the Literature Review investigated the impact of trust on behaviour intention, which further shows that trust has a positive impact on behaviour intention. The findings from this study are thus consistent with those findings (Abu-Shanab, 2014; Alshehri, Drew and Alhussain, *et al.*, 2012; Bélanger and Carter, 2008; Fakhoury and Aubert, 2015; Lian, 2015; Shareef *et al.*, 2011; Weerakkody *et al.*, 2013). However, some research that investigated trust as two constructs showed that trust in technology does not has a positive impact on intention (Lee *et al.*, 2011; Wang and Lo, 2013). The explained variance of trust in the findings is 67%, whilst in Lian's (2015) study was only 9%.

Security perception also was found to have a positive effect on trust, which supports H6. The findings from this study are consistent with the findings of previous e-government studies (Lian, 2015; Shareef *et al.*, 2011), whilst other e-services studies (Bonsón Ponte *et al.*, 2015; T. Escobar-Rodríguez and Carvajal-Trujillo, 2014; C. Kim *et al.*, 2010; Kim *et al.*, 2011; Pavlou, 2001; Riquelme and Román, 2014; Roca *et al.*, 2009; Shin, 2010). This research is the first to investigate the antecedents of security perception in e-government services, and the findings show that the explained variance of security perception is 54%.

Privacy perception also was found to have a positive effect on trust, supporting H7. The findings are consistent with those of previous e-services studies (Escobar-Rodríguez and Carvajal-Trujillo, 2014; Riquelme and Román, 2014; Shin, 2010). In e-government studies, privacy was investigated with security as one construct, and the findings show that they positively affect trust (Abu-Shanab, 2014). However, the findings are contradicted by previous e-services studies (Bonsón Ponte *et al.*, 2015; Escobar-Rodríguez and Carvajal-Trujillo, 2014; Roca *et al.*, 2009). This might be because e-government services in Saudi Arabia are linked with the user's national identity number, which makes privacy important to Saudi citizens. Baldoni and Antonio (2012) indicated that using users' national identity number in e-government systems leads to several privacy risks.

8.7.3. UTAUT2 Constructs

The third group of hypotheses is related to UTAUT2 constructs. H9 tested the influence of performance expectancy on behaviour intention. The findings show that performance expectancy has a strong influence on behaviour intention. These findings are consistent with previous e-government studies (Abu-Shanab, 2014; Alshehri, Drew and Alhussain, *et al.*, 2012; Belanche *et al.*, 2014; Weerakkody *et al.*, 2013). The findings of Lian (2015) show that

performance expectance has no significant effect on behaviour intention to use the e-invoice service in Taiwan; this is because the e-invoice service in Taiwan is in a transitional stage and paper invoicing also is used as well.

H10 tested the influence of effort expectancy on behaviour intention. The findings show that effort expectancy has no significant effect on behaviour intention, which is contradicted by previous research into e-government (Alshehri, Drew and Alhussain, *et al.*, 2012; Lian, 2015; Weerakkody *et al.*, 2013). This might be because previous e-government studies have focused on initial intention, whilst this study focuses on post-adoption as the behaviour intention in UTAUT2 and is based on continuance intention. However, the findings in this study are consistent with the study of Alsaif (2014), which is the latest study to have applied the UTAUT model in e-government services adoption in Saudi Arabia as the findings from that study showed that effort expectancy has an insignificant impact on the behaviour intention for using e-government services.

The findings also show that habit is influenced by behaviour intention, supporting H11. This explains the importance of habit in relation to behaviour intention. Effort expectance plays an important role in the initial intention. However, the findings show that, when citizens become familiar with e-government and are used to using it, they will continue with the intention to use the service even if it becomes more complex. Escobar-Rodríguez and Carvajal-Trujillo (2013) conducted empirical research investigating the factors affecting the purchase of airline tickets online and established that effort expectance does not have a significant influence on the intention, whilst habit does, which is consistent with the findings. In addition, other empirical studies further highlight habit as being positively influenced by behaviour intention (Escobar-Rodríguez and Carvajal-Trujillo, 2014; Jiang and Deng, 2011).

H12 tested the impact of social influence on behaviour intention. The findings show that social influence has a positive impact on behaviour intention. These findings are consistent with the findings of previous e-government studies (Abu-Shanab, 2014; Lian, 2015; Weerakkody *et al.*, 2013; Yahya *et al.*, 2012). In addition, they are consistent with other studies on e-services (Ain *et al.*, 2015; Chen *et al.*, 2012; Escobar-Rodríguez and Carvajal-Trujillo, 2014; Mouakket, 2015; Sun *et al.*, 2014; Zhou and Li, 2014). However, the findings are contradicted by the findings of Alshehri (2012) and Alsaif (2014) who both investigated the critical factors affecting e-government acceptance in Saudi Arabia using UTAUT. Their findings show that social influence has no significant effect on behaviour intention. The findings show that social influence is at ($p < 0.05$), which is the lowest level of significance. This means that social influence is becoming important in relation to behaviour intention to use e-government services in Saudi Arabia. The reason for this might be the recent increased use of social network websites and applications amongst Saudi citizens (Al-homoud *et al.*, 2014).

H13 tested the impact of facilitation conditions on behaviour intention, and the findings show that behaviour intention is positively influenced by facilitation conditions. These findings are consistent with previous e-government studies (Alshehri, 2012; Ovais et al., 2013; Alsaif, 2014) and in e-service studies (Escobar-Rodríguez and Carvajal-Trujillo, 2014; Tomás Escobar-Rodríguez and Carvajal-Trujillo, 2013). However, the findings are contradicted by previous e-government studies, such as Lian (2015), who showed that facilitation conditions as a factor has no significant influence on behaviour intention in the use of e-invoice adoption. This might be due to the difference in platform used; Lian (2015) mentions that the platform most used in e-invoices is mobile devices, which are user-friendly, meaning facilitating conditions are not a significant issue. However, in e-government services in Saudi

Arabia, the platform most commonly used for applying e-government services is a laptop or desktop as shown in the results of the initial survey (**Error! Reference source not found.**). The findings show that behaviour intention variance explained by this research model is 55%.

8.8. Conclusion

This chapter has shown how the research model was assessed, that is, by assessing both the measurement and structure models. The research hypotheses were tested, and the findings show that user interface quality, cybersecurity law and security culture have a positive influence on security perceptions. However, two of the initial security antecedents were eliminated as they do not have a positive influence on security perceptions. Both security and privacy were positively influenced by trust, which is ranked as the third factor influencing end users to adopt e-government services. The next chapter will provide a summary and conclusion for the study. This includes answering the research questions, highlighting the research contributions and noting the limitations of the study as well as making suggestions for future work.

9. Conclusion

9.1. Introduction

After analysing and assessing the research model, this chapter will provide a conclusion by providing a general overview of the study. It also addresses the research questions and answers these questions based on the research findings. The final research model will be provided, which is based on accepted hypotheses, excluding non-supported hypotheses. The conclusion will highlight the main significant contributions of this study for both theoretical and practical sides. Five main limitations in the study will be mentioned, along with suggestions as to the direction for future works at the end of the chapter.

9.2. The Research Overview

Lack of security is considered one of the challenges facing the end users of e-services in general and e-government specifically. However, the role of security in e-government post adoption studies was not investigated, especially by technology acceptance models. Thus, this research sought to fill the research gap by investigating the role of security in the behaviour intention for using e-government services. The research also tried to investigate the factors influencing end users' perception in e-government security to provide a better understanding of the phenomena. Thus, the research followed a mixed-methods approach that started with a qualitative study to determine the initial security antecedences followed by a quantitative study to confirm these security antecedences and accordingly determine the role of security in e-government adoption. An initial survey has been conducted at the beginning of this research to determine the security challenges facing end users in e-government and to further investigate the status of e-government security based on end users' perspectives. The data have been collected from 189 participants; the results from this survey helped the research

during the completion of the first phase of this study, besides the information obtained from the Literature Review. The aim of this phase was to determine the factors influencing end users' perceptions in e-government security. Thus, two focus groups were carried out in this phase to discuss and investigate these factors. The first group has 7 participants who are general users of e-government services, whilst the second group has 6 participants who are experts in information security and have good experience in e-government. The research used the Grounded Theory method to analyse the qualitative results. The findings from the first phase were used in the second phase to represent the security antecedences in the research model. The second phase was a quantitative study aiming at investigating the role of security in behaviour intention of using e-government services. This has been done by developing a research model by integrating trust, security and privacy with the UTAUT2 model. The data in this phase were collected from 625 participants who had used e-government services before. For analysing the research model and testing the research hypotheses, Structural Equation Modelling was used by adopting WarpPLS 5.0 software. The results from this phase identify the role of security and accordingly confirm the factors influencing end users' perceptions of e-government security. The findings showed that security strongly influences trust in e-government, which is ranked as the third factor influencing behaviour intention for using e-government services after performance expectance and habit. The findings also show that the security perception in e-government is influenced by three factors, namely user interface quality, cybersecurity law and security culture. Statistically, this model explained 54% of the variance influencing security perceptions and 55% of the variance influencing the behavioural intention of using e-government services.

9.3. Achievements of research program

This research has achieved the objectives that were mentioned in Chapter 1, as is outlined below:

1. The research reviewed the previous studies that have investigated the challenges that face end users in the adoption of e-government, one of which is a lack of security.

2. The research critically reviewed the models and theories of acceptance technology that were used to investigate the adoption of e-government services. This step also incorporated a review of the empirical studies that have used these models and theories to investigate the factors that influence the adoption of e-government services.

3. An initial survey was conducted to investigate the security challenges that face end users in adopting e-government services. Data from 189 participants were collected and analysed for purposes of determining these challenges.

4. Two focus groups were conducted to investigate the factors that influence end users' perception of e-government security. The findings from the initial survey were discussed with the groups in addition to the existing security challenges that were mentioned in the literature review. The findings from this step were used to determine the security antecedents of e-government adoption.

5. The research model was developed based on UTAUT2 to investigate the role of security and its antecedences in e-government adoption. The research hypotheses were also developed and discussed in this step.

6. The research model was evaluated, and the research hypotheses were tested by using Structural Equation Modelling (SEM). Data from 625 participants were used for this purpose, and the final model was confirmed.

7. The findings from evaluating the research model were discussed and compared with previous studies in this field. Suggestions for future work were provided at the end of this step.

Several conference and journal papers were published based on this research. In addition, feedback and comments from experts in this field were considered in an attempt to improve the quality of this research in order to make a valid contribution in the context of e-government security.

9.4. Answering the Research Questions

There were two main research questions in this study, as mentioned in Section 1.4. This section provides answers for these questions based on the findings of the study.

9.4.1. First Question

As the first question focused on what factors influence end users' perceptions on e-government security, this study has followed a mixed approach to answer this question. The study firstly conducted a qualitative study to determine these factors based on end users' perspectives. The results from this study provide the initial five main factors, which are Tangible Security Features (TSF), General Information Security Awareness (GISA), User Interface Quality (UIQ), Cybersecurity Law (CL) and Security Culture (SC). However, after conducting the second step, which is a quantitative study with data from 625 participants to confirm the effected factors, the results from this study show that there are only three main

factors that influenced the end users' perceptions in e-government security, which are User Interface Quality (UIQ), Cybersecurity Law (CL) and Security Culture (SC). Thus, based on the results of the study, it can be stated that these three factors are considered as the security antecedences in e-government adoption research. The results also have shown that the security perception variance explained in this model was 54%.

9.4.2. Second Question

The second question focused on the role of security in e-government adoption. In order to answer this question, this research conducted a quantitative study to investigate the impact of security in e-government adoption. An amended UTAUT2 model was used to investigate the critical factors influencing the behaviour intention to use e-government services by integrating UTAUT2 constructs with trust, security and privacy. The results indicate that trust is a mediator between security perception and behaviour intention, which is ranked as the third important factor influencing behaviour intention after performance expectancy and habit. The results indicate that security perception has a strong influence on the trust of e-government services.

9.5. The Final Research Model

After analysing and assessing the research model and testing the research hypotheses, it has come to light that there is a need to redesign the research model based on the supporting hypotheses and the exclusion of non-supported hypotheses. The findings have shown that there are three security antecedences that influence end users' perceptions in e-government security, which are user interface quality, cybersecurity law and security culture. Two constructs of security antecedences were eliminated as the hypotheses related to these constructs were not supported, which are tangible security features and general information

security awareness. Trust, security and privacy constructs were kept in the final model as they played important roles in e-government adoption. Both security and privacy were found to strongly influence trust in e-government services. In addition, the findings have shown that trust has a positive influence on behavioural intention for using e-government services. With regards to UTAUT2 constructs, only the effort expectancy construct was eliminated as the findings show that there is an insignificant influence on behaviour intention, whilst the remaining constructs were kept in the final model, which are performance expectancy, habit, social influence and facilitating conditions. Figure 9.1 shows the final research model.

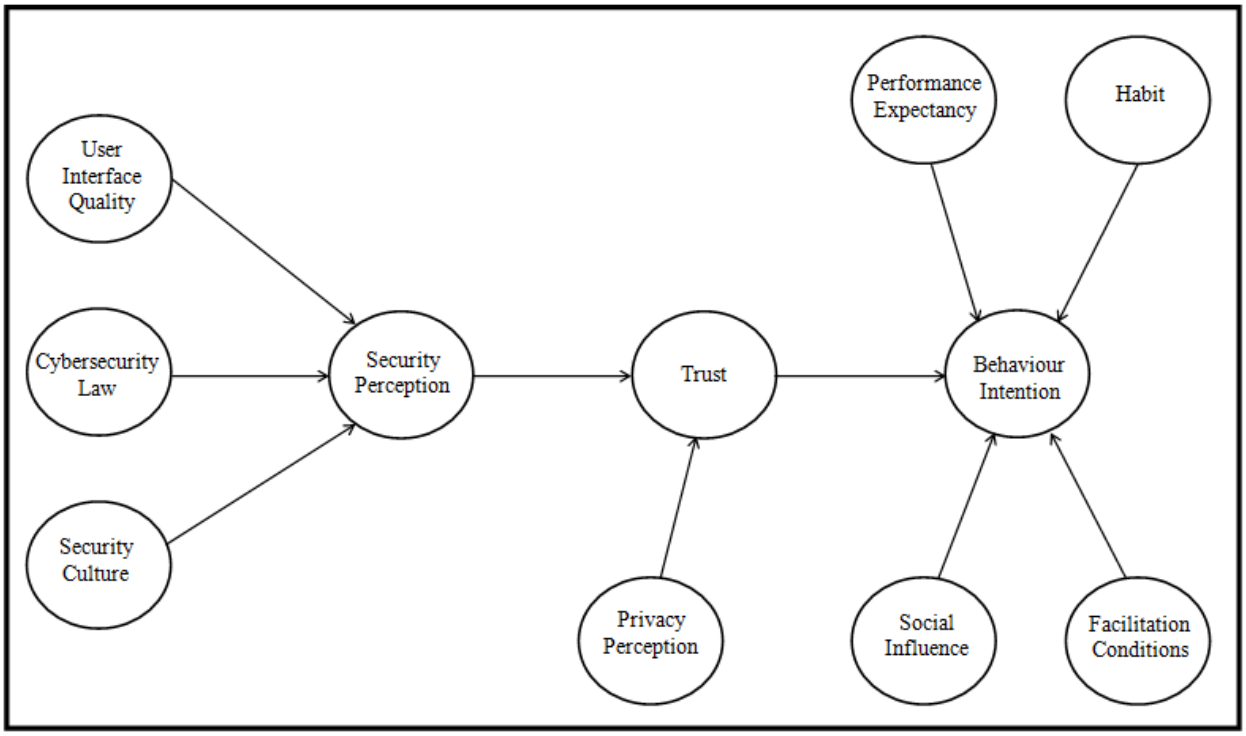

Figure 9.1: Final Research Model

9.6. Research Contributions

The results of this research make a significant contribution to the field and are of importance to both decision-makers in the government and academia. The practical and theoretical implications for both are explained in the following section.

9.6.1. Theoretical Contributions

This research is the first research to have investigated the factors influencing end users' perceptions in e-government security as the findings show that the variance explained in terms of security perception in this model was 54%. This will open the door to researchers to investigate additional factors and accordingly validate the security antecedences explored in this study into another e-government program in other different countries. In addition, this research is the first research to have investigated the role of security in e-government post adoption with using technology acceptance models by integrating trust, security and privacy with the UTAUT2 model. Moreover, this research validates the UTAUT2 constructs in e-government and emphasises the important of the additional constructs in UTAUT2 as the habit is ranked in this research as the second factor influencing behavioural intention for using e-government services. This research also provided an updated Literature Review regarding studies that have applied the UTAUT and UTAUT2 in the content of e-government.

9.6.2. Practical Contributions

The results of this study indicate the factors influencing end users' perceptions of e-government security. Thus, decision-makers in governments may be able to increase users' trust in e-government by focusing more so on these factors. Furthermore, the results also indicate the critical factors affecting the continuance intention of end users when using e-government services. Focusing on influential factors will help decision-makers in the government to increase citizens' intention to continue using e-government services.

9.7. Limitations and Directions for Future Research

This research has five main limitations. Firstly, the data used in this research were collected from only Saudi citizens as e-government services in Saudi Arabia were used as a case study. Thus, future research should apply this study to different countries in order to gain a better understanding of other contexts. Secondly, there is a limitation regarding the number of focus group participants. Future work should conduct more focus groups sessions and interviews to discover additional factors affecting perceptions relating to security in e-government adoption. Thirdly, security perceptions in this research were measured as a first-order construct covering the original CIA triad. Thus, future research should investigate security perception as a second-order construct covering security dimensions, in addition to the CIA triad, such as authentication, access control and non-repudiation. Fourthly, security culture was measured in this study as a first-order construct. However, it also should be measured as a second-order construct as this will be helpful in relation to increasing the reliability of this construct. Finally, this research was single cross-sectional in nature, meaning that the data were collected during one single period. Thus, conducting a longitudinal study by collecting the data in different points of time would be helpful in terms of providing a better understanding of the phenomena.

References

[1] Abdullah, A., Rogerson, S., Fairweather, N. B. and Prior, M. (2006) 'The motivations for change towards e-government adoption: Case studies from Saudi Arabia', *eGovernment Workshop*. pp. 1-21.

[2] Abu-Shanab, E. (2014) 'Antecedents of trust in e-government services: an empirical test in Jordan'. *Transforming Government: People, Process and Policy*, 8 (4). pp 480-499.

[3] Ain, N., Kaur, K. and Waheed, M. (2015) 'The influence of learning value on learning management system use An extension of UTAUT2'. *Information Development*, pp 1-16.

[4] Ajzen, I. (1985) *From intentions to actions: A theory of planned behavior.* Springer.

[5] Ajzen, I. and Fishbein, M. (1980) 'Understanding attitudes and predicting social behaviour'. Prentice Hall.

[6] Al-Athmay, A. (2013) 'Citizens' Perceptions towards e-Governance: Field Study'. *World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic and Management Engineering*, 7 (9). pp 1304-1312.

[7] Alateyah, S., Crowder, R. M. and Wills, G. B. (2012) 'Citizen adoption of E-government services', *Information Society (i-Society), 2012 International Conference on*. IEEE, pp. 182-187.

[8] Alateyah, S. A., Crowder, R. M. and Wills, G. B. (2013) 'Identified Factors Affecting the Citizen's Intention to Adopt E-government in Saudi Arabia', *Proceedings of World Academy of Science, Engineering and Technology*. World Academy of Science, Engineering and Technology (WASET), pp. 904.

[9] AlAwadhi, S. and Morris, A. (2008) 'The Use of the UTAUT Model in the Adoption of E-government Services in Kuwait', *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. IEEE, pp. 219-219.

[10] Al-Khouri, A. and Bal, J. (2007) 'Electronic government in the GCC countries'. *International Journal of Social Sciences*, 1 (2). pp 83-98.

[11] Almarabeh, T. and AbuAli, A. (2010) 'A general framework for e-government: definition maturity challenges, opportunities, and success'. *European Journal of Scientific Research*, 39 (1). pp 29-42.

[12] AlNuaimi, M., Shaalan, K., Alnuaimi, M. and Alnuaimi, K. (2011) 'Barriers to electronic government citizens' adoption: A case of municipal sector in the emirate of

abu dhabi', *Developments in E-systems Engineering (DeSE), 2011*. IEEE, pp. 398-403.

[13] Alotaibi, S. J. and Wald, M. (2012) 'Towards a UTAUT-based model for studying the integrating physical and virtual Identity Access Management Systems in e-government domain', *Internet Technology And Secured Transactions, 2012 International Conference for*. IEEE, pp. 453-458.

[14] Alqahtani, S. S., Al, H. and Al, M. (2014) 'The impact of twitter advertisement on university students purchase intentions'. *International Journal of Logistics and Supply Chain Management Perspectives*, 3 (4). pp 1298.

[15] Al-Qeisi, K. I. (2009) *Analysing the use of UTAUT model in explaining an online behaviour: Internet banking adoption*. Brunel University Brunel Business School PhD Theses.

[16] Alsaif, M. (2014) *Factors affecting citizens' adoption of e-government moderated by socio-cultural values in Saudi Arabia*. University of Birmingham.

[17] Alshehri, M. and Drew, S. (2010) 'Challenges of e-government services adoption in Saudi Arabia from an e-ready citizen perspective'. *International Scholarly and Scientific Research and Innovation,* 4 (6), pp. 1086-1092.

[18] Alshehri, M., Drew, S., Alhussain, T. and Alghamdi, R. (2012) 'The Impact of Trust on E-Government Services Acceptance: A Study of Users' Perceptions by Applying UTAUT Model'. *International Journal of Technology Diffusion (IJTD)*, 3 (2). pp 50-61.

[19] Alshehri, M. A. (2012) 'Using the UTAUT Model to Determine Factors Affecting Acceptance and Use of E-government Services in the Kingdom of Saudi Arabia'. Griffith University.

[20] Al-Sobhi, F. (2011) *The roles of intermediaries in the adoption of e-government services in Saudi Arabia*. Brunel University, School of Information Systems, Computing and Mathematics.

[21] Al-Sobhi, F., Weerakkody, V. and El-Haddadeh, R. (2011) 'The relative importance of intermediaries in egovernment adoption: A study of Saudi Arabia'. *Electronic Government*. Springer, pp 62-74.

[22] Alzahrani, M. and Goodwin, R. (2012) 'Towards a UTAUT-based model for the study of E-government citizen acceptance in Saudi Arabia', *International Scholarly and Scientific Research and Innovation,* 6 (4), pp. 376-382.

[23] Antony, J. and Fergusson, C. (2004) 'Six Sigma in the software industry: results from a pilot study'. *Managerial Auditing Journal*, 19 (8), pp 1025-1032.

[24] Bagozzi, R. and Yi, Y. (1988) 'On the evaluation of structure equations models. Academic of Marketing Science, 16 (1), pp. 76-94.

[25] Baldoni, R. (2012) 'Federated identity management systems in e-government: the case of Italy'. *Electronic Government, an International Journal*, 9 (1), pp. 64-84.

[26] Baum, C. and Di Maio, A. (2000) 'Gartner's four phases of e-government model'. *Gartner Group*,

[27] Belanche, D., Casaló, L. V., Flavián, C. and Schepers, J. (2014) 'Trust transfer in the continued usage of public e-services'. *Information and Management*, 51 (6), pp. 627-640.

[28] Belanche-Gracia, D., Casalo-Arino, L. V. and Pérez-Rueda, A. (2015) 'Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions'. *Government Information Quarterly*, 32 (2), pp. 154-163.

[29] Belanger, F., Hiller, J. S. and Smith, W. J. (2002) 'Trustworthiness in electronic commerce: the role of privacy, security, and site attributes'. *The Journal of Strategic Information Systems*, 11 (3), pp. 245-270.

[30] Ben Fairweather, N. and Rogerson, S. (2006) 'Towards morally defensible e-government interactions with citizens'. *Journal of Information, Communication and Ethics in Society*, 4 (4), pp. 173-180.

[31] Berdykhanova, D., Dehghantanha, A. and Hariraj, K. (2010) 'Trust challenges and issues of e-government: E-tax prospective', *Information Technology (ITSim), 2010 International Symposium in*. IEEE, pp. 1015-1019.

[32] Black, S. A. and Porter, L. J. (1996) 'Identification of the Critical Factors of TQM*'. *Decision sciences*, 27 (1), pp. 1-21.

[33] Black, T. R. (1999) *Doing quantitative research in the social sciences: An integrated approach to research design, measurement and statistics.* Sage.

[34] Bryman, A. (2015) *Social research methods.* Oxford university press.

[35] Bryman, A. and Bell, E. (2015) *Business research methods.* Oxford University Press, USA.

[36] Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness'. *MIS quarterly*, 34 (3), pp. 523-548.

[37] Caldow, J. (1999) *The quest for electronic government: A defining vision.* Institute for Electronic Government, IBM Corporation Washington DC.

[38] Carlos Roca, J., José García, J. and José de la Vega, J. (2009) 'The importance of perceived trust, security and privacy in online trading systems'. *Information Management and Computer Security*, 17 (2), pp. 96-113.

[39] Carter, L. and Belanger, F. (2004) 'Citizen adoption of electronic government initiatives', *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*. IEEE, pp. 1-10.

[40] Carter, L. and Bélanger, F. (2005) 'The utilization of e-government services: citizen trust, innovation and acceptance factors*'. *Information Systems Journal*, 15 (1), pp. 5-25.

[41] Cegielski, C. (2008) 'Toward an interdisciplinary information assurance curriculum: knowledge and skill sets required of information assurance professionals'. *Decision Sciences Journal of Innovative Education*, 6 (1), pp. 29-49.

[42] Chandler, S. and Emanuels, S. (2002) 'Transformation not automation', *Proceedings of 2nd European Conference on E-government*, pp. 91-102.

[43] Chang, H. H. and Chen, S. W. (2009) 'Consumer perception of interface quality, security, and loyalty in electronic commerce'. *Information and Management*, 46 (7), pp. 411-417.

[44] Charmaz, K. (2006) 'Constructing grounded theory: A practical guide through qualitative analysis' Sage Publications Ltd, London.

[45] Chellappa, R. K. and Pavlou, P. A. (2002) 'Perceived information security, financial liability and consumer trust in electronic commerce transactions'. *Logistics Information Management*, 15 (5/6), pp. 358-368.

[46] Cheng, T. E., Lam, D. Y. and Yeung, A. C. (2006) 'Adoption of Internet banking: an empirical study in Hong Kong'. *Decision support systems*, 42 (3), pp. 1558-1572.

[47] Cheung, C. M. and Lee, M. K. (2001) 'Trust in Internet shopping: instrumental development and validation through classical and modern approaches'. *Journal of Global Information Management*, 9 (3), pp. 25-41.

[48] Choudrie, J. and Dwivedi, Y. (2005) 'A survey of citizens' awareness and adoption of e-government initiatives, the 'Government Gateway': A United Kingdom perspective', *eGovernment Workshop'05 (eGOV05)*. Brunel University, London, UK.

[49] Coakes, S. (2005) 'SPSS 12.0 Analysis without anguish'. *Johm Wiley and Sons Australia, Ltd*,

[50] Cohen, L., Manion, L. and Morrison, K. (2013) *Research methods in education.* Routledge.

[51] Creswell, J. W. (2013) *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage publications.

[52] D'Arcy, J. and Greene, G. (2014) 'Security culture and the employment relationship as drivers of employees' security compliance'. *Information Management and Computer Security*, 22 (5), pp. 474-489.

[53] Davis, F. D., Bagozzi, R. P. and Warshaw, P. R. (1989) 'User acceptance of computer technology: a comparison of two theoretical models'. *Management science*, 35 (8), pp. 982-1003.

[54] Deloitte, T. (2001) 'The citizen as customer'. *CMA Management*, 74 (10). p 58.

[55] Denzin, N. K. and Lincoln, Y. S. (2002) *The qualitative inquiry reader.* Sage publications.

[56] Denzin, N. K. and Lincoln, Y. S. (2005) *The Sage handbook of qualitative research.* Sage publications.

[57] Doong, H.-S., Wang, H.-C. and Foxall, G. R. (2010) 'Psychological traits and loyalty intentions towards e-Government services'. *International Journal of Information Management*, 30 (5), pp. 457-464.

[58] Ebrahim, Z. and Irani, Z. (2005) 'E-government adoption: architecture and barriers'. *Business Process Management Journal*, 11 (5), pp. 589-611.

[59] Elsheikh, Y. (2012) *A model for the Adoption and Implementation of Web-based Government services and applications. A Study Based in Grounded Theory Validated by Structural Equation Modelling Analysis in a Jordanian Context*. University of Bradford.

[60] Escobar-Rodríguez, T. and Carvajal-Trujillo, E. (2013) 'Online drivers of consumer purchase of website airline tickets'. *Journal of Air Transport Management*, 32 (1), pp. 58-64.

[61] Escobar-Rodríguez, T. and Carvajal-Trujillo, E. (2014) 'Online purchasing tickets for low cost carriers: An application of the unified theory of acceptance and use of technology (UTAUT) model'. *Tourism Management*, 43 (1), pp. 70-88.

[62] European Commissionn. (2016) 'Interoperability Maturity Model'. [ONLINE] Available at: http://ec.europa.eu/isa/documents/eudig12a-1401-i01-imm-leaflet_en.pdf. [Accessed 20 August 16].

[63] Fakhoury, R. and Aubert, B. (2015) 'Citizenship, trust, and behavioural intentions to use public e-services: The case of Lebanon'. *International Journal of Information Management*, 35 (3), pp. 346-351.

[64] Fang, X., Chan, S., Brzezinski, J. and Xu, S. (2005) 'Moderating effects of task type on wireless technology acceptance'. *Journal of Management Information Systems*, 22 (3), pp. 123-157.

[65] Fidock, J. and Carroll, J. (2009) 'Combining variance and process research approaches to understand system use', *Proceedings of the 20th Australasian Conference on Information Systems*. 2-4 Dec, Melbourne, pp. 325-345.

[66] Fisher, C. (2004) 'Research and writing a dissertation for business students'. *Financial Times/Prentice Hall,* UK.

[67] Flavián, C. and Guinalíu, M. (2006) 'Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site'. *Industrial Management and Data Systems*, 106 (5), pp. 601-620.

[68] Fornell, C. and Larcker, D. F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error'. *Journal of marketing research*, pp. 39-50.

[69] Gil-García, J. R. and Pardo, T. A. (2005) 'E-government success factors: Mapping practical tools to theoretical foundations'. *Government Information Quarterly*, 22 (2), pp. 187-216.

[70] Gillenson, M. L. and Sherrell, D. L. (2002) 'Enticing online consumers: an extended technology acceptance perspective'. *Information and Management*, 39 (8), pp. 705-719.

[71] Glaser, B. G. (2002) 'Conceptualization: On theory and theorizing using grounded theory'. *International Journal of Qualitative Methods*, 1 (2), pp. 23-38.

[72] Glaser, B. G. and Strauss, A. L. (2009) *The discovery of grounded theory: Strategies for qualitative research.* Transaction Publishers.

[73] Goulding, C. (2002) *Grounded theory: A practical guide for management, business and market researchers.* Sage publications.

[74] Gurbani, V. K. and McGee, A. R. (2007) 'An early application of the Bell Labs Security framework to analyze vulnerabilities in the Internet telephony domain'. *Bell Labs Technical Journal*, 12 (3), pp. 7-19.

[75] Ha, I., Yoon, Y. and Choi, M. (2007) 'Determinants of adoption of mobile games under mobile broadband wireless access environment'. *Information and Management*, 44 (3), pp. 276-286.

[76] Hadi, F. and Bin Muhaya, F. T. (2011) 'Essentials for the e-government security', *Information Society (i-Society), 2011 International Conference on*. IEEE, pp. 237-240.

[77] Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E. and Tatham, R. L. (2006) *Multivariate data analysis.* Pearson Prentice Hall Upper Saddle River, NJ.

[78] Halaweh, M. (2012) 'Modeling user perceptions of e-commerce security using partial least square'. *Journal of Information Technology Management*, 23 (1), pp. 22-33.

[79] Halchin, L. E. (2004) 'Electronic government: Government capability and terrorist resource'. *Government Information Quarterly*, 21 (4), pp. 406-419.

[80] Hartono, E., Holsapple, C. W., Kim, K.-Y., Na, K.-S. and Simpson, J. T. (2014) 'Measuring perceived security in B2C electronic commerce website usage: A respecification and validation'. *Decision support systems*, 62(4), pp. 11-21.

[81] Hiller, J. S. and Belanger, F. (2001) 'Privacy strategies for electronic government'. *E-government*, Rowman and Littlefield publishers.

[82] Howard, M. (2001) 'E-government across the globe: how will" e" change government?'. *Government finance review*, 17 (4), pp. 6-9.

[83] Hox, J. and Bechger, T. (1998) 'An introduction to structural equation modelling'. *Family Science Review*, 11 (1), pp. 354-373.

[84] Huang, Z. and Bwoma, P. O. (2003) 'An overview of critical issues of e-government'. *Issues of Information Systems*, 4 (1), pp. 164-170.

[85] Hughes, C. (2006) 'Qualitative and quantitative approaches to social research'. *Coventry: Department of Sociology, Warwick University.[Accessed 29 October 2013]*.

[86] Huijsman, k. (2012) 'Measuring interoperability maturity in government networks', Master thesis, Utrecht University.

[87] Hung, S.-Y., Chang, C.-M. and Kuo, S.-R. (2013) 'User acceptance of mobile e-government services: An empirical study'. *Government Information Quarterly*, 30 (1), pp. 33-44.

[88] Hussein, M. E., Hirst, S., Salyers, V. and Osuji, J. (2014) 'Using grounded theory as a method of inquiry: Advantages and disadvantages'. *The Qualitative Report*, 19 (27), pp. 1-15.

[89] Hwang, M.-S., Li, C.-T., Shen, J.-J. and Chu, Y.-P. (2004) 'Challenges in e-government and security of information'. *Information and Security*, 15 (1), pp 9-20.

[90] Isaac, W. C. (2007) *Performance measurement for the e-Government initiatives: A comparative study.* ProQuest.

[91] Jiang, G. and Deng, W. (2011) 'An empirical analysis of factors influencing the adoption of Mobile Instant Messaging in China'. *International Journal of Mobile Communications*, 9 (6), pp. 563-583.

[92] Jorgensen, D. J. and Cable, S. (2002) 'Facing the challenges of e-goverment: A case study of the city of Corpus Christi, Texas'. *SAM Advanced Management Journal*, 67 (3), pp. 15.

[93] Kaiser, H. F. (1970) 'A second generation little jiffy'. *Psychometrika*, 35 (4), pp. 401-415.

[94] Kamoun, F. and Halaweh, M. (2012) 'User interface design and e-commerce security perception: an empirical study'. *International Journal of E-Business Research (IJEBR)*, 8 (2), pp. 15-32.

[95] Karokola, G., Kowalski, S. and Yngström, L., (2011) 'Secure e-government services: Towards a framework for integrating it security services into e-government maturity models'. In 2011 Information Security for South Africa. pp 1-9.

[96] Karokola, G., Kowalski, S. and Yngstrom, L. (2013) 'Evaluating a Framework for Securing E-Government Services--A Case of Tanzania', *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. IEEE, pp. 1792-1801.

[97] Karokola, G. and Yngström, L. (2009) 'Discussing E-Government Maturity Models for the Developing World-Security View', *ISSA*. pp. 81-98.

[98] Khan, F., Khan, S. and Zhang, B. (2010) 'E-government challenges in developing countries: a case study of Pakistan', *Management of e-Commerce and e-Government (ICMeCG), 2010 Fourth International Conference on*. IEEE, pp. 200-203.

[99] Kim, C., Tao, W., Shin, N. and Kim, K.-S. (2010) 'An empirical study of customers' perceptions of security and trust in e-payment systems'. *Electronic Commerce Research and Applications*, 9 (1), pp. 84-95.

[100] Klein, R. (2007) 'An empirical examination of patient-physician portal acceptance'. *European Journal of Information Systems*, 16 (6), pp. 751-760.

[101] Kline, R. B. (2015) *Principles and practice of structural equation modeling.* Guilford publications.

[102] Krishnaraju, V., Mathew, S. K. and Sugumaran, V. (2015) 'Web personalization for user acceptance of technology: An empirical investigation of E-government services'. *Information Systems Frontiers*, pp.1-17.

[103] Kumar, V., Mukerji, B., Butt, I. and Persaud, A. (2007) 'Factors for successful e-government adoption: a conceptual framework'. *The electronic journal of e-Government*, 5 (1). pp 63-76.

[104] Kurdi, R., Taleb-Bendiab, A., Randles, M. and Taylor, M. (2011) 'E-government information systems and cloud computing (readiness and analysis)', *Developments in E-systems Engineering (DeSE),* IEEE, pp. 404-409.

[105] Lancaster, G. (2007) *Research methods in management.* Routledge.

[106] Layne, K. and Lee, J. (2001) 'Developing fully functional E-government: A four stage model'. *Government Information Quarterly*, 18 (2), pp. 122-136.

[107] Lean, O. K., Zailani, S., Ramayah, T. and Fernando, Y. (2009) 'Factors influencing intention to use e-government services among citizens in Malaysia'. *International Journal of Information Management*, 29 (6), pp. 458-475.

[108] Lee, A. S. (1991) 'Integrating positivist and interpretive approaches to organizational research'. *Organization science*, 2 (4), pp. 342-365.

[109] Lee, J., Kim, H. J. and Ahn, M. J. (2011) 'The willingness of e-Government service adoption by business users: The role of offline service quality and trust in technology'. *Government Information Quarterly*, 28 (2), pp. 222-230.

[110] Legris, P., Ingham, J. and Collerette, P. (2003) 'Why do people use information technology? A critical review of the technology acceptance model'. *Information and Management*, 40 (3), pp. 191-204.

[111] Lian, J.-W. (2015) 'Critical factors for cloud based e-invoice service adoption in Taiwan: An empirical study'. *International Journal of Information Management*, 35 (1), pp. 98-109.

[112] Lian, J.-W. and Lin, T.-M. (2008) 'Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types'. *Computers in Human Behavior*, 24 (1), pp. 48-65.

[113] Liang, J. (2012) 'Government cloud: enhancing efficiency of e-government and providing better public services', *Service sciences (IJCSS), 2012 international joint conference on*. IEEE, pp. 261-265.

[114] Liao, Z. and Wong, W.-K. (2008) 'The determinants of customer interactions with Internet-enabled e-banking services'. *Journal of the Operational Research Society*, 59 (9), pp. 1201-1210.

[115] Lin, F., Fofanah, S. S. and Liang, D. (2011) 'Assessing citizen adoption of e-Government initiatives in Gambia: A validation of the technology acceptance model in information systems success'. *Government Information Quarterly*, 28 (2), pp. 271-279.

[116] Liu, Y. (2010) 'The Management Perspective of Chinese E-government Security', *2010 International Conference on Electrical and Control Engineering*. IEEE, pp. 2367-2370.

[117] Ma, Q. and Pearson, J. M. (2005) 'ISO 17799:" Best Practices" in Information Security Management?'. *Communications of the Association for Information Systems*, 15 (1), pp. 32.

[118] Martínez-López, L., Martínez-López, F., Lu, J., Shambour, Q., Xu, Y., Lin, Q. and Zhang, G. (2010) 'BizSeeker: a hybrid semantic recommendation system for personalized government-to-business e-services'. *Internet Research*, 20 (3), pp. 342-365.

[119] May, T. (2011) *Social research.* McGraw-Hill Education (UK).

[120] MCIT 2016. ICT Indicators in K.S.A by end of 2015. [ONLINE] Available at: http://www.mcit.gov.sa/En/aboutmcit/sectordevelopment/pages/sectorindices.aspx. [Accessed 22 March 16].

[121] Milovanović, M., Bogićević, M., Lazović, M., Simić, D. and Starčević, D. (2010) 'Choosing authentication techniques in e-procurement system in Serbia', *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*. IEEE, pp. 374-379.

[122] Monga, A. (2008) 'E-government in India: Opportunities and challenges'. *JOAAG*, 3 (2), pp. 52-61.

[123] Moon, M. J. (2002) 'The evolution of e-government among municipalities: rhetoric or reality?'. *Public administration review*, 62 (4), pp. 424-433.

[124] Mouakket, S. (2015) 'Factors influencing continuance intention to use social network sites: The Facebook case'. *Computers in Human Behavior*, 53(1), pp. 102-110.

[125] Myers, M. D. and Avison, D. (2002) '*Qualitative research in information systems: a reader*'. Sage publications.

[126] Narain Singh, A., Gupta, M. and Ojha, A. (2014) 'Identifying factors of "organizational information security management"'. *Journal of Enterprise Information Management*, 27 (5), pp. 644-667.

[127] Navarrete, C. (2010) 'Trust in E-Government Transactional Services: A Study of Citizens' Perceptions in Mexico and the US', *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*. IEEE, pp. 1-10.

[128] Ndou, V. (2004) 'E-government for developing countries: opportunities and challenges'. *The electronic journal of information systems in developing countries*, 18(1), pp. 1-24.

[129] Ngai, E. W. and Wat, F. (2005) 'Fuzzy decision support system for risk analysis in e-commerce development'. *Decision support systems*, 40 (2), pp. 235-255.

[130] Nikkhahan, B., Aghdam, A. J. and Sohrabi, S. (2009) 'E-government security: A honeynet approach'. *International Journal of Advanced Science and Technology*, 5(1), pp. 75-84.

[131] Nkwe, N. (2012) 'E-Government: Challenges and Opportunities in Botswana Department of Accounting and Finance University of Botswana Gaborone'. *Botswana International Journal of Humanities and Social Science*, 2 (17). pp. 39-48

[132] O'cass, A. and Fenech, T. (2003) 'Web retailing adoption: exploring the nature of Internet users Web retailing behaviour'. *Journal of Retailing and Consumer services*, 10 (2), pp. 81-94.

[133] Oates, B. J. (2005) *Researching information systems and computing.* Sage publications.

[134] Odat, A. M. (2012) 'E-Government in developing countries: Framework of challenges and opportunities', *Internet Technology And Secured Transactions, 2012 International Conference for*. IEEE, pp. 578-582.

[135] OECD. (2005) 'OECD E-government project', [ONLINE] Available at: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/PGC/EGOV(2005)1&docLanguage=En. [Accessed 20 August 16].

[136] Ovais Ahmad, M., Markkula, J. and Oivo, M. (2013) 'Factors affecting e-government adoption in Pakistan: a citizen's perspective'. *Transforming Government: People, Process and Policy*, 7 (2), pp. 225-239.

[137] Pallant, J. (2013) *SPSS survival manual.* McGraw-Hill Education (UK).

[138] Parent, M. (2007) 'The 6th and biggest lie of all: lessons from a decade of e-tailing'. *Ivey Business Journal*, 71 (8), pp. 1-7.

[139] Pavlou, P. (2001) 'Integrating trust in electronic commerce with the technology acceptance model: model development and validation'. *AMCIS 2001 Proceedings*, pp 816-822.

[140] Petrick, J. F. and Backman, S. J. (2002) 'An examination of the construct of perceived value for the prediction of golf travelers' intentions to revisit'. *Journal of Travel Research*, 41 (1), pp. 38-45.

[141] Pina, V., Torres, L. and Royo, S. (2010) 'Is e-government leading to more accountable and transparent local governments? An overall view'. *Financial Accountability and Management*, 26 (1), pp. 3-20.

[142] Pokharel, M. and Park, J. S. (2009) 'Issues of interoperability in e-governance system and its impact in the developing countries: A Nepalese case study', *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*. IEEE, pp. 2160-2164.

[143] Ponte, E. B., Carvajal-Trujillo, E. and Escobar-Rodríguez, T. (2015) 'Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents'. *Tourism Management*, 47(1), pp. 286-302.

[144] Punch, K. F. (2009) *Introduction to research methods in education.* Sage publications.

[145] Rehman, M. and Esichaikul, V. (2011) 'Factors influencing the adoption of e-government in Pakistan', *E-Business and E-Government (ICEE), 2011 International Conference on*. IEEE, pp. 1-4.

[146] Riquelme, I. P. and Román, S. (2014) 'Is the influence of privacy and security on online trust the same for all type of consumers?'. *Electronic Markets*, 24 (2), pp. 135-149.

[147] Rogers Everett, M. (1995) 'Diffusion of innovations'. *The free press, New York.*

[148] Rose, S., Spinks, N. and Canhoto, A. I. (2014) *Management research: applying the principles.* Routledge.

[149] Salisbury, W. D., Pearson, R. A., Pearson, A. W. and Miller, D. W. (2001) 'Perceived security and World Wide Web purchase intention'. *Industrial Management and Data Systems*, 101 (4), pp. 165-177.

[150] Sang, S., Lee, J.-D. and Lee, J. (2009) 'E-Government challenges in least developed countries (LDCs): a case of Cambodia', *Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on*. IEEE, pp. 2169-2175.

[151] Sarabdeen, J., Rodrigues, G. and Balasubramanian, S. (2014) 'E-Government users' privacy and security concerns and availability of laws in Dubai'. *International Review of Law, Computers and Technology*, 28 (3), pp. 261-276.

[152] Schumacker, R. E. and Lomax, R. G. (2004) *A beginner's guide to structural equation modeling.* Psychology Press.

[153] Science, P. O. o. and Technology (1998) *Electronic government: information technologies and the citizen.* Parliamentary Office of Science and Technology.

[154] Shahkooh, K. A., Saghafi, F. and Abdollahi, A. (2008) 'A proposed model for e-Government maturity', *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*. IEEE, pp. 1-5.

[155] Shareef, M. A., Kumar, V., Kumar, U. and Dwivedi, Y. K. (2011) 'e-Government Adoption Model (GAM): Differing service maturity levels'. *Government Information Quarterly*, 28 (1), pp. 17-35.

[156] Sheppard, B. H., Hartwick, J. and Warshaw, P. R. (1988) 'The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research'. *Journal of consumer Research*, 15(3), pp 325-343.

[157] Shin, D.-H. (2010) 'The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption'. *Interacting with computers*, 22 (5), pp. 428-438.

[158] Siddiqui, A. T. and Singh, A. K. (2012) 'Secure E-business Transactions By Securing Web Services', *Management of e-Commerce and e-Government (ICMeCG), 2012 International Conference on*. IEEE, pp. 79-84.

[159] Siponen, M. T. and Oinas-Kukkonen, H. (2007) 'A review of information security issues and respective research contributions'. *ACM Sigmis Database*, 38 (1), pp. 60-80.

[160] Smith, S. and Jamieson, R. (2005) 'Key Factors in E-Government Information System Security'. Proceedings of *SCI,* pp. 96-120.

[161] STATS. (2016). General Authority of Statistics. [ONLINE] Available at: http://www.stats.gov.sa/en/node. [Accessed 22 March 16].

[162] Sun, Y., Liu, L., Peng, X., Dong, Y. and Barnes, S. J. (2014) 'Understanding Chinese users' continuance intention toward online social networks: an integrative theoretical model'. *Electronic Markets*, 24 (1), pp. 57-66.

[163] Syamsuddin, I. and Hwang, J. (2010) 'A new fuzzy MCDM framework to evaluate e-government security strategy', *Application of Information and Communication Technologies (AICT), 2010 4th International Conference on*. IEEE, pp. 1-5.

[164] Ullman, J. B. and Bentler, P. M. (2003) *Structural equation modeling.* Wiley Online Library.

[165] UN, (2001) 'Government Report (2001)"Benchmarking E-Government: A Global Perspective-Assessing the UN membestates"'. *UN Publication,[online] http://www. upan1. org/egovernment2. asp*,

[166] UN, (2014) '*E-GOVERNMENT SURVEY 2014*'. [ONLINE] Available at: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf. [Accessed 22 March 16].

[167] Vatanasombut, B., Igbaria, M., Stylianou, A. C. and Rodgers, W. (2008) 'Information systems continuance intention of web-based applications customers: The case of online banking'. *Information and Management*, 45 (7), pp. 419-428.

[168] Venkatesh, V. and Davis, F. D. (2000) 'A theoretical extension of the technology acceptance model: Four longitudinal field studies'. *Management science*, 46 (2), pp. 186-204.

[169] Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003) 'User acceptance of information technology: Toward a unified view'. *MIS quarterly*, 27(3), pp 425-478.

[170] Venkatesh, V., Thong, J. Y., Chan, F. K., Hu, P. J. H. and Brown, S. A. (2011) 'Extending the two-stage information systems continuance model: Incorporating UTAUT predictors and the role of context'. *Information Systems Journal*, 21 (6), pp. 527-555.

[171] Venkatesh, V., Thong, J. Y. and Xu, X. (2012) 'Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology'. *MIS quarterly*, 36 (1), pp. 157-178.

[172] Wang, H.-J. and Lo, J. (2013) 'Determinants of citizens' intent to use government websites in Taiwan'. *Information Development*, 29 (2), pp. 123-137.

[173] Wang, Y.-S. and Shih, Y.-W. (2009) 'Why do people use information kiosks? A validation of the Unified Theory of Acceptance and Use of Technology'. *Government Information Quarterly*, 26 (1), pp. 158-165.

[174] Weerakkody, V., El-Haddadeh, R., Al-Sobhi, F., Shareef, M. A. and Dwivedi, Y. K. (2013) 'Examining the influence of intermediaries in facilitating e-government adoption: An empirical investigation'. *International Journal of Information Management*, 33 (5), pp. 716-725.

[175] Wescott, C. G. (2001) 'E-Government in the Asia-pacific region'. *Asian Journal of Political Science*, 9 (2), pp. 1-24.

[176] West, D. M. (2004) 'E-government and the transformation of service delivery and citizen attitudes'. *Public administration review*, 64 (1), pp. 15-27.

[177] Williams, Z., Ponder, N. and Autry, C. W. (2009) 'Supply chain security culture: measure development and validation'. *The International Journal of Logistics Management*, 20 (2), pp. 243-260.

[178] Willig, C. (2013) *Introducing qualitative research in psychology.* McGraw-Hill Education (UK).

[179] Yahya, M., Nadzar, F. and Rahman, B. A. (2012) 'Examining user acceptance of E-Syariah portal among Syariah users in Malaysia'. *Procedia-Social and Behavioral Sciences*, 67(1), pp. 349-359.

[180] Yauch, C. A. and Steudel, H. J. (2003) 'Complementary use of qualitative and quantitative cultural assessment methods'. *Organizational Research Methods*, 6 (4), pp. 465-481.

[181] Yenisey, M. M., Ozok, A. A. and Salvendy, G. (2005) 'Perceived security determinants in e-commerce among Turkish university students'. *Behaviour and Information Technology*, 24 (4), pp. 259-274.

[182] Yousafzai, S., Pallister, J. and Foxall, G. (2009) 'Multi-dimensional role of trust in Internet banking adoption'. *The Service Industries Journal*, 29 (5), pp. 591-605.

[183] Zhang, W. (2010) 'Notice of Retraction E-government information security: Challenges and recommendations', *Computer Application and System Modeling (ICCASM), 2010 International Conference on*. IEEE, pp. 1-15.

[184] Zhiming, Q. (2009) 'Rough sets and its application in evaluating security problems of E-government affairs', *Power Electronics and Intelligent Transportation System (PEITS), 2009 2nd International Conference on*. IEEE, pp. 66-69.

[185] Zhou, T. and Li, H. (2014) 'Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern'. *Computers in Human Behavior*, 37(1), pp. 283-289.

[186] Zhou, T., Lu, Y. and Wang, B. (2010) 'Integrating TTF and UTAUT to explain mobile banking user adoption'. *Computers in Human Behavior*, 26 (4), pp. 760-767.

[187] Zikmund, W., Babin, B., Carr, J. and Griffin, M. (2012) *Business research methods.* Cengage Learning.

[188] Zulhuda, S. (2012) 'The state of e-government security in Malaysia: reassessing the legal and regulatory framework on the threat of information theft'. *1st Taibah University International Conference on Computing and Information Technology (ICCIT 2012)*, pp. 12-14

Appendix A: Ethical approval letter

RESEARCH WITH PLYMOUTH UNIVERSITY

15 June 2015

CONFIDENTIAL
Nawaf Alharbi
School of Computing, Electronics and Mathematics

Dear Nawaf

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

E-government security focused adoption

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Dr Maria Papadaki
Dr Paul Dowland

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

+44 (0) 1752 584 584
F +44 (0) 1752 584 540
W www.plymouth.ac.uk

Mrs Christine Mushens BA
Faculty Business Manager

Appendix B: Initial survey (English version)

Evaluating e-government security based on end users' perspective

Centre for Security, Communications and Network Research (CSCAN)

This survey is being conducted for PhD research on "Evaluating e-government security" at Plymouth University, United Kingdom.
The survey aims to investigate current security level of e-government based on the end users perspective and security challenges that they are faced. There are 3 main sections organised as follows:

1. General information - general information for respondents such as age, gender, education background, employment status, and nationality.
2. Participant's e-government usage - analysing respondents' experience of using e-government services and determining current challenges.
3. Participant's experience of e-government security - Analysing respondents' experience of the security of e-government.

Researcher
Nawaf Alharbi

Research Supervisors
Dr Maria Papadaki
Dr Paul Dowland

There are 17 questions in this survey

Consent Form

Dear participants,

This survey is designed for adult participation. If you are **UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY.** Anyone 18 years old and above can take part in the survey and has the right to withdraw up until the final submission of their responses. All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data. Should you have any questions about the study or you wish to receive a copy of the results, please contact the researcher Nawaf alharbi via email or address below:

Researcher details:
Nawaf alharbi
Centre for Security, Communications and Network Research (CSCAN)
School of Computing and Mathematics
Plymouth University
Plymouth, PL4 8AA
United Kingdom
Mail to: nawaf.alharbi@plymouth.ac.uk

If you have any concerns regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Technology Ethics Committee:

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Environment
Plymouth University

Plymouth, PL4 8AA
United Kingdom
Phone:+44 (0)1752584503
Mail to: paula.simson@plymouth.ac.uk

I'm 18+ years old and understand that I am free to withdraw up until the point of submission of my responses and I confirm that I have read and understand the information given and agree to take part in the study?

- ○ Agree

General information

What is your gender?

- Male
- Female

What is your age group (in years)?

- 18 - 29
- 30 - 39
- 40 - 49
- 50 - 59
- 60 >

What is your country of residence? (optional)

Please choose (list)

What is your highest educational level?

- Secondary School
- Diploma/ Bachelor
- Master/ Doctorate
- Other:

What is your employment status?

- Student
- Government employed
- Private sector employed
- Self-employed
- Other:

How would you rate your information security awareness?

- Basic (e.g. you know general information about information security)
- Intermediate (e.g. you have a short course in information security)
- Advanced (e.g. you have undergraduate/postgraduate degree in information security)

Participant's e-government usage

Have you applied to any government service via the Internet such as paying passport fee, fines?

- Yes
- No

What are the reasons for not using the e-government services (government websites)?

- I prefer traditional way
- I do not trust e-government security
- Applying via the Internet is complex

- Most of government services are no available online
- Other:

What is your preferred method making a payment for e-government services (e.g. passport fee, fines)?

- Face to face (Traditional way)
- Via phone
- Via the Internet using lap top or desktop
- Via mobile applications
- Via ATM machines

What is the thing that you most worry about when you used e-government services?

- Online payment
- Personal information such as (Names, numbers or private information)
- The delay in the completion of the process
- Failure to follow procedures exactly
- There is nothing specific that I'm worried about it
- Other:

When you encounter a problem through using e-government websites, what action do you usually take?

- Contacting a friend to ask for help
- Passing your information to another person to apply on your behind
- Contacting technical support

- Applying on another time
- Applying manually (traditional way)
- Other:

Participant's experience of e-government security

What is your opinion about the following statements?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I'm worried about my privacy when using e-government services	○	○	○	○	○
I do not trust the e-government security	○	○	○	○	○
Website design of e-government services is influenced me in determining the level of e-government security	○	○	○	○	○
Culture and social relationships are playing an impor□ant role in e-government security (e.g getting personal information of the users by using social relationships)	○	○	○	○	○
Users' security awareness is one of main factors that affect the e-governme□t security	○	○	○	○	○
Security advices provided to use□s via the media and e-government websites are very few	○	○	○	○	○
Most of current security issues are coming from non-technical side such as lack of users' awareness and lack of trust	○	○	○	○	○

Do you encounter complex security procedures (such as: one-time password) when applying for e-government services?

- Always
- Sometimes
- Just with financial matters
- No

When you have accessed e-government websites, have you had difficulty completing process regarding due to slow response or unavailability of services?

- Always
- Sometimes
- Rarely
- No

Do you always check if the website is safe (e.g. SSL lock icon) when you update your information or making a payment through e-government websites?

- Always
- Sometimes
- No
- Don't know

When you access your information on e-government websites, is it accurate?

- Always

- Sometimes
- Rarely
- No

Have you ever found your information has been deleted or have you been asked to submit it again?

- Always
- Sometimes
- Rarely
- No

Your comments are very important. If you have any comments regarding to the security of e-government services please add them below.

Answer

The survey has been completed successfully

Thank you for your cooperation

Appendix C: Initial survey (Arabic version)

إستبيان عن تقييم مستوى الحماية في أنظمة الحكومة الإلكترونية من وجهة نظر المستخدم

Centre for Security, Communications and Network Research (CSCAN)

مركز أبحاث أمن المعلومات، الإتصالات، والشبكات

يجري عمل هذا الإستبيان ضمن بحث لمرحلة الدكتوراة عن تقييم مستوى الحماية في أنظمة الحكومة الإلكترونية، جامعة بليموث، بريطانيا.

تهدف هذه الدراسة إلى تحديد الصعوبات الأمنية التي تواجه المستخدم أثناء استخدامه للمواقع الحكومية الإلكترونية، يحتوي هذا الإستبيان على ثلاثة أقسام رئيسية مرتبة كالآتي:

(1) معلومات عامة عن المشارك: معلومات عامة عن المستخدم تحتوي على العمر والجنس والمؤهلات العلمية والبيانات الوظيفية.

(2) خبرة المشارك في استخدام الحكومة الإلكترونية: تحليل خبرة المستخدم للحكومة الإلكترونية وطريقة تعامله مع الصعوبات اللتي تواجهه.

(3) رأي المشارك في مستوى الحماية في الحكومة الإلكترونية: تقييم مستوى الحماية بناء على وجهة نظر المستخدم ومستوى تعقيدها، وتحديد المشاكل الأمنية التي تواجهه.

الباحث
نواف الحربي

المشرفين
Dr Maria Papadaki
Dr Paul Dowland

يحتوي هذا الإستبيان على 17 سؤال

إفادة بالموافقة على المشاركة في الإستبيان

عزيزي المشارك،

هذا الإستبيان معد لمشاركة البالغين. **إذا كان عمرك أقل من 18 سنة، آمل عدم الإجابة على أسئلة الإستبيان**. أي مشارك بلغ ال18 سنة فما فوق يحق له المشاركة في إستطلاع الرأي و له الحق في الإنسحاب في أي وقت قبل التسليم النهائي للإجابات.

جميع الإجابات سيتم التعامل معها بسرية و الردود ستكون مجهولة المصدر خلال جمع البيانات، التخزين، أو نشر المادة العلمية. هذا الإستبيان مستضاف عبر الإنترنت بواسطة مركز أمن المعلومات و الإتصالات و الشبكات بجامعة بليموث. بعد مرحلة جمع البيانات سيتم التعامل مع قاعدة البيانات بعيداً عن الإنترنت في بيئة آمنة يتم خلالها استخراج إجابات المشاركين و تحليلها و نشر النتائج في مجلة علمية مناسبة. إضافة إلى ذلك قد تستخدم تلك النتائج كجزء من رسالة مرحلة الدكتوراة. إجابات المشاركين سيتم التعامل معها بسرية تامة في جميع اوقات ومراحل العمل وسيتم عرضها بطريقة لا يمكن من خلالها الربط بين هوية المشارك و المعلومات المنشورة.

في حالة الرغبة في الإستفسار حول الدراسة أو الحصول على نسخة من النتائج، آمل التواصل مع الباحث/ نواف الحربي من خلال عنوان البريد الإلكتروني أو العنوان التالي:

بيانات الباحث:

Nawaf alharbi

Centre for Security, Communications and Network Research (CSCAN)

School of Computing and Mathematics

Plymouth University

E-mail: mailto:paula.simson@plymouth.ac.uk

إذا كان لديك ما يثير تحفظك بخصوص طريقة إجراء هذه الدراسة، آمل التواصل مع سكرتير لجنة الأخلاقيات بكلية العلوم والتكنولوجيا:

Paula Simson

009, Smeaton, Drake Circus

Faculty of Science and Environment

Plymouth University

Phone:+44 (0)1752584503

E-mail: paula.simson@plymouth.ac.uk

*** عمري فوق 18 عام وأؤكد بأني قرأت و فهمت المعلومات المعطاه وأوافق على المشاركة في هذه الدراسة وأعلم أنه بإمكاني الإنسحاب من المشاركة في الإستبيان في أي وقت قبل التسليم النهائي للإجابات**

- ○ موافق

معلومات عامة

ما هو جنسك؟

- ذكر
- أنثى

ما هي فئتك العمرية (بالسنوات)؟

- 18 - 29
- 30 - 39
- 40 - 49
- 50 - 59
- 60 >

ما هو بلد الإقامة؟ (سؤال اختيار)

من فضلك اختر (قائمة)

ما هو آخر مؤهل علمي حصلت عليه؟

- الثانوية العامة
- دبلوم / بكالوريوس
- ماجستير / دكتوراه
- اخرى :

ما هي حالتك الوظيفية؟

- طالب
- موظف حكومي
- موظف في القطاع الخاص
- غير موظف
- اخرى :

ما هو تقييمك لمستوى معرفتك حول أمن المعلومات؟

- مبتدىء (مثال: لديك معلومات بسيطة حول أمن المعلومات).
- متوسط (مثال: حصلت على دورة مصغرة في أمن المعلومات).
- متقدم (مثال: حصلت على شهادة جامعية في أمن المعلومات).

خبرة المشارك في استخدام الحكومة الإلكترونية

هل سبق أن استخدمت إحدى الخدمات الحكومية عن طريق الإنترنت مثل سداد المخالفات المرورية أو دفع رسوم الجواز؟

- نعم
- لا

ما هو سبب عدم استخدامك لخدمات الحكومة الإلكترونية (المواقع الحكومية الإلكترونية)؟

- أفضل التقديم عن طريق الفرع
- لا أثق بمستوى الحماية في الحكومة الإلكترونية
- التقديم عن طريق الإنترنت صعب ومعقد
- أغلب الخدمات الحكومية غير متوفرة على الإنترنت

- اخرى :

ما هي طريقتك المفضلة للتقديم على الخدمات الحكومية؟

- التقديم عن طريق الفرع (الطريقة التقليدية).
- عن طريق الهاتف
- عن طريق الإنترنت باستخدام الجهاز المكتبي أو المحمول
- عن طريق تطبيقات الجوال
- عن طريق أجهزة الصراف الآلي

ما هي أكثر الأشياء اللتي تقلق عليها عند استخدامك لخدمات الحكومة الإلكترونية؟

- الدفع عن طريق الإنترنت (الأمور المالية).
- البيانات الشخصية (الأسماء والأرقام والمعلومات الخاصة).
- التأخير في تنفيذ الخدمة
- الفشل في إتمام الإجراءات بالشكل الصحيح
- ليست هنالك أشياء محددة أخشاها عند استخدامي لأنظمة الحكومة الإلكترونية
- اخرى

ما هو الإجراء الذي تتخذه عادة عندما تواجه مشكلة أثناء تقديمك على إحدى خدمات الحكومة الإلكترونية؟

- الإتصال بصديق لطلب المساعدة
- تمرير بياناتك لشخص آخر من أجل التقديم على الخدمة نيابة عنك
- إرسال بريد إلكتروني إلى قسم الدعم الفني
- التقديم في وقت آخر
- التقديم عن طريق الفرع

- اخرى :

خبرة المشارك حول الحماية في الحكومة الإلكترونية

ما هو رأيك حول العبارات التالية:

	أوافق بشدة	أوافق	متوسط	غير موافق	غير موافق بشدة
أخشى كثيراً على خصوصيتي عند استخدام الحكومة الإلكترونية	○	○	○	○	○
أنا لا أثق بمستوى الحماية في الحكومة الإلكترونية	○	○	○	○	○
طريقة تصميم مواقع الحكومة الإلكترونية تؤثر في تقييمي لمستوى الحماية فيها (أو بمعنى آخر، استطيع تقييم مستوى حماية الموقع مبدئياً من خلال طريقة تصميم الموقع).	○	○	○	○	○
العلاقات الإجتماعية والعادات والتقاليد تؤثر في حماية الحكومة الإلكترونية (مثال: من الممكن معرفة بعض المعلومات الشخصية للمستخدمين بطريقة غير شرعية عن طريق العلاقات الإجتماعية).	○	○	○	○	○
وعي المستخدمين حول أمن المعلومات هو من أهم العوامل المؤثرة في حماية الحكومة الإلكترونية	○	○	○	○	○
الإرشادات والنصائح حول أمن المعلومات قليلة جداً سواء في المواقع الحكومية أو في الإعلام	○	○	○	○	○
معظم المخاطر الحالية التي تواجه المستخدمين تأتي من الجانب الغير تقني مثل قلة وعي المستخدمين وعدم ثقتهم بمستوى الحماية	○	○	○	○	○

هل تواجه إجراءات أمنية معقدة (مثل كلمات المرور المؤقته عبر الجوال) عند استخدامك لخدمات الحكومة الإلكترونية؟

- دائماً
- أحياناً

- فقط في الأمور المالية
- لا

عند استخدامك لخدمات الحكومة الإلكترونية، هل واجهت صعوبة في إكمال عملية ما بسبب عدم توفر الخدمة أو البطىء في الإستجابة؟

- دائماً
- أحياناً
- نادراً
- لا

عندما تقوم بإدخال بياناتك الشخصية أو المالية في إحدى الخدمات الحكومة الإلكترونية، هل تتأكد بأن الموقع آمن (على سبيل المثال التأكد من وجود علامة القفل بجانب عنوان الموقع في المتصفح)؟

- دائماً
- أحياناً
- لا
- لا أدري

عند استعراضك لبياناتك المتوفرة على الحكومة الإلكترونية هل تجدها صحيحة؟

- دائماً
- أحياناً
- نادراً
- لا

هل صادفت بأن بياناتك قد تم حذفها، أو طلب منك إدخال بياناتك من جديد في إحدى خدمات الحكومة الإلكترونية؟

- o دائماً
- o أحياناً
- o نادراً
- o لا

ملاحظاتك ووجهة نظرك مهمة جداً بالنسبة إلي، إذا كان لديك أي تعليق أو إضافة تتعلق بالحماية في الحكومة الإلكترونية الرجاء كتابته هنا مشكوراً

جواب

تمت تعبئة الإستبيان بنجاح. شكراً جزيلاً على تعاونك

Appendix D: Main survey (English version)

□actors affecting end user's perception of e-government security and their impact on using e-government services

INFOSECURITY WITH PLYMOUTH UNIVERSITY

Centre for Security, Communications and Network Research (CSCAN)

This survey is a part of PhD research on e-government security at Plymouth University. The aim of this research is to investigate the factors that influence the end user's perception of e-government security and their impact on using e-government services in Saudi Arabia.

There are 3 main sections organised as follows:

1. General information
2. Factor influence end user's perception of e-government security.
3. Factors influence the end user's usage of e-government services.

This survey is designed for adult participation. **IF YOU ARE UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY.** Anyone 18 years old and above can take part in the survey and has the right to withdraw up until the final submission of their responses.

All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data. Should you have any questions about the study or you wish to receive a copy of the results, please contact the researcher Nawaf alharbi via email or address below:

Researcher details:
Nawaf alharbi
Centre for Security, Communications and Network Research (CSCAN)
School of Computing, Electronics and Mathematics

Faculty of Science and Engineering

Plymouth University
United Kingdom
Mail to: nawaf.alharbi@plymouth.ac.uk

If you have any concerns regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Engineering Ethics Committee:

Paula Simson
Faculty of Science and Engineering
Plymouth University, Plymouth, United Kingdom
Phone:+44 (0)1752584503
Mail to: paula.simson@plymouth.ac.uk

Project Supervisors:
Dr Maria Papadaki
Dr Paul Dowland

This survey takes 8 to 15 minutes to be answered.

*** Please note that e-government services mean the government services that you need to use the Internet to perform them (e.g. www.epassport.gove.sa)**

By submitting a response you agree that: I'm 18+ years old and understand that I am free to withdraw up until the point of submission of my responses and I confirm that I have read and understand the information given and agree to take part in the study?

General information

Gender:

- Male
- Female

Age (in years):

- 18 - 24
- 25 - 30
- 31 - 40
- 41 - 50
- 51+

Educational level:

- High School
- Diploma/ Bachelor
- Master/ Doctorate
- Other

What is your employment status?

- Student
- Government employed
- Self-employed
- Other

How long have you been using the Internet? (in years)

- Less than 1 year
- 1 - 3

- 4 - 10
- 10+

Do you use the Internet to apply for e-government services?

- Don't use
- Rarely
- Sometimes
- Often
- Always

Factors that influence end user's perceptions of e-government security

To what extent do you agree with the following statements?

I check the presences of http(s) in the URL when I use e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I check the small padlock icon on e-government websites.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Government websites require users to follow security practices in the selection and use of passwords.

- Strongly disagree
- Disagree

- Neutral
- Agree
- Strongly agree

Government websites has useful mechanisms to verify my identity (such as password + SMS).

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Overall, I am aware of the potential security threats and their negative consequences.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I have sufficient knowledge about the cost of potential security problems.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I understand the concerns regarding information security and the risks they pose in general.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Government websites look organised.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Government websites look secure and safe for carrying out transactions.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Website navigation in government websites is easy.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Anti-cyber-crimes law is helpful for reducing cybercrimes.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Anti-cyber-crimes law is helpful for protecting citizens' private information.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

The government has disciplinary procedures for dealing with citizens who violate information security policy.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I believe that citizens' Internet activities are monitored by the government.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

The government considers information security an important priority.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

The government provides useful security advices through the media and government websites to increase the citizens' security awareness.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Factors influence end user's usage of e-government services

In general, I feel secure using e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I believe the information I provide with government websites will not be manipulated by inappropriate parties.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I am confident that the private information I provide with government websites will be secured.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I think government websites have sufficient technical capacity to ensure that the data I send will not be intercepted by hackers.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I think government websites have sufficient technical capacity to ensure that the data I send cannot be modified by a third party.

- Strongly disagree
- Disagree
- Neutral

- Agree
- Strongly agree

I think e-government shows concern for the privacy of its users.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I feel safe when I send personal information to e-government.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I am not concerned that the information I submitted on e-government could be misused.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

The Internet is trustworthy.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I have confidence in the technology used by government agencies to operate the e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Government agencies can be trusted to carry out online transactions faithfully.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I believe that e-government services are trustworthy.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I intend to continue using e-government services in the future.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I will always try to use e-government services in my daily life.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I plan to continue to use e-government services frequently.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I find e-government services useful in my daily life.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Using e-government services help me accomplish things more quickly.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Using e-government services would save citizens' time.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

It is easy for me to become skilful at using e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I find e-government services easy to use.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Learning how to use e-government services is easy for me.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

The use of e-government has become a habit for me.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I must use e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Using e-government has become natural to me.

- Strongly disagree
- Disagree
- Neutral
- Agree

- Strongly agree

I have the resources necessary to use e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I have the knowledge necessary to use e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

I can get help from others when I have difficulties using e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

People who influence my behaviour think that I should use e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

People who are important to me think that I should use e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

People whose opinions that I value prefer that I use e-government services.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

The survey has been successfully completed

Thank you for your cooperation

Appendix E: Main survey (Arabic version)

العوامل التي تؤثر على تصور المستخدم لمستوى الحماية في الخدمات الحكومية الإلكترونية ومدى تأثيرها على استخدامه للخدمات

INFOSECURITY WITH PLYMOUTH UNIVERSITY

Centre for Security, Communications and Network Research (CSCAN)

مركز أبحاث أمن المعلومات، الإتصالات، والشبكات

استبيان عن العوامل التي تؤثر على تصور المستخدم لمستوى الحماية في الخدمات الحكومية الإلكترونية بالمملكة العربية السعودية ومدى تأثيرها على استخدامه للخدمات.

يجري عمل هذا الاستبيان ضمن بحث لمرحلة الدكتوراة عن الحماية في الحكومة الإلكترونية، جامعة بليموث، بريطانيا.

يحتوي الاستبيان على ثلاثة أقسام رئيسية وهي:

1- **معلومات عامة عن المشارك.**

2- **العوامل التي تؤثر على تصور المستخدم لمستوى الحماية في الخدمات الحكومية الإلكترونية.**

3- **العوامل التي تؤثر على استخدامه للخدمات الحكومية الإلكترونية.**

هذا الاستبيان معد لمشاركة البالغين. **إذا كان عمرك أقل من 18 سنة، آمل عدم الإجابة على أسئلة الاستبيان.** أي مشارك بلغ ال18 سنة فما فوق يحق له المشاركة في هذا الاستبيان و له الحق في الإنسحاب في أي وقت قبل التسليم النهائي للإجابات.

جميع الإجابات سيتم التعامل معها بسرية و الردود ستكون مجهولة المصدر خلال جمع البيانات، التخزين، أو نشر المادة العلمية. إجابات المشاركين سيتم التعامل معها بسرية تامة في جميع اوقات ومراحل العمل وسيتم عرضها بطريقة لا يمكن من خلالها الربط بين هوية المشارك و المعلومات المنشورة.

في حالة الرغبة في الإستفسار حول الدراسة أو الحصول على نسخة من النتائج، آمل التواصل مع الباحث على العنوان التالي:

بيانات الباحث:
Nawaf alharbi
Centre for Security, Communications and Network Research (CSCAN)
School of Computing, Electronics and Mathematics, Plymouth University
Mail to: nawaf.alharbi@plymouth.ac.uk

إذا كان لديك ما يثير تحفظك بخصوص طريقة إجراء هذه الدراسة، آمل التواصل مع سكرتير لجنة الأخلاقيات بكلية العلوم والتكنولوجيا:

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Engineering, Plymouth University
Phone:+44 (0)1752584503
Mail to: paula.simson@plymouth.ac.uk

المشرفين على البحث:
Papadaki Dr Maria
Dr Paul Dowland

هذا الاستبيان يستغرق من 8 إلى 15 دقائق لإكماله

ملاحظة

المقصود بالخدمات الحكومية الإلكترونية هي الخدمات الحكومية التي يتم التقديم عليها عن طريق الإنترنت مثل (أبشر والخدمات الإلكترونية لوزارة الداخلية).

بتسليم أجاباتك فأنت توافق على ما يلي: عمري فوق 18 عام وأؤكد بأني قرأت وفهمت المعلومات المعطاه وأوافق على المشاركة في هذه الدراسة وأعلم أنه بإمكاني الإنسحاب من المشاركة في الاستبيان في أي وقت قبل التسليم النهائي للإجابات

القسم الأول: معلومات عامة

الجنس

- ذكر
- أنثى

الفئة العمرية (بالسنوات)

- 18 - 24
- 25 - 30
- 31 - 40
- 41 - 50
- 51+

آخر مؤهل دراسي حصلت عليه

- الثانوية العامة
- دبلوم / بكالوريوس
- ماجستير / دكتوراه
- أخرى

ماهي حالتك الوظيفية

- طالب
- موظف حكومي
- موظف في قطاع خاص
- أخرى

منذ متى وأنت تستخدم الإنترنت؟ (بالسنوات)

- أقل من سنة
- 1 - 3
- 4 - 10
- 10+

هل تستخدم الإنترنت لإنجاز معاملاتك الحكومية؟

- لا استخدم
- نادراً
- أحياناً
- غالباً
- دائماً

القسم الثاني

العوامل التي تؤثر على تصور المستخدم

لمستوى الحماية في الخدمات الحكومية الإلكترونية

إلى أي مدى توافق على العبارات التالية من وجهة نظرك؟

أنا أتحقق من وجود https في بداية عنوان المواقع الحكومية الإلكترونية.

- غير موافق بشدة
- غير موافق
- محايد
- موافق
- موافق بشدة

أنا أتحقق من وجود أيقونة القفل في المواقع الحكومية الإلكترونية.

- غير موافق بشدة
- غير موافق
- محايد
- موافق
- موافق بشدة

المواقع الحكومية الإلكترونية تطلب من المستخدمين استخدام كلمات سر معقدة.

- غير موافق بشدة
- غير موافق
- محايد
- موافق
- موافق بشدة

المواقع الحكومية الإلكترونية تستخدم وسائل مفيدة للتحقق من هوية المستخدم (مثال، كلمة سر ورسالة جوال)

- غير موافق بشدة
- غير موافق

- **محايد**
- **موافق**
- **موافق بشدة**

بشكل عام، لدي الوعي حول التهديدات المحتملة التي تواجه أمن المعلومات وأدرك الآثار السلبية المترتبة عليها.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

لدي المعرفة الكافية حول تكلفة المشاكل التي قد تواجه أمن المعلومات.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أنا مدرك للمخاوف المتعلقة بأمن المعلومات والمخاطر التي تحدث بسببها بشكل عام.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

المواقع الحكومية الإلكترونية تبدو منظمة بشكل ممتاز.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

المواقع الحكومية الإلكترونية تبدو آمنة وموثوقة.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**

- **موافق**
- **موافق بشدة**

يمكنني التنقل من قسم إلى قسم داخل المواقع الحكومية الإلكترونية بسهولة.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

نظام مكافحة الجرائم الإلكترونية يساعد في تقليل الجرائم الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

نظام مكافحة الجرائم الإلكترونية مفيد في حماية معلومات المواطنين السرية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

الدولة لديها إجراءات تأديبية للتعامل مع المواطنين الذين يخالفون سياسة أمن المعلومات.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أعتقد بأن الدولة تراقب أنشطة المواطنين على الإنترنت.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

الدولة تعطي أمن المعلومات أولوية هامة.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

الدولة تقدم نصائح مفيدة للمواطنين عن الحماية لزيادة وعي المواطنين بأمن المعلومات.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

القسم الثالث

العوامل التي تؤثر على استخدام الخدمات الحكومية الإلكترونية

بشكل عام، أشعر بأن الخدمات الحكومية الإلكترونية آمنة.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أعتقد بأن معلوماتي التي أقدمها من خلال الخدمات الحكومية الإلكترونية لن يتم التلاعب بها عن طريق أطراف أخرى مجهولة.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أنا واثق بأن معلوماتي السرية التي أقدمها خلال استخدامي للخدمات الحكومية الإلكترونية سوف تكون آمنة.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**

- **موافق**
- **موافق بشدة**

أعتقد بأن الخدمات الحكومية الإلكترونية لديها القدرة التقنية الكافية لضمان عدم اعتراض قراصنة الإنترنت للبيانات التي أرسلها.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أعتقد بأن الخدمات الحكومية الإلكترونية لديها القدرة التقنية الكافية لضمان عدم حدوث تغيير على بياناتي عن طريق أطراف أخرى مجهولة.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أعتقد أن الخدمات الحكومية الإلكترونية تظهر اهتمام حول خصوصية المستخدمين.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أشعر بالأمان عندما أرسل معلومات شخصية عبر الخدمات الحكومية الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أنا لا أخشى بأن يساء استخدام معلوماتي الشخصية عند استخدامي للخدمات الحكومية الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**

- **محايد**
- **موافق**
- **موافق بشدة**

أعتقد بأن الإنترنت موثوق بشكل كاف.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

لدي الثقة في الأدوات والبرامج المستخدمة في الخدمات الحكومية الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

القطاعات الحكومية موثوقة وقادرة على تقديم خدمات إلكترونية موثوقة ومؤتمنة.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

من وجهة نظري أن الخدمات الحكومية الإلكترونية موثوقة.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أنا أنوي الاستمرار في استخدام الخدمات الحكومية الإلكترونية في المستقبل.

- **غير موافق بشدة**
- **غير موافق**

- **محايد**
- **موافق**
- **موافق بشدة**

سوف أحاول دائماً أن استخدم الخدمات الحكومية الإلكترونية في حياتي اليومية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

أنا أخطط لاستخدام الخدمات الحكومية الإلكترونية بشكل متكرر.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

الخدمات الحكومية الإلكترونية مفيدة في حياتي اليومية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

استخدام الخدمات الحكومية الإلكترونية يساعدني على إنجاز معاملاتي الحكومية بشكل أسرع.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

استخدام الخدمات الحكومية الإلكترونية يزيد فرص العدل والمساواة بين المواطنين.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

من السهل بالنسبة لي أن أصبح ماهراً في استخدام الخدمات الحكومية الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

الخدمات الحكومية الإلكترونية سهلة الاستخدام.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

تعلم كيفية استخدام الخدمات الحكومية الإلكترونية سهل بالنسبة لي.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

استخدام الخدمات الحكومية الإلكترونية أصبح شيئاً اعتيادياً بالنسبة لي.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

بالنسبة لي، استخدام الخدمات الحكومية الإلكترونية أمر لا بد منه.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

استخدام الخدمات الحكومية الإلكترونية أصبح أمراً طبيعياً بالنسبة لي.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

لدي المتطلبات الضرورية لاستخدام الخدمات الحكومية الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

لدي المعرفة الكافية لاستخدام الخدمات الحكومية الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

يمكنني الحصول على مساعدة من الآخرين عندما أواجه صعوبات في استخدام الخدمات الحكومية الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

الأشخاص الذين لهم تأثير على قراراتي يعتقدون بأنه يجب أن استخدم الخدمات الحكومية الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**
- **محايد**
- **موافق**
- **موافق بشدة**

الأشخاص المهمون بالنسبة لي يعتقدون أنه يجب أن استخدم الخدمات الحكومية الإلكترونية.

- **غير موافق بشدة**
- **غير موافق**

- محايد
- موافق
- موافق بشدة

الأشخاص الذين تعجبني آرائهم يفضلون أن استخدم الخدمات الحكومية الإلكترونية.

- غير موافق بشدة
- غير موافق
- محايد
- موافق
- موافق بشدة

تمت تعبئة الاستبيان بنجاح،
شكراً جزيلاً لك على تعاونك