ASSESSING USABLE SECURITY OF MULTIFACTOR AUTHENTICATION

MAHA MOHAMMED ALTHOBAITI

A thesis submitted to the School of Computing Sciences of the University of East Anglia for the fulfilment of the degree of Doctor of Philosophy (PhD) in Computing Sciences

June 2016

DEDICATION

بسم الله الرحمن الرحيم

إلى والديّ الكريمين

محمد الثبيتي حفظه الله
شريفه الثبيتي حفظها الله

For their infinite wisdom, this thesis is dedicated with much love to my parents,

Mohammed Althobaiti
Sharifa Althobaiti

هذا من فضل الله

ABSTRACT

An authentication mechanism is a security service that establishes the difference between authorised and unauthorised users. When used as part of certain website processes such as online banking, it provides users with greater safety and protection against service attacks and intruders. For an e-banking website to be considered effective, it should provide a usable and secure authentication mechanism. Despite existing research on usability and security domains, there is a lack of research on synthesising the contributions of usable security and evaluating multifactor authentication methods. Without understanding the usability and security of authentication mechanisms, the authenticating process is likely to become cumbersome and insecure. This negatively affects a goal of the authentication process, convenience for the user.

This thesis sought to investigate the usability and security of multifactor authentication and filled an important gap in the development of authenticating processes. It concentrated on users' perspectives, which are crucial for the deployment of an authenticating process.

To achieve the thesis goal, a systematic series of three studies has been conducted. First, an exploratory study was used to investigate the current state of the art of using multifactor authentication and to evaluate the usability and security of these methods. The study involved a survey of 614 e-banking users, who were selected because they were likely long-term users of online banking and they had two different bank accounts, a Saudi account and a foreign account (most foreign accounts were British). The study indicated that multifactor authentication has been widely adopted in e-banking in Saudi Arabia and the United Kingdom, with high levels of security and trustworthiness as compared to single factor authentication.

The second study was a descriptive study of the most common authentication methods. This study aimed to learn more about commonly used methods that were identified in the previous study and sought to propose an appropriate combination of authentication methods to be evaluated in the third study. The third study was an experimental study with 100 users to evaluate the usable security of three different multifactor authentication methods: finger print, secure device and card reader. A web based system was designed specifically for this study to simulate an original UK e-banking website. One of the main contribution of this study was that the system allowed users to choose their preferred authentication method. Moreover, the study contributed to the field of usable security by proposing security evaluation criteria based on users' awareness of security warnings. The key result obtained indicated that fingerprinting was the most usable and secure method. Additionally, the users' level of understanding security warnings was very low, as shown by their reaction to the security indicators presented during the experiment.

ACKNOWLEDGMENT

First and foremost, I would like to express my thanks and sincerest gratitude to Allah, my creator, who provided me with the time, health and ability to accomplish this work.

Next, I owe deep thanks and gratitude to my supervisor, Dr. Pam Mayhew, for kindly contributing her valuable time and effort in providing advice, enthusiastic encouragement and moral support at every step of this work. Dr. Pam's advice helped me to gain a real sense of perspective and clarity.

I would also like to extend my gratitude to Dr. Joost Noppen and Dr. Dan Smith for their continuous help, valuable discussions and support throughout my studies at the University of East Anglia. I would also like to thank Prof. Raul Sanchez-Reillo (University Carlos III of Madrid) for comments and advice on earlier drafts of this thesis as it was being shaped.

I am indebted to my parents who encouraged me from the beginning to complete my higher education. Many thanks to both of them for giving me, throughout my life, their continuous and unconditional love, prayers, support, encouragement and guidance, without which I would not have been able to finish this work.

I would also like to extend my gratitude to my husband, Dr. Salem Alalwani, who has shared the journey with me to complete my higher education. Many thanks to my brothers, who encouraged me throughout my studies. Finally, special thanks to Waleed, Hazim and Dr. Asim Althobaiti for their continuous help and prayers.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AM	**A**uthentication **M**ethod
BBA	**B**iometrics **B**ased **A**uthentication
CIA	**C**onfidentiality, **I**ntegrity and **A**vailability
HCI	**H**uman **C**omputer **I**nteraction
ISO	**I**nternational **S**tandard **O**rganisation
KBA	**K**nowledge **B**ased **A**uthentication
MFA	**M**ulti **F**actor **A**uthentication
MMI	**M**an **M**achine **I**nteraction
SDLC	**S**oftware **D**evelopment **L**ife **C**ycle
SEC	**SEC**urity
SFA	**S**ingle **F**actor **A**uthentication
SPSS	**S**tatistical **P**ackage for the **S**ocial **S**cience
TBA	**T**oken **B**ased **A**uthentication
UI	**U**ser **I**nterface
USA	**USA**bility
USA-SEC	**USA**ble - **SEC**urity
WWW	**W**orld **W**ide **W**eb

LIST OF PUBLICATIONS

Conference:

- Althobaiti, M.M., Mayhew, P., (2014). Security and usability of authenticating process of online banking: User experience study. *In the Proceedings of the 48 Annual IEEE International Carnahan Conference on Security Technology*, ICCST 2015, IEEE.

- Althobaiti, M.M., Mayhew, P., (2015). Usable Security of Authentication Process: New Approach and Practical Assessment. *In the Proceedings of 10th International Conference for Internet Technology and Secured Transactions*, ICITST 2015 14 -16 Dec 2015.IEEE.

- Althobaiti, M.M., Mayhew, P. (2016). "Usable Security of Authentication Process: Experimental Study". 9th Scientific Saudi Conference (SSC9). 13-14 Feb 2016.

Journal:

- Althobaiti, M.M., Mayhew, P., (2015). Assessing Usable Security of Multifactor Authentication. *Journal of Internet Technology and Secured Transaction*. 4 (4), pp 420- 426.

- Althobaiti, M.M., Mayhew, P. (in press). Users' Awareness of Visible Security Design Flaws. *International Journal of Innovation, Management and Technology*. (Accepted).

The following publications stemmed from the author's MSc thesis, which helped her to expand and build her knowledge in the field of Human Computer Interaction:

- Althobaiti, M.M., Mayhew, P., (2016). Assessing the Usability of Learning Management System: User Experience Study. *In the Proceedings of e-learning, E-education and Online Training – Second International Conference*, eLEOT 2015. Springer Berlin Heidelberg.

- Althobaiti, M.M., Mayhew, P., (2016). How Usable Are the Learning Management Systems? The Users Have Their Say. EAI Endorsed Transactions on e-Learning [Special Issue]. (Accepted).

Chapter 1

Introduction

Authentication mechanisms are considered the typical method to secure financial websites. Context authentication has become increasingly important in the arena of online banking. Multifactor authentication is the most commonly used method of strengthening the login process in e-banking. Despite existing research on usability and security domains, there is a lack of research on synthesising the contributions of usable security and evaluating multifactor authentication methods. Therefore, this thesis seeks to investigate the usability and security of multifactor authentication and fills an important gap in the development of authenticating processes.

The current chapter gives an overview of the current research and identifies the research gap that motivated this study. Then, the justification of the research is provided, followed by the research aims and objectives. A list of the proposed questions for the research is presented, and finally, an overview of the research structure and thesis organisation is given to conclude the chapter.

1.1 Research Overview and Motivation

Recent advances in communication and computer technology have revolutionised the Internet and the field of information technology, which play an essential role in business and affect all other aspects of society. Financial institutions have been eager to establish their own websites and use the Internet to provide customers with virtual access replicating traditional services that take place in person at an institution's building and are frequently associated with unnecessary standing in queues. The benefits of financial websites include user convenience, simplified transactions and 24-hour availability. The increasing number of Internet users has driven financial institutions to provide electronic services; according to the Office for National Statistics (2015), 86% of adults in the UK (44.7 million) use the Internet.

Financial websites deal with sensitive information, which makes security a priority. High-risk information, such as user names, passwords and credit card details, is sent from a website to a destination server and thus needs to be protected. Secure websites deploy protocols, such as secure socket layer (SSL) certificates, to encrypt sensitive information (Soghoian and Stamm, 2010).

Bank customers use electronic banking (e-banking) to conduct financial transactions. Authentication, the first step in account access, takes place when a user's identity is verified. The level of website security depends upon the strength of the website's authentication mechanisms.

The authentication process is mainly an interaction between a human and a computer, and, thus, a high usability level is required to provide users with an easy-to-use

process. At the same time, a good level of security is required to protect user information from attackers. Achieving high security depends not only on the system features provided by the financial organisation but also on user behaviour. A US Secret Service survey of 500 US business executives has shown the relationship between the security leaks that have occurred amongst major companies in the US and user practice (US Secret Service et al., 2014).

Several authentication methods are available in the market. For example, using a password to confirm user identity is one way that can be utilised during the authentication phase. Other methods, such as the use of tokens, cards and biometrics, can also be combined with a password to strengthen the authentication process. This technique is called multifactor authentication. Companies tend to improve authentication security and usability according to developers' and experts' recommendations. For example, the European Union Agency for Network and Information Security (2013) conducted a survey involving 100 professionals. The goals were to identify the authentication mechanisms used in financial and payment services and determine the risks associated with them. The results of the survey led to several recommendations, which promote the adequacy of the Electronic IDentity and Authentication Systems method for context and, specifically, the 'proportionality of method and risk' (ENISA, 2013). The recommendations included using two-factor (2F) authentication, such as utilising tokens and passwords for all operations, including low-risk ones, and improving the knowledge and behaviours of both customers and professionals, including those who improve e-finance security environments, e-finance application development and distribution security (ENISA, 2013). These recommendations underline the responsibility of e-banking in improving

security and usability and suggest that having 2F authentication is one way to improve the security level.

Little research has discussed the conflict between security and usability (Besnard and Arief, 2004; Furnell, 2005; Nodder, 2005). The challenge of integrating usability into security has motivated researchers to investigate numerous authentication methods, but considerable room exists for further research to find a satisfactory solution. The lack of proper assessment methods has created a gap that needs to be examined. This thesis aims to fill such a gap through an in-depth assessment of the usability and security of the most advanced authentication mechanisms widely available.

1.2 Justification: Why Authentication and Usability?

Without authentication, a computer system has no foundation to establish whether access should be granted. For online banking, proper and strong authentication is a major concern to determine if a user is eligible to access a specific system. In information technology, humans are considered the weakest link that can make a certain system vulnerable to attack (Vacca, 2013). Therefore, strong authentication is required to make access to e-services difficult to hack.

Prior research indicates that users' typical behaviours with single-factor authentication, such as the use of passwords and PINs, reduce the security level of already-weak mechanisms (Carullo et al., 2012; Brostoff et al., 2010). Other research shows that multifactor authentication improves the security level against attacks because it asks users to provide more than one identifying entity (Bhivgade et al., 2014). However, other studies (Bonneau et al., 2012; Gunson et al., 2011) indicate the

low level of usability of multifactor authentication. These studies emphasise the conflict between usability and security in the provision of authentication mechanisms (Besnard and Arief, 2004; Furnell, 2005; Nodder, 2005). Considerable research has acknowledged that authentication methods as solutions can benefit from improvements in usability (Hafiz et al., 2008). However, robust literature reviews have revealed a limited amount of research related to evaluating the usability of multifactor authentication (Krol et al., 2015; Weir et al., 2009). The current study fills the gap in the area of assessing the usable security of multifactor authentication to offer guidance in the development of a new security technology and usable interface.

The research encompasses users' perceptions and attitude towards authentication methods, which may lead to improvements in bank providers' online security (Voice, 2005). In addition, the findings might reduce the use of low-cost methods that are associated with usability issues (Knight, 2008). The study will involve a non-Western context because previous studies focused only on developed countries. Saudi Arabia, which is considered the powerhouse of the Middle East and has an attractive potential market for e-commerce application (Png et al., 2001), is selected as the focus of the research.

In general, this research will extend previous work by

1. Investigating the current use of single and multifactor authentication,
2. Comparing each in terms of usability and security,
3. Studying the difference between developing and developed countries in their use of multifactor authentication,
4. Examining user perceptions of single and multifactor authentication,

5. Providing quantitative and qualitative assessments of the usability of each type of authentication,
6. Exploring user preferences for different types of multifactor authentication methods,
7. Examining the conflict between security and usability in different combinations of authentication,
8. Investigating users' awareness of security warnings.

1.3 Research Objectives

The primary aim of this research is to explore the current state of using multifactor authentication methods and to experimentally determine the most usable and secure method. Multifactor authentication methods will be carefully selected for the study, and a list of recommendations based on the results will be produced.

The study will

1. Provide an understanding of the literature that addresses authentication and the usability and security offered by authentication,
2. Explore the current state of single and multifactor authentication methods,
3. Evaluate the usability of single and multifactor authentication techniques in developing and developed countries from users' perspectives,
4. Review the available authentication methods and propose suitable methods for the experimental study,
5. Experimentally assess the usability, security and trustworthiness of different multifactor authentication techniques,
6. Experimentally measure security through an examination of users' awareness of security warnings, and

7. Propose recommendations based on the research results and the researcher's experiences.

1.4 Research Questions

The main research question involves identifying the most usable multifactor authentication method.

The specific research questions are as follows:

1. What are the authentication methods used by online banking websites?
2. What are users' perceptions of the usability and security of these authentication methods?
3. What is the most usable and secure multifactor authentication method for online banking usability?
4. To what extent does the security level affect the usability rate when different kinds of authentication techniques are used?
5. To what extent do security warnings affect users' behaviour?

1.5 Contributions and Achievements

The key contributions of this thesis are as follows:

Identifying the research gap

Chapter Two reviewed studies related to the security and usability of authentication methods and identified the limitations in this field. Of these, only five papers focused on the usability of multifactor authentication, whereas none examined the methods that were explored in this thesis. The current literature lacks a focus on the security attributes to be measured during usable security evaluation. The current thesis

therefore explores studies in the security warnings area and links these to the security tasks of the authentication process to show the relationship between the two concepts.

Current state of authentication methods

A usability evaluation was conducted with a survey involving 614 respondents to investigate the current state of authentication. This survey included questions on security, trustworthiness and usability. To the best of our knowledge, this is the first study that focuses on Saudi customers of online banking. The sample was selected carefully; the participants were ensured to have a long experience with e-banking and have two different bank accounts from a developed and a developing country.

Analysis of the usability of single and multifactor authentication

The exploratory study in Chapter Four showed different authentication methods, including single factor authentication. An analysis to compare the usability and security between single and multifactor authentication was conducted, and the results provided a clear picture of the high security of multifactor authentication on the basis of the perceptions of users who have a long experience in using both methods.

Analysis of different authentication methods

A comprehensive and extensive analysis of seven popular authentication approaches was conducted objectively and in a way that guided the finding of a combination of the most appropriate methods that could be examined in the experimental stage of this thesis. The study found that a biometric method should be included to achieve new and logical evaluation results.

Novel approach to evaluating authentication methods

The experiment presented in Chapter Six was designed to evaluate the suggested authentication methods in terms of usability and security. The approach simulated online banking at the HSBC Bank because the participants were British, and many HSBC customers were expected to take part in the experiment. The approach included three different methods (card reader, secure device and fingerprint) for usability and security comparison, and it gave each participant the opportunity to have a real experience with each method so that the results are more accurate. To the best of our knowledge, no previous studies used the same assessment methods (Chapter Six).

Security analysis

The security analysis undertaken in Chapter Six focused on the proposed criteria related to users' awareness of security warnings. The results revealed a clear picture of the low level of user awareness of security warnings.

1.6 Overview of the Thesis

The remainder of the thesis is organised as follows:

- Chapter Two presents a comprehensive and extensive review of the concepts and previous research related to this thesis. It starts by reviewing system usability and the methods to evaluate usability. Then, it reviews the concepts of security, online banking, trust, usable security and security warning. Finally, the chapter ends with a review of the classification of authentication methods.

- Chapter Three gives readers a clear picture of the three methodology strategies used in this thesis (exploratory, descriptive and experimental), followed by the ethical considerations and the data analysis strategy.

- Chapter Four presents the exploratory study that investigates the usability and security of the methods used in different countries. This chapter also explains the data collection process and the results.

- Chapter Five describes the advantages and disadvantages of different authentication approaches. The analysis includes biometrics authentication, and the chapter proposes a combination of different methods to be examined practically in the following chapter.

- Chapter Six presents the experiment study that was designed to evaluate three different authentication methods in terms of usability and security. The experiment steps, starting from designing the platform to performing the experiment, are explained in detail, followed by an in-depth analysis of the collected data.

- Chapter Seven discusses the interpretations of all study findings. In particular, the researcher intends to link the results from all studies with prior research

conducted in the field of usable security. This chapter also provides a list of the researcher's recommendations.

- Chapter Eight offers a summary of the research and identifies the key contributions made by this study to the field of usable security. This chapter also presents a discussion of the research limitations and addresses avenues for the expansion of future work.

Chapter 2

Literature Review

In this chapter, the state of the art of the evaluation of usable and secure authentication processes is reviewed. The chapter identifies common themes in the fields of human computer interaction (HCI) and security. Based on the scope of this thesis, the chapter involves several other themes: online banking, trust, authentication, and warnings, in order to set up the bases of all themes that are related to the thesis context.

The chapter also includes a review of the studies and research that have explored the usability of authentication methods. Finally, the chapter presents the scope of the thesis, and a conclusion to the chapter.

2.1 Human computer interaction

The terms HCI or man-machine interaction have been widely used since the early 1980s. According to Dix et al. (2004), they relate to the interaction between machines

and humans and the effect of the physical characteristics on user performance. Generally, HCI is subject to issues that interfere with the availability of functionality or the proper use of the system by the user, not the guarantee of a usable system. Rogers (2004) stated that HCI has been used to define the properties of an object that allow the user to know how to use them. The main two terms that HCI illuminates are usability and functionality (Te'eni et al., 2007). An effective system can be achieved when there is a balance between usability and functionality (Nielsen, 1993).

The HCI discipline helps us to understand the performance differences between software systems, and why there are 'good' and 'bad' systems. The definition of HCI according to Computer Science Curricula (2013) is ' Human Computer Interaction (HCI) is concerned with designing interactions between human activities and the computational systems that support them, and with constructing interfaces to afford those interactions.' (p.89)

2.2 Usability

Usability is easy to understand, but its practical, high-level application to a website can be more difficult. Nielsen's (1996) definition of usability encapsulates five components: learnability, efficiency, memorability, few errors and user satisfaction (see Figure 2.1).

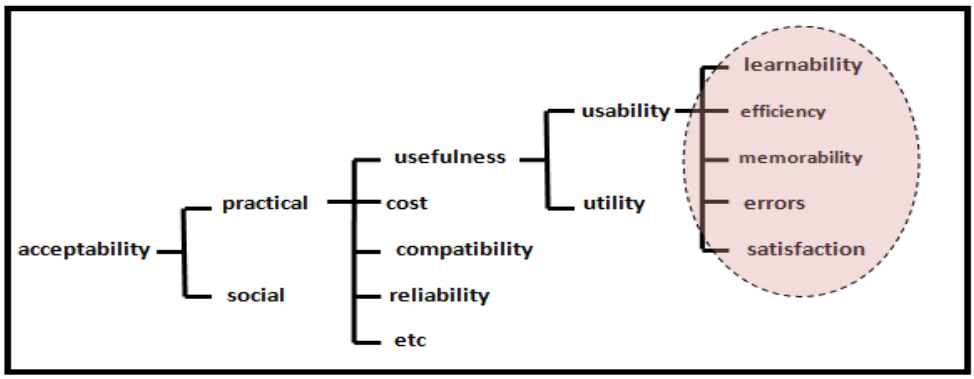


Figure 2.1 The definition of the usability according to Nielsen (1994)

Three international standards have defined usability (Table 2.1). The literature makes it clear that usability reflects ease of use, one of the main goals of HCI, which in turn involves the study of the interactions between users and technology (Battleson et al., 2001). Usability also measures consumers' subjective experiences with an application. Do they like it? Do they feel that they have painlessly achieved their objective(s)? For banking websites, the second question which we are talking about here is especially relevant.

Standard	***Usability definition***
(IEEE Std.610.12, 1990, p. 80)	"The ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component."
(ISO9241-11, 1998)	"The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."
(ISO/IEC 9126-1, 2000)	"The capability of the software product to be understood, learned, used, and attractive to the user, when used under specified conditions."

Table 2.1 Different definitions of usability according to different standards

2.2.1 Benefits of Usability

Usability offers benefits, not merely for end users, but also for organisations that develop software and applications. Xerox (cited in Pieratti, 2005) stated that usability:

1. Provides a more efficient design for developing products,
2. Helps to orient the design toward the needs of real users,
3. Can reduce training and support development costs,
4. Satisfies customers by offering more usable products.

Several leading corporations, for example, Apple Inc., American Airlines and Microsoft Corporation, integrate usability engineering into their product development cycles (Pieratti, 2005).

2.2.2 Usability Attributes

As shown in Table 2.1, the ISO defines three primary factors of usability: effectiveness, efficiency and satisfaction. While Nielsen's definition of usability consists of five attributes: learnability, efficiency, memorability, errors and satisfaction. Each is considered a base for achieving the usability of a website (Nielsen, 1993). Brief explanations of these attributes follow.

Learnability

The system should be easy to learn. Learnability can be measured by counting the number of correct steps when performing a particular task after the first time.

Efficiency

A system should be efficient. High productivity can be achieved if the system is easy to understand and the user can complete the task within an acceptable amount of time. The efficiency can be measured by calculating the time consumed to complete a task.

Memorability

The system functions should be easy to remember, so that a casual user can return to the system without relearning how to use it. Memorability can be measured by counting the number of steps remembered and performed by the user in the second usage.

Errors

A system should have a low error rate. The error rate can be measured by counting the number of errors made by the user while performing a specific task.

Satisfaction

The system should be pleasant to the user, which will be reflected in user satisfaction. Satisfaction can be assessed by subjective, qualitative inquiry into whether the user was happy with the system.

Nielsen's attributes were applied in different studies, however, other standards and models have similar or different attributes, as summarised in Table 2.2 below:

Standard	**Nielsen (1993)**	**Shackel (1991)**	**Preece et al. (1994)**	**ISO 9241-11 (1998)**	**Constantine & Lockwood (1999)**	**Shneiderman (2005)**	**Quesenbery (2010)**
Attribute	Learnability	Learnability	Learnability	Effectiveness	Learnability	Time to learn	Easy to learn
	Efficiency	Effectiveness	Throughput	Efficiency	Efficiency	Performance	Efficient
	Satisfaction	Attitude	Attitude	Satisfaction	Satisfaction	Satisfaction	Effective error tolerant
	Errors	Flexibility			Reliability	Errors	Engaging
	Memorability				Memorability	Retention	

Table 2.2 Overview of usability attributes

2.2.3 Methods for evaluating usability

The evaluation of usability refers to gathering information about the usability of a system in order to assess it. According to Fitzpatrick (1998, p.2), a usability evaluation method is a 'systematic procedure for recording data relating to end-user interaction with a software product or system'. The data gathered from the evaluation process is analysed and assessed to determine the usability level. There are three general goals of the assessment: evaluate users' experience of the interaction with the system, identify the system's problems during a specific task and evaluate the system's functionality (Dix et al., 2004).

There are different approaches to evaluation. According to Faulkner (2000), evaluation is divided into two categories: formative and summative. Formative evaluation is conducted during the system development life cycle (SDLC) to advance and improve the system design. This process is repeated until the desired usability level is achieved.

A summative evaluation is conducted after the development phase has been completed, to assess the usability and overall performance of the system. The system can also be compared with other systems.

According to Dix et al. (2004), evaluation can be categorised according to the location, for example, the normal, working environment or the laboratory. Lewis and Rieman (1994) divided the approach to evaluation according to whether the system was assessed with or without the user.

Table 2.3 below summarises different approaches to evaluating a system.

	Faulkner (2000)	**Dix et al. (2004)**	**Lewis & Rieman (1994)**
Category	Formative	Laboratory environment	User involved
	Summative	Natural environment	Without user

Table 2.3 Different approaches for evaluating system

2.2.4 Usability evaluation methods classification

An important stage of usability evaluation is choosing one or more evaluation methods—depending on the assessment aim—to discover usability problems and to measure users' performance in reaching the goals of a certain task. Several authors have identified a number of different evaluation methods (Preece, 1993; Shneiderman and Plaisant, 2005; Dix et al., 2004), some of which require the involvement of users, and others that require the involvement of experts in the field (Anandhan et al., 2006). Table 2.4 presents an overview of the various usability evaluation methods, followed by a discussion of each method.

Method	***Evaluator***	***Example of techniques***	***Evaluators' role***
Model based	Expert	GOMS , Web Metrics.	Use model to extract usability measure
Inspection	Expert	Cognitive walkthrough, Heuristic evaluation.	Review the examined user interface to identify the problems.
Testing	User	Thinking aloud, Co-discovery learning, Remote testing	Observe users during using the system and analyse the collected data to identify problems
Inquiry	User	Interviews, focus groups, questionnaire	Asked the users to get insights to define the problems.

Table 2.4 Overview of usability evaluation methods

2.2.4.1 Model based method

A model-based evaluation creates a model of how a user responds to a proposed system (Kieras, 2003). Different versions of the technique exist based on the goals, operators, methods, and selection (GOMS) procedure (CMN-GOMS, KLM, NGOMSL and CPM-GOMS), which is used to predict the time needed to complete a task and the most effective steps for completing a task (Preece et al., 2002). Although GOMS has proven effective in evaluating user interfaces (UIs), it is not widely used (John & Kieras, 1996). The most complex model from the GOMS family is CPM-GOMS, developed by Gray et al. (1993). In this method, the predicted execution time

is based on sequential dependencies between the users' perceptual, motor, and cognitive processes.

All GOMS techniques produce quantitative results of how the user will use the system. However, these techniques are limited by their need for skilled users, as intermediate or beginner users may make errors that affect the data (Preece et al., 2002). Additionally, the GOMS model is considered a time-consuming method to evaluate the system (Lewis & Rieman, 1994). Kieras (2007) stated that several issues are associated with analysing the GOMS model: "The mental processes of the user are incredibly complex; trying to describe all of them would be hopeless" (p. 5). Owing to the complexity inherent in their implementation, the model-based evaluation methods will not be addressed in this thesis.

2.2.4.2 Inspection Method

The usability inspection method is an approach to assess system usability; it includes cognitive walkthrough and heuristic evaluation, and it requires human inspectors to identify usability problems. This method can usually be conducted in less time compared to other evaluation methods (Sears & Hess, 1999).

- ***Cognitive walkthrough***

  Cognitive walkthrough originally developed from the code walkthrough familiar to software engineers (Blackmon et al., 2002). In this evaluation process, the evaluator walks through a systematic sequence of actions in the proposed system to uncover potential problems. To ensure the user can learn the system easily, the evaluator will try to answer the following questions:

- Will the user be able to perform the task?
- Will the user be able to access all the functionality of the system?
- Will the user obtain feedback about each action, either correct or incorrect? (Preece et al., 2002).

This method is considered fast and does not require prior training (Sears & Hess, 1999). However, Lewis and Rieman (1994) pointed out that this method does not test the real users, and the evaluators are required to discover the usability problems without having an optimal sequence of actions for the task that may be performed by the user.

- ***Heuristic Evaluation***

Heuristic evaluation, developed by Nielsen and Mohlich (1990), is a list of usability principles known as heuristics, which the authors recommend evaluators use to examine the UI. Preece et al. (2002) revised the heuristic list to include the following items:

1. Visibility of system status,
2. User control and freedom,
3. Match between system and the real world,
4. Error prevention,
5. Recognition rather than recall,
6. Consistency and standards,
7. Aesthetic and minimalist design,
8. Flexibility and efficiency of use,
9. Help and documentation,
10. Help for users to recognize, diagnose and recover from errors.

> While evaluators do not need prior training, their effectiveness in identifying the usability problems depends on the evaluators' experience. The advantages of heuristic evaluation include its simplicity, speed, and low cost (Nielsen, 1992), and few evaluators are needed. Based on 19 practices of heuristic evaluation, Nielsen (1992) pointed out that, on average, each evaluator could discover 20%–60% of the usability problems.

In summary, as empirical studies (Nielsen, 1992; Desurvire et al., 1992; Jeffries et al., 1991) have shown that evaluators discover a low percentage of usability problems while using these inspection techniques, this thesis does not address methods that require a panel of expert evaluators to assess system usability.

2.2.4.3 Usability Testing

Usability testing is an adapted form of experiment designed to test the usability of a system (Preece, 1993). Usability engineering emphasises that a systems' users should be observed directly by the evaluator to evaluate the usability (Karat, 1988). Usability testing observes and records the users' behaviour to analyse the usability issues within the system. Other techniques can also be employed to supplement the usability testing, such as the thinking-aloud protocol, co-discovery learning, remote testing, and observation. Each of them will be discussed briefly below:

- ***Thinking-aloud protocol***

This protocol is a type of empirical research that asks users to perform a task and verbalise their thoughts during the task (Jaäskeläinen, 2001). According to Ericsson and Simon (1993), the thinking-aloud protocol is a valid method for analysing cognitive processes, as it accesses the users' issues and thoughts arising in their short-term memory during the testing. This method is considered advantageous because it elicits data from short-term memory that is unaffected by users' perceptions (Ericsson & Simon, 1993).

Nielsen (1994) stated that the thinking-aloud protocol could be used effectively with minimum training. However, problems arise when using the thinking-aloud protocol; Ericsson and Simon (1993) pointed out that users' utterances are often incoherent, and Haak and Jong (2005) stated that users might not be able to express their thoughts freely. This problem was identified in practice when Branch (2000) found that the cognitive load of problem speaking was difficult for some users participating in her study.

- ***Co-discovery learning***

In this technique, two users are observed while helping each other to perform a specific task. This method is considered more natural than the thinking-aloud method as the thoughts shared while performing the task are between the two users, which is thus considered a normal, natural discussion (Zaphiris & Kurniawan, 2006). According to Nielsen (1993), it is preferable to pair two

subjects who know each other well to ensure they feel comfortable discussing any issues; however, this requirement cannot always be achieved.

- ***Remote testing***

Remote usability testing allows the researcher to conduct the test with participants in a convenient remote location by employing screen-sharing software tools or other online services. The main challenge with this technique is the uncertainty that the researcher will achieve accurate results, as the participants may claim that they have completed the task successfully when they have not (Soucy, 2010).

- ***Observation***

In the observation method, data are collected from actual users while they interact with a system. This method can be applied in the laboratory or in a working environment (Preece, 1993). The investigator monitors users while they perform the task and the investigator take notes about their activities. The method is useful for obtaining qualitative data and can be combined with other query methods to achieve even more useful results. It is considered simple compared to other usability testing techniques, as it does not require additional software or tools.

Generally, three main factors should be considered for usability testing methods: the sample, the variables, and the hypothesis (Dix et al., 2004). An experiment tests a hypothesis to obtain knowledge. To conduct an experiment, the aim of the study should first be identified by developing the study question(s), and—for experiments involving people—the choice of participants should be planned. The

main challenge in recruiting participants is selecting the optimum number, which is recommended to be a minimum of ten (Dix et al., 2004). The experiment should measure numerous variables. The most common variables in a usability evaluation are the time needed to complete a task, the number of errors, and the quality of user performance (Dix et al., 2004).

From Alshamari and Mayhew's (2008) perspective, various other factors affect usability testing, including the usability measures, the number of users, the tasks, the evaluator's role, the usability problem report, the test environment, and other minor factors such as the type of system and the participants' characteristics. Matera et al. (2006) identified five stages that need to be planned before starting usability testing: defining the goal of the test, selecting test participants, designing the task, establishing usability metrics, and preparing the test material and equipment. These key stages will be considered and carefully followed during the design of the experiment presented in Chapter 6.

2.2.4.4 Query Method

The query technique directly obtains users' perceptions about what they like and dislike. It can also be used to find the users' requirements and goals for a system. The technique includes questionnaires, focus groups, and interviews.

- ***Questionnaires***

Questionnaires, which are used to collect subjective usability information and people's perceptions, have proven effective in the assessment of interactive

applications (Keller & Keller, 1989; Whitelock & Scanlon, 1996; Matsubara & Nagamachi, 1996) and are considered highly appropriate for this purpose because they are inexpensive and easy to use (Feldstein, 2002; Zaharias, 2004). Questionnaires have also been applied to assess authentication methods. For example, De Cristofaro et al. (2014) conducted a survey with Mechanical Turk users to evaluate their perceptions of the usability of two-factor authentication.

- ***Interviews***

One of the most commonly used methods for eliciting data is speaking directly to respondents via a meeting or interview. According to Dix et al. (2004), an interview is a useful technique for gathering high-level information. Creswell (2009) laid out three interview models: the structured interview, the semi-structured interview, and the unstructured interview. In the structured interview, all questions are predetermined, and the researcher has full control for the duration of the interview. This type of interview is easy to conduct and analyse (Preece, 1993). In the semi-structured interview, the researcher prepares limited questions and adds more questions as the interview progresses. The interviewee is allowed the flexibility to shape the flow of information. Finally, in an unstructured interview, the interviewee guides the discussion issues based on the focus established by the researcher. The benefit associated with this model is the richness of the data collected; however, this makes the analysis phase difficult and time-consuming (Preece, 1993). Within the context of authentication methods, a study by Krol et al. (2015) used semi-structured interviews with 21 UK online banking customers to analyse the usability of two-factor authentication. The study revealed a wide range of usability issues in using two-factor authentication; however, in the

cases where the study aims to elicit both quantitative and qualitative data from a large pool of users, the interview method is unacceptable and unsuitable for the exploratory study in this thesis.

- ***Focus group***

The focus group method is used to obtain qualitative information and is widely employed in various types of research, including product planning and usability studies (Rubin, 1994). It is considered a useful method for gaining insight and exploring the differences between the group members' perspectives (Rabiee, 2004). However, recruiting participants for the focus group method and analysing the huge amount of qualitative data generated present significant challenges (Rabiee, 2004).

2.3 Security

The aim of security is to provide restricted and safe access to a system. In 2008, the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC) explained that information security "is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisation structures and software and hardware functions" (ISO/IEC 27002, 2008, p. 11). The term security is defined as the "freedom of danger or risk of any sort" (Harcourt, 2010); consequently, only authorised users are allowed to access the requested data. Vijayasarathy (2004) defined security for online purchasing as, "the extent to which a consumer believes that making payments online is secure" (p. 751). However, Garfinkel (2005) pointed out that no system can be fully secured.

Each system has its weaknesses, whether in design, operation, or implementation. Security should be applied in the design phase, but often it is delayed until too late in the software cycle—during the development, deployment, and maintenance stages (Taterh et al., 2012). Including security planning in the software development cycle will lead to a high level of security by identifying the weaknesses that are prone to attack (Byers & Shahmehri, 2007). Each security system aims to achieve three properties: confidentiality, integrity, and availability (Pfleeger & Pfleeger, 2006).

The main problem with security is that users are unaware of how to recognise, understand, or respond to a security warning. The results from prior studies indicate that users ignore a warning because it did not convince them to respond or take action (Seifert et al., 2006; Wu et al., 2006). Meanwhile, the user may not care about maintaining security; for example, the user might write down a password, and either save it in a note on a PC or photograph their credit card. In other situations, the user might be forced to disable the security features in cases when the user switches off the firewall to use a local network printer, or has difficulty understanding the security applications (Weir & Zonidis, 2005). As a result, the user becomes the weakest link in the security system. Several studies, therefore, emphasise security aspects over usability (Sabzevar & Stavrou, 2008).

2.3.1 Security properties

The three core principles mentioned earlier (confidentiality, integrity, and availability) are known as the CIA triad (Andress, 2011; see Figure 2.2). Other experts add

accountability as the fourth principle (Feruza & Kim, 2007). The following are brief explanations of these principles.

Figure 2.2 CIA- triad items

- ***Confidentiality***

Confidentiality describes the ability of a security system to prevent the disclosure of data to an unauthorised user. It is designed to protect sensitive information from reaching the wrong people. One way confidentiality can be maintained is by encrypting data entered by the users, such as passwords.

- ***Integrity***

Integrity maintains the trustworthiness and accuracy of the data by preventing unauthorised alteration, which may otherwise produce mistakes in the data or infect the computer with a virus (Feruza & Kim, 2007).

- ***Availability***

Availability ensures that all requested hardware and software are available for the authorised users. Any required hardware repairs should be conducted immediately, and all software should be kept updated and upgraded.

- ***Accountability***

  Accountability refers to the ability to track users' actions and processes by analysing their logs to identify and prevent a violation incident.

Applying the above fundamental principles to a computer system properly will ensure that the security of the system is achieved.

2.4 Security warnings

Most users encounter antivirus software on a daily basis. To understand how to deal with security tools, software, and functions, users need to be aware of security warnings. Wogalter (2006) defined warnings as a method of communication designed to inform users about threats or risks to be minimised or avoided. Tuchscheerer et al. (2010) provided a different definition: a warning is a way to draw users' attention to an action that may result in harm to the user. User awareness of where their attention is being directed is considered one of the factors that can be measured during the execution of a security task (Kainda et al., 2010). Wogalter (2006) characterised the four functions of a security warning as providing users with safety information, encouraging users to behave safely, reducing potential problems and reminding users about expected danger.

Egelman et al. (2008) conducted an empirical study with 60 participants to investigate the effectiveness of phishing warnings by simulating a spear phishing attack (i.e., an email that appears to be from someone that they know; however, it is not). The results revealed that 97% of the participants failed to understand at least one of the phishing

messages, indicating that users' awareness and understanding affect their responses to security messages.

Seifert et al. (2006) investigated the effectiveness of security warnings via a case study of Internet Explorer. The users (n=114) were asked to install an insecure ActiveX component. The study focused on whether security warnings would prevent users from insecure actions. The results showed that the warning indicator was successful at warning the users about an insecure installation but did not prevent it.

Sharek et al. (2008) reviewed differences in the visual design of warnings by sending three fake popup windows containing standard Windows XP error messages to the users. Each fake popup had a different design. The authors observed the participants' responses to the fake messages, such as *close, minimise,* or *OK*. The results indicated that users did not understand the potential risks, as 73% responded incorrectly.Wu et al. (2006) conducted a study with 30 users to evaluate the effectiveness of three browser security toolbars and found that all three failed to prevent users from taking risks. Although the authors aimed to design a realistic scenario in which security was not the primary goal for the participants, the users were told that the study would test security indicators, which may have affected the results.

Whalen and Inkpen (2005) conducted a study with 16 participants to examine user attention to browser security, using an eye-movement tracker to gather data. They found that users failed to pay attention to Web security indicators. The authors suggested several improvements for the design of the certificate data so that it could be meaningful to users. Kolb et al. (2014) also used an eye tracker to examine user

attention to security indicators. Their study focused on colour and movement. The user was shown websites that used different colours for the security indicators. Most of the 29 participants focused longest on a red password field.

Falk et al. (2008) used an automated tool to analyse 214 American financial websites and detected that 76% had at least one flaw. These flaws included a break in the chain of trust, secure login options on insecure pages, contact information on insecure pages, inadequate policies for user passwords, and security information emailed insecurely.

Although the above studies focus either on improving the security indicators or examining the effectiveness of security indicators, they show that users' awareness and reactions have an enormous impact on security issues. Thus, it could be said that users' awareness and reactions can be used as a core measurement for security issues that involve users' decisions or behaviour.

2.5 Usability of a secure website

Garfinkel and Spafford (1996) stated that a "computer is secure if you can depend on it and its software to behave as you expect." This statement highlights the importance of involving users in the security process and supports the previous section, which clarified how users' responses and reactions affect the systems' security.

Websites that deal with sensitive information, such as credit card details, should be secured, and data transfers via these websites should be encrypted to prevent unauthorised access to personal data. In the United Kingdom, this requirement is

mandated by the UK Data Protection Act (DPA, 1998), which defines types of personal data and guidance and gives examples of how to apply it in practice.

In practice, secure websites use authentication mechanisms and encryption to protect sensitive information and transactions conducted via the Internet. The most secure websites use secure socket layer (SSL) technology to protect hypertext transfer protocol (HTTP) transactions, as well as Internet message access protocol (IMAP) and lightweight directory access protocol (LDAP) (Rouse, 2014). These protocols essentially work when a connection between two machines is established, such as the connection between the Web and mail server, and they start to secure the connection using public-key encryption to validate the certificate, which affirms that a server is the server it claims to be (Rouse, 2014).

Nevertheless, users should protect their information. Herzog and Shahmerdi (2007) summarised four usability requirements for a secure application:

1. Improve the users' awareness regarding security tasks,
2. Help users to complete these tasks successfully,
3. Prevent users from making errors,
4. Provide users with a comfortable interface.

Whitten and Tygar (1999) conducted the first study that examined the usability of secure systems by performing a walkthrough analysis of user interactions using Pretty Good Privacy (PGP) software, version 5.0, which was widely used. They concluded that PGP 5.0 was not easily usable, although it had an attractive graphical UI (GUI). The researchers stated that a specific usability standard should be developed for

security systems. Wool (2004) focused on the usability of firewalls, particularly direction-based filtering, which is the capability of filtering based on a packet's direction.

The above studies show that employing the usability concept into security applications and systems, which started in 1999, has proved to be important. The usability factors stated in Section 2.2 have been applied to evaluate the usability of secure systems, such as the study by Weir et al. (2009). While, to our knowledge, no scientific study identifies security measures that can be used to assess the security of secure systems, Section 2.4 showed how the role of users' awareness and responses regarding security features can be used to identify security measures. Thus, Chapter 6 will provide a detailed list of proposed security measures that can be used to assess the secure systems based on users' awareness of security design flaws and security indicators.

2.6 Usable security

Most people are familiar with computer technology, as they carry mobile phones, tablets, electronic pens, etc. They are also encouraged to conduct many tasks electronically, such as shopping and paying bills, and to take advantage of other e-services, such as filing tax returns. However, a concern remains regarding how to ensure that e-services are accessible and secure. In 2014, 55% of large businesses were attacked (Information Security Breaches Survey, 2014); thus, companies are under pressure to offer usable and secure web pages and authentication.

Complicated passwords can be an effective form of defence against brute force attacks; however, they are ineffective against a host of other attacks (Herley & van

Oorschot, 2012) such as when information is stolen by breaching the system security or using a key logger attack that tracks users' logs to find out everything typed by the users, including their passwords. Therefore, the challenge is to investigate whether the security methods and techniques are effective if used properly by the user (Mannan & Oorschot, 2008; Cuthbert, 2009; Sasse et al., 2001). Many authentication methods are hard to use or include lengthy instructions and are thus inconvenient to the user. In 2003, the Computing Research Association identified human computer interaction security (HCI-SEC) as one of the "four grand challenges in trustworthy computing." Usability and security are both essential for any secure system or product, including authentication methods, and they should go hand in hand, as usability is concerned with easy access to a system, and security is concerned with secure access to a system. Whitten and Tygar (1999) defined usable security as that which increases users' confidence in using the security system interface and enables them to avoid errors. Smetters and Grinter (2002) claimed that designing a usable security system means achieving a useful, secure application from the user's perspective.

Flechais et al. (2007) applied Appropriate and Effective Guidance for Information Security (AEGIS) to the development of secure and usable systems. They treated usability as a requirement for a successful system (Flechais et al., 2007).

Figure 2.3 shows the relationship between security and usability.

Figure 2.3 relationship between security and usability

The experts' views of usability and security can be divided into three groups:

1. A conflict exists between usability and security (Besnard & Arief, 2004; Furnell, 2005; Nodder, 2005).
2. Security should be given priority over usability (Fleschais et al., 2007)
3. Security and usability should be treated equally and a balance made between them (Dewitt & Kuljis, 2006).

As the above information shows, the nature of the relationship between usability and security is still not clear, and more effort is required to identify the acceptable attributes of usable security.

2.7 Online banking

In the past two decades, e-banking has become an essential gateway for bank customers to conduct transactions. Most banks provide customers with the services they need electronically (Mockel, 2008). Shah and Clarke (2009) defined e-banking

as, "the provision of information about the bank and its services via a homepage on the World Wide Web (WWW)" (p. 21).

The number of e-banking users is large; for example, in the United Kingdom, approximately 25 million people use e-banking (Hyde, 2012). Banks focus on applying advanced security requirements and tools to their websites to encourage their customers to use e-banking instead of making in-person visits to bank branches. However, the security and usability of e-banking are major concerns for website owners, as e-banking security remains limited or altogether lacking (Moeckel, 2011). For example, in the United Kingdom, losses from fraud in 2012 amounted to £39.6 million (UK Cards Association, 2014). This huge loss motivated the investigation into the methods used by e-banking to authenticate users.

Mannan and Oorschot (2007, p.1) stated that online banking is "one of the most sensitive tasks performed by general Internet users". The majority of banks today offer banking services online, and customers are strongly encouraged to use online banking with the guarantee of security. However, the fine print contained in the user agreement conditions indicates that this guarantee is based on specific user requirements. Mannan and Oorschot (2007) opened accounts at five of the largest Canadian banks and found that users faced difficulty following security requirements. The authors also conducted a survey of 123 technically advanced users from a university environment; the results confirm the importance of filling the gap between user behaviour when complying with security requirements and bank expectations (Mannan & Oorschot, 2007). This study, therefore, affirms the importance of applying the usability concept to secure systems.

2.8 Trust and online banking

The concept of trust is related to three dimensions of individual behaviours: integrity, benevolence, and competence (Ridings et al., 2002). Integrity is "the expectation that another will act in accordance with socially accepted standards of honesty" (Ridings et al., 2002), while competence refers to a group of skills that allow the party to have an impact within a specific domain (Mayer et al., 1995). Benevolence is the expectation that the trusted parties have the desirability to perform positive actions to the trustee (Ridings et al., 2002); therefore, the trust of the system is only met if all the three dimensions are achieved.

In the online banking context, and due to the sensitive nature of user information such as credit card details, trust is an essential factor required to complete financial transactions (Bargh & McKenna, 2004). The issue of trust is a critical challenge that faces online banking managers, designers, and providers (Aladwani, 2001). How to gain consumers' trust in conducting online banking is not yet understood (Jones et al., 2000). However, several researchers have highlighted the relationship between trust and the quality of the design of an interface (Lanford, 2006). Laberge and Caird (2000) concluded that an effective UI is the gateway to gaining user trust. The study justifies the relationship between the trust and the effective UI that can be measured through usability assessment; thus, involving trust within usability assessment is reasonable and acceptable. Geven (2003) stated that trust is an excellent predictor that can be used to measure the use of technology.

2.9 Authentication mechanisms

Authentication is a confirmation process that must be completed by the users to verify their identity. Yang and Shieh (1999) stated that secrecy and authentication are the two main components of network security. Monrose and Reiter (2005) stated that the goal of user authentication is to "confirm the claimed identity of a human user". The authentication process is comprised of three security components that differ between authorised and unauthorised users: confidentiality, which ensures that the information is unavailable to unauthorised users, integrity, which ensures that the data has not been modified in an unauthorised way, and availability, which ensures that the computer systems are available to authorised parties when needed (Braz & Aïmeur, 2005).

Renaud (2005) described three stages of authentication: identification, authentication, and authorisation:

1. User identification refers to the process in which the system starts to identify the user's identity and define who they are. During this process, the users usually type a name or identification code, and the system makes a match between the database and the input. However, as user identification alone is insufficient, the next two phases are essential.
2. User authentication is the main process that confirms the users' identity. During this stage, the user provides a secret factor such as a password, secure answer, or a number that should match the assigned one in the user's record.
3. User authorisation gives the user access to the secured page, which can only be done after successfully completing the previous two stages.

Figure 2.4 shows the three stages of the authentication process.

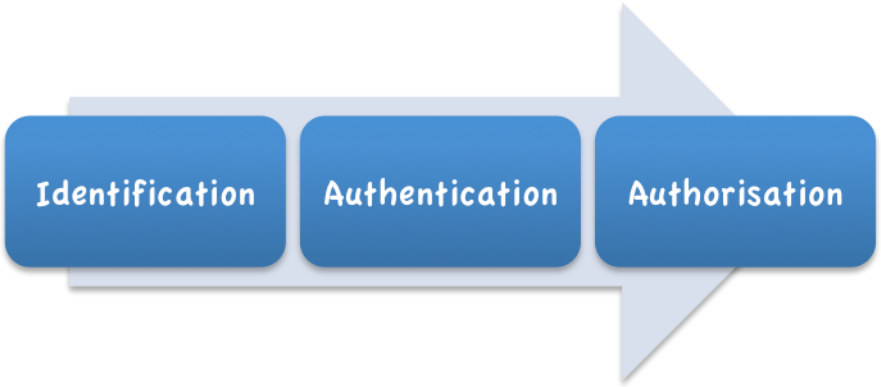


Figure 2.4 phases of authentication process

Authentication is based on aspects such as behaviour, knowledge, facts, or characteristics. These aspects refer to the methods created or given to the user to complete the authentication process, such as ID, personal identification number (PIN), password, token, and secure question. Passwords, the most common authentication methods, ask the user to provide a previously designated piece of knowledge (Sasse et al., 2001). There are three different categories of authentication: knowledge-based, token-based, and biometric-based authentication (Suo et al., 2005). A brief explanation of each method is provided below.

2.9.1 Knowledge-based authentication

Knowledge-based authentication (KBA) confirms a user's identity using restricted information. It is considered the most commonly used authentication method (Jorstad & Thanh, 2007). Examples of KBA are passwords, PINs, and secure questions. The use of a password is the most common KBA, where the user's identity is verified by requesting a set of numbers and letters. Users tend to use a password that is easy to memorise, and they use it in multiple places (Yan et al., 2004; Florêncio & Herley, 2007). Secure systems request strong passwords (Yan et al., 2004) (see Figure 2.5).

The conflict between security and usability appears clearly when using passwords: security requires a hard-to-guess password, while usability requires an easy-to-remember password (Fidas et al., 2010).

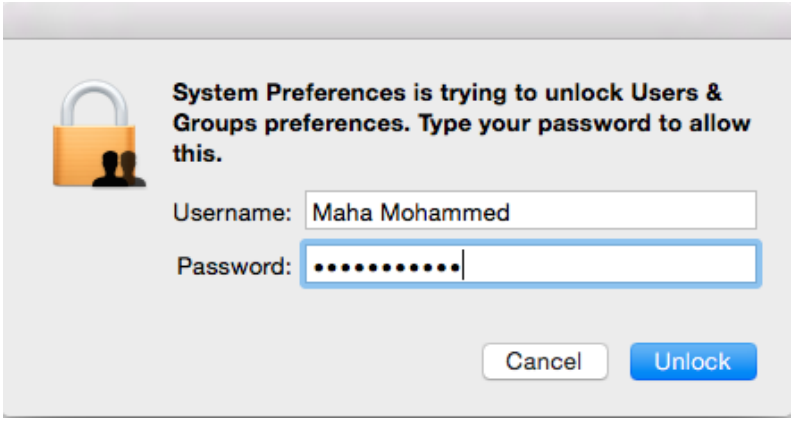


Figure 2.5 example of Knowledge-based authentication

2.9.2 Token-based Authentication

Token-based authentication (TBA) refers to physical or electrical tokens held by the user to verify his or her identity. The authentication process with this kind of method relies on the real user who owns the token. Some TBA methods are based on generating one-time PINs, which avoids the problem of guessing or forgetting a password. These methods require the user to hold the token for each login to the system and start the process by inserting a credit card or agreed password. The user then follows the instructions to generate a random PIN for one login. However, the security issue is that the device can be stolen, while the usability issue is that the user needs to hold the token for every single login (see Figure 2.6).

Figure 2.6 Examples of token-based authentication

2.9.3 Biometric-based Authentication

The use of physiological and behavioural biometrics to verify user identity is called biometric-based authentication (Renaud, 2004). The physiological methods include fingerprints, facial structure and voice (see Figure 2.7), while the behavioural methods include, for example, signature keystrokes. For the authentication process, the user must present the biometrics required by the secure system. Although there are several benefits to using biometrics, this method has some limitations, such as cost and error rate (Clarke & Furnell, 2005). Chapter 5 discusses the authentication methods in more detail.

Figure 2.7 Examples of biometrics-based authentication

2.10 Authentication classification

2.10.1 Single Factor Authentication (SFA)

SFA uses one factor for user authentication on a website. Knowledge-based factors, such as passwords, passphrases and PINs, are the most widely used factors, but they are considered to provide the weakest security. The usability of SFA mechanisms is a concern for many researchers, including Ma and Feng (2011), who evaluated the usability of three types of passwords: traditional, mnemonic and graphical. The mnemonic password takes the first letter from a particular phrase (Microsoft Corporation, 2005), while for a graphical password, the user is required to remember a graphic instead of text, following the assumption that pictures are easy to remember (Shepard, 1967). However, Ma and Feng (2011) demonstrated that graphical passwords resulted in longer user authentication times compared to traditional and mnemonic passwords for two reasons: the time taken to load the images and the time the user spent viewing the 30 images presented on the page. The researchers also found that text and graphical passwords were equally memorisable (Ma and Feng, 2011).

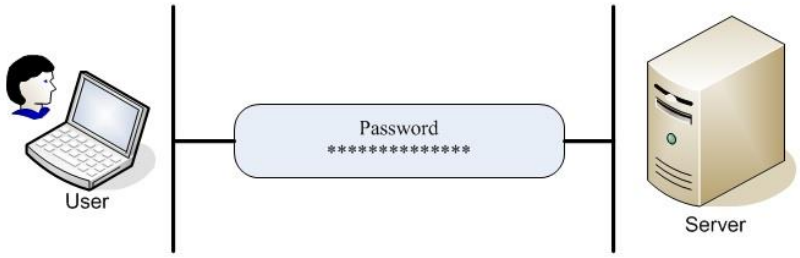


Figure 2.8 Single factor authentication

Karole et al. (2010) studied the usability of three password managers: an online manager, a phone manager and a USB manager. The difference between these passwords and traditional passwords is that these passwords are stored and generated by a computing device, such as the online manager Mozilla Weave Sync, rather than the user (Karole et al., 2010). The researchers collected users' perceptions of the security and usability of the three password modes and found that users preferred portable and standalone managers to online managers (Karole et al., 2010). However, the usability of online managers was found to be the best, and the researchers found non-technical users preferred phone managers (Karole et al., 2010).

Hafiz et al. (2008) conducted a comprehensive study of graphical password mechanisms to identify their usability and security features. The results showed that graphical schemes are strong enough to defend against an attack (Hafiz et al., 2008). Some participants in the study acknowledged it was easier for them to remember graphical passwords than traditional passwords (Hafiz et al., 2008). The scheme of the study was intended to satisfy users' requirements (Hafiz et al., 2008). In the study conclusions, Hafiz et al. (2008) emphasised the need to balance usability and security features.

To compare two authentication processes and to understand users' perceptions of trust in online banking, Nilsson et al. (2005) studied security boxes that generate passwords and traditional passwords. The results from the survey and in-depth interviews with 86 users demonstrated that security boxes are perceived as significantly more trustworthy than constant passwords (Nilsson et al., 2005). However, this study failed to examine the usability levels or any aspects related to the UI.

2.10.2 Multi-factor authentication

Multi-factor authentication (MFA) involves the use of two or more independent security factors to authenticate a user. Two of the following factors are commonly used in MFA:

1. Something the user knows (KBA)
2. Something belonging to the user (TBA)
3. Something identifying the user (biometric authentication) (O'Gorman, 2003)

KBA uses three kinds of passwords: text, mnemonic and graphical. With mnemonic passwords, the users are required to insert the first letter from each word in a previously identified phrase to make the password more complex, while with graphical passwords, a set of images is presented to the user, and the user is authenticated by identifying the image previously selected during the registration phase. TBA involves an item that the user can hold such as a smart card or a security box that generates a password; however, such tangible items can be stolen and are difficult to transport while travelling. Biometric-based authentication employs a user's physiological characteristics; however, it is rarely used in e-banking due to the cost involved and the difficulty of use for persons with disabilities.

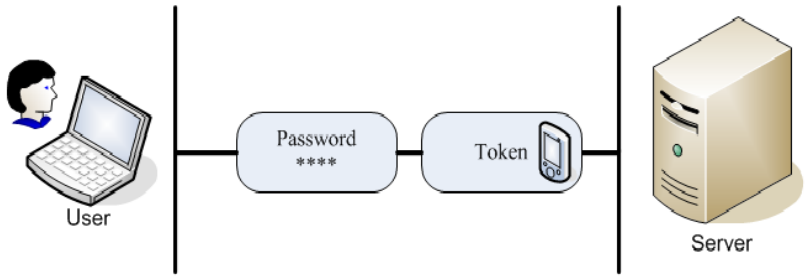


Figure 2.11 Multi factor authentication

To strengthen the authentication process, the secure system utilises more than one factor to identify the user. Previous research has focused on the usability and security of the three most common factors described earlier. Paul et al. (2011) conducted a field study using 24 participants to investigate user perceptions and behaviour when using a smart card authentication system. They identified a list of issues related to user behaviour, including forgetting to use the smart card for authentication, leaving the smart card in the reader and the difficulty understanding digital encryptions and signatures. The researchers also found that user perceptions were influenced by the personal benefits of the experience, instead of increased security (Paul et al., 2011). De Cristofaro et al. (2014) examined the attitudes of MFA users in a qualitative study of nine participants. Users were interviewed face-to-face and online. The study found that the participants used codes generated by a security token and received via SMS or email, or codes generated by a dedicated smartphone app and entered along with a username and password. However, the findings show that participants used MFA either by force or incentive (De Cristofaro et al., 2014). De Cristofaro et al. (2014) also studied the motivations for using MFA in work, personal and financial contexts with 219 users. In the work context, 60.84% of users were forced to use two factors,

while 27.97% voluntarily used two factors (De Cristofaro et al., 2014). In the personal context, 51.26% used two factors voluntarily, and 34.73% reported being forced to use two factors (De Cristofaro et al., 2014). Finally, in the financial context, 45.45% of participants reported the voluntary use of two factors, while 42.91% were forced to use two factors (De Cristofaro et al., 2014). The study concluded that employing two factors was perceived as usable, a finding that might be considered surprising and counterintuitive (De Cristofaro et al., 2014). A similar study by Weir et al. (2010) compared three authentication methods – one SFA and two MFA – used by 141 participants to explore the effect of experience, as well as the participants' perspectives on usability and security. The results show that the majority of experienced participants perceived the SFA method as the most secure and convenient option (Weir et al., 2010). These results differ from those of De Cristofaro et al. (2014). Gunson et al. (2011) conducted a study comparing SFA and MFA in automated telephone banking by administering a survey with 22 questions about usability and security. They found the MFA method was perceived as less usable but more secure. Weir et al. (2009) conducted experiments with 50 e-banking customers to compare the security, usability and convenience of three MFA methods using different token devices (card-activated token, push-button token and the chip-and-PIN method). The researchers found that card-activated tokens were considered usable and secure, the push-button token usable and secure, and the chip-and-PIN method less usable by participants (Weir et al., 2009).

The six research studies reviewed above focused on one type of authentication method, none of which examined using biometrics authentication methods and four were in the context of authentication process in online banking. Moreover, the researchers of the

above-mentioned studies often used surveys in which participants were asked to use SFA or MFA or to indicate whether they had previously used SFA or MFA. The researcher therefore argues that the sample is the most important aspect of any user study and suggest that studies that do not consider the long-term user experience are unlikely to provide a realistic picture of the levels of security and usability in SFA or MFA (Althobaiti and Mayhew, 2014). Table 2.5 summarises the studies conducted to assess MFA and demonstrates the main findings.

Name	***Research method***	***Including SFA***	***Assessed methods***			***Usability Dimensions***			***Security***	***Participants***	***Main Finding***
			KBA	TBA	BBA	Efficiency	Effectiveness	Satisfaction			
Weir et al. (2009)	Experiment	No	×	✓	×	✓	✓	✓	1 factor	50	Card-activated token perceived usable and secure comparing to other tokens used.
Weir et al. (2010)	Experiment	Yes	✓	✓	×	×	✓	✓	1 factor	141	SFA is the most secure and convenient option for the user.
Gunson et al. (2011)	Experiment	Yes	✓	✓	×	✓	✓	✓	1 factor	62	MFA had a high level of security and low level of usability comparing to SFA.
Paul et al. (2011)	Field study	No	×	✓	×	×	×	×	No	24	The users faced several issues with using smart card.
De Critofaro et al. (2014)	Interview	No	×	✓	×	×	×	✓	No	9	The authors identified different contexts and reasons to use MFA by the users.
	Survey	No	×	✓	×	×	×	✓	1 factor	219	MFA perceived as usable regardless of motivation and context.
Krol et al. (2015)	Interview	No	×	✓	×	×	×	✓	No	21	The users reported several issues associated with using hardware tokens.

Table 2.5 Comparison between studies in the area of assessing MFA

2.11 Chapter Summary

This chapter presented an overview of the usability and security of online banking, the methods used to assess usability, and the authentication methods. As the literature review showed, several studies have focused on assessing the usability of single and multifactor authentication. However, few studies have focused on the security and usability of multifactor authentication in an online context.

The main points from this review are as follows:

1. HCI was defined with a focus on usability concepts and its benefits and attributes based on the reviewed literature.
2. Various methods for evaluating usability were explained; however, the evaluation method will be decided after defining the system, the environment, and the time available for the evaluation.
3. Security as a concept and security properties were reviewed.
4. A review of studies focusing on security warnings highlighted not only the relationship between security warnings and user awareness, but also the lack of studies that examined user awareness of security warnings in online banking.
5. A review of usable security presented the history of the concept and three approaches to evaluating the usability of security. Online banking and trust were also reviewed for the main context of this thesis.
6. Three classifications of authentication methods and three processes of authentication were reviewed followed by a review of single factor authentication and multifactor authentication.

This review of the literature has shown that security warnings and biometrics methods have not been considered in evaluating secure systems. Additionally, previous research has failed to target real customers of online banking from different contexts. Thus, investigating users' perceptions from different contexts and examining real long-term experiences with online customers would be valuable. In addition, designing a careful methodology that considers security warnings indicators would derive great benefits for the usable security field and e-banking developers and managers. The next chapter describes the basic methodology used to conduct the studies in this thesis.

Chapter 3

Research Methodology

Preface

Chapters 1 and 2 have introduced the thesis and contextualised it in relation to the existing literature. This chapter discusses the methodology that underpins the contributions of this dissertation process, which includes the processes adopted to obtain primary data for the research topic. This primary data was used to derive, present and substantiate the research conclusions.

3.1 Research Paradigm

A paradigm is considered a holistic approach for research methodology (Kassim, 2001). Guba (1990: p.17) defined a research paradigm as 'the basic set of beliefs that guides action', which reflects the philosophy that dictates the way knowledge can be obtained (Trochim, 1998). In essence, there are three fundamental research philosophies that do not mutually exclusive: ontology, which defines the nature of

reality; epistemology, which focuses on acceptable knowledge in the field of study; and methodology, which describes the type of techniques used to explore reality (Saunders et al., 2009). It is important for the researcher to understand the philosophy adopted for the study (Tashakkori and Teddlie, 1998) because the research paradigm or philosophy involves important assumptions with which the researcher views the nature of science (Saunders et al., 2009).

The ontology philosophy considers the nature of the phenomenon investigated and examines processes, events and properties of reality (Floridi, 2003). In other words, for ontology, the emphasis is the nature of real knowledge. Epistemology explores the scope of knowledge in terms of bases and presuppositions (Schwedt, 2003) and asks questions such as 'What is considered fact or knowledge?' and 'How is knowledge formed'? Methodology refers to the techniques, methods and strategies that are used to acquire the knowledge required (Ernest, 1994). Each research perspective agrees differently with these philosophies. Healy and Perry (2000) presented three categories of research philosophies (paradigms). Positivism assumes that 'science quantitatively measures independent facts about a single apprehensible reality' (Healy and Perry, 2000, p. 119). Constructivism is based on the assumption that the 'truth is a particular belief system held in a particular context, and it is interested in the values which underpin the findings' (Healy and Perry, 2000, p. 120). Realism is a paradigm that has features of both positivism and constructivism because researchers have emphasised the necessity of using multiple research methods to acquire real knowledge (Healy and Perry, 2000). Realism assumes that 'a perception for realists is a window onto reality from which a picture of reality can be triangulated with other perceptions' (Perry et al., 1997, p.554). In social science research, realism has arguably been the most

influential philosophy since the 1970s (Maxwell and Mittapalli, 2007; Suppe, 1977). The core feature of the realism perspective is that it accepts the validity of the concept of 'cause' in scientific research, which is a fundamental goal of the positivism paradigm (Maxwell and Mittapalli, 2007). The present research adopted a realism paradigm, as the aims were to understand the usability and security of authentication methods through users' perceptions and to obtain an objective understanding of the methods' features. According to Orlikowski and Barioudi (1991) and Chen and Hirschheim (2004), the Information Systems (IS) field would benefit from a broader range of research philosophies. Bryman (1998) argued that once a research paradigm has been chosen, it must be associated with begining the process of selecting the proper data collection methods for the research.

3.2 Research Approach

Bell (1984) identified two major approaches for research: the quantitative approach and the qualitative approach. A quantitative approach is defined as 'an inquiry into social or human problems, based on testing theory composed of variables, measured with numbers and analysed with statistical procedures in order to determine whether the predictive generalization of the theory hold true' (Creswell, 1994). In contrast, Creswell (2003, p. 198-199) described the characteristics of the qualitative approach:

> 'it occurs in natural settings, where human behavior and events occur; [and is] based on assumptions that are very different from quantitative designs. Theory or hypotheses are not established a priori; the researcher is the primary instrument in data collection; the data that emerge from a qualitative study are descriptive. That is, are reported in words (primarily the participant's words) or pictures, rather than numbers; the focus is on participants' perceptions and

> experiences... on the process that [is] occurring as well as the product or outcome'.

From an analytical perspective, quantitative research is categorised as deductive reasoning that focuses on general observations and then involves more specific observations of the research results. On the other hand, qualitative research is associated with inductive reasoning that focuses on specific observations used to develop a final theory or conclusion.

Deductive reasoning consists of one or more statements (premises) followed by a conclusion: if the premises are true, then logically, the conclusion reached is true as well (Schechter, 2013). It is also known as the top-down approach. Deductive reasoning has been studied intensively in psychology, cognitive science and philosophy (Schechter, 2013). For inductive reasoning, the data are collected and analysed to frame a theory. The main difference between both approaches is the progress of reasoning: deductive reasoning begins with a theory to reach a final conclusion, while inductive reasoning involves actual experiences used to develop principles and theories. Figure 3.1 outlines the differences between the approaches.

Relying on a single research approach, either quantitative or qualitative, in the post-positivist (realism) paradigm is fairly unlikely (Hirschheim, 1992). In other words, the philosophy of post-positivism suggests using mixed research techniques, including quantitative and qualitative methods (Godfrey and Hill, 1995). Mixed-method research is defined as 'research in which the investigator collects and analyses data, integrates the findings, and draws inferences using both qualitative and quantitative approaches or methods in a single study or program of inquiry' (Tashakkori and

Creswell, 2007, p.4). A quantitative research study examines the relationship between variables to deductively test a theory from the literature (Flick, 1998), and the results reached using this approach provide fewer details on users' attitudes and behaviours (Scandura and Williams, 2000). Thus, using mixed research methods helps obtain details and provides insight into the phenomenon at hand (Punch, 2005). The current research adopted mixed research methods in which the researcher used quantitative and qualitative techniques to answer the research questions.

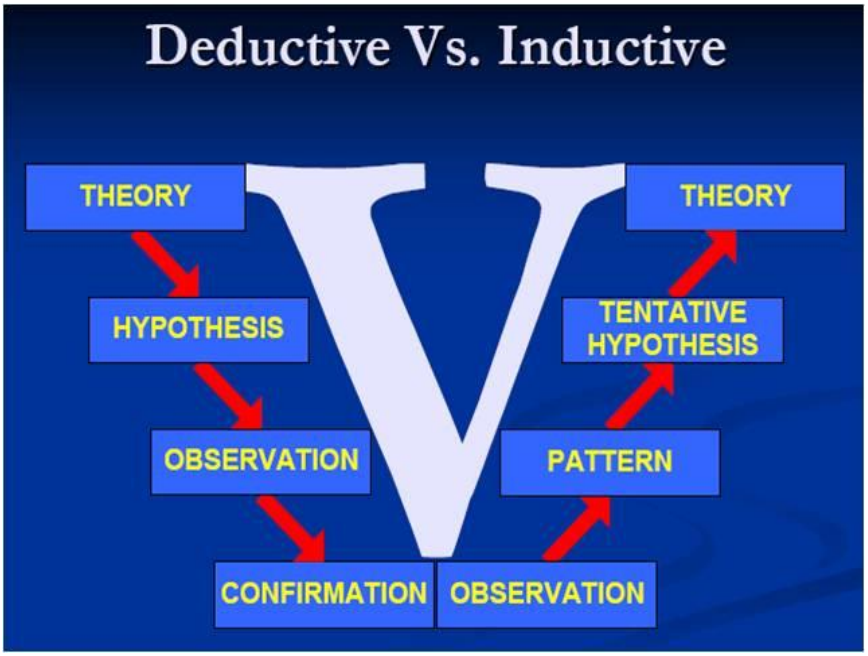


Figure 3.1 Deductive versus inductive research approaches (Zamir, 2014)

3.3 Research Strategy

According to Marshall and Rossman (1999:61), a research strategy is "a road map, an overall plan for undertaking a systematic exploration of the phenomenon of interest". In this section, the research strategy is explained by presenting the methodologies used in this research followed by a description of the research design, which involves an explanation of the different approaches and a description of the data collection

instruments used in each study.

Several methodology approaches have been identified. For example, Alavi and Carlson (1992) developed 18 categories, while Galliers (1991) listed 13 types of approaches, as follows:

- Laboratory experiment,
- Field experiment,
- Survey,
- Theorem proof,
- Forecasting,
- Simulation,
- Subjective/argument,
- Reviews,
- Action research,
- Case studies,
- Descriptive/interpretive,
- Future research,
- Role/game playing.

Other researchers have classified the research approach frameworks into three traditional approaches: exploratory, descriptive and causal, which refers to the investigation of cause-and-effect, such as experimental and statistical research (Burns and Bush, 2002; Hair et al., 2003b; Aaker et al., 2000; Churchill and Iacobucci, 2004; Saunders et al., 2007). The studies in this thesis follow this classification, which is also mentioned in Churchill's (1999) definition of a research methodology approach (Figure 3.2). The approaches of exploratory research, descriptive research and experiments as a type of causal research have been utilised in this thesis to achieve the research objectives; however, while it is not necessary to use all of these

methodologies, it is common to utilise multiple methodologies (Burns and Bush, 2002). The decision to adopt a specific methodology is based on the purpose and scope of the research. In addition, as mentioned in Section 3.2, the current research utilised mixed-methods approach. Therefore, following Churchill's (1999) methodology by involving all research methods was appropriate for the objectives and approaches of this research, which sought to obtain quantitative and qualitative results that provide sufficient details to understand the level of authentication regarding the usability and security of the methods.

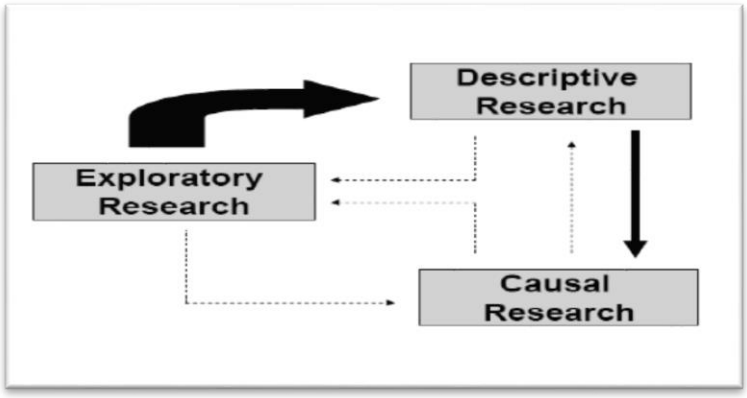


Figure 3.2 Relation of research designs (Churchill, 1999)

For this thesis, an exploratory study was first conducted to provide essential information regarding applying multifactor authentication (MFA) and users' perceptions to proceed to the descriptive study. In turn, the information and proposed methods from the descriptive study will help to describe the experimental study.

Figure 3.3 illustrates a conceptual view of the flow of the research methodology. It indicates that each stage of the research begins after the previous stage is completed; however, in each stage, the researcher referred to all previous steps, as they were all connected.

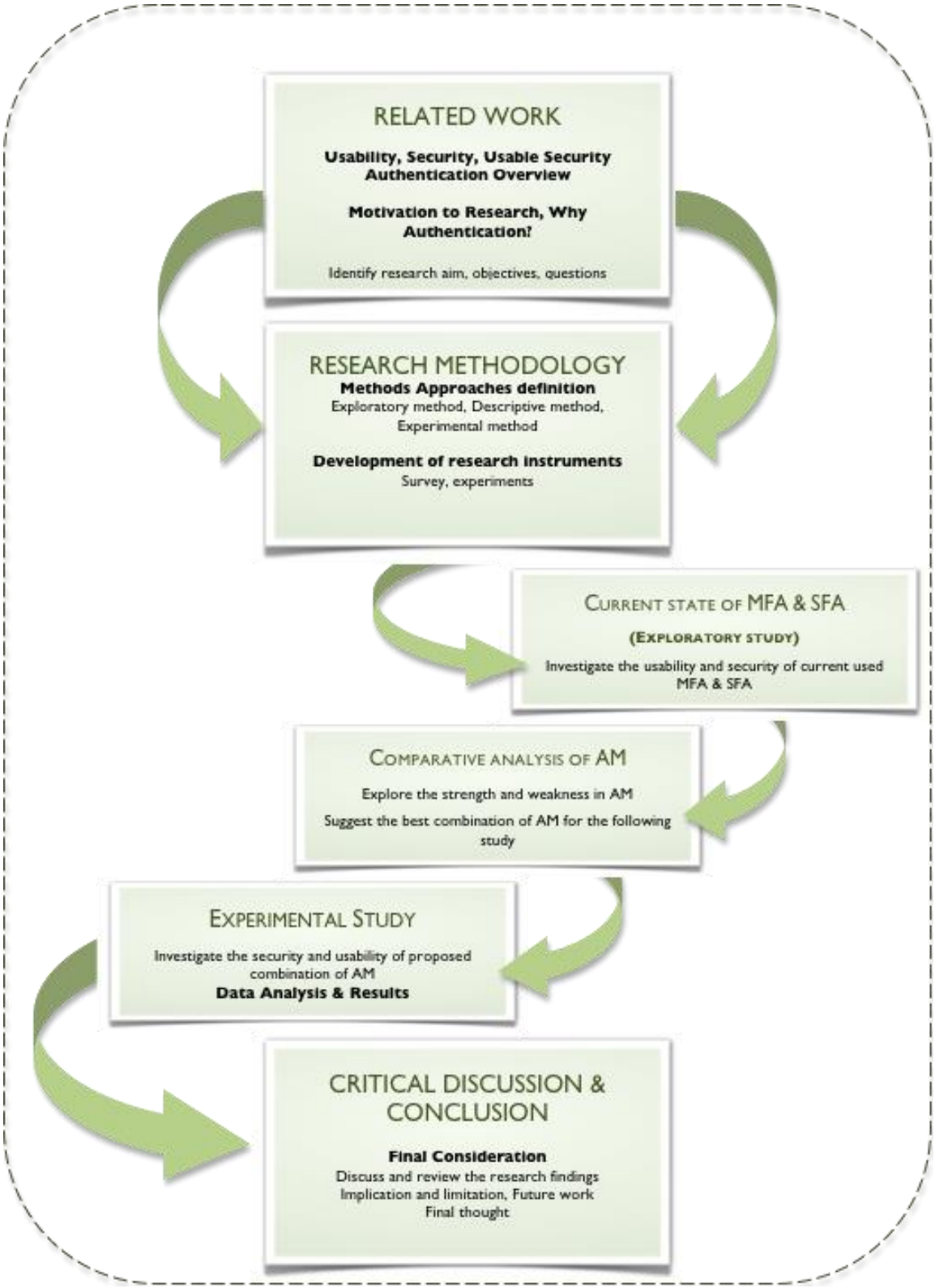


Figure 3.3 Conceptual view of research methodology

3.4 Research Design

A research design is 'the fundamental plan for a piece of research, which contains major ideas of the research, such as the framework of the research, and presents which tools and procedures the researcher will use to collect and analyse the research data' (Punch, 2005). Moreover, Kothari (1990, p. 8) stated that 'research methodology is a way to systematically solve the research problem'. The research methodology is planned by carefully designing the research and identifying the research tools and the procedures that should be used in conducting the study and in the stages of analysis of the data. Punch (2005) stated that the research design should involve all research procedures, from defining the research problem to presenting the results.

The research was carried out in different stages in which different methodological approaches were used, which is similar to the majority of information systems research. Information systems research typically employs several different research methods and approaches to acquire the knowledge that is needed to answer the research questions (Land, 1992). Therefore, three studies were conducted to answer the thesis questions. The first was an exploratory study that aimed to investigate and assess the current authentication methods used in online banking. The second study was a comparative analysis that aimed to review the existing literature by focusing on the strengths and weaknesses of each authentication method in relation to the first study's results and the literature review. In the second study, a proposed combination of authentication methods and a proposed approach for the usable security evaluation was tested in the third stage of the research. In the third study, an experimental-based approach that aimed to evaluate the three different authentication methods and to

examine the conflict between usability and security was used. These stages follow the design methods defined by Churchill (1999), as there were three types of research approaches based on the research questions. This thesis involved a range of research approaches (exploratory, descriptive and experimental) to answer the research questions. Each research method is explained in detail.

3.5 Exploratory Research

Based on the research questions and objectives, the author intended to investigate the current usage of single factor authentication (SFA) and MFA as well as to assess their usability and security. The investigation was conducted to gain an understanding of the current state of the usage of MFA and SFA. This approach is considered exploratory research. The primary purpose of exploratory research is to develop a better understanding of a problem or to assess phenomena (Hair et al., 2003). Exploratory studies are valuable and useful if the research is needed to gain new insights and to provide directions for further research (Malhotra, 1999; Parasuraman, 1991). Indeed, MFA is considered a new phenomenon, especially in the Middle East, and based on the literature reviewed in Chapter 2, there is no empirical evidence regarding the extent to which MFA is applied to financial websites in developing or developed countries. Also, there is a lack of empirical evidence on users' perceptions of usability and security in SFA and MFA. Therefore, the purpose of the exploratory study was to obtain more information based on realistic and long-term experiences with e-banking.

As mentioned in Chapter 2, Section 2.2.4.4, several methods can be used for exploratory research, such as interviews, focus groups and surveys. The aim of the

survey technique used in the exploratory study was to gather information, and it was selected for several reasons, which will be discussed in Section 3.5.1.1. According to Gill and Johnson (1997), the quality of the collected data will be reflected in the quality of the results of the research. Fowler (2002) emphasised that there is a strong relationship between understanding the survey process and the success of a project. Figure 3.4 shows the steps of the survey process according to Sue and Ritter (2007).

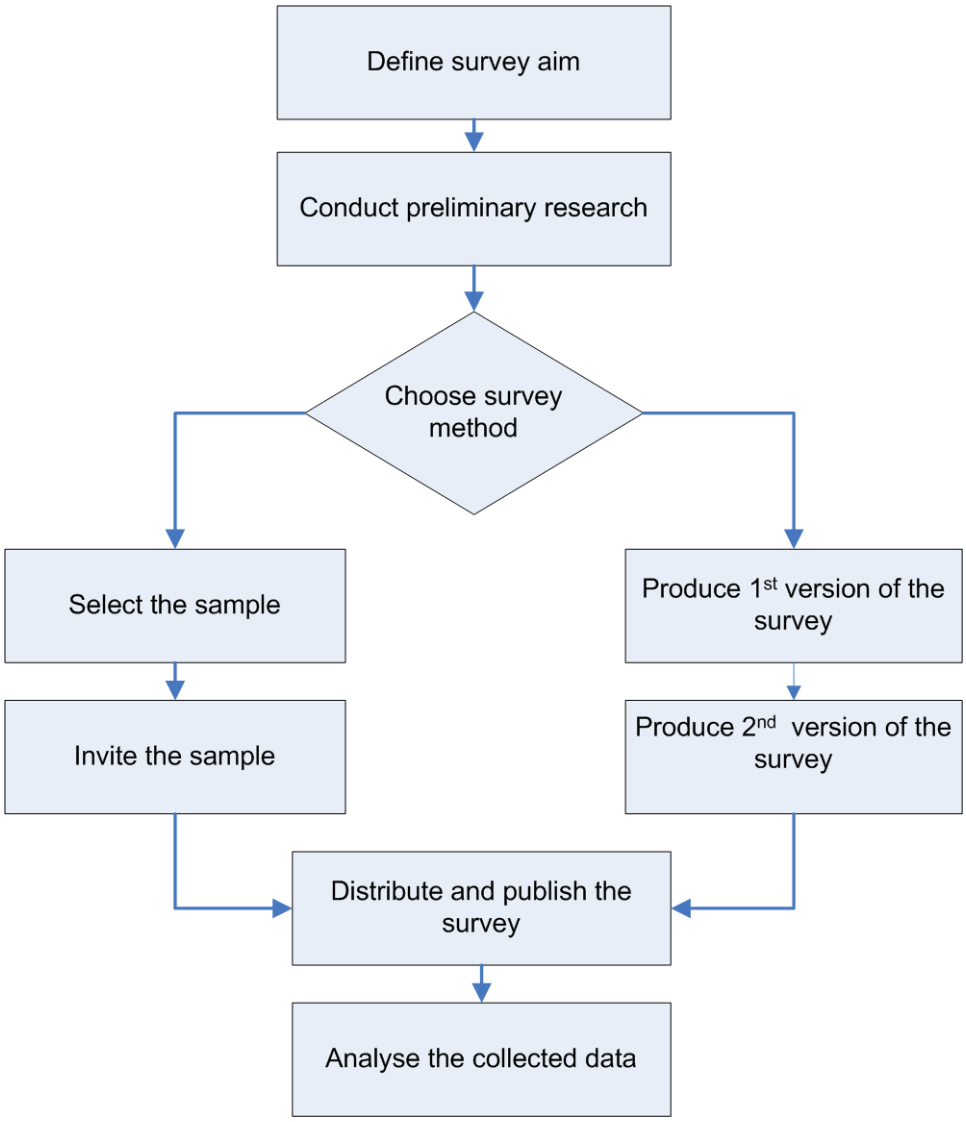


Figure 3.4 Steps of survey process

The process begins by defining the research aim and objectives and continues with a preliminary research interview; however, some research studies do not utilise this step

(Sue and Ritter, 2007). Then, the researcher determines whether the research method will be paper or electronic, such as using mobile phones or websites. Two versions of the questionnaire are designed: the first is a draft that is tested and revised by experts, and the second is the final version that will be distributed to the selected and invited sample. The data collected from the sample will be monitored and analysed to yield the findings and results (Sue and Ritter, 2007).

3.5.1 Data Collection Instruments

In any research endeavour, there are usually two forms of data: primary and secondary. As stated in Section 3.3, the questionnaire method was used to collect data for the exploratory study. Secondary data is information that is already available, either published or unpublished, including books, journals and census data (Marshall and Rossman, 1989). The following sections provide additional details regarding the method used in the exploratory study.

3.5.1.1Questionnaires

Questionnaires are commonly used to collect data about user perceptions; they are the most frequently used technique in the social science field (Easterby-Smith et al., 2002). Most questionnaires are used to gather data from a large pool of users. These data are considered suitable for assessing the usability of a product because they are inexpensive, easy to administer (Feldstein, 2002; Zaharias, 2004) and can be used in large group settings (Preece, 1993). Oppenheim (1992) stated that a survey has the benefit of increasing the generalisation of information while also providing the respondents with the opportunity to express their perspectives. Questionnaires can be

classified under two main methodologies: positivistic and phenomenological. Positivistic paradigm questionnaires can be used for a large pool of users. This methodology suggests the use of closed questions, while the phenomenological approach suggests using open-ended questions and is not useful for a large-scale survey (Hussey and Hussey, 1997). The questionnaire was utilised in the exploratory study instead of other inquiry techniques, such as interviews and focus groups, for the reasons discussed in Chapter 2, Section 2.2.4.4.

Barriocanal et al. (2003) listed several reasons that questionnaires are considered an effective method for usability studies:

- They are useful in analysing the user's perspective,
- They can be re-used for similar applications,
- They are inexpensive, and the respondents do not need to interact with the evaluator.

Still, there can be drawbacks of questionnaires, including a low response rate and the complexity of analysing data. These drawbacks can be controlled through good planning. In other methods, such as heuristic evaluations, an application is evaluated by a panel of experts from the domain area (Ssemugabi and de Villiers, 2010) to detect usability problems. Ssemugabi and de Villiers (2007) found that questionnaires and heuristic evaluations produce similar results. Ssemugabi and de Villiers (2010) also noted that heuristic evaluations are more time-efficient than questionnaires and that there are benefits associated with working with a small panel of experts compared to working with several users who complete questionnaires; however, in the absence of a panel of experts willing to participate, a questionnaire approach is a desirable assessment method. Moreover, in the context of online banking, it is unlikely that an

expert panel would be used for an authentication assessment due to the privacy of online bank accounts.

3.5.1.2 Purpose

In the exploratory study, the aim of using the questionnaire was to elicit data from those who use two different bank accounts (a local bank account and a foreign bank account) to investigate the current state of using single and multifactor authentication mechanisms and to explore users' evaluations of the usability of the explored methods.

3.5.1.3 Questionnaire Design

The first step in developing a questionnaire is to identify its broad aims. In this study, the broad aim was to investigate and evaluate the usability of the authentication methods used by the respondents. The second step involved selecting the measurement scale, question phrasing and the sequence of the questions. The first version of the questionnaire in this study was written in English (see Appendix B). In addition, in order to ensure the accuracy of the writing and wording, the questionnaire was proofread by an expert who is a native speaker. Then the second version was developed in Arabic (see Appendix C) by translating and reviewing it with a Saudi academic, as Arabic is the predominant language of the sample population.

3.5.1.4 Measurement Scale

As this study aimed to evaluate the usability of authentication methods by collecting users' perceptions regarding the authentication methods used, multiple-item scales

were deemed appropriate, as they are the most used in usability studies. In this study, three types of measurement scales were used: nominal, ordinal and interval. The nominal scale, which has numeric values, was used for some questions, such as questions about gender, while the ordinal scale was used for age groups. Interval scales were used to measure the subjective characteristics of participants; for example, participants were asked to rate several factors of the used method. This scale was used because it is appropriate for arranging ratings, and it can measure the distance between the differences in the rating scale (Burns and Bush, 2002; Churchill and Iacobucci, 2004).

The measures used in this study followed Nielsen's requirements for usability of system (Nielsen, 1996): learnability, efficiency, memorability, errors and satisfaction. Nielsen's definition covers more aspects compared to the ISO definition of usability and has been adopted in several usability studies, as mentioned in Chapter 2, Section 2.2.2. Two other factors were added to address the aspects related to authentication methods: security and trust. These two dimensions have been utilised in previous studies on secure systems (De Critofaro et al., 2014; Weir et al., 2009; Weir et al., 2010).

3.5.1.5 Wording of Questions

Two types of questions can be used for a questionnaire: closed-ended questions, which give respondents a range of answers from which to choose, and open-ended questions, which allow the respondents to answer the question in any way or form. The advantage of using open-ended questions is that it allows participants to provide answers in their own words, and they can communicate their perspectives as precisely as possible. On

the other hand, closed-ended questions are convenient for researchers and easy to analyse, but they require more effort in designing the answer choices so that all possible perspectives are included (Weisberg et al., 1996). In this study, both open-ended and close-ended questions were used. The questionnaire consisted of five sections. The first section included questions regarding demographic and general information, the second section involved rating the usability of the authentication methods of local bank account and the third section included two open-ended questions regarding what users like and dislike about the method used in the local bank account. The last two sections are about the foreign bank account: the first section included rating questions similar to those in the second section, and the fifth section included two open-ended questions. The reason for including open-ended questions was to allow respondents to impartially answer the questions regarding what they like or dislike in the used methods without opinions or inferences on the part of the researcher. This bolsters the level of objectivity in the data elicited and in the conclusions derived from the data.

According to Wilkinson and Birmingham (2003), an effective questionnaire enables researchers to gather information easily and accurately. A web-based questionnaire may help achieve these objectives, especially when the questionnaire aims to gather information from a large pool of users. Also, a web-based survey allows for exporting Excel files and administering questionnaires as well as the potential to design an attractive interface.

3.5.1.6 Response Format

As mentioned in the previous section, there were two sections in which the users were

requested to evaluate the authentication methods. For these two sections, a labelled scale response format was used because it was easy to administer and easy to carry out for further statistical analysis (Burns and Bush, 2002). In this study, a labelled Likert scale was adopted for the following reasons:

- It offers higher reliability coefficients with few items (Hayes, 1998),
- It is widely used in usability research (Hornbek, 2006),
- It yields a high probability of accurate responses that reflect participants' perspectives (Burns and Bush, 2002).

Regarding the number of points on the scale, there is no standard that indicates an ideal number. Several researchers have stated that opinions can be presented best using 5- to 7-point scales (Aaker et al., 2000; Molhotra, 1999). In the context of usability, studies most often include 5- or 7-point Likert scales (Hornbaek, 2006). Increasing the points of the scale does not lead to improvement in the reliability of the ratings (Elmore and Beggs, 1975); thus, most researchers have indicated that 5 points is enough to present the differences between responses (Malhotra, 1999). Others have indicated that a 5-point Likert scale reduces the level of frustration among participants (Buttle, 1996). Therefore, the survey in the exploratory study included a 5-point Likert scale.

3.5.1.7 Length of Survey and Sequence of Questions

The researcher was aware that a long questionnaire might discourage the sample from completing it. Therefore, the researcher designed the survey to be as concise and short as possible. In addition, the questionnaire began with more general information before moving to more specific questions to organise the questions and to provide simplicity for the sample.

3.5.1.8 Questionnaire Piloting

Before conducting a survey, a questionnaire should be tested and reviewed (Shinderman and Plaisant, 2005). The review process was done first with two academic professors from the university. One professor suggested that the rating questions about the local bank account should be first; other comments were related to rewording statements. Then, as recommended by Gillham (2000), a pilot study was conducted with six participants. This helped determine whether there was any ambiguity in the questions (Burns and Bush, 2002), how much time would be required to complete the questionnaire and the level of clarity of the questions. The pilot study resulted in adding one statement, rewording some of the statements, and eliminating spelling mistakes and the participants generally enjoyed completing the survey. As a result, the researcher was satisfied with the questionnaire, which was then improved and prepared for distribution to the participants. Prior to data collection and distributing the questionnaire, an application including the details of the research instruments was submitted to the Research Ethical Committee at the School of Computing Science in the University of East Anglia, and approval was granted.

3.5.1.9 Questionnaire Administration and Access to Sample

To obtain information regarding the current state of using authentication methods and how users perceive the authentication process, the researcher gathered a pool, or sample, of users who had long-term experience with e-banking. To do so, the researcher chose Saudi students who study abroad as the target sample because it was assumed that they would have two bank accounts (their local bank account in Saudi

Arabia and their foreign bank account). This sample was chosen because they had long-term experience with e-banking as well as two different bank accounts from a developed and a developing country. None of the studies reviewed in Chapter 2, Section 2.10.2 included a non-Western context; thus, this sample choice compensates for the shortage in the literature and contributes to the expansion of knowledge. In addition, a sample with long-term experience could provide new and realistic results. Moreover, bank service providers and authentication methods developers would benefit from exploring their customers' perceptions regarding the usability and security of the provided methods from actual users.

To access the sample, the researcher (who studied in the United Kingdom) sent an introductory email to several Saudi club coordinators in different cities in the United Kingdom asking them to distribute the questionnaire. At the same time, the researcher began to distribute the questionnaire, along with the aforementioned email, via social media. While waiting for user replies, the researcher monitored the progress of the responses and prepared for the statistical analysis.

3.6 Descriptive Research

Descriptive research involves a direct analysis and an exploration of specific issues (Streubert and Carpenter, 1999). This type of research uses guidelines and a clear and structured hypothesis. It is designed carefully to assess the characteristics described in the research questions. Data for descriptive research can be gathered from a literature search, interviews or surveys, and Punch (2005) pointed out that this method can be considered an in-depth view that can contribute to the research area effectively. In this type of research, it is important to have insight into and an understanding of the

phenomena for which the researcher gathers data (Saunders, 2007). The benefit of conducting this type of the research is the ability to reflect reality; however, the main issue associated with this approach is that it is dependent on the researcher's skills. Within the context of authentication methods (AMs), the second study aimed to objectively compare the different existing AMs and to review the strengths and weaknesses of each AM. As a result, a proposal of a suitable combination of AMs that can contribute to improving the overall security of the authentication process could be tested in the experimental study.

3.7 Experimental Research

According to Gay (1992, p. 298), 'the experimental method is the only method of research that can truly test hypotheses concerning cause-and-effect relationships'. Beginning in the twentieth century, experimental research has been considered a highly effective method in behavioural science (Lazar et al., 2010). There are several benefits and weaknesses of experimental research. It is considered to be fast and less expensive than other methods (Wolf et al., 1989); it is also convenient for both the participant and the experimenter, and it is precise in presenting the required results. In contrast, Denscombe (2003) stated that experimental research allows only limited control of the experiment, and users' behaviours may differ from behaviours in the natural environment. Moreover, the observation may be biased.

The basic steps of an experimental design are as follows (Lazar et al., 2010):

1. Identify research hypotheses,
2. Identify dependent and independent variables,

3. Determine the structure of the experiment.

3.7.1 Experiment Hypotheses

Identifying the hypothesis is the first step in designing an experiment. A hypothesis is a statement that can be tested through an experiment (Lazar et al., 2010); it differs from a theory, as it is short and focused. When conducting the experiment, it is essential to have both null and alternative hypotheses. The null hypothesis indicates that there is no difference between two conditions (Lazar et al., 2010), while the alternative hypothesis indicates that there is an observed effect of the experiment. In addition, it is common to use research questions with experimental research.

3.7.2 Variables

Identifying the experimental variables is the second essential step in an experimental design. There are two main types of variables: dependent and independent. A dependent variable is the 'effect' that the researcher focuses on, while the independent variable is the 'cause' that influences the dependent variable (Rosenthal and Rosnow, 1991). The dependent variables examined in this research were task completion counts, authentication step timing and the use of help. The independent variables included each option of multifactor authentication. Another type of variable is the confounding variable, which is a variable that might affect the dependent variables. Failure to control for confounding variables may lead to false findings and conclusions (Howitt and Cramer, 2008). The confounding variables in this study were the type of biometric method, the evaluator's experience and the experiment environment.

3.7.3 Experiment Design

The first step in designing an experiment is defining its broad aim. The aim of the present experimental study was to assess the usable security of different multifactor mechanisms. The second step involves defining the measurements, selecting the sample and defining the data collection instruments. The target sample in the experimental study included students who were familiar with e-banking concepts. Therefore, students who studied at the University of East Anglia were chosen, as it was easy to access them. Generally, using students as a sample has both advantages and disadvantages. Its chief advantages are that students are accessible, easy to recruit and control and inexpensive as participants, as they do not need transport to access them and they are readily at hand. In contrast, there is a common claim from several researchers, including Sears (1986), that a sample comprised of students constitutes a 'narrow data base'. Druckman and Kam (2009) pointed out that Sears' argument does not provide empirical evidence that student subjects create an issue, and they empirically showed that student subjects 'do not intrinsically pose a problem for a study's external validity'. Moreover, recruiting subjects from remote locations is considered time- and effort-consuming, and most usable security studies have recruited a sample from a student population.

3.7.4 Measurements

The measurements used in the experimental study were classified into usability measures and security measures. Usability measures are the basic usability attributes in the ISO definition of usability (efficiency, effectiveness and satisfaction). In general, usability measures are difficult to select because there are different measures

identified in the literature, which exceed 50 measures (Hornbek and Effie, 2007); however, the ISO usability measures of effectiveness, efficiency and satisfaction, which were selected for the experimental study, are widely used.

The security measures were classified according to the type of security warning that appears during the experiment. As mentioned in Section 2.4, user awareness of where their attention is directed is considered one of the factors that can be measured during the execution of a security task (Kainda et al., 2010). Accordingly, users' awareness of the main security warning was categorised, and then it was used as a security measure. The main security warning that appears during the authentication process involves:

- Login into insecure page (Falk et al.,2008; Mannan and Oorschot, 2008),
- Security information emailed insecurely (Falk et al., 2008),
- Providing sensitive data insecurely,
- Proceeding despite the warning message (Seifert et al., 2006).

The third security warning refers to providing a finger scan, which was used during the experiment. The taxonomy used for categorising the above security warning reflects the meaning of the users' awareness of the security issues, which are attention, caution, motivation and wariness (further details are provided in Chapter 6).

3.7.5 Data Collection Instruments

In the experimental study, different methods were used to collect both qualitative and quantitative data. The first method used was recording users' input into the system. To do so, a table schema was created on the database to save the input in the database for later use during the analysis phase. The second method was the observation of users'

behaviours and reactions during the experiment. In the experimental study, the observation was controlled using a structured observation method that was previously prepared for the study (see Appendix I). The third method was the questionnaire, which was designed following the design steps mentioned in Section 3.3.1.3.

3.7.6 Piloting the Experiment

Before carrying out the experiment, a pilot study was conducted to identify any difficulties or ambiguities in the experimental procedure (Matera et al., 2006). Therefore, before conducting the experiment, a pilot study was performed with four students to determine how long the experiment would last and to identify any ambiguities in the experimental scenarios or questionnaire. The pilot study did not require any changes in the experiment scenarios or questionnaire, but the researcher decided to use two laptops, one for the experiment and another for the questionnaire, so participants could finish the experiment and then use the other laptop to complete the questionnaire, which was already opened to the web page. Also, the second laptop was used as a stand for the scenario paper so the participants would feel comfortable following the scenario steps. These minor changes saved time during the experiment.

3.8 Ethical Considerations

For ethical considerations, a consent form that informed the participants about all aspects of the study (UEA, 2011) was included at the beginning of the questionnaire used in the exploratory and experimental studies. It asked the participants to voluntarily agree to take part in the research. It also informed the participants that the data would remain confidential and that they could withdraw at any time if they did

not desire to complete the questionnaire or the test. It confirmed that they did not need to provide any personal information or authentication tools. Finally, they were notified that there were no risks associated with participating in the research.

3.9 Data Analysis

A data analysis involves steps such as cleaning, screening and coding the data and selecting the proper statistical analysis procedure (Churchill and Iacobucci, 2004; Luck and Rubin, 1987; Malhotra, 1999). The analysis of the collected data for each study was conducted in two phases: a preliminary analysis that familiarised the researcher with the data and an in-depth analysis using external tools. The preliminary analysis of the data collected from the questionnaire was performed by reviewing the charts provided through Google Docs or Qualtrics, reading the answers to the open-ended questions and coding the issues that were raised by these questions in the report. The in-depth analysis for quantitative data began by reviewing the data to identify errors or incomplete records, and then the data were simplified in graphs that showed the frequency of each answer. Most of the statements were phrased positively, which helped to obtain the percentages for all answers related to each usability factor. A high percentage score implied a positive user perception of a particular aspect of usability in the system, and a low percentage score indicated possible usability issues. Moreover, some phrases were phrased negatively to avoid issues of bias or automatic completion of similar answers that can result when all questions are phrased positively. After analysing each item in the questionnaire individually and in comparison with other items, an overall rating for the system was created by examining all statements and providing a table or graph that summarised the results; this generated an overview of the users' satisfaction with the authentication method. In addition, to enhance the

understanding of the data, the researcher identified different relationships between usability factors and the socio-demographic characteristics of the respondents. This helped identify which result changed the most, potentially leading to interesting findings that could be linked with the collected qualitative data. The data were transferred to SPSS software for an in-depth analysis and to identify additional correlations between different variables using parametric and non-parametric statistical tests.

For the qualitative data, a code-based analysis was utilised, which is a systematic method used to analyse the original written data (Weber, 1990). Thus, the data classified as 'coded' were used to identify a 'categorical variable', after which the frequency count method was used to measure the content.

3.10 Chapter Summary

This chapter provides a detailed description of the methodologies adopted in this research. First, the selection of multiple methodologies for this research is justified, followed by a detailed description of each study. As stated, three different research approaches were adopted in this research beginning with exploratory research, which utilised a survey for collecting the data, and the process for developing a final version of the questionnaire has been presented. The descriptive research approach has been explained by identifying the main purpose of this research. Finally, the experimental research approach is described along with the details involved in designing the experiment, followed by an ethical consideration pertaining to the collection of data. The data analysis strategy is also explained. The next chapter discusses the first step used to answer the research questions by conducting an exploratory study to investigate the current use of MFA.

Chapter 4

Exploratory Study

Investigation of the current state of MFA

Preface

This chapter discusses the results of investigating the authentication methods currently used by e-banking and users' perceptions of those methods. First, the chapter discusses the need for the study and defines its objectives and research questions. Then, it describes the method used to gather the data and the design of the survey. Next, the chapter discusses the sample, including sample size and participant recruitment. Then, it discusses the findings of both the quantitative and qualitative data and the study's results. Finally, the chapter ends by summarising the chapter.

4.1 The Need for an Exploratory Study

The present study was needed because there is a lack of usable security research in general and, in particular, a lack of research regarding current practices in using single

factor authentication (SFA) and multifactor authentication (MFA) in various e-banking enterprises in various countries. The study involved the United Kingdom (UK) and Saudi Arabia because they represent an example of a developed, industrialised country and a less-developed, less-industrialised one, respectively, and online banking is widely used in both countries (Alsajjan, 2008). In addition, both countries have large numbers of e-banking users (Alsajjan, 2008). Therefore, investigating users' perception of e-banking services may help to increase users' trust over the long run (Mannan and Oorschot, 2008). The present study also aimed to investigate which authentication methods are more-commonly used in e-banking, evaluate those methods and measure users' perceptions of them.

Based on the results of various studies presented in section 2.10.2 of Chapter 2 and as discussed in section 3.3.1 of Chapter 3, the present study contributes to the knowledge of this topic by studying a unique sample of actual long-term users of online banking. This approach was used because previous studies were experiments or surveys in which participants were asked to use either SFA or MFA or to indicate whether they had previously used SFA or MFA. Therefore, the present study was conducted to affirm that choosing the sample is the most important part of any usability study and to suggest that studies that do not consider the experiences of long-term users are unlikely to provide a realistic picture of the perceived security and usability of SFA or MFA.

4.2 The Study's Objectives

The objectives of this study were as follows.

- Give an indication of the current use of MFA in Saudi Arabia and United Kingdom.

- Compare the perceived usability of SFA and MFA.
- Compare the perceived security of SFA and MFA.
- Gather qualitative data about users' perceptions of SFA and MFA.

4.3 Study Questions

To achieve the study's aims and objectives, the following research questions were developed as the basis for designing the survey.

1. What types of authentication methods do online banking websites use?
2. To what extent has online banking adopted MFA in Saudi Arabia and United Kingdom?
3. How do users perceive both the usability and security of the MFA and SFA authentication methods?

4.4 Survey Design

As mentioned in section 3.3.1 of Chapter 3, this usability study's data collection method was a questionnaire. This method was chosen for the following reasons.

- Questionnaires are useful for analysing the users' perceptions.
- They can be re-used for similar applications.
- They are inexpensive.
- The respondents do not need to interact with the evaluator.

To investigate current practices in SFA and MFA use and to explore and evaluate users' perceptions of the usability and security of those authentication methods, the present study used a questionnaire to obtain data from respondents who use two types of bank accounts: local and foreign.

The questionnaire designed (see Appendix B) consisted of three sections (see Figure 4.1). The first was designed to gather participants' demographic data, including gender, age, education, length of time using the Internet, length of time using e-banking and number of bank accounts. The second was designed to obtain information about participants' local bank accounts at Saudi banks. As such, it began by asking the name of the bank and the authentication methods it uses and then asked users to respond to 20 statements designed to evaluate the authentication process associated with the method the bank uses. In addition, this section asked two open-ended questions: what participants liked and what they disliked about these methods. The third section of the survey was similar to the second section except that it focused on foreign bank accounts, those in the countries the participants were studying in.

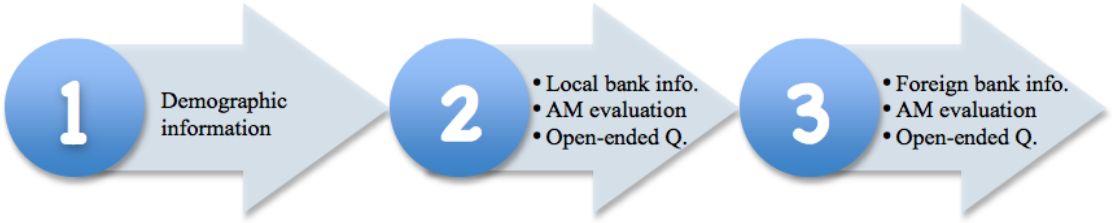


Figure 4.1 Survey design

In the rating section, the evaluation measurements are based on different metrics, which themselves were based on other things. Five metrics were based on the definition of usability (learnability, memorability, efficiency, errors and satisfaction). Two metrics were based on the System Usability Scale, as it covers the factors (ease of use and cognitive effort) considered important for measuring the authentication methods used; they are also used to determine the accuracy of the data and to evaluate the usability of the findings (Bangor et al., 2008). The last two metrics (security and trustworthiness) were added because they determine users' perceptions of a system's security and trustworthiness and, as mentioned in section 3.3.1.4, they have been used

in previous studies that evaluated authentication methods (De Critofaro et al. 2014; Weir et al., 2009; Weir et al., 2010).

Table 4.1 lists all the statements used in the questionnaire. Likert scales (Likert, 1932) were used to measure participants' attitudes toward the characteristics of the authentication methods (Coolican, 1990). The final version of the questionnaire was a web-based one using the Google Docs tool (see Appendix C), which has an attractive interface and provides the ability to export files and monitor the respondents' progress.

Factor	*Statement*
Ease of use	The log-in process is complicated. I need help logging in. I can easily log in I can quickly log in. The log-in process needs improvement. I always successfully log in at the first attempt
Learnability	I need to learn how to log in. I needed written instructions to log in for the first time.
Efficiency	The log-in process is efficient.
Satisfaction	I will be happy to use the log-in process again. The log-in process is unsatisfying.
Memorability	I can easily remember how to log in.
Errors	I often log in after the first try failed. It often takes me two tries to log in. It often takes me three tries to log in.
Cognitive efforts	I need to concentrate hard to log in. I feel stressed when logging in. I feel frustrated when logging in.
Security	The log-in process is secure.
Trust	The log-in process is trustworthy.

Table 4.1 Details of survey statements in Likert scale

4.5 The Pilot Study

To identify any drawbacks that might cause respondents problems with the questionnaire (Altman et al., 2006), a pilot study was conducted first, using six students. The pilot study's aims were as follows.

- Determine the time required to complete the survey,
- Elicit participants' opinions about the survey design,
- Identify ambiguity in questions/statements so they could be clarified.

The results of the pilot study showed that it took 20 minutes to complete the survey. Results also showed that participants thought the survey was well organised and attractive. Participants indicated the need for more answer choices for the question about log-in attempts. Therefore, we added a statement that would denote an additional failed attempt: 'It often takes me three tries to log in'. In addition, as a result of the pilot study, some statements were reworded to clarify them.

4.6 Sample Size and Recruitment

The study's sample was specifically selected to represent long-term users of online banking, as previously mentioned in section 4.1. The participants were Saudi students studying abroad who had a local bank account in Saudi Arabia and a foreign bank account in the country in which they studied. They were selected because they were long-term users of online banking involving financial institutions in two different countries, both of which met the study criteria.

To determine the sample size needed, the researcher referred to Research Advisor (2006), which provides a table indicating the sample sizes needed based on population

sizes. Since there are about 14,000 Saudi students studying in the UK, the estimated sample size needed was approximately 378. To obtain the exact sample size the researcher calculated this sample size using the following formula from Research Advisor (2006), which was also used by Krejcie and Morgan (1970).

$$n = \frac{x^2 * \mathrm{N} * \mathrm{P} * (1 - \mathrm{P})}{\left(\mathrm{ME}^2 * (\mathrm{n} - 1)\right) + (\mathrm{X}^2 * \mathrm{P} * (1 - \mathrm{P}))}$$

Where:

n = Sample size

X^2 = Chi-square for the specified confidence level at 1 degree of freedom (95%, standard value of 1.96)

N = Population size (14000 Saudi students studying in the United Kingdom[1])

P = Population proportion (0.5, following the table of sample size in Research Advisor (2006)).

ME = Desired margin of error expressed as a proportion (5%, proportion 0.05)

Required sample size (n) = **374.**

The study recruited participants by sending an introductory e-mail to the coordinators of several Saudi clubs based in several UK cities. The e-mail contained a link to the survey and asked the clubs' coordinators to distribute the e-mail to their members. Because social media is very strong in Saudi Arabia, a collectivist society in which people act on group goals (DePauw, 2006), the researcher also used Twitter and

[1]Arabian Business (2014). Retrieved June 2014 from http://arabic.arabianbusiness.com/business/education/2014/apr/14/358658/

Facebook to distribute the survey and to invite students to participate. All participants were offered a $5 honorarium for their participation.

To fulfil ethical considerations, the survey included a consent form (see Appendix A) that asked participants to voluntarily agree to take part in the study before they began filling out the questionnaire. In addition, it informed the participants that all data would remain confidential and that they could withdraw at any time if they did not want to complete the questionnaire. Furthermore, it informed them that there was no risk associated with participating and that no authentication tools or personal information were required. After the participants agreed to the terms in the consent form, they could proceed to the questionnaire by clicking the 'Continue' button.

4.7 Results and Discussion

4.7.1 Reliability of the Measures

According to Veal (2005), reliability is the degree to which research results are accurate and would be the same if repeated with a different sample. In addition, reliability indicates the integrity of the survey's measures (Sekaran, 2003). Using the Statistical Package for the Social Sciences (SPSS), the Cronbach's coefficient alpha (Cronbach, 1951), the most popular test of inter-item consistency, was used to test the consistency of the participants' responses to all survey items. A good reliability should produce a coefficient value of at least 0.7 (Pallant, 2001), although that value can be reduced to 0.6 for exploratory research (Robinson, 1991). For the present study, the survey proved to be reliable, with a Cronbach's alpha coefficient value of 0.905. In addition, an item-to-total correlation, which measures the correlation of the item to the

total scale (Hair et al., 2006), was performed and showed that all item-total correlation values exceeded 0.3 (Robinson et al., 1991). Table 4.2 shows the item-total statistics.

Statement	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
The log-in process is complicated.	.646	.898
I need help logging in.	.709	.896
I can easily log in.	.640	.898
I can quickly log in.	.578	.900
The log-in process needs improvement.	.499	.902
I always successfully log in at the first attempt.	.573	.900
I need to learn how to log in.	.628	.898
I needed written instructions to log in for the first time.	.350	.906
The log-in process is efficient.	.480	.902
I will be happy to use the log-in process again.	.441	.903
The log-in process is unsatisfying.	.584	.899
I can easily remember how to log in.	.601	.899
I often log in after the first try failed.	.321	.906
It often takes me two tries to log in.	.551	.900
It often takes me three tries to log in.	.632	.898
I need to concentrate hard to log in.	.562	.900
I feel stressed when logging in.	.639	.898
I feel frustrated when logging in.	.666	.897
The log-in process is secure.	.356	.905
The log-in process is trustworthy.	.352	.905

Table 4.2 Item total statistics

4.7.2 Overview of the Participants

The survey's response rate was high in comparison to the required sample size (374), as 614 respondents completed the survey. Of those, 491 (80%) were male and 123 (20%) were female. This difference in gender was expected and was consistent with

the Saudi Ministry of Education's reports[2] indicating that the proportion of Saudi students studying abroad who are females is 24.5%. Nearly all participants (99%) had used the Internet for more than three years, and most (83%) had used online banking services for more than three years. In addition, 13% had used online banking services for between one and three years, while 4% had used them for less than a year. Regarding frequency of e-banking use, 36% of the participants used e-banking more than ten times a month, 31% used it from six to ten times a month and 33% used it from zero to five times a month (see Figure 4.2).

The participants included Saudi students studying in a variety of countries, including Australia, Canada, Ireland, New Zealand, the UK and the United States (US) and also included various age groups and education levels. Table 4.3 shows participants' demographic characteristics

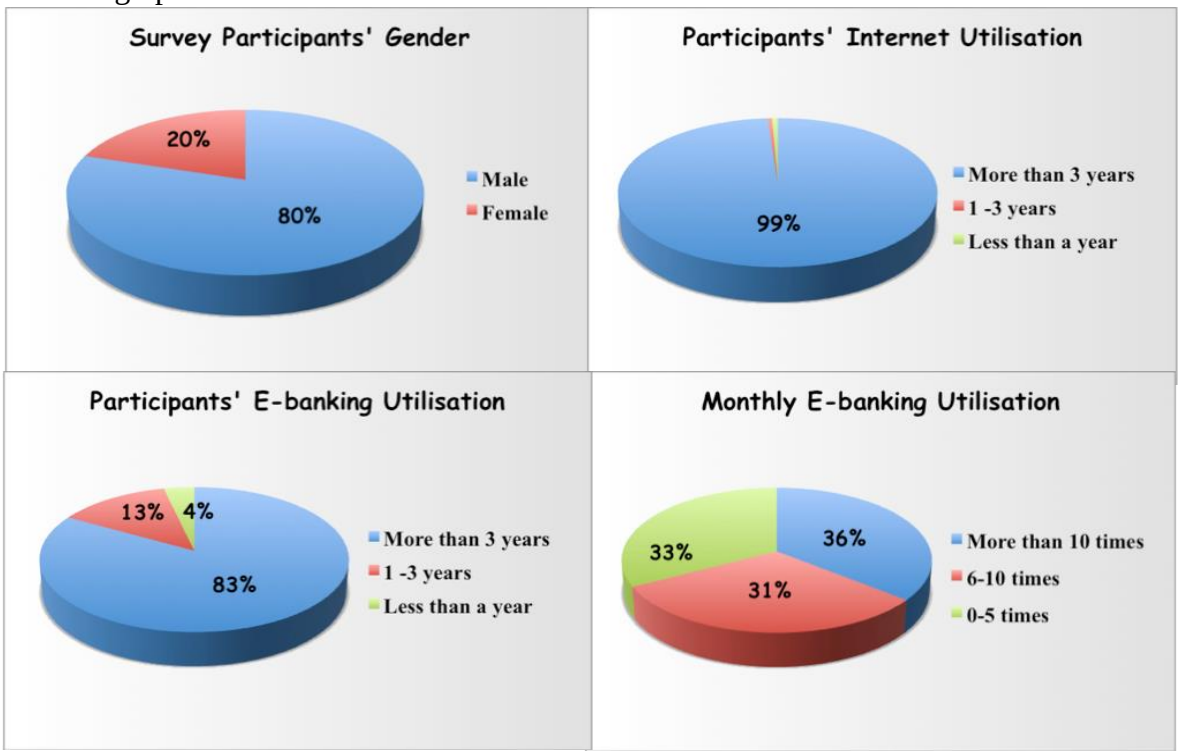


Figure 4.2 Participants' profiles

[2] Riyadh News (2014). Retrieved November 2015 from http://www.slaati.com/2013/03/03/p17126.html

Characteristics	Freq.	Percentage
Age		
18-25	82	13.4
26-30	218	35.5
31-35	191	31.1
36-40	97	15.8
41-45	14	2.3
Over 45	12	2.0
Education level		
School	19	3.1
College	36	5.9
Undergraduate	163	26.5
Master's degree	329	53.6
PhD	67	10.9
Foreign bank country		
Australia	14	2.3
Canada	32	5.2
Ireland	27	4.4
New Zealand	4	0.7
United Kingdom	478	77.9
United States	59	9.6

Table 4.3 Participants' characteristics

4.7.3 Using SFA or MFA

As previously mentioned in section 4.1, the study was designed to investigate the current use of MFA in online banking. The study's results indicated that 603 of the 614 participants used MFA in Saudi Arabia and that the MFA mechanisms used by all included a password and a personal identification number (PIN) via mobile phone.

Only 11 participants indicated that they used SFA to access their bank accounts in Saudi Arabia (see Figure 4.3).

In addition, of these 614 participants, 478 (78%) had a foreign bank account in the UK, and 326 (68%) of those 478 used MFA to access their accounts, while 152 (32%) used SFA. The results of further investigation showed that half the participants (50%; f = 239) had an account with HSBC, and half (239) had accounts with other UK banks, including Barclays, Lloyds, NatWest and the Bank of Scotland. There were two reasons why HSBC was so popular with Saudi students: the bank has a branch near the Saudi Embassy in London, and HSBC provides 'Shariah-compliant products' that follow the Islamic business structure.

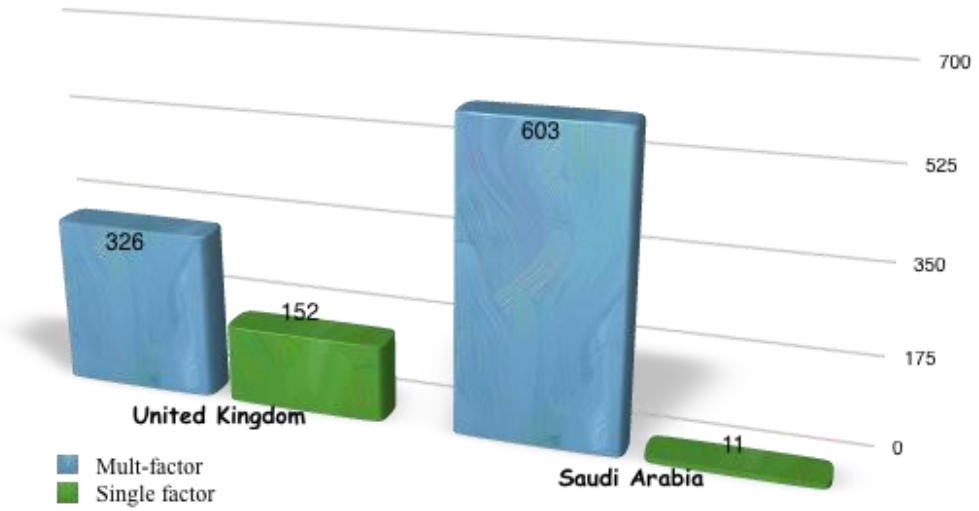


Figure 4.3 Authentication methods classification in UK and SA

Results showed that 136 Saudi students studying abroad in countries other than the UK had foreign accounts in those countries. Of the 14 participants who were studying in Australia, 8 used MFA, while the vast majority of the 59 participants studying in

the US (f = 56) used SFA. All 32 participants studying in Canada used SFA, and the majority of the 27 participants studying in Ireland (f = 24) used SFA. All four participants studying in New Zealand used SFA and had their bank account with ASB bank. Table 4.4 illustrate these results.

Results of the present study indicated that most (68%) UK banks had adopted MFA using a variety of authentication methods, including secure devices, card readers and PINs via mobile phone. In contrast, most Saudi banks used MFA with only one authentication method: a PIN via a mobile phone.

Country	***SFA***	***MFA***
Saudi Arabia	11	603
Foreign countries	274	340
Australia	6	8
Canada	32	0
Ireland	24	3
New Zealand	4	0
United Kingdom	152	326
United States	56	2

Table 4.4 SFA and MFA in different countries

4.7.4 Analysis by Authentication Factor

A parametric independent t-test was used to empirically assess whether there were significant differences between the overall perceived usability, security and trustworthiness of SFA and MFA. This type of t-test was used because the sample size was greater than 30 and the variables were normally distributed, with values close to

0 for the two statistical measures' skewness and kurtosis. Table 4.5 illustrates the normality test for the three main attributes.

Measure		Saudi Arabia		Foreign Countries	
		Statistic	**Std. Error**	**Statistic**	**Std. Error**
Usability	Skewness	-0.27	0.199	-0.297	0.193
	Kurtosis	0.265	0.197	0.1	0.194
Security	Skewness	-0.296	0.196	-0.184	0.196
	Kurtosis	0.298	0.197	0.291	0.195
Trust	Skewness	-0.309	0.195	-0.095	0.195
	Kurtosis	0.186	0.197	0.256	0.197

Table 4.5 Normality test

The independent t-test results was performed for the groups of participants in the foreign countries, and the results indicated significant differences in the overall usability scores for SFA, with a p value < 0.01 (p = 0.00). In contrast, the results showed significant differences in the participants' attitudes toward security and trustworthiness regarding MFA, with p values of 0.00 for both. Table 4.6 shows the t-test results, which indicated that MFA was perceived as more secure and trustworthy than SFA. While Figure 4.4 shows the differences based on the mean values.

Measure	Authentication factor?	N	Mean	Std. Deviation	t	df	sig
Usability	Single Factor	274	3.8114	0.67412	5.113	612	.00
	Multi Factor	340	3.5562	0.56256	5.016	530.783	
Security	Single Factor	274	4.01	0.994	-4.338	612	.00
	Multi Factor	340	4.31	0.726	-4.198	485.616	
Trustworthy.	Single Factor	274	3.95	0.998	-4.965	612	.00
	Multi Factor	340	4.29	0.694	-4.782	469.673	

Table 4.6 Comparing SFA and MFA in foreign countries and Table 4.1 lists all the statements

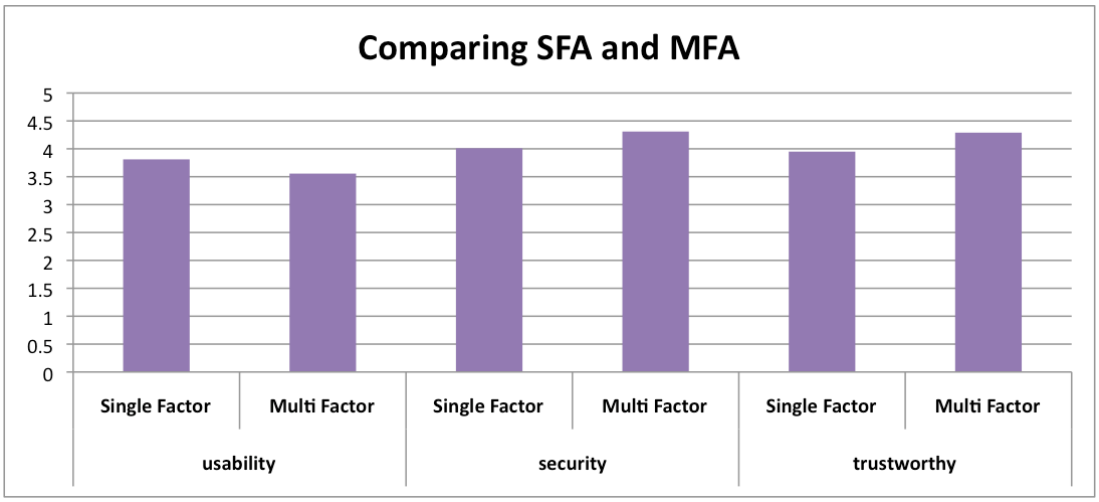


Figure 4.4 Comparing SFA and MFA based on mean values

In addition, to validate the results, the data was also tested using non parametric techniques and similar results were obtained (see Appendix J).

4.7.5 Analysis by Individual Usability Attributes

A repeated-measures independent t-test was carried out on each of the study's 20 usability statements used to measure SFA and MFA. The results showed no differences between the two methods for some of the usability measures, including the 'errors' attribute; the p values for all three statements about the number of failures encountered when logging into the system were > 0.05, indicating no difference between the usability scores of the two methods. In addition, there were no significant differences between the scores for the memorability attribute and for a statement related to the satisfaction measure ('The log-in process is unsatisfying') based on the authentication method used.

For the other 15 usability statements, there were a number of differences between the SFA and MFA methods. The SFA scored better on ease-of-use measurements, with p values < 0.01. The SFA was also rated more positively in terms of learnability (needing written instruction, needing help), with p values < 0.01 ($p = 0.001$ and $p = 0.003$, respectively). In addition, the SFA scored high in terms of efficiency ($p = 0.008$) and willingness to use the method again ($p = 0.00$). Therefore, the results in general confirmed that the overall usability of SFA was better than that of MFA, as shown in section 4.7.4.

4.7.6 Analysis by Method

The ANOVA test was performed to determine whether there were differences in scores among various factors related to the authentication method used. The results

indicated that there were significant differences between the authentication methods used to access a foreign bank account, with (p value < 0.01, degree of freedom 4.6). To understand the exact differences, a post-hoc test was performed using the least common denominator (LCD) method to identify the fewest number of differences. The results showed several significant differences. For example, in terms of security, using a secure device to log in was better than using a PIN via a mobile phone. There were significant differences in scores ($p < 0.01$) related to using a PIN via a mobile phone and using a password. Using a PIN via a mobile phone was considered to be easier and safer, which was an unexpected result. There were no significant differences between the security and trustworthiness scores regardless of whether a secure device or a card reader was used.

A paired sample t-test was conducted to identify the differences in MFA scores for the same user who used MFA in local bank account and foreign bank account. This enabled the researcher to form a clear conclusion about whether using a PIN via a mobile phone or some other MFA was seen as the most usable, secure and trustworthy authentication option for accessing bank accounts in foreign countries. The results indicated that there were significant differences between these options in terms of both security and trustworthiness ($p < 0.01$). The larger mean was awarded to the MFA in foreign bank accounts, accessed either via a secure device or a card reader. Table 4.7 illustrates the results.

Measure	Bank account of MFA	N	Mean	Std. Deviation	t	sig
Usability	Local bank	336	3.5055	.67987	1.253	0.211
	Foreign bank	336	3.5549	.56578		
Security	Local bank	336	3.90	.991	7.342	**0.00**
	Foreign bank	336	**4.31**	.729		
Trustworthy.	Local bank	336	3.83	1.032	7.803	**0.00**
	Foreign bank	336	**4.29**	.698		

Table 4.7 Paired comparisons MFA in two bank accounts
* Bold values indicates the significant difference awarded to the larger means

4.7.6 Analysis by Other Measures

Some analyses took into account several types of demographic information from MFA users, including gender, length of time using e-banking, number of times per month using it and the participant's education level. An independent t-test was performed to test the variance between females and males using MFA, and Levene's test was run to test the homogeneity between males and females (see Figure 4.5). The results indicated no differences in the usability scores between the two groups and only small differences in terms of perceived security and usability.

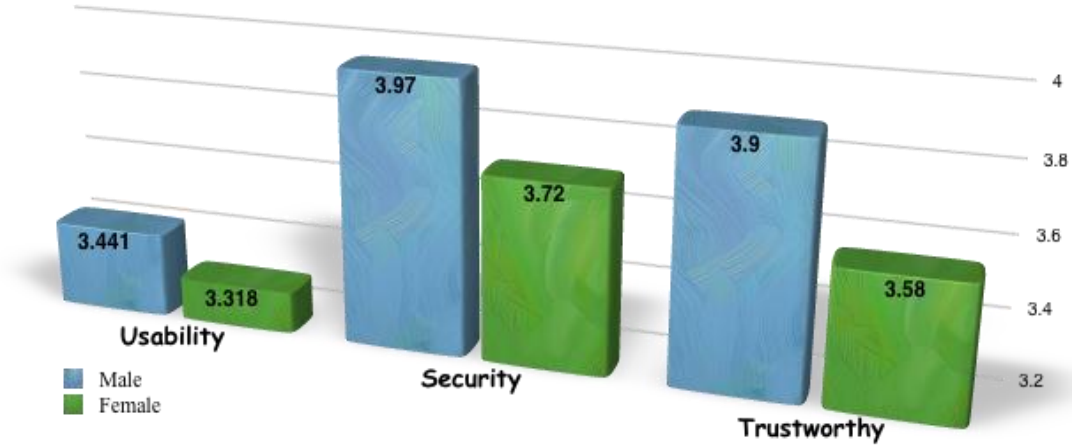


Figure 4.5 Mean differences by gender

To empirically assess whether there were significant differences in overall usability, security and trustworthiness scores, (taking into account the length of time using e-banking), the independent ANOVA (the parametric equivalent of the t-test for more than two groups) was used, followed by a post-hoc test to determine the exact differences between the groups by comparing the mean of each group to the mean of every other group. The ANOVA test showed that there were differences in terms of perceived security and trustworthiness, with $p < 0.05$ ($p = 0.016$ and $p = 0.003$, respectively). The post-hoc test showed that there were differences between the groups. The group that had used e-banking between one and three years perceived the MFA to be more secure. Figure 4.6 shows the differences between the means among the three groups.

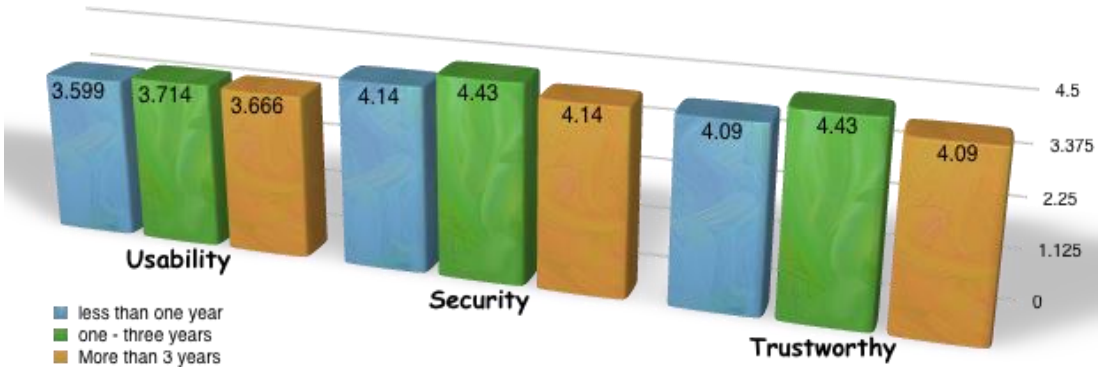


Figure 4.6 Mean differences by e-banking usage

To investigate differences among groups based on the number of times they used e-banking monthly, an empirical assessment using ANOVA was conducted. The results showed no significant differences among the groups in terms of perceived security and trustworthiness, with p values > 0.05 ($p = 0.67$ and $p = 0.16$, respectively). In contrast, there were differences among the groups in terms of perceived usability ($p = 0.002$);

the group that used e-banking more than ten times a month perceived the MFA to be more usable. Figure 4.7 shows the differences in the means among the three groups.

A final analysis was performed to investigate whether the MFA scores differed based on the education level of the participants. First, an independent ANOVA test was performed to identify the significant values, and the results indicated that there were small differences between the groups (p value < 0.05) in terms of perceived usability, security and trustworthiness (p = 0.021, p = 0.003 and p = 0.049, respectively). After a post-hoc test, the differences appeared to be small; the group with school education perceived the MFA to be more usable, while the group with college education perceived the MFA to be more secure and more trustworthy. Figure 4.8 indicates the differences between the means among these groups.

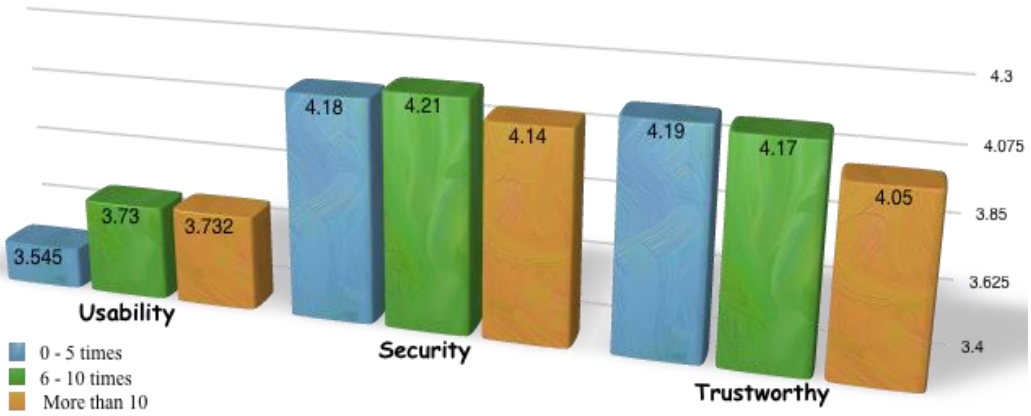


Figure 4.7 Mean differences by monthly visits

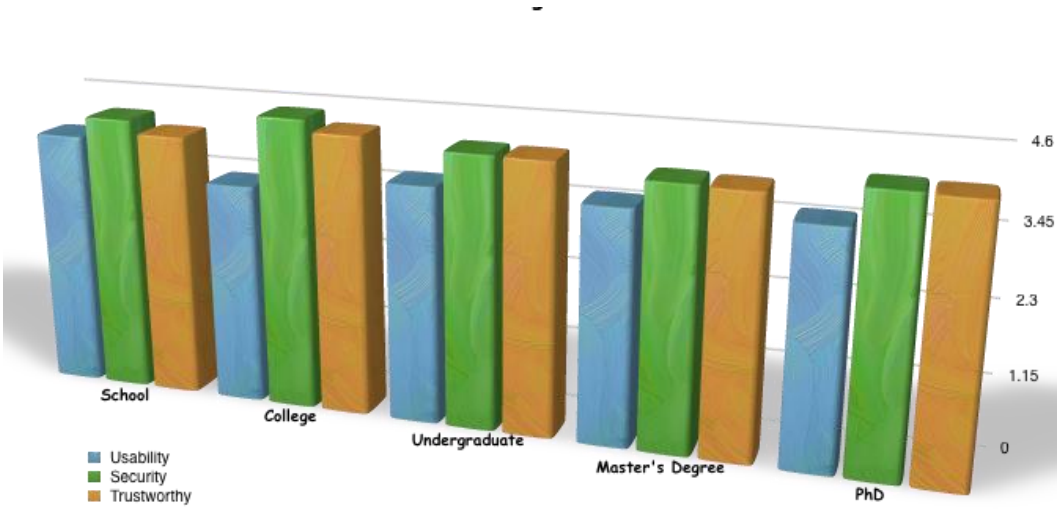


Figure 4.8 Mean differences among different education level

4.7.8 Analysis of the Qualitative Data

The survey contained four open-ended questions designed to elicit subjective information. They did not contain any of the researcher's opinions or inferences, thus enabling the respondents to answer the questions with influence. Two questions after the section that rated the local bank asked the participants what they liked and disliked about their local bank's authentication methods. Similar questions were included after the section that rated the foreign bank. The participants often provided detailed answers to these questions, which provided significant insights. As mentioned in section 3.7 in Chapter 3, the qualitative data was analysed using systematic, code-based analysis. This process begins with the researcher familiarising him or herself with the data to gain insights into their content. This is followed by codifying the data, which means grouping, regrouping and relinking to consolidate their meaning and explanation (Gribch, 2007). After coding the data, the categorical variables are determined. Then, the frequency-count method is used to calculate the measures. The

next four subsections present the various issues and advantages of the authentication methods used by both local and foreign banks.

4.7.8.1 Issues Identified in the Local Bank Accounts

The first open-ended question asked what the participants disliked about their local bank's authentication method. The participants provided 457 statements in response. Table 4.8 classifies these responses, including general statements of opinion (20%) (e.g. '*The process is boring', 'I hate typing the password' and 'The process is very bad'*) and issue- specific statements (80%), which were classified into four categories: technical issues, banking limitation issues, usability issues and authentication method issues. The taxonomy for these issues was based on the researcher's understanding; therefore, even if other researchers have different taxonomies, it does not affect the totality and nature of the problem. As Table 4.8 shows, 25% of the problems were related to technical issues, including connection interruptions and time spent loading to receive a PIN via short message service (SMS) on a participant's mobile. One participant indicated that the system was refreshed overnight, so he was not allowed to make a payment. The most significant, unique problem in this category was system slowness, but this problem was not related to the authentication process, so it was not relevant to the usability of the authentication process or the quality of the e-banking service.

Banking limitations accounted for 4% of the issues. For example, the issues included the bank's failure to approve a payment for online shopping or the lengthiness of the process for transferring funds to an international bank. Usability issues were raised in 13% of statements (e.g. '*The design of the website is unclear'*). Usability was also

noted as an issue when the authentication process was perceived as complicated or insufficient.

Saudi Arabia		
Statements	Frequency	Percentage
General statements of opinion	92	20%
Specific Issues	365	80%
Nature of Specific Issues	Frequency	Percentage
Technical issues	93	25%
Banking limitation issues	13	4%
Usability issues	49	13%
Authentication methods issues	210	58%
Nature of AM Issues	Frequency	Percentage
Type of the method	120	57%
Password issues	17	8%
Insecure method	23	11%
Number of steps	43	21%
Number of failures	7	3%

Table 4.8 List of issues in local bank account

Various issues were related to the authentication method: 58% of the specific problems were identified as authentication problems, and after further analysis, the majority of these issues were grouped under the 'Type of method' category, which, in all cases, referred to 'PIN via mobile' as the type of MFA. The participants identified several problems with this method. They mentioned that it was not effective because they had to spend a long time waiting for the PIN and they faced additional delays when using their phones abroad. Another issue was that the mobile sometimes became disconnected so they would have to repeat the process because the PIN became invalid. One participant mentioned that there was no need to use the 'PIN via mobile'

MFA, because most of the time he only needed to view the account without making any transactions.

Other participants indicated that because this method was so complicated, they had to have their cell phones with them everywhere they went in case they needed to access their account. Others stated that they could not even open a bank account because they would need a cell phone, which might not work in a foreign country. One participant asked why there was a request to enter a PIN via mobile for customers living abroad when the bank does not accept foreign phone numbers. The following are examples of similar issues:

'As an international student, the SMS PIN that the bank requires is difficult to get because of my mobile network, so I have to keep my cell phone with someone at home to get access to my bank PIN number each time I want to log in. It seems secure but is so complicated'.

'You have to have your cell phone all the time around you, otherwise, you can't log in'.

The group that used a password as a type of SFA indicated several issues related to that method, and 8% of the statements mentioned the difficulty of creating and remembering a password. In the second category of authentication method, 'insecure method', 11% of the statements described the method as insecure, and three statements by those using MFA indicated that they worried about being hacked. Under the 'number of steps' category, 21% of statements noted the number of steps needed for authentication, ranging from entering the username to entering the password and then typing the PIN received from the mobile. The participants felt that there were too many steps and that the steps took too much time (e.g. '*There are too many steps to log in*

to my online banking' and '*It needs more than one step'*). The final category was 'number of failures', and 3% of participants indicated that they had failed to log in successfully and had to type their password several times.

The above findings suggest that the authentication processes in local bank accounts have several issues, the most significant of which are related to authentication methods, specifically, using a PIN via mobile to authenticate the user. Users also mentioned that it is difficult to apply this method when travelling abroad, unless accepting international phone number.

4.7.8.2 Advantages of the Local Bank Account

In response to the question, 'What do you like in the authentication process?', a total of 482 statements were submitted. A few of them (12%) were general statements (e.g. '*All good*' and '*Generally, I can say I am satisfied with the service*'), while 88% of the statements were related to other aspects (see Table 4.9). As shown in Table 4.9, the most significant advantages were identified for authentication methods, with 83% of statements indicating that the participants had a positive impression of the authentication process. After analysis, this authentication method was further classified into four categories: type of method, usability, security and trustworthiness. While 13% of the participants' statements were about the speed of the process and the speed of their ability to log in (e.g. '*It is faster to not use the code generator'*), 4% of participants noted that they were satisfied with the banking feature that was provided and that it met their needs (e.g. '*I benefit from paying bills via e-banking')*.

Saudi Arabia		
Statements	Frequency	Percentage
General statements of opinion	57	12%
Specific advantages	425	88%
Nature of the advantages	Frequency	Percentage
Speed of the service	55	13%
Banking features	18	4%
Authentication methods	352	83%
AM positive points	Frequency	Percentage
Type of the method	41	12 %
Usability	144	41 %
Security	152	43 %
Trustworthy	15	4 %

Table 4.9 List of strength points in Local bank account

The type of authentication method, either a password or a PIN via mobile, was considered to be a good method to verify the participants' identities. Of the participants' statements, 41% related their level of ease of use with the method, and 43% of statements considered PIN via mobile to be a secure method that they liked to use (e.g. *'It provides a high level of security*' and *'It is secure because it is associated with inserting a PIN via mobile*'). Finally, a few of the statements, 4%, indicated that the authentication method was trustworthy.

The above findings suggest that there are several advantages of the authentication processes in local bank accounts. Most of these advantages are related to the usability

and security of the authentication method, and a few of them are related to the trustworthiness and the number of steps in the authentication processes.

4.7.8.3 Issues Identified in the Foreign Bank Accounts

The third open-ended question asked participants what they disliked about their foreign bank's authentication method. The participants submitted 312 responses. Table 4.10 classifies their responses into general statements of opinion (17%) (e.g. '*The process is boring*' and '*Why do they not use the Arabic language?*') and mentions of various issues (83%), which were classified into four categories: technical issues, banking limitation issues, usability issues and authentication method issues.

United Kingdom		
Statements	Frequency	Percentage
General statements of opinion	53	17%
Specific Issues	259	83%
Nature of Specific Issues	Frequency	Percentage
Technical issues	25	10%
Banking limitation issues	5	2%
Usability issues	15	6%
Authentication methods issues	214	82%
Nature of AM Issues	Frequency	Percentage
Type of the method	82	38%
Password issues	42	20%
Insecure method	24	11%
Number of steps	56	26%
Number of failures	10	5%

Table 4.10 List of issues in foreign bank account

As Table 4.10 shows, 10% of the statements described technical issues, including slow connections or unavailability. Five statements (2%) expressed the lack of some banking features, including an inability to make a payment at a specific time or a lack of short identification numbers (e.g. *The ID number it too long*). In addition, a few of the statements, 6%, noted difficulties with the login process and the complexity of the authentication method.

Because 82% of the responses were related to the authentication method, this group of statements was analysed further. Most statements were grouped according to the specific type of authentication method (38%). The participants identified various issues related to the authentication method, using the category 'secure device' to indicate the difficulty they had in carrying the device with them at all times and to indicate technical problems with the screen (sometimes all the numbers did not appear due to long usage and difficulties in refreshing the device). For example:

'*I need to carry the password generator, usually in my pocket'*.

'*I have to have the secure device with me all the time'*.

'*The code generator became unable to show the third digit and I have not yet solved the problem*'.

In addition, the participants used 'password as SFA' to indicate difficulty in remembering the password and guessing the missed, random numbers from the password used by Lloyds in the UK. Feeling insecure with the authentication method used was an issue for 11% of the participants, who indicated that they thought it had a low level of security. Many statements, 26%, noted that there were too many steps

in the authentication process. Finally, 5% of the statements noted that they needed several attempts to log in successfully; this issue was grouped under 'number of failures'.

The above findings suggest that the authentication processes at foreign banks have some significant problems. The participants also indicated some technical problems and difficulties in using secure devices.

4.7.8.4 Advantages Identified in the Foreign Bank Accounts

The fourth open-ended question asked participants what they liked about their foreign bank's authentication method. The participants submitted 571 responses, 15% of which reflected participants' perceptions of the method (e.g. '*The process is good*' and '*I am happy to use the method'*). However, 85% of the responses noted the advantages of specific aspects, as shown in Table 4.11, which classifies these responses into three categories: speed of service, banking features and authentication methods. Fifty statements describing the speed of service comprised the first category and 10 described other features of the bank, such as sending annual statements via e-mail. The third category consisted of 424 responses related to the authentication method. After further analysis, the majority of responses (216) in this category described the authentication method as highly secure (e.g. '*It shows me how secure it is, and I feel that nobody can access my account'* and '*It has a high level of security'*, while 124 described the participants' attitudes about usability. Only a few of the statements 4% considered the authentication method to be trustworthy, and all of them were participants who were using a secure device with an HSBC account in the UK. In addition, 14% noted that the authentication steps made them feel secure and that they

liked being able to complete the verification process (e.g. '*The thing that I like about using this type of service is that there are stages users need to follow to access their accounts that provide security for the users' accounts'*).

These findings suggest the conclusion that the strengths of the authentication processes in foreign bank accounts outweigh the disadvantages, and that users have a high level of satisfaction with the security of the authentication methods.

United Kingdom		
Statements	Frequency	Percentage
General statements of opinion	87	15%
Specific advantages	484	85%
Nature of the advantages	Frequency	Percentage
Speed of the service	50	10 %
Banking features	10	2 %
Authentication methods	424	88 %
Authentication Method Advantages	Frequency	Percentage
Type of the method	7	2 %
Authentication steps	61	14 %
Usability	124	29 %
Security	216	51 %
Trustworthy	16	4 %

Table 4.11 List of strength points in foreign bank account

4.8 Chapter Summary

This chapter presented the findings of an exploratory study that used a survey to investigate the current state of the authentication methods used in e-banking. This chapter explained the study's objectives and the need to fill the gap in the literature regarding studies that investigate the extent of MFA adoption for online banking services. The chapter covered the process of designing the survey, including how its questions were designed and how the pilot test was conducted. The pilot study helped to identify problems and to design a precise final survey. For example, the suggestion to ask about the number of failed login attempts was very useful, as some users indicated that number in the open-ended questions.

The survey's results indicate that most UK banks have adopted the MFA method and use a variety of authentication methods; this data meets the main objective for conducting this study. In contrast, 98% of Saudi banks have adopted the MFA but only use one authentication method, a PIN via mobile. Multiple MFA authentication methods were perceived as being more secure and trustworthy when using either a secure device or a card reader, while SFA was perceived as being more usable, and these findings parallel the findings of Gunson et al. (2011).

Analysing the qualitative data from the open-ended questions identified several issues with the authentication process, including technical problems and limited banking features. The problems cited most often were difficulty in receiving a PIN via mobile while abroad and the loading time to receive the PIN. Other issues with using a secure device for banking in a foreign country were the inconvenience of needing to carry the phone at all times and the long process of replacing it or receiving technical support.

Chapter 5

Descriptive Study

Preface

The previous chapter described the exploratory study that investigated the current state of the use of authentication methods in Saudi Arabia and the United Kingdom by surveying 614 customers. The study showed that most of the online banking in Saudi Arabia and the United Kingdom adopted multifactor authentication, with a variety of methods. Based on users' attitude towards using these methods, several issues were reported. Therefore, this chapter focuses on a descriptive analysis of the currently available authentication methods in order to understand the characteristics of each method. This chapter begins by identifying the study's aim and objectives, followed by a review of various authentication approaches. Finally, the chapter concludes with a summary of the results of the analysis.

5.1 Study Objectives

The aim of this study is to propose a combination of authentication methods to be assessed in the experimental study. A set of objectives is formulated to achieve the study goal as follows:

- Learn about commonly used methods that were identified in the exploratory study.
- Review other currently available authentication methods.
- Identify the strengths and weaknesses of each method.
- Propose an appropriate combination of methods for a practical in-depth evaluation.

5.2 Authentication Methods

Authentication is a tool used to verify users' identities and it usually does not require identification rather, it establishes that the individual presenting credentials actually has valid credentials. Monrose and Reiter (2005) state that the goal of user authentication is to "confirm the claimed identity of a human user". According to Suo et al. (2005), the currently available authentication methods can be divided into three categories: knowledge-, token- and biometrics-based authentication. In the following sections, a descriptive analysis is conducted for these three approaches that have been deployed in the market (Bonderud, 2014). Additionally, to achieve the study objectives, the analysis will cover all available approaches, four of which (location-, formula-, process- and relationship-based authentication) are still under research and

there is no indication in the available published literature that any of them have been deployed in the market.

5.2.1 Knowledge-Based Authentication

Knowledge-based authentication refers to a method of authentication which requires a user to remember a sequence of secret numbers, answers to questions or graphical images as a password (see Figure 5.1), and in which the user is presented with a group of images and asked to recognise the image that he or she selected in the registration phase (Ma and Feng, 2011). All secret information is generated by the user during the registration process and is saved in the system's database, so that it can be compared with the user's input during later login attempts. Knowledge-based authentication is considered the most ubiquitous authentication approach used in distributed systems (Jørstad and Thanh, 2007). However, in the context of online banking, the results of the exploratory study indicate that most e-banking has adopted multifactor authentication (MFA), combining knowledge-based authentication with other methods of authentication in order to increase the level of security. Moreover, the results of an open-ended survey of those using knowledge-based authentication indicate that it has a high acceptance rate (Erlich and Zviran, 2008).

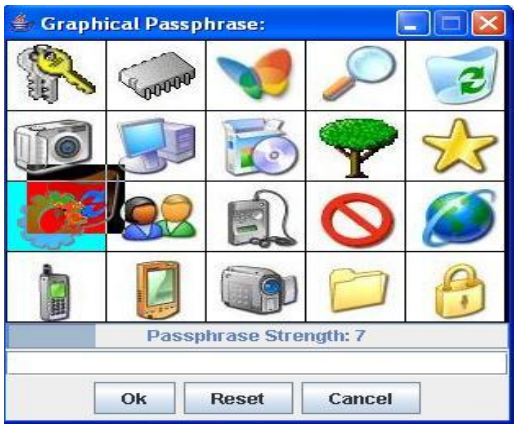


Figure 5.1 Graphical password

Despite passwords' strengths, such as inexpensive implementation and easy management, they have several weaknesses. They are inconvenient, as they require memorisation, and some users have difficulty remembering multiple passwords (Jones et al., 2007), although research has suggested methods for creating strong passwords without reducing their memorability (Yan et al., 2004). Another problem with passwords is their vulnerability to attacks. Password cracking programs, some of which are available to download for free, make it easy to overcome passwords (Keith et al., 2007). Studies have reviewed various ways that knowledge-based authentication—both conventional passwords and image passwords—may be attacked (Summers & Bosworth, 2004; Towhidi et al., 2011; Rittenhouse, 2013).

5.2.2 Token-Based Authentication

A token is an object in the user's possession, embedded with unique hardware or software, for use by a user to prove his or her identity. The use of tokens in the authentication process is prominent on many websites, and their use is intended to address the weaknesses in knowledge-based authentication.

Authentication tokens can be categorized into two types: contact tokens and noncontact tokens. Contact tokens require physical contact between a token and a device reader, for example a magnetic strip on a card swiped by the user at an ATM. Another example of a contact token is a USB which must be inserted into a USB port on a computer in order to access a website (see Figure 5.2).

Figure 5.2 USB token

Noncontact tokens are used most often in online banking. They do not require psychical contact with a reader; instead, they generate a new code, called a one-time password (OTP), for each authentication attempt. Examples of these tokens include secure device authentication, mobile phone authentication and card calculators (see Figure 5.3). OTPs are generated by the host system for single-use user authentication in the system. The main advantage to this authentication method is that it does not rely on a user's memory. Overall, token-based authentication provides more security than knowledge-based authentication, because all information is saved on the client side and the code generated by the token expires after a short period of time. E-commerce makes widespread use of this method (Ku and Chen, 2004) due to user acceptance. However, the exploratory study indicates that users prefer to use a secure device for this method, and prefer not to receive OTPs via mobile devices. Therefore, attention should be paid to which type of token is appropriate or preferred in different circumstances.

Tokens do have drawbacks of their own, such as the high cost of maintaining a token-based system, especially when it is implemented on a large scale, such as with online customers.

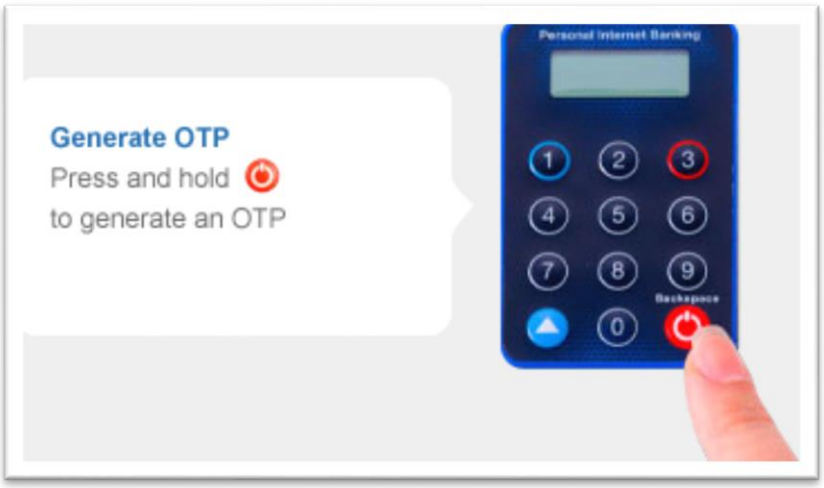


Figure 5.3 Example of OTP generator

5.2.3 Biometrics-Based Authentication

The use of physiological and behavioural biometrics to verify users' identities is called biometrics-based authentication (Renaud, 2004). Physiological methods of authentication include analysis of fingerprints, facial structure or voice to verify users' identities, while behavioural methods include the use of signature keystrokes, for example. The reliability of biometrics is increasing, as they depend upon characteristics that are unique to individual users. However, there is a chance of errors and failures like any other technology

While biometrics-based authentication has a high degree of reliability, it costs much more than knowledge- or token-based authentication. Kay (2005) reports that, while passwords represent an affordable and effective authentication method, they offer

relatively little security. Security tokens must be carried by users and represent an additional layer of security. Although they are more expensive than simple passwords, they are much more affordable than biometric devices (Kay, 2005). Biometrics-based authentication is commonly regarded as the safest authentication method available, as it relies on users' unique physical characteristics for authentication.

Thirty years ago, biometric devices were slow, intrusive and very expensive, but today, biometrics-based authentication systems are much more efficient and much less expensive. As explained by (Kay, 2005; Clarke, 2011), there are several types of biometrics-based authentication:

- Signature dynamics: This method records the way in which the user writes their signature (e.g. pressure, hand movement and fluidity).
- Typing patterns: This method relies on users' chosen passwords, but also measures how fast they type their passwords, the intervals between characters and overall patterns.
- Eye scan: This method uses a rather expensive device to scan a user's retina or iris. (This may make the user uncomfortable.)
- Fingerprint recognition: This method reads users' fingerprints through a dedicated device.
- Hand geometry: This method records the features of the entire hand (e.g. length, distance between fingers, curves) to authenticate the user.
- Facial recognition: This method records users' facial features, including their eye sockets, the shape of their cheekbones, etc. (Figure 5.4 shows different example of biometrics devices.)

Figure 5.4 Examples of some biometrics devices

This authentication method offers a high level of security against attacks, but the cost of implementation is high due to the high cost of the devices needed to read the biometrics. Additionally, not all users are willing to scan their characteristics; some may avoid laser reading, and others may have a medical phobia.

User acceptance of biometrics varies, based on the type of biometrics. Fingerprinting, for example, seems to be more acceptable to users than face recognition and signature dynamics (Morales, 2010). However, none of the users surveyed in the exploratory study reported having used biometrics-based authentication, which indicates its limited use in the context of e-banking.

5.2.4 Location-Based Authentication

A user's location is considered sensitive information that can be exploited to identify the user (Jaros & Kuchta, 2010). The use of location-based authentication is still under research, and has not been adopted in online banking. Denning and MacDoran (1996) were the first to propose the idea of using users' locations for authentication systems. Since then, a few researchers have improved the technique (such as Jaros & Kuchta, 2010; Zhang et al., 2012; and Ghogare et al., 2012). The location-based authentication proposed by Denning and MacDoran (1996) is based on defining a unique, geodetic location for the user at a specific time, created using a location signature sensor (LSS) on microwave signals. The researchers claimed that this method of authentication would be 'extremely valuable' for 'financial transactions'; however, this authentication method has not yet been adopted.

As reported by Oluoch (2014), location-based authentication (LBA) offers multiple benefits, such as a high level of security level and protection against hijacking attacks (Denning & MacDoran, 1996). For instance, if a cybercriminal tries to log into a user's account from a location that is far from the user's smartphone, the login attempt will not be successful, even if the cybercriminal possesses the user's login credentials (Oluoch, 2014). As such, this authentication method makes it possible for users to write down their passwords without having to worry about security issues (Oluoch, 2014). The weakness of LBA is that it can be used to track users' locations all the time. Therefore, the user's privacy is compromised. Additionally, this method requires the use of a global positioning system, which limits its usability with some applications.

5.2.5 Formula-Based Authentication

In 2007, Ginzberg and Rockaway invented a method that uses a formula for the authentication process. In formula-based authentication, the user is presented with a mathematical formula containing values, characters and operators, and the user must provide the results of the formula for each login.

The main advantage of this method is that, instead of entering a known password, the user is required to apply a formula that uses an unpredictable set of values and work out the result. The formula can be made more complex by using two or more publicly accessible and variable values (Mohan, 2015). Onlookers would find it very difficult to deduce the underlying formula, unlike a password or token. As explained by Mohan (2015), the formula is defined by the user and generates a dynamic passcode based on a variable value that can be easily obtained online (e.g., temperature, a stock price, the current date or time). What makes this authentication method particularly resilient is the fact the passwords change continuously and cannot be guessed without identifying the formula that generates them.

On the down side, formula-based authentication may be perceived as time-consuming and inconvenient, because it requires users to obtain their chosen variable values in order to work out their passwords. It is also worth mentioning that this approach is not completely safe, as onlookers may still manage to deduce users' 'secret' variable parameters, especially if they are written down.

5.2.6 Process-Based Authentication

As reported by Shah et al. (2009), traditional computing systems authenticate users using one of four factors: something the user knows, something the user has, something the user is and someone the user knows. In other words, users can enter a password or a PIN code (something they know), use a token to generate a password (something they have), use their facial features or fingerprints (something they are) or provide information about a third person (someone they know) to verify their identities. As cybercriminals continuously seek new ways to obtain users' credentials in order to steal sensitive data, it is increasingly important for security-conscious organizations to employ more sophisticated authentication methods. According to Shah et al. (2009), process-based authentication is a valid option which requires users to recall their passwords and perform certain calculations in order for the system to authenticate them. Specifically, after entering their passwords or PIN codes, users are prompted to calculate an additional password on the basis of system-generated character-value combinations. Specifically, if the combination is (B:3), it refers to char:value (c:v), where c is a set of alphabets {A,B,C…Z}, v is a set of numbers {0,1,2..9} and the op is a set of simple operators {+,-,*}. Each c will be assigned a random value and the user will be asked to recall the formula and perform a computation as required. For example, if the formula is B + C – A and the result is given as 14, then on subsequent logins, the result will be different and the user may not enter the results he or she recalls (Figure 5.5 shows the authentication interface). Shah et al. (2009) claim that their approach is easier than formula-based authentication because formula-based authentication requires users to have technical skills. Shah et al. (2009) identify various security threats in their work and demonstrate how process-

based authentication's multilevel security counters them.

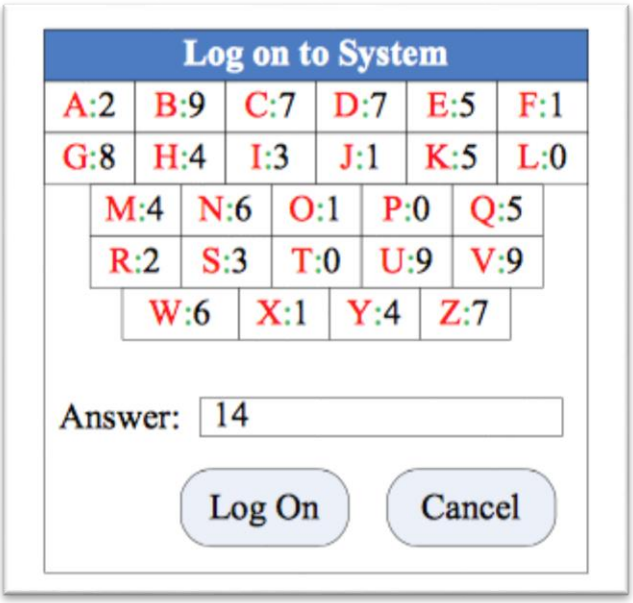


Figure 5.5 General interface of authentication (Shah et al.,2009)

5.2.7 Relationship-Based Authentication

Relationship-based authentication differs from other forms of authentication, in that it relies almost exclusively on human beings, rather than on systems.

Brainard et al. (2006) explore the mechanisms, advantages and disadvantages of fourth-factor authentication (i.e., authentication based on somebody the user knows). Brainard et al. (2006) argue that fourth-factor authentication is particularly useful in case of emergency, when users cannot retrieve their passwords or do not have their tokens with them. Simply put, this authentication method, which the authors call vouching, allows every user to select a helper who will be required to assist the asker (i.e. the user who cannot authenticate him- or herself) to complete the emergency authentication process (Brainard et al., 2006). Vouching relies on SecurID, a token that is commonly used together with a password or PIN code; when the primary user fails to authenticate him- or herself, the helper will use his or her personal SecurID to

grant the primary user temporary access to the account. Figure 5.6 shows some of the following nine steps of the basic vouching process where Alice (the Asker) asks Harry (the Helper) to aid her to obtain a temporary password (Brainard et al., 2006):

1. Asker contacts helper
2. Helper authenticates asker
3. Helper authenticates to server
4. Helper obtains vouchcode
5. Helper gives vouchcode to asker
6. Asker enters vouchcode
7. Server authenticates asker
8. Asker obtains temporary password
9. Logging.

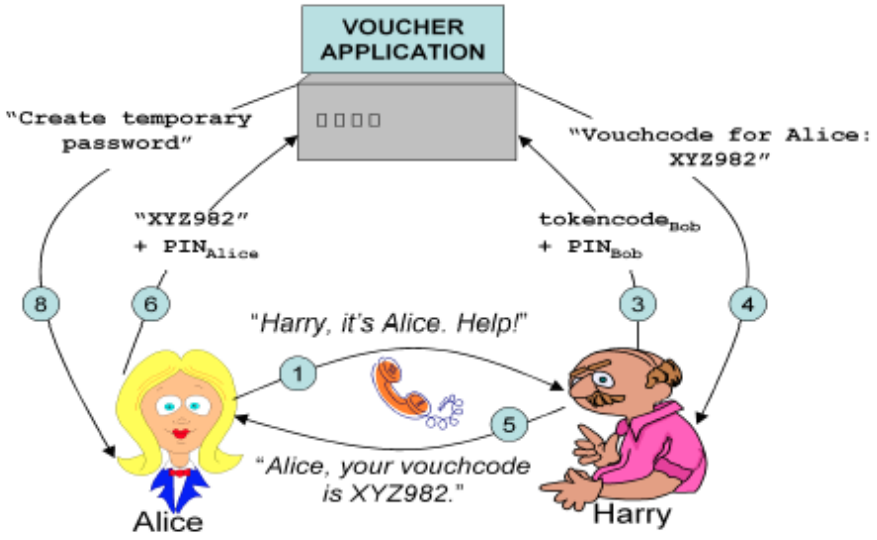


Figure 5.6 Basic vouching process (Brainard et al., 2006)

* Some of step numbers are omitted

The main advantage of this method is that it allows users to authenticate themselves when they cannot remember or have lost their passwords and do not have their tokens

with them. Its main weakness is that it requires users to rely on other users, which means that a user who cannot complete the authentication process will have to get in touch with his or her chosen helper in order to obtain a temporary code. If the helper is unreachable, the user will not be able to log into the account. Additionally, this approach offers little privacy. It is not applicable for many users and works as a backup authentication method in urgent cases.

5.3 Summary of the Descriptive study

Based on the strengths and weaknesses of each authentication approach, the Table 5.1 below summarises the main differences between each approach in terms of the security level and user acceptance. The levels (high, medium and low) were created according to the results of literature reviewed in Chapter 2, the results of exploratory study and the discussion presented earlier in the previous sections.

Approach	***Example***	***Security level***	***User acceptance***
Knowledge-based authentication	PIN Password Image password	Low	High
Token-based authentication	Secure device Card reader USB reader PIN via mobile	High	Medium
Biometrics-based authentication	Fingerprint Signature dynamics Eye scan Hand geometry Facial recognition	High	Medium
Location-based authentication	Location signature	High	NA
Formula-based authentication	Formula result	Medium	NA
Process-based authentication	Mathematical calculation	Medium	NA
Relationship-based authentication	Vouchcode	Low	NA

Table 5.1 Differences between different approaches

5.4 Proposed Methods for the Experimental Study

The descriptive analysis reveals that each method has its own drawbacks, and poses problems related to implementation. Location-, process-, relationship- and formula-based authentication methods are still in the research phase and there is no indication in the available published literature that they have been deployed in the market. Additionally, no empirical studies are available that investigate security or usability of these methods.

Knowledge-based authentication is appropriate as a first factor, due to its simplicity and high acceptance rate. The second factor should be either token-based authentication or biometrics-based authentication, so as to overcome the problem of 'sniffing password' when the authentication is performed (Erlich and Zviran, 2008). The sniffing password refers to a way that is used by the hacker to attack the password by using techniques to monitor the network. These methods have been selected for examination due as well to their high security and user acceptance rates. An examination of MFA using token-based authentication will lend insight into the usability and security of this method in order to compare them to the usability and security of various tokens (e.g., card, secure device and PIN via mobile), that have been investigated in Chapter 4. An examination of an MFA using biometrics-based authentication will contribute to the available research on usable security, as none of the studies reviewed in Chapter 2, Section 2.10.2 assess the usability and security of biometrics-based authentication.

The researcher chose secure devices and card readers out of the various token-based authentication methods available on the market. These two methods are available in

the United Kingdom, where the study will take place, and have been adopted by several financial websites such as HSBC and Barclays banks, meaning the target sample may be familiar with these methods. The most common token used in Saudi Arabia, the PIN code via mobile, is not being used, due to problems revealed in the exploratory study and detailed in Chapter 4.

The fingerprint or finger scanner has been chosen from the available biometrics devices. According to Jones et al. (2007), the fingerprint scanner is considered the most accepted biometrics-based authentication method by users. To reach this conclusion, Jones et al. (2007) surveyed 115 users to compare their acceptance of various of biometrics, and more than half of the respondents reported familiarity with finger scanners. Users are more familiar with finger scanners because such scanners are used in airports, private buildings and to unlock mobile phones. In general, many scholars believe that biometric techniques including fingerprint will be used for authentication process in future because the cost of such devices continues to drop and the public become familiar with these technologies (Aljahdli, 2014).

5.5 Chapter summary

This chapter presented an overview of the available authentication approaches, along with their strengths and weaknesses. The chapter introduction detailed the study aim, which proposed a combination of authentication methods to be assessed in the experimental study. Following the study aim was a presentation of the objectives of the study, which included learning about commonly used methods that were identified in the exploratory study, reviewing other currently available authentication methods, identifying the strength and weaknesses of each method and proposing a suitable

combination of methods for a practical in-depth evaluation. Next, the various authentication methods were defined. The chapter then summarised the differences between the authentication approaches in terms of security and user-acceptance levels. Finally, a justification was given for choosing an authentication method that combines knowledge-, token- and biometrics-based methods for the experimental study.

Chapter **6**

Experimental Study

Usable security of multifactor authentication

Preface

This chapter presents the experimental study design through which the three authentication mechanisms suggested in Chapter 5 were assessed. The chapter begins by highlighting the importance of conducting the study by identifying the gaps in the present literature. This is followed by the study's aims and research questions. Then, the evaluation methodology is presented in detail, from the proposed approach though an assessment of the methodology. Finally, the results of the evaluation process are presented, followed by a chapter summary.

6.1 The Need for the Experimental Study

Usability and security are two key aspects that go hand in hand during the evaluation phase of secure systems. Security relies on principles that aim to protect users from attacks, while usability aims to provide those who use the system with easy-to-use tools. The contradicting goals of experts in both fields have led to conflicts of interest between security and usability (Furnell, 2005; Nodder, 2005). A new field, known as usable security, has emerged to address the problem (Balfanz et al., 2004). Whitten and Tygar ((1999) define *usable security* as a user's ability to figure out security tasks by avoiding harmful errors and being confident with the system interface. The Computing Research Association (2003) identified human computer interaction security (HCI-SEC) as one of the 'four Grand Challenges in Trustworthy Computing'.

Authentication is a rich area that needs to be explored to identify the usability and security conflicts of interest (Payne and Edwards, 2008), and an evaluation approach and metrics are needed assess the authentication process. The evaluation approach proposed in this chapter is based on the usability principle by involving users in each step of the authentication process, including the selection of the preferred method. The approach designed specifically for this study aims to assess the usability and security of the three different methods, as suggested in the descriptive study outlined in Chapter 5. These methods are a secure device, card reader and fingerprint verification, as discussed in Section 5.4. The proposed approach was designed under a model that can be used for further studies employing different authentication methods.

Rigorous measures are needed to perform the assessment using the proposed approach.

Only a few studies to date have explored the usable security of authentication; these were reviewed in Chapter 2. They rely on standard usability metrics and added security associated with trustworthiness as additional attributes; for example, Weir and colleagues (2009) compared three different token devices as multifactor authentication methods in an experiment with 50 e-banking customers to compare their security, usability and convenience and used the three attributes of usability (effectiveness, efficiency and satisfaction) and added security as another measure. De Cristofaro and colleagues (2014) conducted a quantitative study using a survey to examine the usability of a two-factor authentication based on the system usability scale and adding security as a metric. Two additional studies (Gunson et al., 2011; Weir et al., 2010) used experiments that have added security as a single attribute to be rated by the users.

The current study follows Herzog and Shahmerdi's (2007) definition of the usability requirement of secure systems, which should improve users' awareness regarding security tasks. Therefore, the study involves an evaluation of the system's usability using standard usability measures and security by identifying four measures, each of which reflects users' awareness of security warnings. This is because users' awareness is one of the factors that can be measured during the execution of a security task (Kainda et al., 2010). The security warnings were identified in Section 3.5.4 as follows:

1. Log in to an insecure page (Falk et al., 2008; Mannan and Oorschot, 2008).
2. Security information emailed in an insecure way (Falk et al., 2008).
3. Providing sensitive data insecurely.
4. Proceeding despite the appearance of a warning message (Seifert et al., 2006).

The third security warning above refers to providing a finger scan to be used during the present experiment.

Based on the above description, we can summarise the main differences between the current study and the previous studies that were reviewed in Section 2.10.2:

- The current study involves evaluating a biometric-based authentication process that has not been studied as a factor for authentication in the current literature in terms of usability and security.
- The current study involves evaluating the usability and security of a card reader as an example of a token-based authentication system that – to our knowledge – has not been assessed elsewhere. The two studies that used similar experiments (Weir et al., 2009; 2010) used either a secure device or PIN via mobile as their types of token-based authentication.
- The current study is designed to follow a specific approach that allows each user to gain experience with the three proposed security methods. This differs from Weir and colleagues' (2010) study where different groups of people used only one specific method each.
- The current study is designed using actual methods belong to the author, the simulation of a real user platform and the users have been informed that they are completing a real transaction with authentic bank account details. Previous studies used real methods without preparing a specific platform and real banking tasks, and the users were informed that they were participating only for research purposes.
- The current study involves a systematic security evaluation of users' awareness

of most security warnings, each of which represents one measure. While other studies (see Weir et al., 2009; Weir et al., 2010; Gunson et al., 2011; Paul et al. 2011; De Critofaro et al., 2014) used security as a single attribute to determine users' perception.

6.2 Study Aim

As mentioned in Section 6.1, this study aims to evaluate and investigate the levels of security and usability of three different types of multifactor authentication (fingerprints, card readers and secure devices). Specifically, it examines users' attitudes towards usability and their awareness of security warnings.

6.3 Study Questions

The experimental study was designed to answer the following questions:

- What is the most desirable authentication method employed by online banking users in terms of usability, security and trustworthiness?
- What are the differences between a fingerprint, a secure device and a card reader in terms of usability, security and trustworthiness, from users' perspectives?

6.4 Study Approach

Typical online banking services provide users with one multifactor authentication method approach. Therefore, the proposed approach **first** aimed to provide users with more than one authentication method, relying on the usability principle and involving

the users in all the process steps, giving them the opportunity to choose their preferred method. Figure 6.1 shows the proposed approach model, which includes clear steps for the authentication process. The process involves an interaction between the client, the authentication server and the authorisation server. There are four main steps in the authentication process: registration authority, choosing the preferred method, confirming the choice and validating the choice. Once the ownership credentials are verified, they are sent to the 'relying party trust', which is an application that confirms the user's claim of identity (Herzberg and Mass, 2001) in order to begin the authorisation step.

Second, the approach aimed to provide users with a realistic experience. In the domain of usability studies, the aim is typically to encourage users to behave as they do in the real world, so the most accurate results can be obtained. Moreover, when dealing with sensitive data, and banking websites in particular, more effort is required to encourage users to interact securely, as if they are dealing with their own information in the real world. To achieve the second goal, the researcher simulated a real online banking system and used the researchers' own information (card and token), hoping that these measures would encourage users to behave securely.

Third, the approach involved asking users to employ the three different methods in a specifically designed scenario to give them an authentic experience with all three methods. The first method was based on the user's choice, as mentioned in the first aim; the second method was used to confirm the payment task; the third method was used while confirming the receipt of the transaction receipt task.

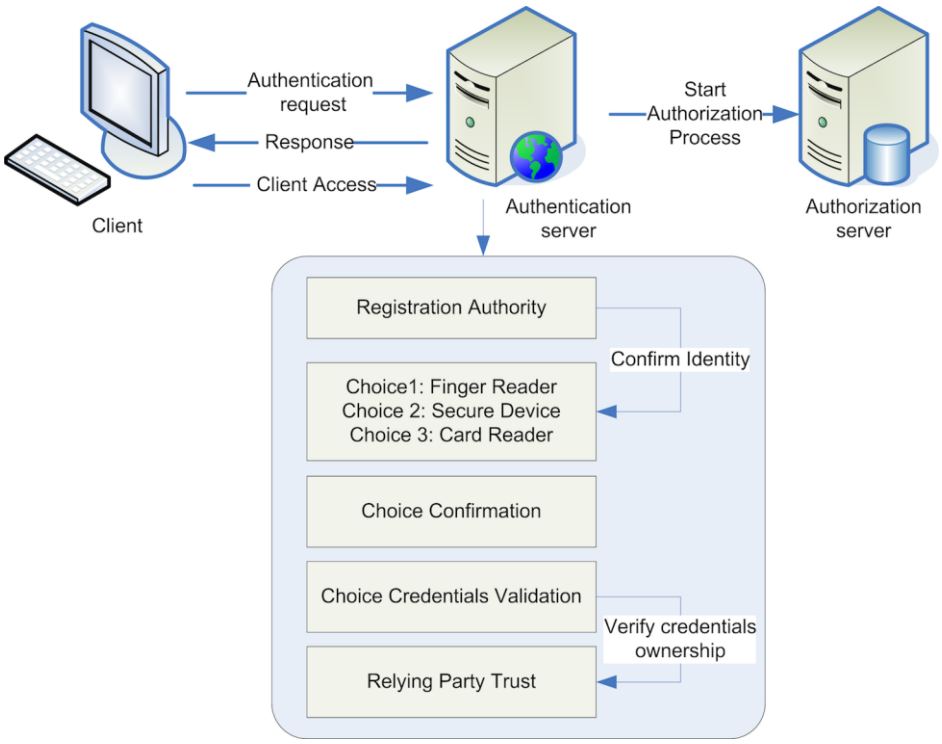


Figure 6.1 Proposed approach model

6.5 System Design and Study Materials

For the experimental study, a system was programmed to simulate an original online banking system used in the United Kingdom (HSBC) following the proposed authentication scenario model in Figure 6.1. HSBC was chosen because the experiment was conducted in the United Kingdom and the bank name is one that most study participants are likely to recognise. Moreover, the researcher has an account with HSBC; therefore, all requested pages could be simulated based on real interactions with the bank's online platform (Figure 6.2 shows the home page for the simulated system). During the programming stage for the website XAMPP (PHP development environment) was downloaded that provides the following components: Web Server, Apache Tomcat, Database Server and MySQL. Webpages on the website were created using server side language PHP and the design elements of webpages were created using CSS (see Appendix K). Regarding the interaction between the website and the

methods the website is designed to pretend that it is reading the finger when the user presses the scan button; then, it displays a saved image of a fingerprint. With the secure device and card reader the website is designed to accept any generated numbers to proceed to the next step.

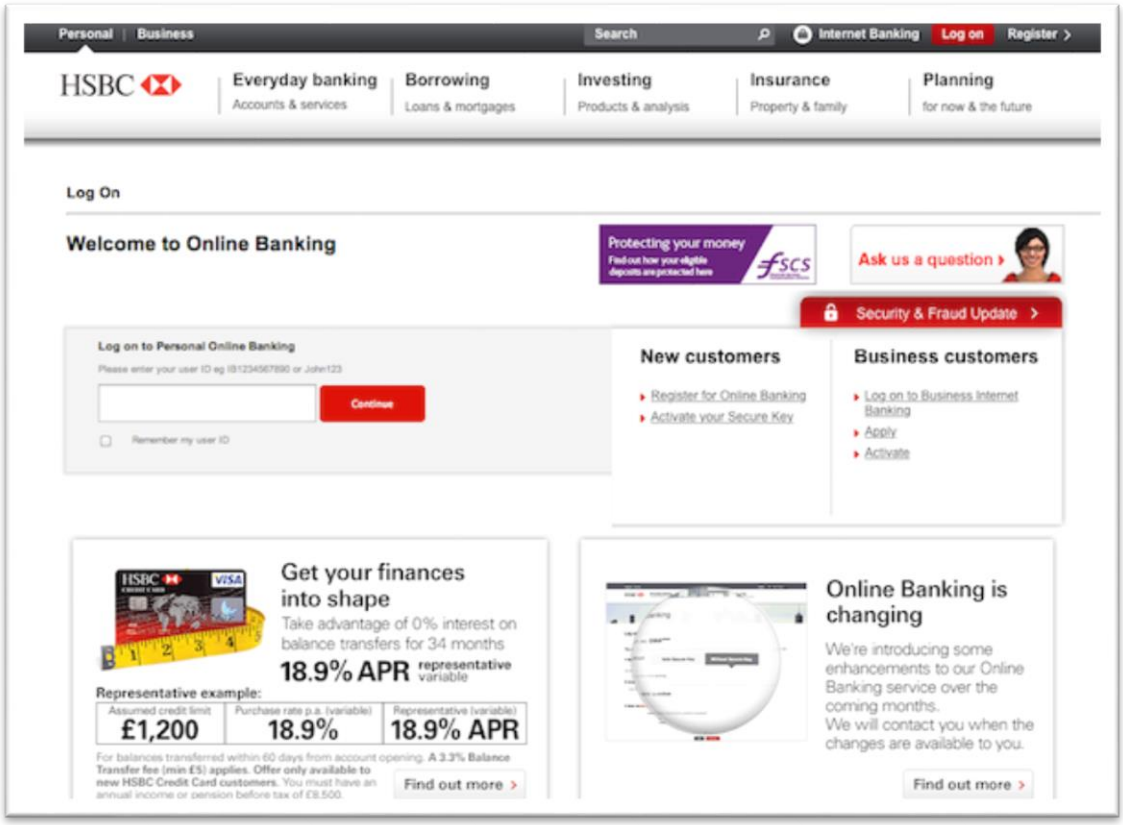


Figure 6.2 Home page for the simulated system

The simulated system provided users with three types of authentication methods (a secure device, a card reader and a fingerprint scanner). HSBC originally used one method, a secure device, and the secure device used in this study belongs to the researcher's account with HSBC. The card reader belongs to the researcher's account with Barclays Bank. For the third method, the fingerprint scanner, a SecuGen Hamster

Plus[3] was chosen, due to its high performance and features, such as flashing in red during the scanning process. The finger scan has its own application that is used in the background; it begins to read the fingerprint when a user puts his or her finger in the designated space. The website is designed to pretend that it is reading the finger when the user presses the scan button; then, it displays a saved image of a fingerprint. Figure 6.3 shows all of the devices employed in the experiment.

Figure 6.3 The devices used in the experiment

The other items used for this experiment include an information sheet and consent form (see Appendices E and F), which users were asked to read and sign prior to the experiment, to acknowledge their agreement to participate and to inform them about their ability to withdraw from the study at any time. The other item is a scenarios sheet (see Appendix H), which outlines the steps that the users need to follow to perform the task. It includes all the requested information, such a user ID for registering on the website, transaction information and an email address, which is needed to complete the task. The third item is the observation sheet (see Appendix I) used to record users'

[3] Full details can be found at http://www.secugen.com/products/php.htm

interactions with each method and other information, such as the date of the experiment, the user's preferred method, responses to the warning messages (which appear during the experiment to warn the user about the missing certificate) and other comments. The last two main items are laptops — one used in the experiment to perform the task and the other to complete the electronic survey.

The researcher was present during the experiment, but did not engage with users during the process; this was done in order to remove bias from the results (i.e., guided browsing through the website). As previously mentioned, the experiment was designed to record various activities performed by users while browsing in a backend database. This location completely removed any interaction with the website user during the experiment. The only engagement the researcher had with the users was to inform them about the requirement of completing the survey after the experiment.

6.6 Study Scenarios

Regarding the study's requirements, three different scenarios were prepared based on the users' first choice of authentication method. For example, if the user's first choice was a fingerprint scanner, then he or she was forced to use a secure device to confirm the transaction process and a card reader to receive the receipt via an email address. Generally, we had three different scenarios, and each employed three different methods (see Table 6.1), in order to give each user some real experience with each method. This approach contributes to achieving results that are based on a clear comparison between all of the used methods. Each scenario is based on the user's first choice of authentication method; for example, if the user chose a fingerprint as his first

preferred method, then he was given Scenario 1 to follow. However, in all cases, users were asked to enter the ID number contained on the yellow card given to them at the beginning of the experiment and to answer a series of secure questions to begin the process.

order	Scenario 1	Scenario 2	Scenario 3
1	Fingerprint	Secure device	Card reader
2	Secure device	Fingerprint	Fingerprint
3	Card reader	Card reader	Secure device

Table 6.1 devices order in three different scenarios

In detail, each user who participated in this study had a real experience with each of the three methods, combined with knowledge-based authentication tools (an ID and secure question). In this experiment, each participant completed the survey and evaluated each method based on recent and real experiences with all three methods. Each scenario consisted of all the details a user needed to perform the assigned task. The task for this experiment was to log in using an ID, to answer a secure question and choose the preferred method. Then, each user completed the task of transferring a certain amount of money to a specific person, after being given all the details for the transfer. The user needed to confirm the payment and enter a given email address to receive a receipt. All users performed the same task, and the differences among them were the sequence of using the three methods, as illustrated in Table 6.1 above and as shown in the diagram in Section 6.8.

6.7 Participants' Recruitment

Participants were recruited through an advertisement for the experiment posted in the University of East Anglia main library; the poster included an invitation to participate in the study, introduced the research aim and objectives and outlined the benefits of participating in the study (see Appendix D). In terms of the sample size, the researcher hoped to attract at least 20 participants. According to Lewis (2006), the minimum number of participants involved in usability studies may vary from researcher to researcher; some suggest that eight participants are sufficient, while others suggest including 12 participants (Turner et al., 2006; Lewis, 2006). Nielsen (2006) suggested that 20 participants are required for comparative studies. Accordingly, the researcher aimed to achieve the required number of 20 participants so that the sample can be considered representative of the targeted users. In the case that more participants were willing to participate in the experiment, the researcher would welcome them.

6.8 Study procedure

The experiment was conducted at the main library of University of East Anglia. All equipment and materials were prepared at the beginning of each day. Each participant was recruited individually and was asked at the beginning of the process to read and sign a consent form. All participants were informed that they would be asked to make a payment using the researcher's account and told that this transaction would be recorded. Then, the participant started the experiment by giving an ID to register on the bank's website, followed by the choosing of his or her preferred authentication method. While the participant verified his or her credentials, the evaluator prepared a

proper scenario based on the participant's choice. Each user utilised three different authentication methods: the first method was used to log into the system, the second

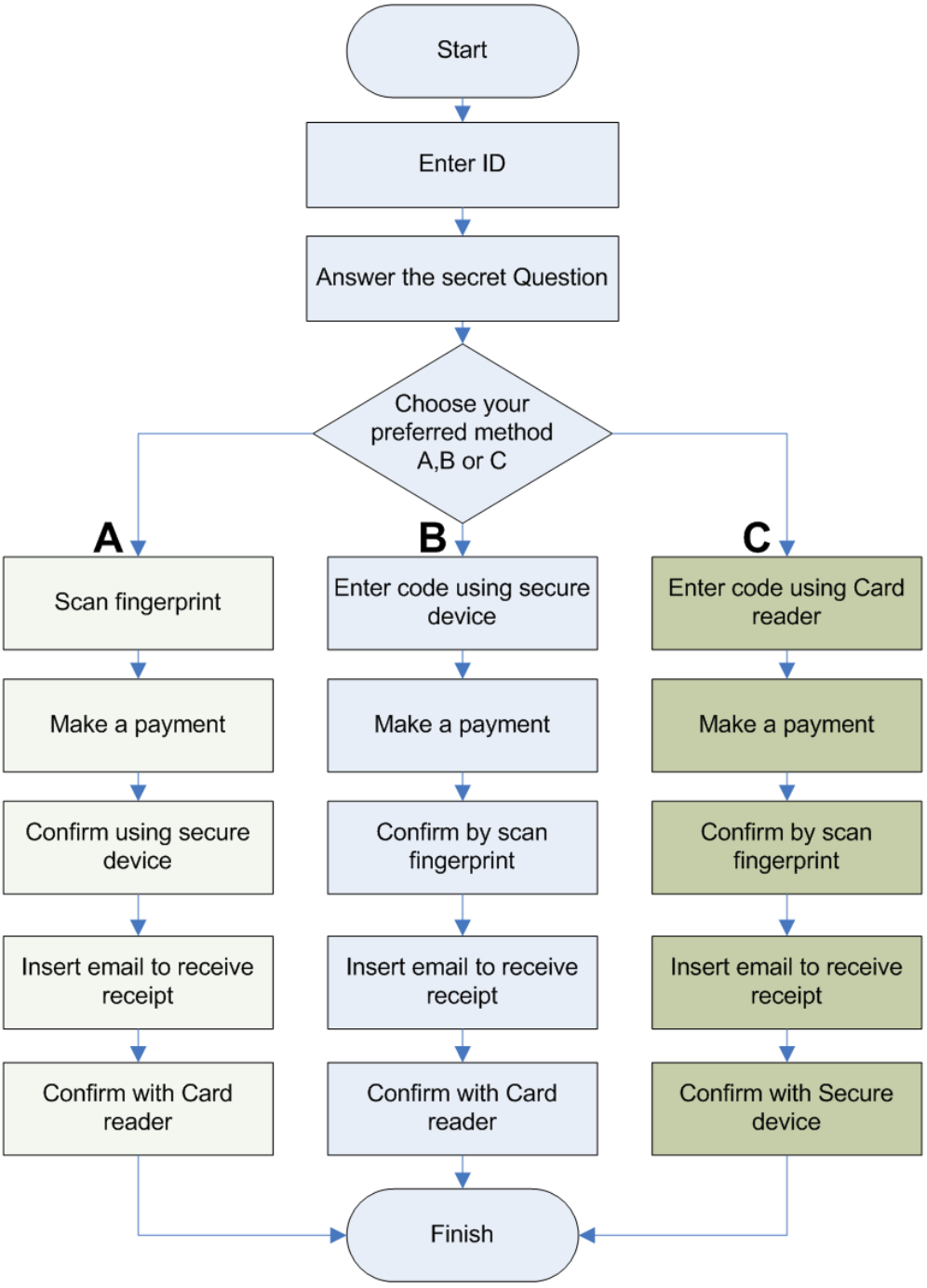


Figure 6.4 flowchart of the scenarios' steps

6.9 Assessment Methodology

The study aimed to perform a comprehensive evaluation of three different authentication methods by assessing the usability and the security of each method, as discussed in Section 3.5.4 and Section 6.1. The usability evaluation in each method was based on the International Organisation for Standards' (ISO) (1998) definition of usability: efficiency, effectiveness and satisfaction. Security was measured according to Herzog and Shahmerdi's (2007) definition of the usability requirements for secure systems, which should improve users' awareness regarding security tasks. Thus, the proposed approach sought to evaluate these methods by integrating existing evaluation criteria for usability with security criteria based on users' awareness of security indicators. These criteria are described below.

6.9.1 Usability assessment

Usability was measured in the current experiment by examining efficiency, effectiveness and satisfaction. As mentioned previously, in Chapter 3, usability measures are hard to select because there are so many available: more than 50 (Hornbek and Effie, 2007). However, the ISO usability measures of effectiveness, efficiency and satisfaction selected for this experiment are widely used.

Efficiency was measured by calculating the time required to use each method. Effectiveness was measured by task completion and the numbers of requests for help, either by clicking the help link or asking the observer. Satisfaction was measured through the data collected from the questionnaire, and the factors employed were

based on Nielsen's definition of usability. The usability attributes from Nielsen's definitions are learnability, efficiency, memorability, errors and satisfaction. The last two attributes assessed in the survey were security and trustworthiness. These attributes were added because they determine users' perceptions of the system's security and trustworthiness, and as mentioned in Section 3.3.1.4. They have been employed in previous studies that have evaluated authentication methods (De Critofaro et al. 2014; Weir et al., 2009; Weir et al., 2010).

6.9.2 Security assessment

As mentioned in Section 6.1, this study follows Herzog and Shahmerdi's (2007) definition of the usability requirements for secure systems, which should improve users' awareness regarding security tasks. Users' awareness can be seen clearly during their interactions with and responses to security warnings. Kainda and colleagues (2010) note that users' awareness is considered one of the factors that can be measured during the execution of a security task. An example of a security task is using authentication methods to log in to e-banking systems and to complete a specific transaction.

Falk and colleagues (2008) identified several security warning indicators during an analysis of 214 banking websites in the United States using an automated tool to search for visible security design flaws. Other studies, such as one by Seifert and colleagues (2006), have considered a warning message to be one security issue that e-banking users face.

The present study identifies a list of security warnings that might appear during the authentication process, referring to the discussed studies as follows:

1. Log in to an insecure page (Falk et al., 2008; Mannan and Oorschot, 2008),
2. Security information emailed in an insecure way (Falk et al., 2008),
3. Providing sensitive data insecurely,
4. Proceeding despite the appearance of a warning message (Seifert et al., 2006).

The third security warning above refers to providing a finger scan that will be used during the current experiment. It has not been – to our knowledge – discussed in any previously published research.

To relate each security warning indicator to users' awareness, a proposed taxonomy for security attributes is used to categorise the above security warning indicators, as shown in Table 6.2:

Security attribute	***Security warning***
Attention	Login in insecure page
Caution	Security information emailed insecurely.
Motivation	Providing sensitive data insecurely.
Wariness	Proceeding with the warning message

Table 6.2 security measurements

Each security attribute was measured. The *attention* attribute was measured by observing users' awareness and whether or not they noticed the missing secure socket layer (SSL) indicator in the address bar. Most financial websites use a secure encrypted connection implemented via SSL; this is usually very clear to the user, due

to the presence of the 'https' and the lock icon in the address bar. These indicate a secure connection and prevent hackers from attacking.

Caution was measured by observing users' interactions with requested sensitive information, such as entering an email address on an insecure page. The presence of an insecure page forced users to be more careful in sending and receiving information (such as email addresses).

Motivation was measured by observing users during their interaction with the authentication methods and measuring their progress in providing a fingerprint and continuing the authentication process. Biometric information is considered highly sensitive and must be sent via a secure, encrypted connection. A user often ensures that his or her own sensitive data is sent via a secure connection.

Wariness was measured by observing users' interactions, behaviours and understanding of the warning messages that appeared during the authentication process. The best way to examine a given user's awareness of security features and to study her ability to read and decide upon a response is to provide her with a warning message. One warning message that frequently appears on financial websites is 'invalid security certificate'. In this study, we provided the subjects with fake warning messages to examine their awareness and understanding of the same. The warning messages used in this study dealt with the absence of a security certificate.

6.10 Data Collection

Different methods were used to collect both qualitative and quantitative data. Data were collected in three different ways (see Figure 6.5): through the database, as the website created a table schema in the website database to record responses from users to various options selected or clicked while browsing the webpage. The strategy used for capturing responses was set to FALSE (0) for all expected responses by default and was updated to TRUE (1) when the user selected certain options.

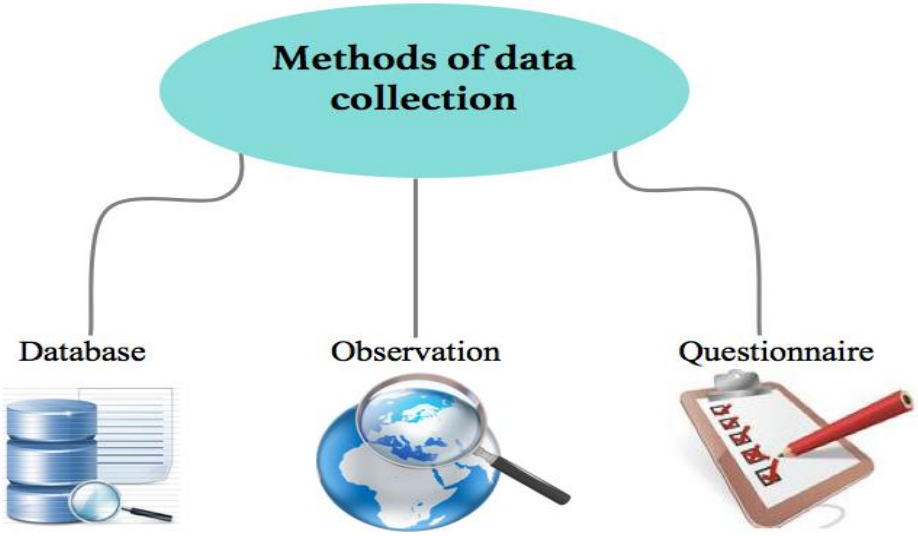


Figure 6.5 Data collection methods for the main experiment

An observation sheet was also used as the researcher observed each participant during the evaluation session to record any difficulties with any of the methods and all comments from participants. The last instrument was the questionnaire, an online survey created using the Qualtrics website (see Appendix G). It was structured to include both closed- and open-ended questions and comprised four sections; the first section had ten general information questions to explore participants' demographic characteristics, including age, gender, education and level of IT and security

experience. The second section had ten statements rated on a five-point Likert scale (1=strongly agree to 5=strongly disagree). Each rating was repeated for the three used methods. The third section had four questions to rank the three methods in terms of preference, ease of use, security and trustworthiness. The last section consisted of open-ended questions that asked participants to add comments regarding the used methods. Figure 6.6 shows the sequence of survey sections.

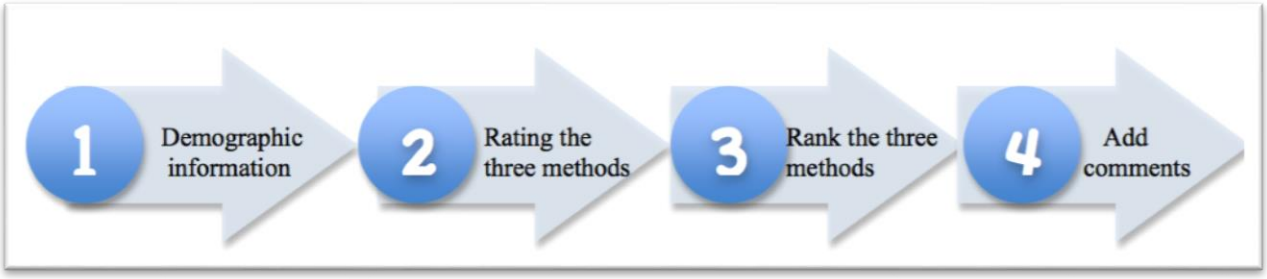


Figure 6.6 Surveys' sections

6.11 Pilot study

Prior to beginning the experiment, the scenario documents, the observation sheet and the online survey were all tested and piloted to address and identify any confusion in terms of the experimental procedure or any drawback in the other instruments that could have resulted in the failure of the main experiment. The experiment was conducted with four students (two Master's level students from the School of Pharmacy, one Master's level student from the School of Computing and one PhD student from the Biological School). Their feedback was used to enhance and refine the experiment to reach the final version of each step.

The results of the pilot study led to the editing of some sentences in the online survey;

a suggestion to open the survey in another laptop, which may decrease the time needed to navigate from the experimental webpage to another; and adding a new row in the observation sheet to record the user's first-choice method, to help organise the collected data. Prior to beginning the main experiment, ethical approval was granted by the School of Computing Science with an assurance that all data was anonymous during the collection and storage stages. In addition, prior the experiment, each user was asked to voluntarily agree to take part in the study, and they were informed that they could withdraw at any time. Users were also informed that none of their personal authentication tools were required, and that they would be using the researcher's own tools and bank account to complete a real transaction.

6.12 Results and Discussion

In this section, the data collected from this experiment are analysed, starting with the respondents' profile and followed by the usability assessment, including all factors and the survey analysis. The security assessment results are then presented, followed by the final discussion and chapter summary.

6.12.1 Respondents' profile

One-hundred users (50 males and 50 females) participated in the experiment. The participants had different nationalities, but the majority (78%) were British. Participants also reflected a broad range of ages, levels of education and different college majors. All subjects had used the Internet for more than three years; based on this, we assumed our respondents had a high IT literacy level. Regarding the usage of

online banking, 3% of our participants had a banking account but had not previously used online banking, while (97%) had used online banking before. More specifically, 12 had used online banking for less than one year, 54 between one and three years and 31 for more than three years. In general, it is a positive finding that almost all of our subjects had previous experience with online banking, which makes the sample an objective and impartial source of data. We also ascertained that 16% of our subjects had an account with our simulated bank (HSBC Bank). In investigating whether subjects had experience in the domain of online security, the results indicate that 12% of them had such experience, while 88% reported no experience. This allowed us to compare the results between those who had experience and those who did not and to observe their interactions more carefully (see Figure 6.7 and Table 6.3).

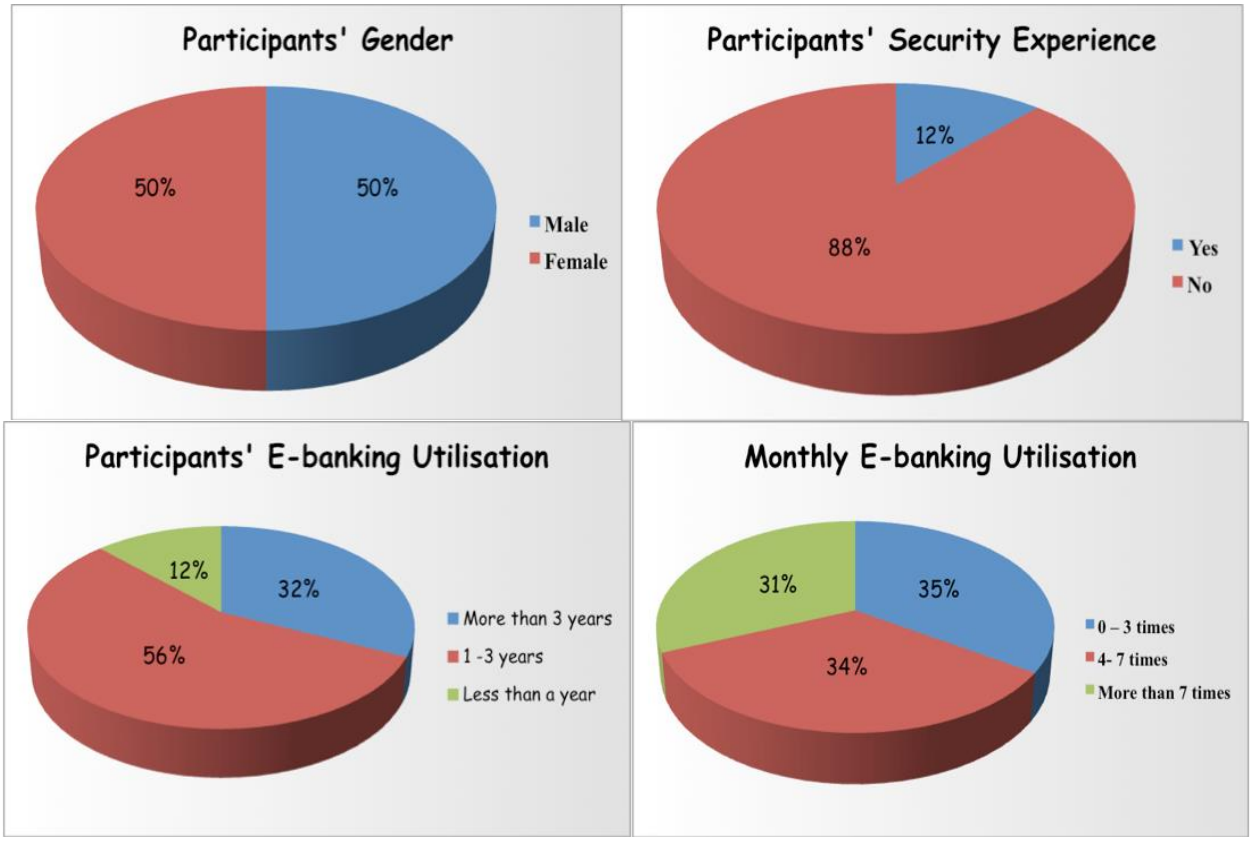


Figure 6.7 Respondents' profiles

Age	
18 – 25	65 %
26 – 30	10 %
31 – 35	20 %
Above 35	5 %
Education	
School	4 %
College	33 %
Undergraduate	48 %
Masters' Degree	10 %
PhD	5 %
Internet Usage	
More than three years	100 %
HSBC Bank account ownership	
Yes	16 %
No	84 %
Barclays Bank account ownership	
Yes	22 %
No	78 %

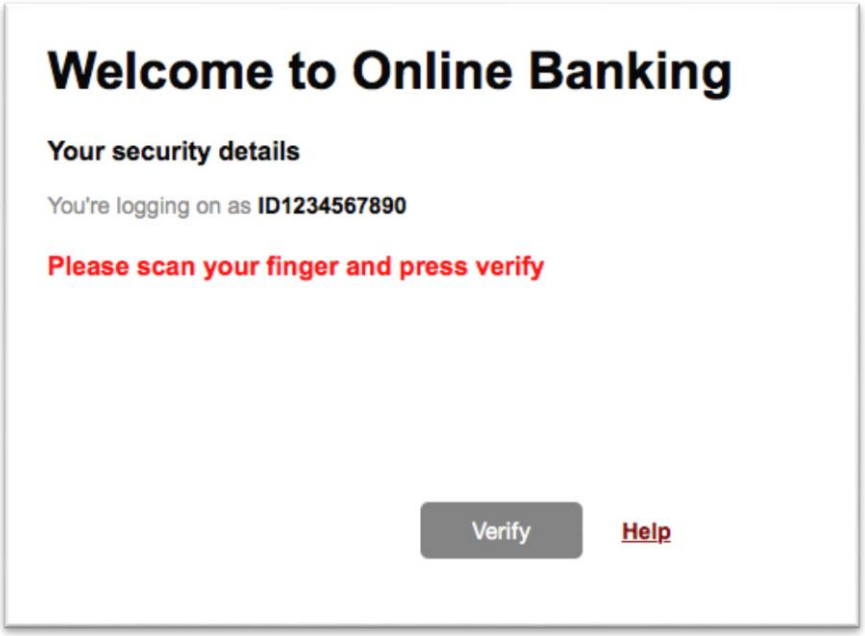
Table 6.3 Participants characteristics for main experiment

6.12.2 Usability Results

6.12.2.1 Efficiency

To measure efficiency, the time required to log in was recorded in the database of the simulated website. The average time for each method was then calculated, and the mean differences between them show that there were significant differences in scores between the three methods (fingerprint scanning, secure device and card reader); the

fingerprint method had a mean value = 5.7 seconds (Standard Deviation (SD) = 2.3), while the secure device was 29.7 (SD= 14.5) and the card reader was 22.34 (SD= 13.06). The results can be related to the number of steps in each method, as the fingerprint scan required the user to press one button to start the scan and then the device started scanning (see Figure 6.8). Alternatively, the secure device required more steps, including pressing and holding the green button, entering the secret digits and finally pressing the green button to get the generated numbers (see Figure 6.9). With the card reader, the user started the process by inserting the card, pressing the identity button, inserting the secret number and pressing enter to get the generated number (see Figure 6.10). Based on the researcher's observations during the experiment, the users were confused when using the secure device, as there was no sign to help them move from one step to another; for example, after entering their password, the HSBC logo appeared and there was no sign to ask users to press the green button again to get the generated number. Therefore, most of them either tried again or asked for help.



patFigure 6.8 Scanning finger process

Figure 6.9 Generating code with HSBC device (HSBC, 2016)

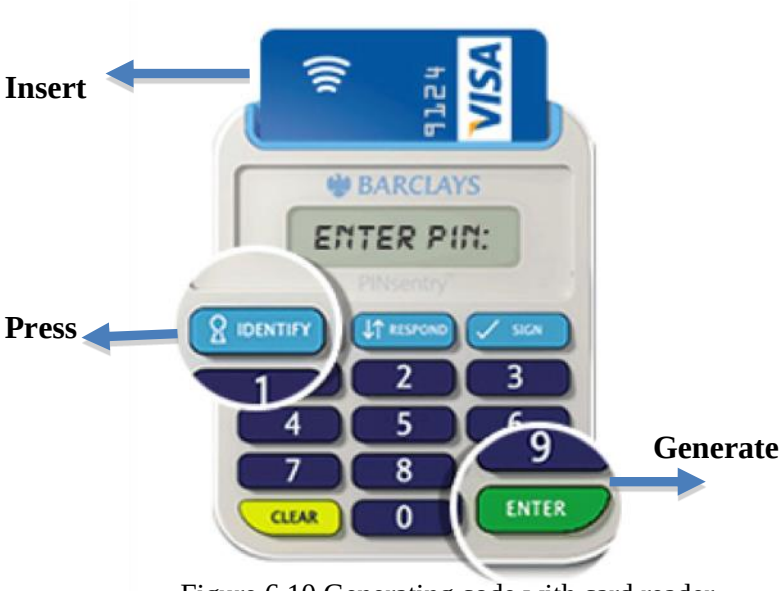


Figure 6.10 Generating code with card reader

6.12.2.2 Effectiveness

All participants completed the required task and finalised the requested steps in the scenario, but several problems were observed while using the methods. With the secure device, the user struggled after inserting the pass code. They expected to get a

generated number, but they got the HSBC logo instead and were required to press the green button again to get the generated number. Others struggled because they had to press and hold the green button for several seconds to start, and they failed to hold the button; therefore, they repeated the process to get started.

There were also a few errors with the card reader, including failing to insert the card properly to start and being confused as to where to find the start button, labelled 'identity'. As a result, they did not realise that this was the start button and kept trying rather than pressing help or reading the instructions for using the card reader. Regarding the number of help requests, the participants could click on the help link or ask the experimenter to help when they reached the stage where they could not continue the process, as shown in Table 6.4. Most help was provided to participants using the secure device, followed by the card reader, while none of the participants requested help with using finger print.

Device	***Number of help***
Secure device	28
Card reader	11
Finger scanner	0

Table 6.4 Number of help requests for each device

6.12.2.3 Satisfaction

Satisfaction was measured by analysing the survey that required the participants to rate the usability attributes, security and trustworthiness of each method. Prior to analysing the data, reliability was tested first to examine the integrity of the survey measures (Sekaran, 2003). Using the Statistical Package for Social Science (SPSS), Cronbach's alpha was used to test the consistency of the sample responses to all the survey items. Good reliability should produce at least a coefficient value of 0.7 (Pallant, 2001), and the current study survey was reliable with a Cronbach's alpha coefficient value of 0.804 for items related to fingerprint scanning, 0.83 when the items related to the secure device and 0.814 when the items related to the card reader. Table 6.5 presents the full list of the survey's statements, while Table 6.6 show the item-total statistics for the reliability test. The following sections present the analysis results for the different methods.

label	***Statement***
Item1	The log-in process with this method is complicated.
Item2	I would like to use this method again
Item3	I can use this method easily.
Item4	This method is efficient for log-in process.
Item5	I found that this method is cumbersome to use.
Item6	I feel confident when using this method.
Item7	I need to learn how to use this method.
Item8	This method is satisfying.
Item9	This method is trustworthy.
Item10	This method is secure.

Table 6.5 List of rating statements of the survey

Statement	***Corrected Item-Total Correlation***	***Cronbach's Alpha if Item Deleted***	***Corrected Item-Total Correlation***	***Cronbach's Alpha if Item Deleted***	***Corrected Item-Total Correlation***	***Cronbach's Alpha if Item Deleted***
	Finger scan		**Secure device**		**Card reader**	
Item1	.506	.827	.623	.805	.584	.787
Item2	.610	.817	.616	.805	.682	.776
Item3	.657	.816	.682	.797	.667	.780
Item4	.685	.810	.564	.811	.415	.805
Item5	.409	.837	.439	.823	.374	.812
Item6	.607	.817	.701	.796	.669	.779
Item7	.337	.843	.436	.826	.402	.809
Item8	.623	.817	.518	.815	.388	.808
Item9	.468	.831	.318	.833	.374	.809
Item10	.481	.830	.306	.835	.435	.804

Table 6.6 item-total statistics

6.12.3 Survey results

6.12.3.1 Fingerprint scanning

An empirical statistical analysis was performed using the nonparametric chi-square (x^2) one variable one classification way test (the data is not normally distributed) to determine whether there are significant differences in frequencies. According to the first statement, 'The log-in process with this method is complicated'. There were differences between frequencies of participants' responses towards the statement (x^2 = 79.1, degrees of freedom = 4, p-value < 0.01). The descriptive statistics in Table 6.7 show that 83% responded negatively (either disagree or strongly disagree) to the statement, viewing the fingerprint scanning method as simple in terms of its usability. For the statement 'I would like to use this method again', there were significant differences between frequencies towards the statement (x^2 = 62.00, degrees of freedom = 4, p-value < 0.01). Looking at the most frequent answer, it can be seen that most of the participants would like to use the method, as 78% agreed with the statement. It can be assumed that those not willing to use the method again have a security concern, as one participant indicated that he worried about his fingerprint being recorded and used for inapplicable purposes. For the statement 'I can use this method easily', which measures this method's ease of use for the authentication process, there were significant differences between frequencies of participants' responses (x^2 = 60.72, degrees of freedom = 3, p-value < 0.01). Most of the participants (87%) rated the statement positively. Regarding its efficiency, the results revealed significant differences between frequencies (x^2 = 88.7, degrees of freedom = 4, p-value < 0.01).

Most of the participants (86%) rated the statement positively (either agree or strongly agree).

The fifth statement in the survey, 'I found that this method is cumbersome to use', revealed significant differences between frequencies (x^2 = 62.8, degrees of freedom = 4, p-value < 0.01). Specifically, 70% of participants responded negatively to the statement, as they did not see the fingerprint scanning method as cumbersome to use, which indicates the method's usability for the authentication process. Regarding participants' confidence to use the method, there were significant differences (x^2 = 49.2, degrees of freedom = 4, p-value < 0.01). Most (72%) agreed with the statement, giving an indication of the method's good usability. To investigate the learnability, participants were asked whether they need to learn how to use the fingerprint scan; there were significant differences between frequencies (x^2 = 57.9, degrees of freedom = 4, p-value < 0.01). Specifically, 68% indicated that they do not need to learn how to use the method. In contrast, 13% agreed that they need to learn how to use it, which may suggest that this group has not seen a scanning device before; however, none of the participants during the experiment asked how to use the fingerprint scanner.

The last three statements were framed positively and asked the participants to rate their satisfaction with the method, its security and its trustworthiness. The results indicate that there were significant differences between frequencies of participants' responses towards these statements. For satisfaction (x^2 = 75.7, degrees of freedom = 4, p-value < 0.01), 82% agreed with the statement. Regarding security, there were significant differences (x^2 = 65.2, degrees of freedom = 4, p-value < 0.01). For trustworthiness, most participants rated the statement positively (78%) (either agree or strongly agree).

Thus, the results from all the statements draw attention to the fact that using a fingerprint scanning method for the authentication process is considered usable and secure and trustworthy from users' perspectives and attitude. (Figure 6.11 shows the participants ratings for all the statements.

N	*Statement*	*Strongly Disagree*	*Disagree*	*NAND*	*Agree*	*Strongly Agree*	*Chi square*	*DF*	*Sig.*
1	The log-in process with this method is complicated.	44	39	10	3	4	79.1	4	.000
2	I would like to use this method again	6	9	7	43	35	62	4	.000
3	I can use this method easily.	0	5	8	35	52	60.72	3	.000
4	This method is efficient for log-in process.	3	7	4	42	44	88.7	4	.000
5	I found that this method is cumbersome to use.	20	50	12	14	4	62.8	4	.000
6	I feel confident when using this method.	2	13	13	41	31	49.2	4	.000
7	I need to learn how to use this method.	20	48	18	11	3	57.9	4	.000
8	This method is satisfying.	2	5	11	42	40	75.7	4	.000
9	This method is trustworthy.	3	9	10	45	33	65.2	4	.000
10	This method is secure.	2	8	13	37	40	60.3	4	.000

* NAND: refer to neither agree and disagree in this table

Table 6.7 Descriptive statistics for rating fingerprint

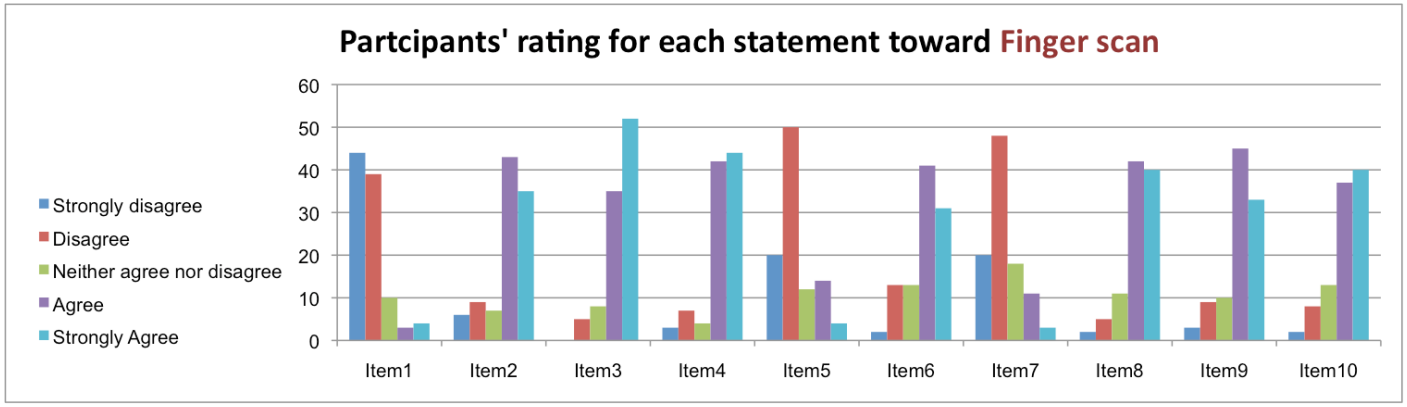


Figure 6.11 Participants' rating for fingerprint

6.12.3.2 Finger scan's overall usability

The data collected and presented above are quantitative in nature in that they are presented in an easily digestible and logical way, which is quintessential of quantitative analysis (Bryman, 2004). The researcher conducted further investigation and statistical analysis to clarify the above results. Therefore, the overall usability, security and trustworthiness of using a fingerprint scanner for the authentication process was assessed statistically using the Friedman test to determine the differences between the three factors (usability, security and trustworthiness) for the method. Table 6.7 illustrates that there are differences between these factors for this method ($x^2 = 7.11$, p-value < 0.05), the highest rating awarded to security. Figure 6.10 indicates the results based on the mean differences more clearly.

Factor	N	Mean	Std. Deviation	Minimum	Maximum	Mean Rank	Chi-Square(D	Asymp. Sig.
Usability	100	3.996	.68752	1.63	5.00	1.83		
Trustworth	100	3.96	1.034	1	5	2.02	7.11(2)	0.029
Security	100	4.05	1.019	1	5	2.16		

Table 6.8 Friedman test results for evaluation fingerprint

An in-depth analysis was performed to compare the three factors, taking into account some demographic information, such as age, gender, education level, security experience and monthly visits to an e-banking account. The nonparametric chi-square test was used, and the results revealed no significant differences in scores between participants (p-value > 0.05).

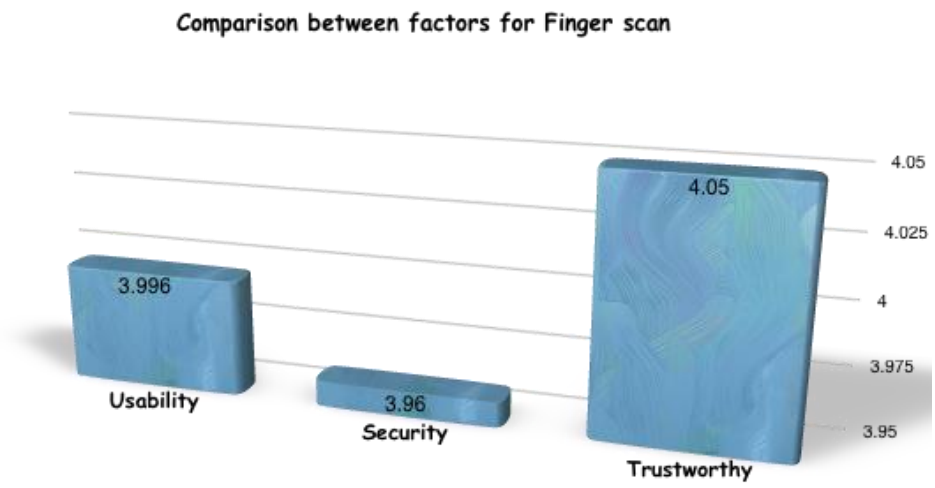


Figure 6.12 Comparison between factors for fingerprint

6.12.3.3 Secure device

To assess the usability of the secure device when used for the authentication process in e-banking, the nonparametric chi-square (x^2) one variable test was used to provide evidence of any significant differences in scores between participants' responses. The first analysis included analysing each statement individually (see Table 6.9 and Figure 6.13). For the first statement, 'The log-in process with this method is complicated', there were significant differences between frequencies of participants' responses (x^2 = 61.3, degrees of freedom = 4, p-value < 0.01), and 35% of participants found using the secure device complicated. This may be due to the number of steps to follow or the problems that several participants had when trying to get the generated number during the experiment. In contrast, 46% found the secure device easy to use. Regarding the users' willingness to use the method again, there were also differences between frequencies (x^2 = 48.6, degrees of freedom = 4, p-value < 0.01). Half of the participants indicate their willingness to use the method again, while 27% admitted that they did not wish to use the method again and thus may find it difficult. Similar results were

provided regarding the ease of using the secure device and its efficiency; most agreed with both statements (58%, 59%). On the other hand, few of them rated the statements negatively (22%, 19%) regarding the ease of use and the efficiency of the secure device; some of this group had difficulty to log in using this method.

Regarding the fifth statement, 'I found that this method is cumbersome to use', the chi-square test determined significant differences between frequencies of participants' responses (x^2 = 54.3, degrees of freedom = 4, p-value < 0.01). According to the descriptive statistics, 48% agreed with the statement, which is a high percentage and indicates their difficulty with using the secure device. The sixth statement in the survey asked them to rate their confidence while using the secure device, and the results indicated significant differences between frequencies (x^2 = 41.8, degrees of freedom = 4, p-value < 0.01). Most participants (56%) rated the statement positively (either agree or strongly agree), suggesting that, in general, they are familiar with using devices or technology and their difficulty might be according to the design and steps followed to operate the device.

As stated in section 6.9.1, the learnability as a main attribute of usability was measured through the survey, and the participants were asked to rate whether they need to learn how to use the secure device for the authentication process. Using chi-square test, the results revealed significant differences between frequencies (x^2 = 22.7, degrees of freedom = 4, p-value < 0.01). According to the responses, 39% indicated a need to learn how to use the method; in contrast, 43% indicated they do not need to learn how to use the method, as they rated the statement negatively. The results from the last three statements are similar regarding the secure devices' satisfaction, security and

trustworthiness. Performing the chi-square one variable test, the results indicate significant differences between frequencies of participants' responses towards the secure device in terms of satisfaction, security and trustworthiness (x^2 = 60.7, 64.2, 46.1, respectively, degrees of freedom = 4, p-value < 0.01). Most participants rated the last three statements positively (52%, 68%, 65%). See Table 6.8 for detailed results. In contrast and more specifically according to the participants' satisfaction with the secure device, 21% indicated that they were unsatisfied with using the secure device, which, as mentioned previously, might be due to the difficulty they faced during the experiment to get the generated number.

N	*Statement*	*Strongly Disagree*	*Disagree*	*NAND*	*Agree*	*Strongly Agree*	*Chi square*	*DF*	*Sig.*
1	The log-in process with this method is complicated.	2	44	19	30	5	61.3	4	.000
2	I would like to use this method again	4	23	23	43	7	48.6	4	.000
3	I can use this method easily.	5	17	20	44	14	42.3	4	.000
4	This method is efficient for log-in process.	2	17	22	48	11	60.1	4	.000
5	I found that this method is cumbersome to use.	2	29	21	42	6	54.3	4	.000
6	I feel confident when using this method.	1	23	20	41	15	41.8	4	.000
7	I need to learn how to use this method.	12	31	18	31	8	22.7	4	.000
8	This method is satisfying.	3	18	27	46	6	60.7	4	.000
9	This method is trustworthy.	1	11	20	49	19	64.2	4	.000
10	This method is secure.	1	12	22	42	23	46.1	4	.000

* NAND: refer to neither agree and disagree in this table

Table 6.9 Descriptive statistics for rating secure device

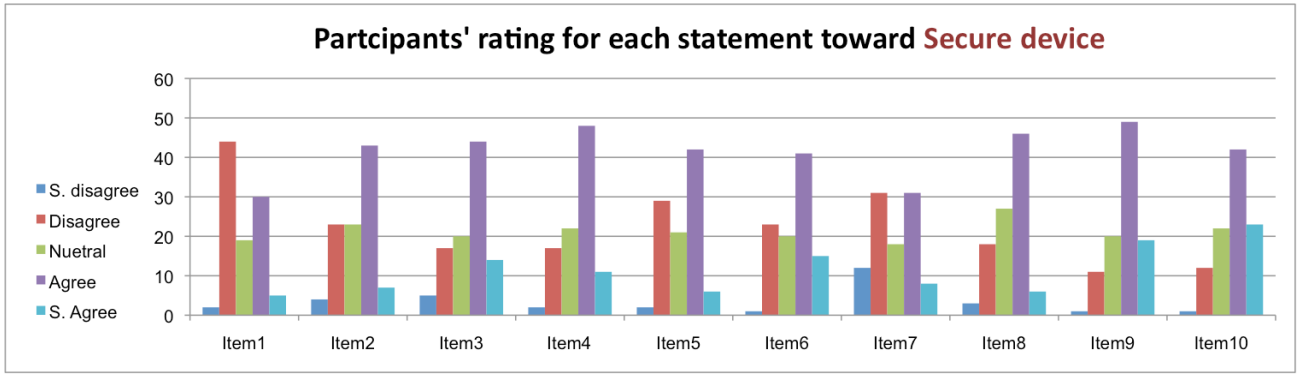


Figure 6.13 Participants' evaluation for secure device

6.12.3.4 Secure device's overall usability

A further investigation was performed to investigate the overall usability of the secure device and compare it with security and trustworthiness. Therefore, the Friedman test was used to determine the differences between the three factors (usability, security and trustworthiness). The results indicate (as can be seen in Table 6.10) that there are differences in scores between usability, security and trustworthiness while using the secure device (x^2 = 28.09, p-value < 0.01) awarded to the security and trustworthiness. Figure 6.12 indicates the results based on mean differences more clearly.

Factor	N	Mean	Std. Deviation	Minimum	Maximum	Mean Rank	Chi-Square(DF)	Asymp. Sig.
Usability	100	3.2438	.72243	1.50	4.63	1.62		
Trustworthy	100	3.74	.928	1	5	2.22	28.09(2)	0.000
Security	100	3.74	.981	1	5	2.17		

Table 6.10 Friedman test results for evaluation secure device

An in-depth analysis was performed to compare the three factors, taking into account some demographic information, such as age, gender, education level, security experience and monthly visits to an e-banking account. For this analysis, the nonparametric chi-square test was used, and the results revealed that there are no significant differences in scores between participants (p-value > 0.05).

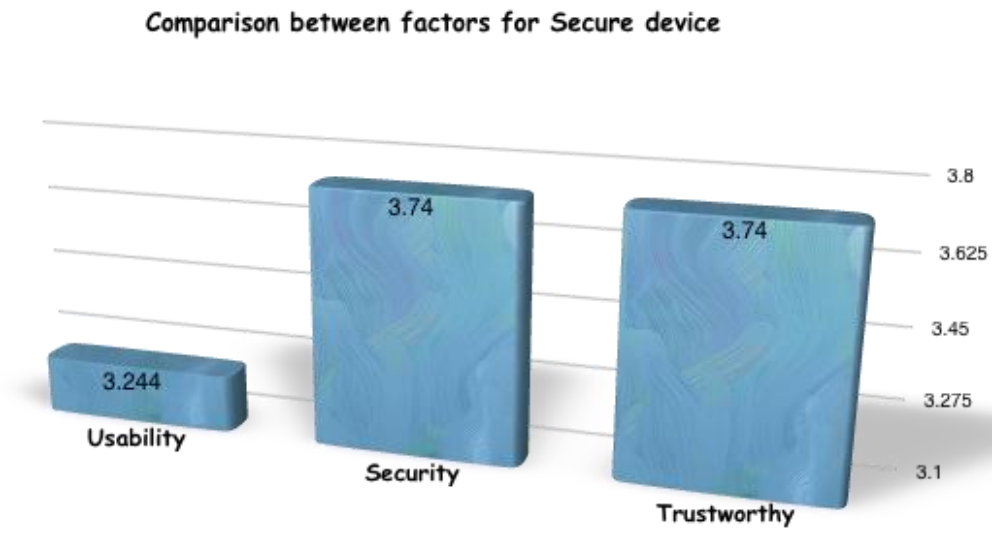


Figure 6.14 Comparison between factors for secure device

6.12.3.5 Card reader

To continue the assessment process for all the methods used in the experimental study, in this section an analysis was performed to evaluate the card reader's usability for the authentication process. The chi-square one variable test was used to determine the significant differences between frequencies of participants' responses towards each statement in the survey (see Table 6.11). For the first statement 'The log-in process with this method is complicated', the results indicate significant differences between frequencies (x^2 = 73.1, degrees of freedom = 4, p-value < 0.01). Most participants disagreed with the statement (63%); on the other hand, 25% found the card reader complicated to use and had difficulty during the experiment, either in recognising the button 'identity' to start the process or with inserting the card properly in the reader. Regarding the three statements that assess participants' willingness to use the method again, the ease of use and the efficiency of the card reader, there were significant differences between frequencies of participants' responses, as illustrated in Table 6.11. Most rated them positively, with high ratings for the ease of use (81%) compared with only 50% for the secure device for the same statement. This variance may due to the

design of both devices: The secure device was quite small and required a button to be pressed and held, while the card reader was large with big buttons.

The fifth statement, 'I found that this method is cumbersome to use', revealed a division between frequencies (x^2 = 45.8, degrees of freedom = 4, p-value < 0.01). This may be due to the problem that some participants faced or felt during the experiment. Assessing their confidence to use the card reader, only 11% responded negatively, stating they were not confident; 29% indicated that they need to learn how to use the card reader, and as mentioned previously, the 'identity' button was not clearly recognised as the first button that the users needed to press to start the process. Some tried to start by pressing 'enter' button on the card reader to get the generated code. The look of the device is similar to a calculator, which might necessitate improvements, as one of the participants stated in the open-ended questions.

The results from the last three statements are similar regarding satisfaction, security and trustworthiness. Performing the chi-square one variable test, the results indicate significant differences between frequencies of participants' responses towards the secure device in terms of satisfaction, security and trustworthiness (x^2 = 82.4, 86.5, 66.4, respectively, degrees of freedom = 4, p-value < 0.01).

Most participants rated the last three statements positively (57%, 76%, 72%) with a particularly positive attitude towards the trustworthiness of the card reader, as shown in Table 6.11 and Figure 6.15.

N	*Statement*	*Strongly Disagree*	*Disagree*	*NAND*	*Agree*	*Strongly Agree*	*Chi square*	*DF*	*Sig.*
1	The log-in process with this method is complicated.	11	52	12	22	3	73.1	4	.000
2	I would like to use this method again	3	12	18	49	18	60.1	4	.000
3	I can use this method easily.	1	9	9	58	23	102.8	4	.000
4	This method is efficient for log-in process.	1	11	17	54	17	80.8	4	.000
5	I found that this method is cumbersome to use.	3	41	19	28	9	45.8	4	.000
6	I feel confident when using this method.	0	11	21	45	23	24.64	3	.000
7	I need to learn how to use this method.	17	43	11	27	2	49.6	4	.000
8	This method is satisfying.	1	13	29	51	6	82.4	4	.000
9	This method is trustworthy.	2	8	14	55	21	86.5	4	.000
10	This method is secure.	2	12	14	50	22	66.4	4	.000

* NAND: refer to neither agree and disagree in this table

Table 6.11 Descriptive statistics for rating card reader

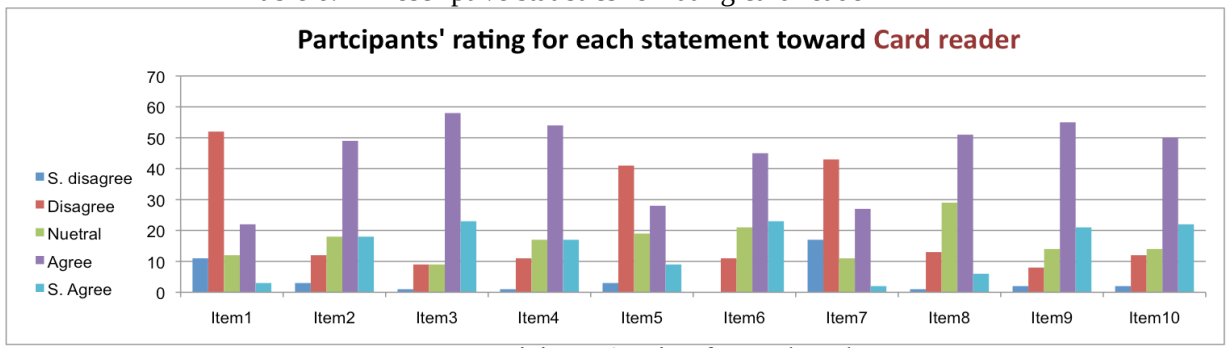


Figure 6.15 Participants' rating for card reader

6.12.3.6 Card reader's overall usability

A further evaluation was performed to investigate the overall usability of the card reader compared with the other two factors: security and trustworthiness. The Friedman test was used to determine the differences between the three factors (usability, security and trustworthiness) (see Table 6.12). The results indicate that there are differences in scores between usability, security and trustworthiness while using a secure device (x^2 = 13.12, p-value < 0.05) awarded to the trustworthy. Figure 6.16 indicates the results based on the mean differences more clearly.

Factor	N	Mean	Std. Deviation	Minimum	Maximum	Mean Rank	Chi-Square(DF)	Asymp. Sig.
Usability	100	3.5700	.64386	1.75	4.75	1.75		
Trustworthy	100	3.85	.914	1	5	2.18	13.12(2)	0.001
Security	100	3.78	.991	1	5	2.08		

Table 6.12 Friedman test results for card reader

An in-depth analysis was performed to compare the three factors, taking into account some demographic information, such as age, gender, education level, security experience and monthly visits to an e-banking account. For this analysis, the nonparametric chi-square test was used, revealing no significant differences in scores between participants (p-value > 0.05).

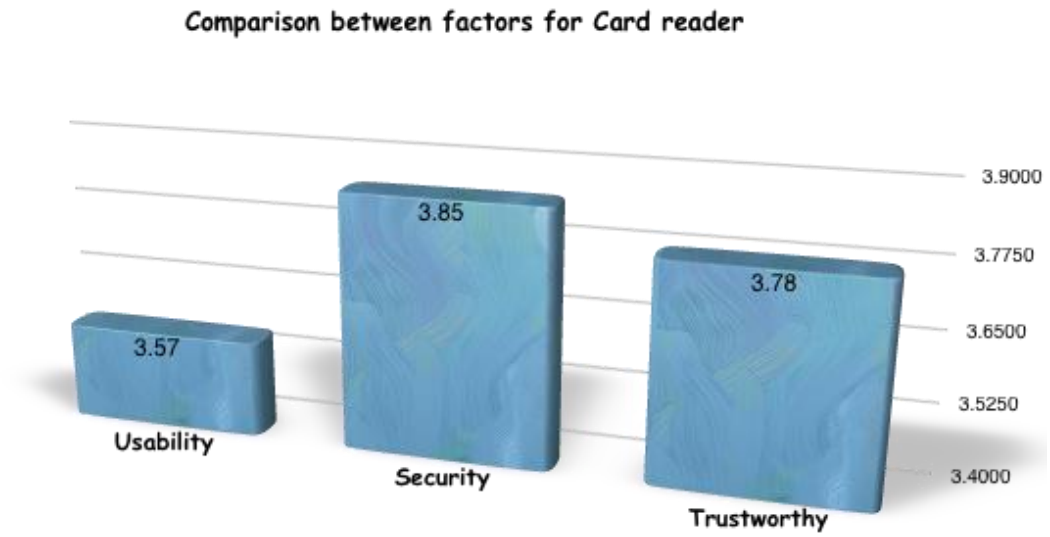


Figure 6.16 comparison between factors for card reader

6.12.3.7 Comparing all methods

There were three statistical approaches used to compare the three methods (fingerprint scan, secure device and card reader) in terms of usability, security and trustworthiness. Figure 6.17 illustrates the first approach by examining the maximum value that each method reached for each factor, showing that the fingerprint scanning method achieved the highest level of the three examined factors based on the mean values' differences.

To determine the differences empirically and confirm the obtained results, the Friedman test was used to determine whether there are significant differences between the three methods' usability, security and trustworthiness. The results revealed no significant differences in scores between participants' attitude towards the methods' security and trustworthiness (p-value > 0.05). In contrast, there were significant

differences in scores between participants' attitude towards the usability (chi-square = 61.6, p-value < 0.01); the preferred method was the fingerprint scan when used for the authentication process in e-banking.

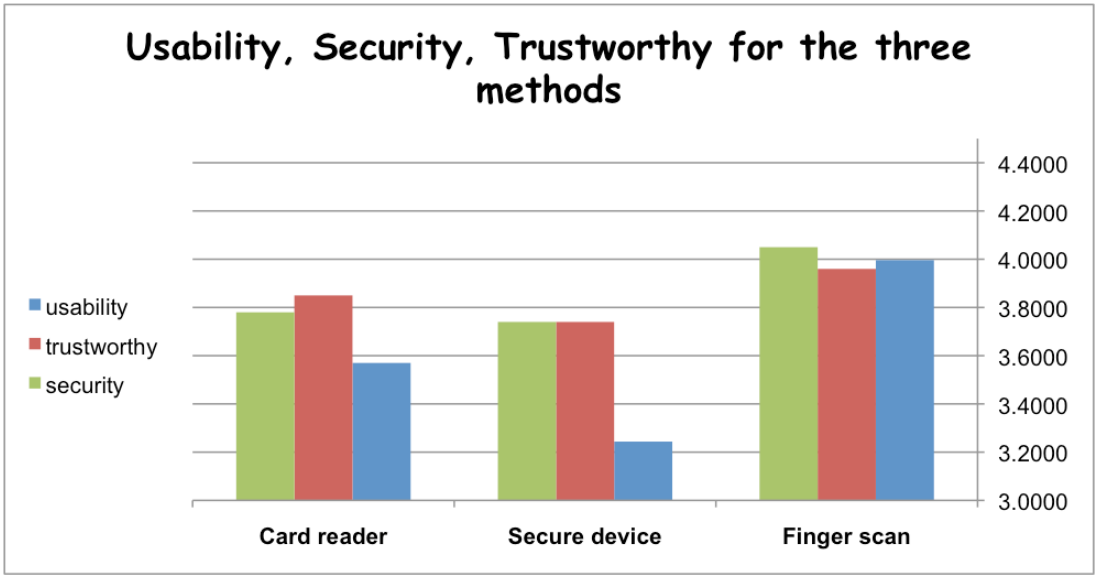


Figure 6.17 Comparison between three methods among three factors

Finally, the last approach analysed the question that asked the participants to rank the three methods based on four factors (preference, ease of use, security and trustworthiness). The results obtained show that the fingerprint scanning method was ranked to be users' preferred method, with 54% ranking it at the top of the list. Regarding the ease of use, security and trustworthiness, the majority of the participants ranked the fingerprint scanner first, followed by the card reader and the secure device. The ease of use had the highest percentage and was awarded to the fingerprint scanner, with 85% of collected responses (see Figure 6.18).

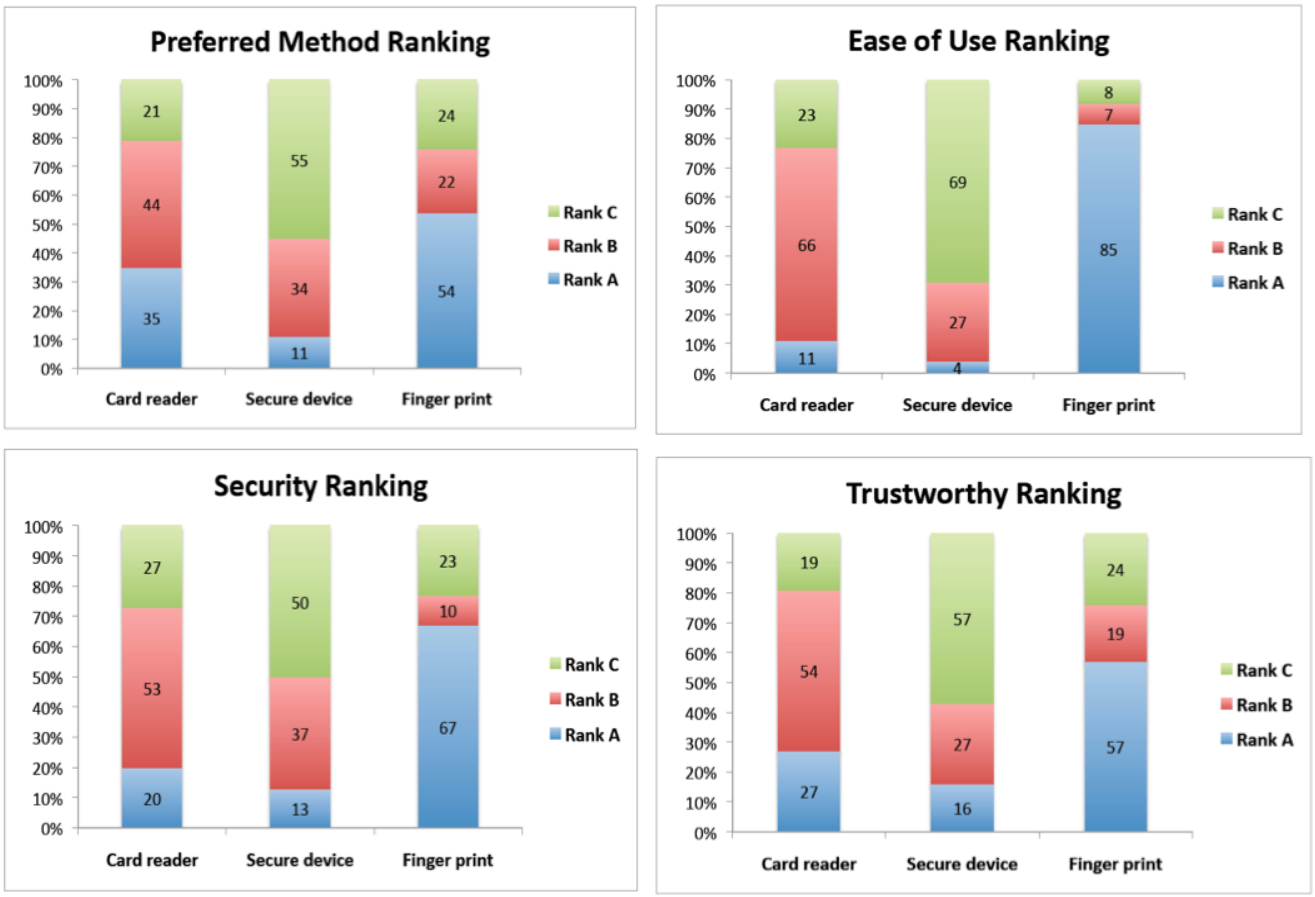


Figure 6.18 Results of ranking questions

It was worthwhile to compare the participants' preference results from the ranking question with their first choice when they started the experiment, as they were given the freedom to choose their preferred method prior to the experiment. Therefore, the contingency coefficient was determined to find the correlation between participants' choice before and after the experiment, and the results show a positive relationship (contingency coefficient = 0.627, p-value <0.01). For example, 39 users preferred to use their fingerprint before and after the experiment while 25 participants preferred to use the card reader before and after the experiment (see Table 6.13).

		After				Contingency Coefficient	Approx. Sig.
		Card Reader	Secure device	Finger print	Total		
Before	Finger	5	0	39	44	0.627	.000
	Secure	5	9	5	19		
	Card	25	2	10	37		
Total		35	11	54	100		

Table 6.13 contingency coefficient result

6.12.3.8 Qualitative data

At the end of the survey, the participants were given free space to add any comments regarding the experiment, and 29 posted their perspective in the comments section. The collected comments have been scanned by the researcher and classified according to five categories (card reader, secure device, fingerprint scanner, experiment and general statements). Table 6.14 illustrates the categories with the frequencies.

Statement	***Frequency***
General statements	2
Experiment	8
Finger scan	16
Card reader	4
Secure device	5

Table 6.14 comments categories

As can be seen, most of the statements about the fingerprint scanning method express participants' positive impressions about using the method and the level of its security. Some comments include:

'A fingerprint scan seems the most secure and reliable, as no one else can imitate it for this purpose and it is with me at all times'. (User 22)

'The fingerprint process was most alien to me'. (User 7)

'The level of efficiency surrounding the use of the fingerprint to log in was undeniable'. (User 23)

'I strongly prefer the fingerprint method'. (User 86)

Regarding the other two methods, the secure device and the card reader, the comments varied from positive to negative. For example, two of the statements indicated that the secure device was complicated and confusing based on their experience, e.g. '*I found the keyboard on the security device to be unresponsive*'. This is due to the fact that the secure device required the users to press and hold it, and not all the users read the instructions. Therefore, they kept trying until they read the instructions or asked for help.

According to Table 6.13, eight statements were made about the experiment in general, such as:

'Very well approached and explained as to what the research was for. Easy to work my way through and quick to complete'. (User 20)

'The experimenter was very helpful and informative where help was needed during the task, and the questionnaire and the experiment itself has made me think more deeply about online banking and the security protecting it'. (User 98)

6.12.4 Security Results

As mentioned in section 6.9.2, security was measured by identifying four attributes: attention, caution, motivation, and wariness. Attention was measured by observing users' awareness and noting a missing SSL in the address bar. Caution was measured

by observing users' interaction with requested sensitive information, such as entering an email address on an insecure page.

Motivation was measured by observing users during their interaction with authentication methods and measuring their progress with providing a fingerprint and continuing the authentication process. Wariness was measured by observing users' interaction, behaviour and understanding of a warning message during the authentication process. The following sections present and discuss the obtained results according to each factor.

6.12.4.1 Attention (Missing SSL)

During the experiment, all the pages were missing the SSL and represented insecure connections; all the pages' links started with 'http' instead of 'https'. Furthermore, the address bar was concealed in the explorer via the full screen view. The researcher observed users' progress during the login, authentication and transaction processes. By observing the users, the researcher monitored for any hesitation or uncertainty concerning how to move from one page to another, any trails to view the address bar to check the website address, complete the authentication process and provide all essential credentials. The results revealed that none of the 100 users participating in the experiment noticed that the 'https' was missing, indicating that the users had poor security experience, even the 12 users who indicated in the survey that they had experience in the security domain. Moreover, none of the participants who held doctoral degrees, had taken classes in computer science/enrolled in school for computer science or were enrolled in business school noticed the absence of the 'https' in the address bars.

6.12.4.2 Caution (Insert email address)

Caution was measured by observing users' ability to type and provide an email address in an insecure page. This has not been empirically examined in prior studies by involving online banking users. However, it has been involved during the automatic analysis for financial websites (Falk et al., 2008). During the experiment, all the participants provided and typed an email address as requested (see Figure 6.19) on an insecure page without any concern or apprehensiveness, which also indicates their weak understanding of the harm that could result.

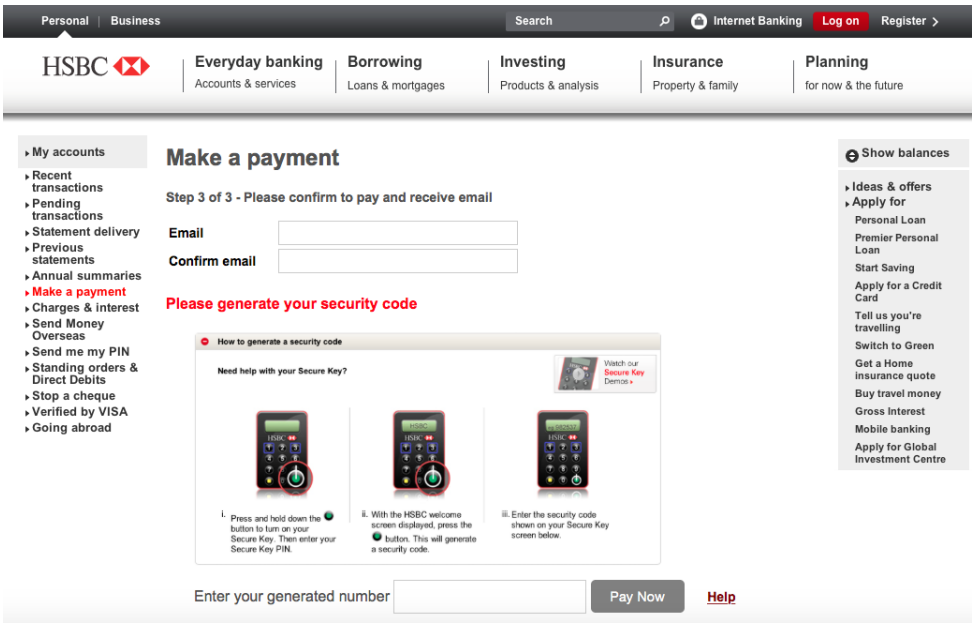


Figure 6.19 Inserting email page in the simulated system

6.12.4.3 Motivation (Providing Biometric Information)

During the experiment, the second step to log in to the bank account was choosing an authentication method. One of the provided methods was the use of a fingerprint reader. For more clarification, the experiment's design aimed to force each user to use each authentication method during part of the experiment. For example, if the user did

not choose the fingerprint reader as an authentication method, he or she was asked to use it to confirm the transaction process. The researcher ensured that the scanning fingerprint stage passed easily and recorded users' reactions (such as confusion i.e. where to put their finger, hesitation i.e. asking the observer or cancelling during scanning, stopping, asking). The results indicated that three out of 100 users wondered if their own fingerprints would be saved on the website database and asked the observer for more clarification. However, all of them completed the experiment after they obtained the answer to this question (two were in the business school; one was enrolled in the development school). One participant expressed surprise after seeing his fingerprint on the screen and noted how fast the scanning process was; however, the fingerprint that appeared in the platform was a fake picture appeared after the scanning. Most of the participants seemed to enjoy the experience of using the machine and scanning their fingerprint and did not express concern about the secure delivery of biometric information. Overall, it can be assumed that the participants do not have any experience in the domain of security and that they are not aware of the effects of their actions or decisions with respect to the provision of fingerprints.

6.12.4.4 Wariness (Invalid Security Certificate)

During the transaction process represented in the experiment, a warning message regarding an invalid security certificate appeared to measure users' wariness regarding the message (see Figure 6.20). They could choose to respond to this in one of two ways: press 'OK' or 'Cancel'. To record users' responses during the experiment, two methods were used. First, the table schema was such that it recorded users' responses to the warning message options. The strategy used for capturing responses was that

the expected response was set by default to FALSE (0) and updated to TRUE (1) when users selected an option. Second, the observer monitored and recorded users' responses to the message and all noticeable reactions recorded in the observation sheet. The expected result that users would respond carefully to the message, as they have been informed that they would perform a real transaction using the researchers' bank account.

The results from the database indicate that 85 of the 100 users pressed 'OK' and proceeded to the next step; the remaining users pressed 'Cancel' to avoid the risk. Of the group defined as having some experience in the domain of security (a total of 12 users), only four pressed 'Cancel', with the other eight selecting 'OK'.

Figure 6.20 Warning message about invalid certificate

Table 6.15 presents details about users' responses from the observation sheets collected after the experiment. The users' responses after the analysis are grouped by themes, with each theme describing one action as follows:

- Confused while reading the message and maintained eye contact with the observer.

- Read the message very carefully, but careful reading did not lead to cancellation or stopping the set of actions related to continuing the online banking transaction represented by the experiment.
- Read the message and hesitated to proceed with the transaction.
- Asked for help from the observer.
- Indicated that he or she did not want to complete the experiment.
- Tried to find instructions.
- Pressed 'OK' with reading the message or without evidently reading the message nor expressing any concern.

Action	***Frequency***
Press OK	85
Press Cancel	15
From observation	
Confusing	1
Reading carefully	16
Hesitate to continue	7
Asking for help	5
Prefer to discontinue	2
Finding instructions	1
No concern	68

Table 6.15 users' reaction toward warning message

Table 6.15 summarises the above observations. The majority of the users (68%) did not spend time reading the message and responded directly (without reading it), while only 16 users read the message very carefully to make a decision. In spite of this careful reading, some of these users pressed 'OK', indicating they may not have

understood the content of the message. Two of the users seemed to indicate that they were concerned about the account and decided to discontinue the task to avoid risk.

6.13 Chapter Summary

This chapter presented an experimental study conducted to evaluate three methods suggested from the Chapter 5 to assess usability and security. The chapter started by justifying the need to conduct the experimental study and its potential contributions by presenting the evaluation approach. The evaluation approach included a usability assessment and security assessment based on users' awareness of security warnings. Then, the chapter presented the study aim, which was assessing the level of security and usability of three different types of multifactor authentication. This was followed by the first research question, involving finding the most desirable authentication method by online banking users, which was answered through the survey results and ranking questions results. The results indicate that fingerprinting was perceived to be the most usable, secure and trustworthiness method from users' perspectives. The second question was: What are the differences between the three methods in terms of usability, security and trustworthiness? The answer was achieved through an in-depth analysis of each factor that measures the usability and security.

The study involved a simulation of an original bank platform, which gave users the ability to choose their preferred method to log in and then made them use the other two methods to complete that task. The freedom to choose a particular method can be used by e-banking to follow usability principles and protect the process from attack. Using all three methods in the experiment gives users a real experience to assess the methods impartially.

The results obtained from the experimental study indicated that fingerprinting was the most usable and secure method from the users' point of view. In contrast, the users' level of understanding security indicators is quite low, based on their reaction to the security features presented in the study. In the next chapter, the findings from all the studies conducted in this thesis in relation to the literature review are discussed.

Chapter 7

Discussion of the Findings

Preface

This chapter highlights the relevant observations that can be drawn from the previous chapters and discusses interpretations of the study's findings. In particular, the researcher intends to link the results from all prior research conducted in the field of usable security. This link will be established beginning with the results obtained from the survey used in the exploratory study, which evaluated the current use of multifactor authentication, followed by the results of the experimental study and the descriptive study, which assessed different types of MFA. Subsequently, the researcher will provide a set of recommendations based on the research findings for banking providers and researchers interested in usable secure systems.

7.1 Discussion of Key Findings

The present research provides a more holistic view than what is currently available in the literature that will extend our understanding of the usability and security of authentication mechanisms in the context of online banking. This holistic view was achieved by using exploratory, descriptive, and experimental research approaches conducted systematically with each study starting after the completion of the previous one. Unlike previous studies, the exploratory study derived important insights from actual long-term users of authentication methods who have bank accounts in two different countries, investigating their perceptions about the usability and security of currently available authentication methods. The experimental study adopted a security evaluation measurement based on users' awareness of security warnings. Users performed the experiment in a real environment, interacting with real authentication methods and behaving as if they were performing a real banking task. The following sections will discuss the key results in relation to the literature and associated works.

7.2 Investigation of Usability and Security of MFA

The results from the survey of the exploratory study revealed that MFA is perceived as offering a higher level of security and trustworthiness than single factor authentication (SFA). This finding is based on the use of two techniques, as the benefit of security can be maintained by one technique if the other is compromised (O'Gorman, 2003). In terms of security, the finding is parallel with the results of the study by Gunson et al. (2011) wherein 62 users compared SFA and MFA. However, the context of that study concerned security methods used in telephone banking. In contrast, the results of the present study do not support the results of the study by Weir et al. (2010), wherein 141 users perceived SFA to be more secure than MFA. The

researcher argues that the type of sample is the most important component of any user study and suggests that studies that do not consider the long-term user experience are unlikely to provide a realistic picture of the levels of security and usability in SFA or MFA. The difference between this exploratory study and that of Weir et al. (2010) is that users in the latter were asked to use each method in order to evaluate them; thus, the evaluation required experience with all methods, which might affect the results. The evaluation in the exploratory study, on the other hand, is based on long-term use of the studied methods. The high level of security of MFA has also been revealed in the qualitative results, as 51% of the submitted statements about authentication methods were about the security of MFA.

While prior studies do not indicate to what extent MFA is adopted in the e-banking context, current research shows that 68% of investigated banks in the United Kingdom use MFA. This may indicate that these banks take into account the European Union Agency for Network and Information Security (ENISA) (2013) recommendation to use MFA, which was described in Chapter 1. Surprisingly, the results revealed that 98% of banks in Saudi Arabia adopted MFA by using PIN via a mobile mechanism. However, the results from the qualitative data show that there are several issues associated with using mobile devices, such as the difficulty of holding the cell phone for the local number and delay in receiving the code via SMS. These issues reinforce the need for banking service providers to seek a solution to this problem. One option could be to give customers the ability to authenticate themselves using their international phone number.

The results from the survey analysis in Chapter 4 allude to the high level of usability

of SFA in comparison to MFA. This finding parallels those of Gunson et al. (2011). In-depth analysis in Chapter 4 showed that PIN via mobile is considered an easier method than a card reader and secure device, but that the device is perceived as the more secure option. These findings elucidated that security and usability are competing goals (Kainda et al., 2010). Additionally, the results revealed that some demographic habits and experiences significantly impact the level of usability, such as the number of monthly visits to the site and education level. Users who visited the online banking site more than ten times perceived MFA to be more usable, as did users with high school level education. Users with college level education perceived MFA to be both more secure and more trustworthy. The effect of user characteristics such as age, gender and education is normally examined during investigations of usability and security level, such as in the studies of De Cristofaro (2014) and Weir et al. (2009). However, the exploratory study also examined other characteristics such as the number of monthly visits to the banking site, which revealed a positive impact on the level of the methods' usability.

More generally, the exploratory study demonstrates the users' perceptions of the usability and security of MFA and SFA and to what extent MFA has been adopted in e-banking. Specifically, it assessed the usability and security of using MFA in the context of Saudi banking.

7.3 Proposed MFA for the Experimental Study

The descriptive study alludes to the characteristics of different authentication methods. Unlike previous reviews and descriptive studies, it involves all recent factors used or invented to authenticate the user. The results revealed that there are three factors in

use in the market: knowledge-based authentication, token-based authentication, and biometrics-based authentication. Conversely, there are four other factors that have not been adopted in the market: location-, process-, formula- and relationship-based authentication. Prior research focussed on of the strengths and weaknesses of SFA and MFA, such as O'Gorman (2003), while the current study involves other factors and links user acceptance with the level of security; more security leads to an increase in user acceptance (Wefel and Molitor, 2012).

The results obtained from the descriptive study revealed that when MFA is adopted the knowledge-based factor is usually chosen as the first factor to overcome the problem of 'sniffing password' when the authentication is performed (Erlich and Zviran, 2008). Thus, the proposed methods used in the experimental study used KBA as the first factor because it does not provide an adequate level of security. This finding parallels the results from Chapter 4 as all the banks investigated via the survey used KBA as the first factor when MFA was adopted.

Regarding the types of biometric methods proposed to be examined in the experimental study, fingerprint is suggested as having a high level of user acceptance in comparison to other biometric identification methods (Morales, 2010; Jones et al., 2007). This is supported empirically by Jones et al.'s (2007) study, which investigated user acceptance of different biometrics methods with a survey of 115 users. Their results showed that the majority of users indicated familiarity with fingerprints. In addition, Wefel and Molitor (2012) state that user acceptance increases as security increases, and the experimental study results presented in Chapter 5 indicate that the

level of fingerprint security was high based on real experience with the method when performing banking tasks.

The results from the descriptive study examined the advances of research in inventing new technology and techniques to authenticate users in a secure system. Such findings reinforce the importance of conducting research that evaluates the invented techniques. Additionally, the obtained results propose three authentication methods to be assessed during the experimental study, which differ from those used in prior studies (De Cristofaro, 2014; Gunson et al., 2011; Weir et al., 2009; Weir et al., 2010; Krol et al., 2015).

7.4 Usable Security of MFA

The findings from the usable security assessment of three different authentication methods (fingerprint, secure device and card reader) indicate the high level of security and usability of fingerprints. One explanation for this finding is the number of steps required to authenticate users by fingerprint in comparison to other methods. A finger scanner requires only one step, which is to scan the finger, after which the user may proceed to the personal account page. This finding cannot be compared with prior research as none of the previous studies compare fingerprints to card readers or secure devices. Moreover, prior research does not compare card readers with secure devices. However, the results obtained from the experimental study showed that card readers are considered more usable than secure devices. The results from the statistical analysis described in Chapter 4 indicate that there is no significant difference between using these two methods. One explanation for this finding is that the number of users

who used card readers in the exploratory studies was very small in comparison to users who used a secure device.

The design of the experiments alludes to the benefit of performing such usable security evaluations within a real environment. The study used a simulation of a real banking website used in the United Kingdom (HSBC) using real authentication methods that belong to the researcher. None of the participants indicated that the banking site was fake, including those who have previously visited the HSBC website. Moreover, some of the participants indicated their concern regarding the research account after the experiment, requesting that the researcher check the account in case of a mistake.

The classic approach for users to login to e-banking is to use the requested method; the approach used in the experiment was to give users the freedom to choose between three methods. This approach allowed the researcher to compare user choices before starting the experiment and after the experiment during answering of the ranking questions, which asked the users to rank the methods in order of their preference. The results obtained by calculating the contingency coefficient showed that the relationship was positive, as most of the participants preferred to use the fingerprint method both before and after the evaluation. Additionally, several users who preferred either the secure device or card reader before the experiment chose the fingerprint method after the experiment. These findings support the results from Chapter 5 that showed high user acceptance of biometrics and conform to the results of a prior study by Jones et al. (2007). They also support the accuracy of the proposed choice in Chapter 5 which suggests examining the fingerprint method as opposed to other

methods to add value to technology providers, banking service providers and researchers.

Prior research in the area of assessing the usability and security of MFA used security as one attribute to indicate users' perceptions of the level of security (De Cristofaro, 2014; Gunson et al., 2011, Weir et al., 2009; Weir et al., 2010). Unlike previous studies, the current study included users' awareness of security warnings as predictors to measure the security level. The results in Chapter 6 showed that participants were not able to recognize the security issues while performing security tasks. This finding supports the conclusions of Lee et al. (2015), who observed 482 users interacting with a website in the absence of a security image; their results revealed that 73% of the users entered their password while the security image was absent and did not recognize this as a security issue. The methods used to observe participants interacting with the security warning message (invalid certificate) indicate responses such as hesitation, confusion, asking for help and finding instructions. This supports the research of Zabaa et al. (2014), who found that users are still confused by security warnings. In general, the results yielded by the security assessment in the experimental study are useful as evidence for researchers and banking service providers and may be used as guides for further improvements and research.

7.5 Discussion Note

The above discussion offers insight into the assessed results of the usable security of MFA. It also linked this research to previous studies in the field of usable security. Table 7.1 briefly present these studies along with the researchers' studies.

Name	***Research method***	***Including SFA***	***Assessed methods***			***Usability Dimensions***			***Security***	***Participants***	***Main Finding***
			KBA	TBA	BBA	Efficiency	Effectiveness	Satisfaction			
Weir et al. (2009)	Experiment	No	×	✓	×	✓	✓	✓	1 factor	50	Card-activated token perceived usable and secure comparing to other tokens used.
Weir et al. (2010)	Experiment	Yes	✓	✓	×	×	✓	✓	1 factor	141	SFA is the most secure and convenient option for the user.
Gunson et al. (2011)	Experiment	Yes	✓	✓	×	✓	✓	✓	1 factor	62	MFA had a high level of security and low level of usability comparing to SFA.
Paul et al. (2011)	Field study	No	×	✓	×	×	×	×	No	24	The users faced several issues with using smart card.

De Critofaro et al. (2014)	Interview	No	×	✓	×	×	×	✓	No	9	The authors identified different contexts and reasons to use MFA by the users.
	Survey	No	×	✓	×	×	×	✓	1 factor	219	MFA perceived as usable regardless of motivation and context.
Krol et al. (2015)	Interview	No	×	✓	×	×	×	✓	No	21	The users reported several issues associated with using hardware tokens.
The exploratory study	Survey	Yes	✓	✓	×	✓	✓	✓	1 factor	614	MFA perceived to be more secure and achieved an acceptable level of usability and adopted in most of e-banking.
The experimental study	Experiment	NO	✓	✓	✓	✓	✓	✓	4 factors refer to security warning s	100	Finger print perceived as the most secure, usable and trustworthy method comparing to card reader and secure device. Users' awareness of security warning that predicts security issues was low.

Table 7.1 Comparison between studies in the area of assessing usable security of MFA

7.6 Researchers' Recommendations

Based on the results of the current research, observation during the experimental study, participants' feedback, and the researcher's experience, the following is a list of recommendations and suggestions provided in an attempt to help banking providers and researchers develop usable and secure online banking systems.

1. Users of Saudi banks indicate several issues associated with using PIN via mobile as a method for authentication. Thus, Saudi banks should start the process of replacing this method with other available methods or, at minimum, find a solution for clients using their accounts from abroad. One such solution is to authenticate these clients using a short-term alternative number.
2. Banks should adopt methods that are perceived by the users as practical, such as fingerprints. These methods take advantage of users' unique features and are perceived to be secure, usable, and trustworthy.
3. Banks should simplify the transaction process and reduce the number of steps necessary to authenticate users. HSBC, as an example, requires the user to enter a personal ID in a text box that does not allow copy/paste functions, thus requiring the individual to type in the ID upon every login and answer the secure question in order to generate a PIN code using the secure device.
4. Banks should continuously ask clients to provide their feedback through quick and compulsory surveys to indicate their satisfaction with the provided services. This survey may include only one or two questions to elicit user perceptions.
5. Banks can increase the level of user awareness via several media modes. For

example:

- During the registration phase, banks can provide users with short videos highlighting most security issues and how to respond to them.
- During the registration phase, banks can provide users with a scanning tool to find any virus or security issues within a client's computer.
- Banks can cooperate with most TV stations to effectively highlight online banking security issues.

6. All banks should unify their authentication methods as a step to satisfy clients who have different bank accounts.

7.7. Chapter Summary

In this chapter, we discussed interpretations of the study results from the exploratory study, descriptive study and experimental study. This chapter has justified the study findings, linking them with prior research in the area of usable security. The chapter also provided a set of recommendations based on the research findings for banking providers and researchers. The next chapter intends to draw a conclusion from this research and provide different directions for future work.

Chapter 8

Research Conclusion

Preface

This chapter offers a summary of the research and central findings derived from the current research. It then identifies the key contributions made by this research to the body of knowledge and the implications of the results. It concludes by discussing the research limitations and addressing avenues for expansion of future work.

8.1 Research Conclusion

After developing a background context for the research, the research motivations were defined, from which the research aim and objectives were drawn. As discussed in the first chapter, this research has been undertaken to evaluate the usability and security of multifactor authentication (MFA) through a series of systematic studies using

different methodological approaches to achieve the research aims. This research achieved the following objectives:

1. Provide an understanding of the literature addressing authentication and the usability and security offered by authentication.
2. Explore the current state of single and multifactor authentication mechanisms.
3. Evaluate the usability of single and multifactor authentication techniques from the perspective of users.
4. Review the available authentication methods and propose methods for the experimental study.
5. Experimentally assess the usability of different multifactor authentication methods.
6. Experimentally measure security through users' awareness of security warnings.
7. Produce recommendations based on research results and researcher experience.

The first objective was met through a comprehensive review of the literature, which discussed three main areas: usability, security and authentication methods. Trust concept, online banking and security warnings have also been reviewed in order to integrate all concepts related to the secure systems and methods into the research. The second and third objectives were achieved through the exploratory study, which investigated the current use of MFA with a survey of 614 actual long-term banking clients. The study also evaluates the usability and security of the methods used and shows that MFA is perceived to be secure and trustworthy with a good level of usability.

The fourth objective was achieved through the descriptive study, which reviewed all available authentication methods and presented the strengths and weaknesses of each mechanism. It proposed the methods examined in the experimental study based on the level of user acceptance, security level and availability of the method in the market. The fifth and sixth objectives were met through the experimental study, which designed a specific approach that suggested giving the participants the opportunity to choose their preferred method to login and perform a task. The task was set within a realistic environment utilising a simulation of a real bank in the United Kingdom (HSBC). The study proposes assessing the security through four measurements (attention, caution, wariness and motivation) that reflects users' awareness of most the visible security warning in e-banking. The main result of this study is that fingerprint authentication, as an example of biometric-based authentication, was perceived to be usable, secure and trustworthy. Moreover, the level of user awareness of security warnings was very low and a list of recommendations to improve user awareness and banking features is presented in Chapter 7. These recommendations demonstrate the achievement of the final research objective.

8.2 Contribution to the Body of Knowledge

The key contributions of this thesis are as follows:

Identifying the research gap

Chapter Two reviewed studies related to the security and usability of authentication methods and identified the limitations in this field. Of these, only five papers focused on the usability of multifactor authentication, whereas none examined the methods that were explored in this thesis. The current literature lacks a focus on the security

attributes to be measured during usable security evaluation. The current thesis therefore explores studies in the security warnings area and links these to the security tasks of the authentication process to show the relationship between the two concepts.

Current state of authentication methods A usability evaluation was conducted with a survey involving 614 respondents to investigate the current state of authentication. This survey included questions on security, trustworthiness and usability. To the best of our knowledge, this is the first study that focuses on Saudi customers of online banking. The sample was selected carefully; the participants were ensured to have a long experience with e-banking and have two different bank accounts from a developed and a developing country.

Analysis of the usability of single and multifactor authentication

The exploratory study in Chapter Four showed different authentication methods, including single factor authentication. An analysis to compare the usability and security between single and multifactor authentication was conducted, and the results provided a clear picture of the high security of multifactor authentication on the basis of the perceptions of users who have a long experience in using both methods.

Analysis of different authentication methods

A comprehensive and extensive analysis of seven popular authentication approaches was conducted objectively and in a way that guided the finding of a combination of the most appropriate methods that could be examined in the experimental stage of this

thesis. The study found that a biometric method should be included to achieve new and logical evaluation results.

Novel approach to evaluating authentication methods

The experiment presented in Chapter Six was designed to evaluate the suggested authentication methods in terms of usability and security. The approach simulated online banking at the HSBC Bank because the participants were British, and many HSBC customers were expected to take part in the experiment. The approach included three different methods (card reader, secure device and fingerprint) for usability and security comparison, and it gave each participant the opportunity to have a real experience with each method so that the results are more accurate. To the best of our knowledge, none of previous studies used the same assessment methods (Chapter Six).

Security analysis

The security analysis undertaken in Chapter Six focused on the proposed criteria related to users' awareness of security warnings. The results revealed a clear picture of the low level of user awareness of security warnings.

8.3 Limitations and Future Work

Like all research, there are several limitations in this study that should be mentioned. These limitations can be used as opportunities for further research:

1. The exploratory study targeted a sample of educated users studying abroad who were motivated to use technology. This sample does not represent older

bank users, who might have other perceptions about technology. Future work may include older people in a different context.

2. Effort was paid to design the experiment to be realistic. However, it used a fake platform in order to adopt the other methods to be examined. This limitation does not affect the study as none of the participants indicated that the platform was not real, but is mentioned for future researchers.
3. During the experiment three participants were apprehensive about using the fingerprint factor for the purpose of authentication. This observation is interesting but outside the scope of this research. It would be useful to conduct further studies where trust relationship between the customer and the bank concerning holding biometric information on third party databases for authentication can be scoped.
4. Similar to the exploratory study, the experimental study does not involve older people who might behave differently with regard to e-banking and finger scanners than other populations.
5. The fingerprint method proved to be both usable and secure. Therefore, it is worth considering disabled people, such as the visually impaired, in further research as they may have different attitudes and perceptions.
6. The experiment study used certain authentication methods (secure device, card reader and fingerprint) combined with knowledge based authentication. Future studies may evaluate other methods and compare the results with the current research results.

8.4 Epilogue

This research has been undertaken to evaluate the usability and security of multifactor authentication through a series of studies using different methodological approaches. The results confirmed that fingerprint authentication is perceived to be usable, secure and trustworthy in comparison to card readers and secure devices. Using MFA increases the security level and has a high level of acceptance by users. However, there are still questions about which MFA will be adopted by the banking sector. It is apparent that the fingerprint method is a good choice that banks should consider. The measurements of security proposed in this research have proven successful in examining users' awareness of security warnings and assessing the usable security of secure systems.

REFERENCES

(Total number of references is 239)

Aaker, A. Kumar, VD. & George, S. (2000). Marketing research. John Wiley and Sons, Inc, New York.

ACM, Chairman-Hewett, T.T. (1992). ACM SIGCHI curricula for human-computer interaction. ACM .

ACM/IEE-CS Joint Task Force on Computing Curricula. (2013) Computer Science Curricula 2013.ACM Press and IEEE Computer Society Press DOI:http:/dx.doi.org/10.1145/2534860

Aladwani, A.M. (2001). "Online banking: a field study of drivers, development challenges, and expectations", *International Journal of Information Management*, Vol. 21, pp. 213-225.

Alavi, M. and Carlson, P. (1992). A review of MIS research and disciplinary development. *Journal of Management Information Systems, 8*(4), 45–62.

Aljahdali, H. (2014). Using Cultural Familiarity for Usable and Secure Recognition-based Graphical Passwords. Glasgow library.

Alshamari, M. and Mayhew, P. (2008). Task design: its impact on usability testing. The Third International Conference on Internet and Web Applications and Services, Athens, 08-13 June. IEEE, pp 583- 589

Althobaiti, M.M., Mayhew, P., (2014). Security and usability of authenticating process of online banking: User experience study. *In the Proceedings of the 48 Annual IEEE International Carnahan Conference on Security Technology*, ICCST 2015, IEEE

Anandhan, A., S. Dhandapani, H. Reza & K. Namasivayam, (2006). Web usability testing -CARE methodology, in the Third conference on Information Technology: New Generations (ITNG'06) IEEE, 450-500.

Andress, J. (2011). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.

Atlman, D. et al. (2006). Why do a pilot study? [online][Accessed 24 June 2015]. Avaliable from http://www.nc3rs.org.uk/downloaddoc.asp?id=400

Balfanz, D., Durfee, G., Smetters, D., and Grinter, R. (2004) "In search of usable security: five lessons from the field," IEEE Security & Privacy, vol. 2, no. 5, pp. 19–24.

Bangor,A., Kortum, P. T. and Miller, J. T. (2008). An empirical evaluation of the system usability scale. *Journal of Human-Computer Interaction*, 24(6).

Bargh, J.A. and McKenna, K.Y.A. (2004), "The internet and social life", Annual Review of Psychology, Vol. 55, February, pp. 573-90.

Barriocanal, E. G. Urban, M. A. Sotos L. A. and Gonzalez, J. R. (2003). An ontology-based approach for designing web usability evaluation questionnaires. Springer Lecture Notes in Computer Science.

Battleson, B. Booth, A. and Weintrop, J. (2001). Usability testing of an academic library web site: a case study. The Journal of Academic Librarianship, 27(3):188–198.

Bell, J. (1984). Conducting Small Scale Investigations in Education Management. London: Harper & Row.

Besnard , D. and Arief, B. (2004). "Computer security impaired by legitimate users,"

Computers& Security, 23 (3) pp. 253-264.

Bhivgade, T., Bhusari, M., Kuthe, A., Jiddewar, B., Dubey, P.(2014) Multi-factor Authentication in Banking Sector. International Journal of Computer Science and Information Technologies, Vol. 5(2), 2014,1185-1189.

Blackmon, M. H., Polson, P.G., Kitajima, M., & Lewis, C. (2002). Cognitive walkthrough for the web. CHI 2002 Conference on Human Factors in Computing Systems. ACM Press, pp. 463-470.

Bonderud, D. (2014). Multifactor Authentication Market to Be Worth $10 Billion by 2017 — But Is the Model All Wrong?. Avaliable online and accessed on 25 May 2016 https://securityintelligence.com/news/multifactor-authentication-market-worth-10-billion-2017-model-wrong/

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 553-567). IEEE.

Brainard, A., Juels, R.L., Rivest, M. Szydlo, M., and Yung, M. (2006). Fourth-factor authentication: Somebody you know. In *ACM CCS*, 168–178.

Branch, J. L. (2000). Investigating the information-seeking processes of adolescents: The value of using think-alouds and think afters. *Library and Information Science Research, 22*(4), 371–392.

Braz, C. and Aïmeur, E. (2005). ASEMC: Authentication for a secure mobile commerce. *RFID Journal*, White Papers, Security.

Braz, C. and J.-M. Robert (2006). Security and usability: The case of the user authentication methods. In: 18th International Conference of the Association Francophone d'Interaction Homme-Machine (pp. 199–203), Montréal,

Canada.

Brostoff, S., Inglesant, P., & Sasse, M. A. (2010, September). Evaluating the usability and security of a graphical one-time PIN system. In *Proceedings of the 24th BCS Interaction Specialist Group Conference* (pp. 88-97). British Computer Society.

Bryman, A. (1998). Quantity and Quality in Social Research . London: Unwin Hyman Ltd. ISBN: 0-415-07898-9.

Bryman, A. (2004). Social Research Methods. 2nd ed. New York, NY: Oxford University Press.

Buttle, F. (1996). *Relationship Marketing, Theory and Practice*, Paul Chapman Publishing, London.

Burns, AC. and Bush, RF.(2002). Marketing research: Online research applications (4th ed). Prentice Hall, New Jersey.

Byers, D. and Shahmehri,N. (2007). "Design of a Process for Software Security", Second International conference on Availability, Reliability and Security (ARES'07), IEEE, pp. 301-309.

Carrol, J. M. (2003) *HCI Models, Theories and Frameworks: Toward a Multidisciplinary Science.* Morgan Kaufmann. ISBN 1558608087.

Carullo, G., Ferrucci, F., & Sarro, F. (2012). Towards improving usability of authentication systems using smartphones for logical and physical resource access in a single sign-on environment. In *Information systems: crossroads for organization, management, accounting and engineering* (pp. 145-153). Physica-Verlag HD.

Chen, W., & Hirschheim, R. (2004). A paradigmatic and methodological

examination of information systems research from 1991 to 2001. *Information systems journal*, *14*(3), 197-235.

Churchill, A.G.J. (1999). *Marketing research: Methodological foundation* (7th ed.). Hinsdale, IL: The Dryden Press.

Churchill, GA. And Iacobucci, D.(2004). Marketing research: Methodological foundations, 9th ed. Thomson South-Western, Ohio.

Clarke, N., Furnell, S.(2005). Biometrics—the promise versus the practice. Computer Fraud & Security. **9**, 12–16

Clarke, N. (2011). *Transparent user authentication: biometrics, RFID and behavioural profiling*. Springer London.

Computing Research Association (2003). "Four Grand Challenged in Trustworthy Computing", Final report of CRA Conference on Grand Challenged in Information Security and Assurance, Airlie House, Warrenton, Virginia, November 16–19.

Coolican H.(1990). *Research methods and Statistics in Psychology*. GB: Hodder & Stoughton.

Constantine L., and Lockwood, L. (1999). *Software for Use: A Practical Guide to the Essential Models and Methods of Usage-Centered Design.* Reading, MA: Addison-Wesley.

Creswell, J. W. (1994). Qualitative and quantitative approaches. *Qualitative and quantitative approaches*.

Creswell, J. W. (2003). Research Design: Qualitative, Quantitative, and Mixed Method Approaches. Thousand Oaks, CA: Sage.

Cuthbert, P. (2009). The importance of usable security. Retrieved October 21, 2014 from: http://www.castelain.com.au/blog/the-importance-of-usable-security

De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. 2014. A Comparative Usability Study of Two-Factor Authentication. [Online] http://arxiv.org/abs/1309.5344v2 [accessed 25 May 2014]

Denning, D. E. and MacDoran,P. F. (1996). "Location-based authentication: Grounding cyberspace for better security," Computer Fraud & Security, vol. 1996, pp. 12-16.

Denscombe, M. (2003). The Good Research Guide for Small-scale Social Research Projects: Open University Press.

DePauw (2009). Hofstede's Value Dimensions: Saudi Arabia . Cultural Portfolios, DePauw University, USA. cited May 2012, from: http://dpuadweb.depauw.edu/$1~mkfinney/teaching/Com227/culturalPortfolios/.

Desurvire, H., Kondziela, J., and Atwood, M. (1992). What is gained and lost when using evaluation methods other than empirical testing. In Monk, A. , Diaper, D., and Harrison, M., editors, *People and Computers VII*, pages 89-102. Cambridge University Press.

DeWitt, A. J. and Kuljis, J. (2006). "Is usable security an oxymoron?" *Interac- tions*, vol. 13, no. 3, pp. 41–44.

Dix, A.J., Finlay, J.E., Abowd, G.D. & Beale, R. (2004). Human-Computer Interaction. 3rd Ed. Harlow Assex: Pearson Education Limited.

DPA. (1998). UK Data Protection Act 1998. Access on line [12-4-2016] from http://www.legislation.gov.uk/ukpga/1998/29/contents >

Druckman, J. N., & Kam, C. D. (2009). Students as experimental participants: A defense of the 'narrow data base'. *Available at SSRN 1498843*.

Easterby-Smith, M., Thorpe, R., and Lowe, A. (2002). Management Research: an introduction. London: Sage.

Egelman, S., Cranor, L. F. & Hong, J. (2008) 'You've been warned: an empirical study of the effectiveness of web browser phishing warnings', *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*. Florence, Italy ACM, pp. 1065-1074.

Elmore, P., and Beggs, D. (1975). Salience of concepts and commitments to extreme judgments in response patterns to teachers, *Education*, vol. 95, no.4, pp. 325- 334.

Ericsson, K. A., & Simon, H. A. (1993). *Protocol analysis: Verbal reports as data (Revised edition)*. Cambridge, MA: MIT Press.

Erlich, Z., & Zviran, M.(2008). Authentication Practices from Passwords to Biometrics. In Encyclopaedia of information Science and Technology, Third Edition

Ernest, P. (1994). An Introduction to Research Methodology and Paradigms. Exeter:School of Education, University of Exeter.

Falk, L., Prakash, A., and Borders, K. (2008). Analyzing websites for user-visible security design flaws. In: ACM SOUPS; pp. 117–126.

Faulkner, X. (2000). Usability Engineering. London: Macmillan Press.

Feldstein, M. (2002). What is usable e-learning?. ACM eLearn Magazine, (9), p.2.

Feruza, S. and Kim, T. (2207). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering*. 2 (2).

Fidas, C.A., A. G. Voyiatzis, and N. M. Avouris (2010). When security meets usability: A user-centric approach on a crossroads priority problem. In 14th Panhellenic Conference on Informatics (pp. 112–117). IEEE.

Fitzpatrick, R (1998). Strategies for evaluation of software usability [Online]. Retrieved April 17, 2014 from: http://www.comp.dit.ie/rfitzpatrick/papers/chi99%20strategies.pdf.

Flick, U. (1998). An Introduction to Qualitative Research. SAGE Publications Ltd.

Florêncio, D. and C. Herley (2007). A large-scale study of web e password habits. In Proceedings. World Wide Web Conference (WWW '07), Banff, Alberta, Canada, May 2007.

Floridi, L. (2003). Blackwell Guide to the Philosophy of Computing and Information, Oxford:Blackwell, , 155-166.

Fowler, F.J., Jr. (2002). *Survey research methods* (2nd ed.). Newbury Park, CA: Sage Publications, Inc.

Furnell, S., 2005. Why users cannot use security. Computers and Security 24, 274 – 279.

Galliers, R. J. (1991). Choosing appropriate information systems research approaches: A revised taxonomy. Information Systems Research: Contemporary Approaches & Emergent Traditions.

Garfinkel, S. (2005). *Design principles and patterns for computer systems that are simultaneously secure and usable*. Ph.D. thesis, Massachusetts Institute of Technology.

Garfinkel ,S. and Spafford, E. (1996). Practical Unix & Internet Security. O'Reilly & Associates, Inc.

Gay, L.R. (1992). *Educational research* (4th Ed).New York: Merrill.

Gefen, D., Karahanna, E., Straub, E.W., 2003, Trust and TAM in Online Shopping: An Integrated Model, MIS Quarterly, Vol. 27, No. 1, March 2003, pp. 51-90.

Ghogare, S., Jadhav, S., Chadha, A., and Patil, H. (2012). "location based authentication: A new approach towards providing security" , International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 ISSN 2250-3153.

Gill,J. and Johnson, P.(1997). *Research methods for managers*.2nd edition . London, Paul Chapman Publishing.

Godfrey, P. & Hill, C. (1995). The problem of unobservable in strategic management research. Strategic management journal, 16 (5), 19– 533

Grbich, C. (2007). Qualitative data analysis an introduction. Sage, London

Gray, W. D., John, B. E., & Atwood, M. E. (1993). Project Ernestine: A validation of GOMS for prediction and explanation of real-world task performance. *Human-Computer Interaction*, **8**, 3, pp. 237- 209.

Guba, E. G. (1990). The alternative paradigm dialog. In E. G. Guba (Ed.), *The paradigm dialog* (pp. 17–27). Newbury Park, CA: Sage.

Gunson, N., Marshall, D., Morton, H., and Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, *30*(4).

Haak, D. and Jong, D. (2005). Analyzing the interaction between facilitator and participants in two variants of the think-aloud method in Professional Communication Conference.

Hafiz, M.D., Abdullah, A.H., Ithnin, N., and Mammi, H.K. (2008). Towards identifying usability and security features of graphical password in knowledge-based authentication technique. In: *Proceedings of the 2nd IEEE Asia International Conference on Modelling & Simulation* (pp. 96–403).

Hair, J., Money, A., and Samouel, P. (2003a). *Essentials of business research*. New York: Wiley.

Hair, JF., Bush, RP., and Ortinau, DJ. (2003b). Marketing research: Within a changing information environment, 2nd edn. McGraw-Hill/ Irwin, New York.

Harcourt, H.(2010). "American Heritage Dictionary, Dictionary of the English Language, Fourth Edition".

Hayes, E. (1998). Measuring customer satisfaction: survey design, use and statistical analysis methods, ASQ Quality Press, Milwaukee.

Healy, M. & Perry, C. (2000). Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. Qualitative Market Research, 3 (3), 118– 126.

Herley, C. and P. C. van Oorschot (2012). A research agenda acknowledging the persistence of passwords, *IEEE Security & Privacy*, *10*(1), pp. 28–36.

Herzberg, A., and Mass, Y. (2001). Relying party credentials framework. In *Topics in Cryptology—CT-RSA 2001* (pp. 328-343). Springer Berlin Heidelberg.

Herzog, A. and N. Shahmerdi (2007). User help techniques for usable security. Proc. CHIMIT 2007, ACM Press, Cambridge, MA, March 30–31, 2007.

Hirschheim, R. (1992). Information Systems Epistemology: A Historical Perspective. In R.D. Galliers (Ed.). Information Systems Research: Issues, Methods and Practical Guidelines. Blackwell Scientific Pub.

Hornbek, K. (2006). Current Practice in measuring usability: Challenges to usability studies and research. *International Journal of Human-Computer Interaction*, 64(2): 79-102.

Hornbek, K. and L. -C. Effie, (2007). Meta-analysis of correlations among usability measures, in Conference on Human Factors in Computing Systems San Jose, California, USA: ACM Press, 617 - 626.

Howitt, O. and Cramer, O. (2008). *Introduction to research methods in psychology*. Harlow: Prentice Hall.

Hussey, J. and Hussey, R. (1997). *Business Research: A practical Guide for Undergraduate and Postgraduate students*. Macmillan Press. London.

Hyde, D. (2012) Feb 6. Hackers crack new online banking security putting 25 m people at risk. *This is Money*. Available from: http://www.thisismoney.co.uk/money/saving/article-2096060/Hackerscrack-new-online-

IEEE. (1990). IEEE standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York: IEEE.

Information Security Breaches Survey. (2014). Department for Business Innovation and Skills. Technical report. Available online: http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf. Accessed on 02/10/2014.

ISO. (1998). Ergonomic requirements for office work with visual display terminals(VDTs)- PartII: Guidance on usability. Geneva, Switzerland: International Organisation for Standardisation.

ISO/IEC. (2001). Software Engineering- Product Quality - Part 1: Quality Model. Geneva, Switzerland: International Organisation for Standardisation.

ISO/IEC 27002 (2007): Information Technology – Security Techniques – Code of Practice for Information Security Management. ISO/IEC, 8, 9.

ISO/IEC 27002.(2008).Organization International Standards. Change.

Jaäskeläinen, R. (2001). Think-aloud protocols. In *Routeledge Encyclopedia of Translation Studies*, pages 269–273. Routeledge.

Jaros, D. and Kuchta,R. (2010). "New Location Based Authentication Techniques in the Access Management", Wireless and Mobile Communications (ICWMC) 6th International Conference, 2010, pp. 426 – 430.

Jeffries, R., Miller, J.R., Wharton, C., and Uyeda, K.M. (1991) . User interface evaluation in the real world: A comparison of four methods. In *ACM CHI'91 Conference Proceedings*, pages 261- 266. ACM.

John, B. E., & Kieras, D. E. (1996). The GOMS family of user interface analysis techniques: Comparison and contrast. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *3*(4), 320-351.

Jørstad, I. and D. V. Thanh (2007). The mobile phone as authentication token, Telenor ASA.

Jones, L.A., Anton, A.I., and Earp, J.B. (2007) Towards understanding user perceptions of authentication technologies. ACM Workshop on Privacy in Electric Society,

Jones, S. Wilikens, M., Morris, P. and Masera, M. (2000). "Trust requirements in e-business", *Communications of the ACM*, Vol. 43 No. 2.

Kainda, R., Flechais, I., Roscoe, A.W. (2010). Security and Usability: Analysis and Evaluation. In: International Conference on ARES 2010, pp. 275–282.

Karat, J. (1988). Software evaluation Methodologies. In: Helander M,editor. Handbook of human computer interaction. Amsterdam: North-Holland;. p. 891- 903.

Karole, A., Saxena, N., and Christin, N. (2010). A comparative usability evaluation of traditional password managers. In International Conference on Information Security and Cryptology (ICISC'10), Seoul, Korea.

Kassim, NM 2001, Determinants of customer satisfaction and retention in the cellular phone market of Malaysia, PhD thesis, Southern Cross University, Lisbon.

Kay R. Biometric Authentication. *ComputerWorld.* April 4, 2005. http://www.computerworld.com/article/2556908/security0/biometric-authentication.html Accessed January 5, 2016.

Keller, J. and Keller, B. (1989). *Motivational delivery checklist*. Florida State University.

Keith, M., Shao, B. and Steinbart. P. J. (2007). The usability of passphrases for

authentication: An empirical field study. International journal of human-computer studies, 65(1):17–28.

Kieras, D.E. (2007). Model-based evaluation. In J. Jacko & A. Sears , *The Human-Computer Interaction Handbook* (2nd Ed). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Krejcie, RV. And Morgan, DW. (1970). *"Determining Sample Size for Research Activities*". *Educational and Psychological Measurement*, #30, pp. 607-610.

Kieras, D. (2003). Model Based Evaluations. In: J.A. Jacko & A. Sears. (Eds), The Human Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications. Mahwah, N.J: Lawrence Erlbaum Associates.

Knight W.(2008). The price of love. Infosecurity. ; 5(1):30–3.

Kolb, N., Bartsch, S. ,Volkamer, M., and Vogt, J.(2014).Capturing attention for warnings about insecure password Fields - systematic development of a passive security intervention. In Human Aspects of Information Security, Privacy, and Trust, pages 172- 182. Springer.

Kothari, C.R. (1990). *Research methodology: Methods and techniques* (Second Revised Edition). New Age International Publisher.

Krol, K., Philippou,E., De Cristofaro, E., Sasse, M.A.(2015). 'They brought in the horrible key ring thing!" analysing the usability of two-factor authentication in UK online banking. In:USEC 2015: NDSS Workshop on Usable Security, San Diego, CA,USA.

Laberge, J., & Caird, J.K. (2000). Trusting the online banking interface: Development of a conceptual model relevant to E-commerce transactions. Designing Interactive Systems for 1-to-1 E-commerce Workshop at the ACM SIG CHI

Conference'00, The Hague, Netherlands. accessed on the 2/12/14 at http://www.zurich.ibm.com/~mrs/chi2000/contributions/laberge.rtf

Land, F. (1992). The Information Systems Domain. In R.D. Galliers(Ed). *Information Systems Research: Issues ,Methods and Practical Guidelines.* Blackwell Scientific Publications. ISBN: 0632028645.

Lanford, P. (2006). E-commerce: a trust perspective. In Proceeding. of the 2006 international conference on semantic web and web services, the 2006 world congress in computer science, computer engineering, and applied, computing.

Lazar J., Feng J.H., and Hochheiser, H. (2010). *Research methods in human-computer interaction*. Wiley, New York.

Lee, L. Bauer, and M. L. Mazurek. 2015. The effectiveness of security images in Internet banking. *IEEE Internet Computing* 19, 1.

Lewis, C. & Rieman, J. (1994). Task-centred User Interface Design. [On-line]. Available: ftp://ftp.cs.colorado.edu Accessed on 23/05/2014.

Lewis, J. (2006). Usability Testing. In G. Salvendy(ed.). *Handbook of Human Factors and Ergonomics*. Hoboken, NJ: John Wiley.

Likert R. (1932). *A technique for the measurement of attitudes*. Archives of Psychology 1932;140.

Luck, D. and Rubin, R. (1987). *Marketing research*. 7th edn, Prentice-Hall international, New Jersey.

Ma,Y., and Feng, J. (2011). Evaluating usability of three authentication methods in web-based application. Ninth International Conference on Software Engineering Research, Management and Application. August 2011. Baltimore, MD.

Malhotra, NK. (1999). *Marketing research: An applied orientation*, 3rd edn, Prentice Hall, NewJersey.

Mannan, M., and Oorschot, V. (2007). Security and usability: The gap in real-world online banking. In: *Proceedings New Security Paradigms Workshop* (NSPW'07), New Hampshire, US.

Marshall, C. and Rossman, G. (1999). Designing Qualitative Research. Newbury Park, CA: Sage.

Matera, M., Rizzo, F., and Carughi, G. (2006). "Web Usability: Principles and Evaluation Methods. In Mendes, E. and Mosley, N. (ed). *Web Engineering*. Berlin: Springer, pp. 143- 180.

Matsubara, Y. and Nagamachi, M. (1996). A comparative study of two usability evaluation methods using a web-based e-learning application. In: Claude Frasson et al. (eds.), Motivation systems and motivation models for intelligent tutoring, in *Proceedings of the Third International Conference in Intelligent Tutoring Systems* (pp. 139–147).

Maxwell, J. A., & Mittapalli, K. (2007). The value of critical realism for qualitative research. *International Association for Critical Realism, 13*.

Mayer, R.C., Davis, J.H., and Shoorman, F.D. (1995) An Integrative Model of Organizational Trust, *Academy of Management Review*, 20(3), pp. 709-734

Microsoft Corporation. (2005). Strong Passwords: How to Create and Use Them.

Mockel, C. (2008). *European B2C E-Commerce in the banking sector*. Diplomica, Hamburg.

Moeckel, C. (2011). Human-computer interaction for security research: The case of

EU E-Banking systems. Human-Computer Interaction – INTERACT 2011. 6949, pp. 406–409.

Mohan RB. (2015). Patent application title: Authentication Utilizing A Dynamic Passcode From A User-Defined Formula Based On A Changing Parameter Value. *Patentdocs.* [Accessed January 5, 2016] from: http://www.patentsencyclopedia.com/app/20150163218

Monrose, F. and Reiter, M. (2005). Graphical passwords. In Carnor ,L. and Grafinkel,S.eds. *Usability and Security*. O'Reilly,pp. 147 -164.

Nielsen, J.(1992). Finding usability problems through heuristic evaluation. In *ACM CHI'92 Conference Proceedings*, pages 373-380. ACM

Nielsen, J.(1993). Usability engineering. San Francisco: Morgan Kaufmann.

Nielsen, J. (1996). Usability metrics: Tracking interface improvements. IEEE software,13(6), pp.12–13.

Nielsen, J. and Mohlich, R.(1990). Heuristic Evaluation of User Interfaces. In *Proceedings of ACM CHI '90 Conference.*

Nilsson, M., Adams, A., and Herd, S. (2005). Building security and trust in online banking. In: *Extended abstracts on human factors in computing systems* (pp. 1701–04) (CHI '05). New York, NY, ACM Press.

Nodder, C. (2005). Users and trust: a microsoft case study. In: Cranor,Garfinkel, editors. Security and usability. O'Reilly; p. 589–606 [chapter 29].

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), pp. 2019-2040.

Office for National Statistic (2015). Internet Users 2015. Accessed online .

http://www.ons.gov.uk/ons/dcp171778_404497.pdf

Oluoch, SJ. (2014). Improving Password Security Using Location –Based Intelligence. *International Journal of Scientific and Research Publications*. 2014, 4(2).

Oppenheim, A.N. (1992). *Questionnaire design, interviewing and attitude measurement*. London: Pinter Publishers.

Orlikowski, W.J. & Baroudi, J.J., 1991. Studying information technology in organizations: Research approaches and assumptions. Information Systems Research, 2, pp.1–28.

Pallant, J. (2001). SPSS survival manual: a step by step to data analysis using SPSS, Allen & Unwin, Australia.

Parasuraman, A. (1991). *Marketing research*, 2nd ed, Addison Wesley, Massachusetts

Paul, C., Morse, E., Zhang, A., Choong, Y.Y., and Theofanos, M. (2011). A field study of user behavior and perceptions in smartcard authentication. Human-Computer Interaction – INTERACT 2011, Lecture Notes in Computer Science. 6949, pp. 1–17.

Payne, B. and Edwards, K. (2008). A Brief Introduction to Usable Security. Internet Computing, IEEE, 12(3):13–21.

Pfleeger, C., and Pfleeger S., (2006). *Security in Computing*. Prentice Hall PTR.

Pieratti, D. (2005). Xerox company document: society for technical communication.[Online] Available at: http://www.stcsig.org/usability/resources/toolkit/brochur4.doc [Accessed on15 February 2010].

Png, I. P., Tan, B. C., & Wee, K. L. (2001). Dimensions of national culture and corporate adoption of IT infrastructure. *Engineering Management, IEEE Transactions on*, *48*(1), 36-45.

Preece, J. (1993). A Guide to Usability: Human Factors in Computing. The Open University: Addison-Wesley.

Preece, J., Rogers, Y., Sharp, H., Benyono, D., Holland, S., and Carey, T.(1994). *Human-Computer Interaction*. Reading, MA: Addison-Wesley.

Preece, J., Rogers, Y. & Sharp, H. (2002). Interaction Design: Beyond Human-Computer Interaction. New York: John Wiley & Sons.

Punch, K.F. (2005). Introduction to Social Research: Quantitative and Qualitative Approaches. London,SAGE Publications Ltd.

Quesenbery, W. (2010). Storytelling for User Experience: Crafting Stories for Better Design, 1 ed.: Rosenfeld Media.

Renaud, K. (2004). Quantifying the quality of web authentication mechanisms: A usability perspective. *Journal of Web Engineering*, *3*, pp. 95–123.

Renaud, K. (2005). "Evaluating authentication mechanisms". *Security and Usability: Designing Secure Systems that People Can Use, ed: O'Reilly Media* ,pp. 103-128.

Research Advisor (2006). Sample size table. Retrieved December 2014 from http://www.research-advisors.com/tools/SampleSize.htm

Ridings, C.M., Gefen, D. and Arinze, B. (2002), "Some antecedents and effects of trust in virtual communities", Journal of Strategic Information Systems, Vol. 11, pp. 271-95.

Rittenhouse, R.G. , Chaudry, J.A. and Lee, M. (2013) ."Security in Graphical

Authentication", International Journal of Security and Its Applications, Vol. 7, No. 3, pp. 347-356, May 2013.

Robinson, P., Shaver, R., and Wrightsman, S. (1991). Criteria for scale selection and evaluation. *Paper presented at the Measures of personality and social psychological attitudes, Academic Press*, New York.

Rogers, Y. (2004). New Theoretical Approaches for Human-Computer Interaction. *Annual review of information science and technology*, 38(1).

Rosenthal, R., and Rosnow, R. L. (1991). *Essentials of behavioral research: Methods and data analysis* (2nd ed.). New York: McGraw-Hill, Inc.

Rouse, M. (2014). Secure Sockets Layer (SSL) definition. Available at :http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL [Accessed on 12/12/2014]

Sabzevar, A.P., Angelos Stavrou. (2008) Universal Multi-Factor Authentication Using Graphical Passwords. SITIS '08 Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems. Pages 625 -632 [Accessed on 12/08/14]Retrieved from http:://Cciteseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.156.541&rep=rep1&type=pdf

Sasse, M. A., Brostoff, S., and Weirich, D. (2001). Transforming the 'weakest link' – A human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), pp. 122–131.

Saunders, M., Lewis, P. & Thornhill, A. (2007). Research methods for business students (4th Ed.). Essex, England: Pearson Education.

Saunders, M.,Lewis,P. and Thornhill, A.(2009). Research Methods for Business Students. (5th Ed) (London:Pitman).

Scandura, A., & Williams, E. (2000). Research Methodology in Management: Current Practices, Trends and Implication for Future Research. Academy of Management Journal, 143 (6), 1248-1264.

Schechter, J. (2013). Deductive reasoning. *Encyclopedia of the Mind, SAGE Publishing*.

Schwandt, T. (2003). Three epistemological stances for qualitative inquiry. In N. Denzin & Y. Lincoln (Eds.), The Landscape of Qualitatii'e Research (pp. 292-331).Thousand Oaks, CA: Sage.

Sears, David O. (1989). "College Sophomores in the Laboratory: Influence of a Narrow Data Base on Social Psychology's View of Human Nature." *Journal of Personality and Social Psychology* 51: 515-530.

Sears, A. & D. Hess, 1999. Cognitive Walkthroughs: Understanding the effect of task description detail on evaluator performance. International Journal of Human-Computer Interaction, 11(3), 185-200.

Seifert, C., Welch, I. & Komisarczuk, P. (2006) 'Effectiveness of security by admonition: a case study security warnings in a web browser setting', *secure Magazine*, pp. 1-9.

Sekaran, U. (2003). *Research methods for business: A skill-building approach* (4th Ed.). new York: John Wiley & Sons, Inc.

Shackel, B. (1991) Usability: Context, Framework, Definition, Design and Evaluation. In: B. Shackel & S. Richardson. (Eds), Human Factors for Informatics Usability. London: Cambridge University Press.

Shah, M. and Clarke, S. (2009). "E-banking Management: Issues, Solutions, and

Strategies", Idea Group Inc(IGI) publisher, New York

Shah SU, e-Hadi F, Minhas AA.(2009). New Factor of Authentication: Something You Process. *International Conference on Future Computer and Communication,* 2009. doi: 10.1109/ICFCC.2009.79.

Sharek, D.,Swofford, C. & Wogalter, M. (2008) 'Failure to Recognize Fake Internet Popup Warning Messages', *Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting,* pp. 557-580.

Shepard,R. N.(1967). "Recognition memory for words, sentences, and pictures", Verbal Learning & Verbal Behavior, 6(1), 1967, pp156-163.

Shneiderman, B. & Plaisant, C. (2005). Designing the User Interface: Strategies for Effective Human-Computer Interaction. 4th Ed. New York: Addison-Wesley.

Smetters, D. K. and Grinter, R. E. (2002). Moving from the design of usable security technologies to the design of useful secure applications. *In the Proceedings of the 2002 workshop on New Security Paradigms*. Virginia Beach, Virginia: ACM, PP. 82 – 89.

Soghoian,C. and Stamm,S. (2010). Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL. In *Proc. of HotPETS.*

Soucy, K. (2010). Unmoderated, Remote Usability Testing : Good or Evil?. Available online [Accessed 12 -01-2016] at http://www.uxmatters.com/mt/archives/2010/01/unmoderated-remote-usability-testing-good-or-evil.php

Ssemugabi, S. and de Villiers, R. (2007). A comparative study of two usability evaluation methods using a web-based e-learning application. Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, pp.132–142. ACM.

Ssemugabi, S. and de Villiers, R. (2010). Effectiveness of heuristic evaluation in usability evaluation of e-learning applications in higher education. Sacjcsuctacza,pp26–39.

Streubert, H. & Carpenter, D. (1999). Qualitative research in nursing: Advancing the humanistic imperative, (2nd Ed.). Philadelphia: Lippincott.

Sue, V.M., and Ritter, L.A. (2007). Conducting online surveys. Thousand Oaks, CA: Sage.

Summers, W.C. and Bosworth, E. (2004). Password policy: the good, the bad, and the ugly. ACM International Conference Proceeding Series; Proceedings of the Winter International Symposium on Information and Communication Technologies 58, 1–6

Suo,X. , Zhu, Y and Owen, G.Scott. (2007). Graphical Passwords: A survey. 21st annual computer security conference.pp.463 -472.

Suppe, F. (Ed.). (1977). *The structure of scientific theories*. University of Illinois Press.

Tashakkori A. and Creswell J. (2007). The new era of mixed methods. Journal of Mixed Methods Research, 1,3-7.

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches.* Applied Social Research Meth- ods Series (Vol. 46). Thousand Oaks, CA: Sage.

Taterh, S., Yadav, K. and Sharma, S.(2012). Threat Modeling and Security Pattern used in Design Phase of Secure Software Development life Cycle. International Journal of Advanced Research Computer Science and Software

Engineering. Vol 2 (4). ISSN: 2277128x.

Te'eni, D., Carey, J. and Zhang, P.(2007). Human Computer Interaction: Developing Effective Organizational Information Systems, John Wiley & Sons, Hoboken.

Thigpen, S. (2005). Authentication Methods Used for Banking. *East Carolina University*.

Towhidi, F., Manaf, A. A. ; Daud, S. M. and Lashkari,A. H. (2011). "The Knowledge Based Authentication Attacks", in World Congress in Computer Science.

Turner, C., Nielsen, J. & Lewis, J. (2006). Determining Usability Test Sample Size. International Encyclopedia of Ergonmics and Human Factors.

UK Cards Association (2014). Decline in fraud losses stalled by rise in deception crimes aimed at consumers, [Online] Retrieved May 19, 2014 from: http://www.theukcardsassociation.org.uk/news/FYFF2012.asp

Vacca, J, ed. (2013). *Network and System Security*. Oxford: Elsevier.

Veal, A. J. (2005). *Business research methods: A managerial approach* (2nd Ed.). Australia: Pearson Education Australia.

Vijayasarathy, L.R. (2004) . Predicting consumer intentions to use online shopping: The case for an augmented technology acceptance model. Information and Management. 41(6), pp. 747–762.

Voice, C. (2005). Online authentication: matching security levels to the risk. *Network Security, 2005*(12), 15-18.

Weber, R. (1990). Basic content analysis (2nd ed.). Newbury Park, CA: Sage.

Weir, C.S., Douglas, D., Carruthers, M., and Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, *28*(1).

Weir, C.S., Douglas, G., Richardson, T., and Jack, M. (2010). Usable security: User preferences for authentication methods in ebanking and the effects of experience. *Interacting with Computers*, *22*(3).

Weir, G.R.S. and Zonidis, N. (2005) *Desktop security as a three-dimensional problem.* KM ITL science and technology journal, 5 (1). pp. 292-302. ISSN 1905-2367

Weisberg, F., Jon, A., Bruce, D (1996). *An Introduction to Survey Research, Polling, and Data Analysis*, Thousand Oaks, CA: Sage.

Whitelock, D. and Scanlon, E. (1996). Motivation, media and motion: Reviewing a computer-supported collaborative learning experience. Pp. 276–283. Edicoes Colibri.

Whalen, T. & Inkpen, K. M. (2005) 'Gathering evidence: use of visual security cues in web browsers', *Proceedings of Graphics Interface 2005*. Victoria, British Columbia Canadian Human-Computer Communications Society, ACM, pp. 137-144.

Whitten, A., and Tygar, J.D. (1999). Why Johnny can't encrypt: A usability evaluation of pgp 5.0. In: *Proceedings of the 8th USENIX Security Symposium, 99,* McGraw-Hill.

Wilkinson, D. and Birmingham, P. (2003). Using Research Instruments: a Guide for Researchers. Routledge.

Wogalter, M.S.(2006). "Purpose and Scope of Warnings, In *Handbook of Warnings*. (Human Factors / Ergonomics)" (Assoc LE, ED), pp. 3 -9, ISBN 0805847243.

Wolf, C., J. Carroll, T. Landauer, B. John & J. Whiteside, (1989). The role of laboratory experiments in HCI: help, hindrance, or ho-hum?, in ACM SIGCHI Bulletin ACM New York, NY, USA 265 -8

Wool, A. (2004). A Quantitative Study of Firewall Configuration Errors. IEEE Computer.

Wu, M., Miller, R. C. & Garfinkel, S. L. (2006) 'Do security toolbars actually prevent phishing attacks?' Proceedings of the SIGCHI conference on Human Factors in computing systems. Montreal, Quebec, Canada ACM, pp. 601-610.

UEA. (2011). University of East Anglia, RESEARCH ETHICS POLICY, PRINCIPLES AND PROCEDURES. Available online https://intranet.uea.ac.uk:443/commercialisation/rs/resethics (accessed 8 July 2014)

US Secret Service, National Threat Assessment Ctr and CSO Magazine. (2014). US Cybercrime: Rising Risks, Reduced Readiness Key Findings from the 2014 US State of Cybercrime Survey. Available at: http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf [Accessed on 13/12/2014].

Yan, J. A. Blackwell, R. Anderson, and A. Grant, (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy*, pp. 25–31

Yang, W.H., and Shieh, S.P. (1999). "Password authentication schemes with smart cards". *Computers & Security*, Vol. 18, pp. 727 – 733.

Zaaba, Z. F., Furnell, S. M., and Dowland, P. S. (2014). A study on improving

security warnings. In *Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on* (pp. 1-5). IEEE.

Zaharias, P. (2004). Developing Usability Evaluation Methods for E-Learning Applications: From Functional Usability to Motivation to Learn. Journal of Human Computer Interaction, [accessed 12-02- 2014] from http://dmst.aueb.gr/en2/diafora2/Phd_thesis/Zaharias.pdf

Zamir, S. (2014). Research Methodology. Available on line on http://www.slideshare.net/shaziazamir3/week-1research-methodology [accessed 25 -08-2016].

Zaphiris, P.and Kurniawan, S. (2006). Human Computer Interaction Research in Web Design and Evaluation: Idea Group Publishing.

Zhang,F. , Kondoro,A. and Muftic,S. (2012). "Location-Based Authentication and Authorization Using Smart Phones," in *Proceedings of 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*.