10

Developing a Theoretical Framework for the Adoption of Biometrics in M-Government Applications Using Grounded Theory

Thamer Alhussain[1] and Steve Drew[2]
[1]*King Faisal University,*
[2]*Griffith University,*
[1]*Saudi Arabia*
[2]*Australia*

1. Introduction

Mobile devices have become the world's most common means of interpersonal communication; and, the growing marketplace for new software, or "apps", enriches an already burgeoning array of purposes to which mobile technology can be lent. We are thus witnessing the advent of conditions for a range of mobile technology enabled information systems. According to the latest statistics produced by the Central Intelligence Agency (CIA), there were 5.3 billion mobile subscriptions worldwide in 2010 out of a world population of about 7 billion people (World Fact Book 2011). With the advancements in mobile technologies, several governments have started looking to provide their services via wireless and mobile devices. Mobile government (m-government) is a new delivery channel using Information and Communication Technology to deliver and improve government services that complements current e-government (Antovski and Gusev 2005). Currently, a number of m-government applications exist in several countries around the world. With the growth of m-government services, the importance of security for its acceptance and adoption has been noted in many studies (NECCC 2001; Al-khamayseh et al. 2006; Clarke and Furnell 2005, 2007). Requirements for user acceptance lead to a greater need for user and government authentication to protect data, services, and the promotion of public trust. The negative security perception is a serious issue that citizens have regarding the use of mobile services which may affect their adoption of the technology for critical applications (Chang and Kannan 2002).

This chapter will describe an enquiry into how biometric technology, which can provide reliable user authentication, can play an integral role in providing secure m-government services. We use Grounded Theory methodology to understand reality from the point of view of the participants including mobile users, service providers, and network operators in order to develop a substantive theory for the adoption of biometric authentication in m-government security. In the field of information systems, Urquhart et al. (2009) indicated that Grounded Theory has been proved to be extremely useful in this field which led them to recommend its application to help generate theories in information systems.

This chapter provides unique perspective on investigating the adoption of biometric authentication in the context of mobile government applications, taking into account requirements and opinions of the people involved in m-government including mobile users, service providers, and network operators. This chapter addresses a gap in the literature regarding the factors influencing the adoption of biometric authentication in m-government security. The main contribution of this chapter is the development of a new substantive theory that provides a theoretical framework for the factors influencing this technology's adoption. Thus, it provides rich insights and increased understanding of the concerns and perceptions of the abovementioned stakeholders regarding the application of biometric authentication to mobile devices for government services. Moreover, this chapter provides a new example of the application of Grounded Theory methodology to qualitative information systems research.

This chapter is structured as follows. It begins with a brief background relating to the information security and mobile government. Next, the chapter discusses the adoption of biometric technology within the context of electronic and mobile government. The chapter then explains and justifies the methodological choices along with the description of Grounded Theory methodology. The chapter also explains the context of the study presented in this chapter in addition to the data collection procedures. The application of Grounded Theory is then detailed and described. Finally, the paper concludes by developing a new theoretical framework for factors influencing the adoption of biometric authentication in m-government security and providing several considerations for the adoption of biometrics in m-government applications.

2. Information security and m-government

The primary entities of m-government are mobile phone users, government agencies as service providers, and the network operators. Although they have several different requirements, they share security as one of the most important system requirements. As mentioned above, security is the most important issue facing m-government applications and it is a basic feature of the mobile communication infrastructure. Specifically, security has five features that need to be considered, which are user authentication, data integrity, service availability, information confidentiality, and non-repudiation of user participation in transactions. A biometric system enhances the identification, authentication and non-repudiation of the information's user to support facets of information security. It can help "to provide identity-based access control and to authenticate integrity of information with respect to subject involved" (Vielhauer 2006, p. 18).

2.1 Authentication strategies

There are three general categories of authentication as follows:

- Something the user knows (e.g. PIN or password).
- Something the user has (e.g. cards or tokens).
- Something the user is (e.g. biometrics).

The Personal Identification Number (PIN) is a secret-knowledge authentication method and consequently relies upon knowledge that only the authorized user has. Although the PIN

and password are the most commonly used methods for authentication in information systems (Scott et al. 2005), such secret-knowledge approaches unfortunately have long-established problems, with weaknesses often being introduced by the authorized users themselves. These are most clearly documented in relation to passwords, with bad practices including the selection of weak and easily guessable strings, sharing passwords with other people, writing them down where others can find them, and never changing them (Clarke and Furnell 2005). Consequently, these approaches are the easiest targets for hackers.

A security token is a physical entity or item that an individual possesses to establish personal identification, such as a passport, ID card, or credit card (Jain et al. 2000). This token based approach is approximately similar to the secret knowledge approach, as it basically relies upon the user remembering to bring along something to ensure security whereby the token needs to be physically present (Clarke and Furnell 2007). Therefore, secret knowledge and token based authentication approaches are unsatisfactory methods of achieving the security requirements of information systems, as they are unable to differentiate between an authorized and an unauthorized person who fraudulently acquires the knowledge or token of the authorized person (Jain et al. 2000). On the other hand, biometric authentication relies upon the unique physiological and behavioural characteristics of an individual; hence, it cannot be forgotten, lost or stolen.

2.2 The current authentication system in m-government

The current security method in mobile phone based m-government applications is based on the use of 4 to 8 digit Personal Identification Numbers (PINs). This method can be applied to both the mobile device and the user's Subscriber Identity Module (SIM) which is a removable token containing the cryptographic keys required for network authentication. As mentioned above, the PIN is an approach providing low level authentication, as it is based on something the user knows. However, the existing SIM card, a token based approach, can be physically removed from the mobile device when not in use; however, users usually leave it inside the mobile device for convenience as well as to avoid loss or damage (Clarke and Furnell 2007). Thus, the PIN and SIM card approached carry the risk of loss or theft which can compromise the security of information, especially with the inclusion of sensitive personal information which confirms the need of advanced approach for ensuring and enhancing the security of data in mobile devices.

Providers of second generation (2G) and third generation (3G) mobile networks deliver smartcards with pre-installed symmetric keys which are used by the network to authenticate the mobile device and, in the 3G case, for the mobile device to authenticate the access network. The authentication system is based on the trust relationship that exists between the access network provider and the service provider via a roaming agreement, and between the user and the service provider via the service subscription. The symmetric session keys for data confidentiality and integrity sent over the airwaves are derived during the authentication process. However, data confidentiality and integrity extending over the whole path between the communicating parties is not provided by the access network security of second and third generation systems which has to be provided on the network at application levels for end-to-end security (Dankers et al. 2004). With this in mind, Public Key Infrastructure (PKI) combined with biometric authentication may present a suitable integrated solution to achieve end-to-end m-government security.

2.3 Biometrics and m-government

Integrating biometric authentication into mobile devices can be done in two different ways. The first technique is to store the biometric template in an external database (Giarimi and Magnusson 2002). In this case, the biometric data have to be sent over the network every time the user wants to be verified and, during that process, the data are encrypted, which forms the external database for storage rather than security. The problem is that the users have no control over their own biometric pattern once it leaves the device. Furthermore, it can potentially take a long time to perform verification when data are being sent over the mobile network due to traffic overload and the number and size of the files in transit. However, it does not take up much memory in the mobile device. The second technique is to store the biometric template in the device or particularly on the smart card which will enable users to control their biometric pattern (Giarimi and Magnusson 2002). The biometric verification should take place when the users want to log in to their mobile device and when they want to perform a government service. Moreover, this can be integrated with the Public Key Infrastructure, as mentioned earlier, to provide a more secure authentication system.

3. Adoption of biometric technology

With the advantage of reliable authentication of biometric technology, many security applications around the world have adopted and implemented biometric technology. Currently, biometric technology has been adopted in many applications such as access control, national identity, immigration, proving attendance, military identification, e-government, and e-commerce applications.

With the application of biometric technology, e-government aims to give its citizens improved services and better access to information as it can provide reliable identification of individuals as well as the ability for controlling and protecting the integrity of sensitive data stored in information systems. Many researchers such as Ashbourn (2004), Bonsor and Johnson (2008), Scott et al. (2005), and Wayman et al. (2005) argue that a wider use of biometric technology can be applied to e-government projects. With variations on attendance registration mentioned above, biometric technology is used for e-voting to ensure that voters do not vote twice. With biometric technology, governments prevent fraud during elections. Moreover, biometric technology can be used to ensure correct working times are recorded and that only authorized personnel have access to government property and resources.

Biometric technology can also be used by e-governments for business. For instance, many banks use facial recognition systems to minimise chances of theft. For example, photos are taken on the bank slips which are stored on computer software. As a result, this has avoided the issue of fraudulent bank slips when withdrawing money, since ATMs are a quick method of withdrawing money. This has helped the government to conduct its activities effectively (Bonsor and Johnson 2008).

In business, there is frequently the need for full identification of employees to ensure that, in case of any problem in that firm, the management is in a position to identify the person responsible for that act. Commercial applications may also require full identification capability, digital certificates, human interface, and one or more authentication devices to ensure that the business can run well. People are also in a position to do their business

properly and invest in any organisation as long as that organisation has an identity as an effective company (Ashbourn 2004).

Biometric technology is also used in the identification of citizens by e-governments. If they choose, every nation should ethically be able to identify its citizens and non-citizens by using national identification cards, visas, and passports. As a result, e-governments are in a position to identify its citizens in the production of these documents, hence reducing the issue of illegal immigration. A good example is the United States whereby, since the events of September 11 2001, it has widely adopted biometric technology. Two laws, relating to identification of transport workers and to immigrants, were made in the United States triggering a mass deployment of biometrics. Now, seven million transportation employees in the United States have biometrics incorporated into their ID cards. Moreover, in order to closely control visitors who enter and leave the country, all foreign visitors are required to present valid passports with biometric data; consequently, over 500 million U.S. visitors have to carry border-crossing documents which incorporate biometrics (Ashbourn 2004). Several European governments have also started to implement the use of biometrics. The U.K. government has established issuing asylum seekers with identification smart cards storing two fingerprints. General plans have also been made to extend the use of biometric technology throughout the visa system in the U.K. as well as in France, Germany and Italy (Scott et al. 2005).

E-governments use the various types of biometric identification in order to control certain illegal behaviour. For example, the Japanese government plans to use biometric technology in passports to tackle illegal immigration and to enable tighter controls on terrorists. This will be applied within a computer chip which can store biometric features like fingerprints and facial recognition data (Scott et al. 2005).

Other e-governments are using the biometric technology to secure access to certain defence bases and similarly secure areas. Biometrics can also provide potential for security cost savings. For instance, hand recognition has been used at the Scott Air Force Base to save more than $400,000 in manpower costs through their metro-link biometric access gate (Frees 2008).

3.1 Technology adoption factors among empirical studies

Empirical studies related to the acceptance and adoption of mobile phones and electronic services via the Internet have mostly applied models based on the use of Diffusion of Innovation (Rogers 1995), the Technology Acceptance Model (Davis 1989), or the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al. 2003). For instance, Jahangir and Begum (2008) introduced a conceptual framework that considered perceived usefulness, ease of use, as well as security and privacy as important factors that influence users' acceptance and adoption of electronic banking services. Another study by Tassabehji and Elliman (2006) highlighted trust and security as major factors affecting e-government adoption. Moreover, AlShihi (2007) indicated that trust has a wide impact on m-government acceptance. Lee et al. (2002) found that social influence and self-efficacy variables significantly affect perceived usefulness and perceived ease of use for user acceptance of the mobile Internet. Moreover, Teo and Pok (2003) found that social factors including perceptions of relative advantage play a significant role in influencing intentions for the adoption of Wireless Application Protocol WAP-enabled mobile phones amongst Internet

users. Kaasinen (2007) found that perceived value, ease of use, trust and ease of adoption are important factors that influence user acceptance of mobile Internet services. AlGhamdi et al. (2011) pointed out that the provision of trustworthy and secure online payment options is a critical key determining the decision for online customers to accept/reject buying online from a specific retailer.

Thus, highly similar acceptance factors appear under various theories and models covering innovation acceptance and adoption. Moreover, the set of factors that proposed in TAM variants and UTAUT correspond closely with factors identified in DOI theory. For instance, Moore and Benbasat (1991) indicated that while developing an instrument based on DOI concepts to determine an individual's perceptions regarding the acceptance and adoption of an information technology innovation recognised the similarity between the construct of perceived usefulness with perceived relative advantage, and between perceived ease of use with perceived complexity.

3.2 Biometric adoption among empirical studies

Although there are a lack of academic studies concentrating on the factors that influence the adoption of biometric authentication systems, most of the published papers in this area (Harris and Yen 2002; Kleist et al. 2005; Lease 2005; Uzoka and Ndzinge 2009) identified different factors that are quite dissimilar to those discussed in the technology adoption theories and models outlined in previous section. For example, Lease (2005) found that managers' positive perceptions of security effectiveness, need, reliability, and cost-effectiveness correlate with their willingness to recommend the use of biometric technology, while Uzoka and Ndzinge (2009) indicated that ease of use, communication, and size and type of organisation are the most important factors affecting the intention to adopt biometric technology in organisations. However, Harris and Yen (2002) stated that the adoption of biometric systems can be influenced by managerial, economical, operational and process-related factors. Kleist et al. (2005) also indicated different affecting factors of biometric systems including users, administration, environment, infrastructure, cost, communication system, as well as security needs and requirements.

As a result, the review of the relevant literature on the technology adoption factors did not lead to any hypotheses, but rather helped to enhance awareness of the existing factors and to identify the gap in relevant knowledge. The case in this chapter discusses the adoption of biometric authentication in the m-government context and in particular, in Saudi Arabia, which adds some specificity to the area of biometric technology adoption.

4. Methodological choices

A review of the extant literature on theories relating to authentication and mobile government security also did not lead to any hypotheses per se, but broadened the considerations relevant to this work. What was needed was a method for determining the full range of stakeholder considerations that would influence the adoption of m-government with biometric security. A review of methods available for an interpretive study with the main purpose of creating a substantive theory to guide development, indicated that Grounded Theory methodology (Strauss and Corbin 1990) was the ideal vehicle for investigating actualities from the real world to generate or discover theory grounded in context specific data that has been systematically gathered and analysed (Creswell, 1998).

The investigation part of this study was carried out by the use of questionnaire and semi-structured interviews for the data collection. By conducting the interviews and questionnaires, we explored the factors influencing the adoption of biometrics in m-government through the concerns and perceptions of mobile communication users', service providers', and network operators' about applying biometric authentication into mobile devices for government services. Data were analysed following Strauss and Corbin's (1990) approach of Grounded Theory. The use of Grounded Theory helped to develop a substantive theory that identifies and describes the factors influencing the adoption of biometric authentication in m-government in Saudi Arabia.

4.1 Grounded theory methodology

Grounded Theory is one of the most widely used methodologies in qualitative research (McLeod 1999). It originated in nursing research by Glaser and Strauss (1967) and then has been adopted in several areas of research such as sociology, business, management, and information systems (Mansourian 2006). More specifically, Grounded Theory was first developed by Barney Glaser and Anselm Strauss in 1967 in their book "The Discovery of Grounded Theory". They defined Grounded Theory as "the discovery of theory from data – systematically obtained and analysed in social research" (Glaser and Strauss 1967, p. 1).

In subsequent years two different approaches of Grounded Theory have emerged, one by Glaser and the other by Strauss and Corbin. These two approaches became more visible by the publication of Strauss and Corbin's book in 1990. The Grounded Theory approach, according to Strauss and Corbin (1990), is a "qualitative research method that uses a systematic set of procedures to develop an inductively derived Grounded Theory about a phenomenon" (p. 24). However, Glaser (1992) clarified that "Grounded Theory is based on the systematic generating of theory from data, that itself is systematically obtained from social research" (p. 2).

Glaser (1992) thought that the research should allow the theory to emerge during the observation of the codes and data analysis. Glaser's approach concerns with a classic philosophy emphasizing an inductive emergence of the theory as well as the researcher's role within that process (Heath and Cowley, 2004). Glaser (1992) focuses on the importance of letting the theory emerge from the data by allowing the data to speak for itself and avoiding imprinting preconceived ideas onto the theory (Creswell 2008). By contrast, Strauss and Corbin's (1990) perspective emphasised more on a systematic approach involving validity and verification (Heath and Cowley, 2004). Strauss and Corbin's (1990) approach indicated that Grounded Theory should be inductively derived from the study of the phenomenon it represents. It should be discovered, developed, and verified through systematic data collection and analysis of the data that pertaining to the phenomenon.

It emerges that the Strauss and Corbin (1990) approach is significantly more prescriptive in specifying the steps to be done during the coding and data analysis. More specifically, Strauss and Corbin (1994) identified Grounded Theory as "a general methodology for developing theory that is grounded in data systematically gathered and analysed. Theory evolves during actual research, and it does this through continuous interplay between analysis and data collection" (Strauss and Corbin 1994, p. 273).

Glaser (1992) and Strauss and Corbin (1990) differed on the role of the literature review as an influence on the methodology. Glaser (1992) believed that specific reading related to the area under study before or during data collection could strongly influence the emerging theory, thus, it should not be reviewed until the theory begins to emerge. While Strauss and Corbin (1990) believed that the researcher will come to the research area with a background about the relevant literature which is a basis of professional knowledge and it is important to acknowledge and use it, as will be discussed in the next section. They believe that some understanding of the research area through the literature review will enhance the theoretical sensitivity of the researcher when generating theory.

However, Grounded Theory has been presented as a general methodology applicable for both qualitative and quantitative studies (Strauss and Corbin 1994). Strauss and Corbin (1998, p.27) stated that "briefly, we maintain that the aim of theorizing is to develop useful theories. So, any methodology, whether qualitative or quantitative, is only a means for accomplishing that aim. We do not believe in the primacy of either mode of doing research"

The study related in this chapter adopted Grounded Theory methodology to develop a substantive theory for the adoption of biometric authentication in m-government security in Saudi Arabia. In particular, this study followed Strauss and Corbin's (1990) approach as it allows researchers to take into account previous relevant theories and literatures to help gain insights into the data. It also provides extensive guidance and a comprehensive framework for researchers, while, Glaser's approach is much less structured. Further justifications for the use of Grounded Theory are provided in the following section.

4.2 Justification for using grounded theory

According to Goulding (2002), the usefulness of the application of Grounded Theory appears where there is a lack of integrated theory in the literature. From the initial literature review provided in the earlier in the chapter, it can be noted that there was a lack existing theories regarding the utilization of biometric authentication and mobile government security, especially which might be applied in developing countries such as Saudi Arabia. Combining this finding with the main application of Grounded Theory for investigating actualities in the real world, the researchers use Grounded Theory to develop a substantive theory that describes how biometric authentication can play an integral role in providing secure m-government services by investigating the phenomenon within the real world entities involved in m-government which are mobile users, service providers, and network operators.

Moreover, comparing with other qualitative analysis methods, Grounded Theory provides systematic method of analysis including open, axial, and selective coding that helps to develop a theory that is grounded in data. This is consistent with Charmaz's (2006) indication that the main strength of Grounded Theory is that it provides means for the analyzing processes including specific steps for developing concepts, categories, and theory. Piantanada et al. (2002) point out the usefulness of the Grounded Theory in such interpretive research. They note "the procedures of Grounded Theory provide interpretive researchers with a disciplined process, not simply for generating concepts, but more importantly for coming to see possible and plausible relationships between them" (p. 3).

Urquhart et al. (2009) indicated that Grounded Theory has been proved to be extremely useful in the field of information systems, which led them to recommend its application to

help generate theories in that research area. Furthermore, Urquhart and Fernandez (2006) stated that the value of Grounded Theory in the field of information system has become widely acknowledged in the research community.

Accordingly, the Grounded Theory approach fits the purpose of this study, which should lead to the development of a substantive theory for the adoption of biometric authentication in m-government security in KSA. Through the interviews and questionnaires, the researchers explore the factors that influence the adoption of biometrics in m-government through users', service providers', and network operators' concerns and perceptions regarding applying biometric authentication into mobile devices for government services.

5. Context of the study

This study was supported by Saudi government and data collection primarily took place in the Kingdom of Saudi Arabia. Therefore, Saudi and Islamic cultural issues needed to be considered throughout this study. The Kingdom of Saudi Arabia is located in the south-eastern part of the Asian continent. It occupies 2,240,000 sq km (about 865,000 sq mi). The total population reached 28.5 million in mid-2009 with an annual growth rate of 2.9 percent; however, it is estimated that approximately 5.5 million of the population are non-Saudis (World Fact Book 2011).

The need for the services, means and methods of e-government in Saudi Arabia has emerged by responding to the developments and changes of the modern world in all fields. Saudi Arabia, like other countries, is seeking to make use of the great technological advancements in communication means and information due to their importance in providing services which are better, faster, more accurate, and with stricter controls. Particular attention has therefore been given to e-government as an international approach and a general trend that requires a response to and the use of modern technology as a means for its success. Based on this, the e-government program was introduced in 2005 and was called "Yesser", an Arabic word meaning "facilitator". This program was set as a result of the execution of the communications and information technology national plan through the support of electronic transactions and applications by government organisations. It plays the role of the enabler/facilitator of the implementation of e-government in the public sector. Moreover, it aims to raise the public sector's efficiency and effectiveness, offer better and faster government services, and ensure availability of the required information in a timely and accurate fashion (E-government program "Yesser" 2011).

Due to the enormous significance of e-government applications, there are now more than 180 electronic services being offered by 50 different organisations. An example of a most successful e-government service is the payment system called "Sadad". Sadad was implemented by the Saudi Arabian Monetary Agency in order to facilitate and streamline the bill payment transactions of end consumers via all banking channels, including bank branches, ATMs, telephone banking, and Internet banking. In 2008, the number of transactions conducted by Sadad exceeded 5 million transactions per month, with a monthly growth rate of 22% (Sadad 2008).

The use of mobile devices is rapidly increasing among the people in the KSA. According to a recent report in 2010 by Communications and Information Technology Commission (CITC) in Saudi Arabia, the latest statistics in 2010 indicated that there were 4.3 million telephones

(fixed lines) in use. By comparison, the total number of mobile subscriptions is 47 million with average annual growth rate for the last eight years at around 43%. This CITC report also stated that mobile penetration in Saudi Arabia stood at 172% which is higher than the world average of 67%, the developing countries average of 57% and the developed countries average of 114%. However, the CITC report indicates an estimated 11 million Internet users with an average annual growth about 33% over the eight years period (2001-2009).

Therefore, as the number of mobile phone users is higher than that of Internet users, the Saudi government is concentrating on developing delivery of its services through mobile devices. Currently however, m-government applications in the KSA are at an early stage and most are based on the use of SMS. For instance, the Ministry of Education has been sending final exam results to the final level high school students via mobile phones since 2003. In the process of this service, the Ministry of Education provides a soft copy of the students' final exam results to the Saudi Telephone Company (STC) and students are required to send an SMS message containing a student number to the STC to receive a text message containing their results. The main disadvantage of this service is the lack of privacy where anyone who knows a student's number can get that student's results without their permission (Abanumy and Mayhew 2005).

The Ministry of Interior also started to provide several services via mobile devices through its different sectors, such as the General Directorate of Passports and General Department of Traffic. For example, drivers can inquire from the General Department of Traffic about their fines via their mobile devices. A driver can send an SMS message containing their ID number and then will receive a text message containing the result.

Another m-government application is weather notifications. Mobile users can get an SMS message containing weather conditions from the weather forecasting authority. Moreover, a number of hospitals have started an appointment reminder application that reminds the patients of their appointments by sending an SMS message containing the date, time and clinic location.

5.1 The use of biometrics in the KSA

As mentioned earlier, several governments have implemented biometric authentication in various types of applications. The Kingdom of Saudi Arabia, as other countries, has implemented biometrics in several places as follows.

Fingerprint technology has been applied for registering employees' attendance in several government agencies such as Ministry of Interior, Ministry of Foreign Affairs, the General Organisation for Technical Education and Vocational Training, the Royal Commission for Jubail and Yanbu, and Supreme Commission for Tourism. Furthermore, a number of agencies such as the Ministry of the Interior, the Ministry of Foreign Affairs, and the Saudi Monetary Fund have implemented biometrics to authenticate employees in special security cases like entering via some doors in their buildings.

Recently, the Ministry of Interior started to require citizens submit their biometrics when they issue or renew their ID national card as well as residents' biometrics when they issue or renew their residential cards. More specifically, the Directorate General of Passports has implemented fingerprint technology in several cities in the Kingdom for foreign people. This system now has the biometrics for about 7 million Saudi residents.

5.2 Conduct of the study

As stated above, this study used both questionnaire and semi-structured interviews for the data collection. In particular, eleven face-to-face semi-structured interviews were conducted in the Kingdom of Saudi Arabia with the managers of online services and IT security managers of mobile e-government service providers including the Ministry of Interior, National Information Center, General Directorate of Passports, The Saudi E-Government Program (Yesser), National Centre for Digital Certification, Al-Elm Information Security Company, and Sadad Payment System. Four semi-structured interviews were also conducted with managers and IT security providers in mobile communication network services including the Saudi Telecom Company (STC) and Etihad Etisalat (Mobily).

Theoretical sampling guided by Grounded Theory methodology was applied in this study, and refers to the selection of participants based on criteria specified by the researcher and according to preliminary findings (Glaser and Strauss 1967). The early stages of continuous data analysis pointed out matters that need further exploration, therefore, the process of sampling was directed by the on-going theory development and interviews were conducted until theoretical saturation was reached.

The interview questions were of an exploratory nature. More specifically, open-ended questions were designed to help identify the factors influencing the successful implementation of biometric authentication in m-government security. These comprised questions on benefits, challenges, barriers, and concerns about this application of biometrics taking into account the different roles of the target organisations. Furthermore, the data collected from the first interviews helped to modify the questions for the subsequent interviews. This was as intended and followed the guidelines of Grounded Theory methodology.

A survey questionnaire was presented to mobile communications users to explore their concerns and perceptions regarding applying biometric authentication in their mobile devices for government services. Users from both genders were chosen as participants from a range of relevant age groups and education levels. The questionnaire sought responses from a selection of choices under the basic headings of "Background Information", "ICT Experience", "Mobile Devices and Government Services", "Mobile Device Security" and "Biometrics and Mobile Government Services". It was also designed to give opportunity for the participants to make comments after each question. 420 questionnaires were distributed and 330 were returned from the participants. Nineteen of the 330 were excluded from the study because they were deemed incomplete. Thus, a total sample of 311 questionnaires was included in the analysis.

It is noteworthy that interviews rather than questionnaires were conducted with the much smaller number of government service providers and network operators in order to more fully explore their individual perspectives. The questionnaire by comparison, was distributed to mobile users in order to collect larger amounts of data about mobile communication users' concerns and perceptions in a shorter time scale than would have been possible with interviewing.

6. Application of the grounded theory

Collected data was subjected to analysis using Grounded Theory methodology which was executed by carefully following Strauss and Corbin's (1990) approach. As mentioned earlier,

this study incorporates the suggested techniques by Strauss and Corbin (1990) including sampling, coding, memo writing, reviewing of literature, and making constant comparisons to analyse the data and enhance theoretical sensitivity. More details about the application of these techniques are provided in the following sections.

6.1 The Use of the literature

"All kinds of literature can be used before a research study is begun: both in thinking about and getting the study off the ground. They can also be used during the study itself, contributing to its forward thrust" (Strauss and Corbin, 1990, p.56). However, Strauss and Corbin (1990) distinguish between different types of literature which are technical and nontechnical literature and they argue that both are of equal usefulness, and can be used at the same points in Grounded Theory analysis procedures.

Technical literature refers to theoretical and philosophical papers as well as other research studies which characterize the writing of a professional discipline and it can be used as background material for comparison against the findings of Grounded Theory. Strauss and Corbin (1990) stated several reasons for the use of technical literature early in the study. For instance, it can be used in order to stimulate theoretical sensitivity by providing concepts and relationships for comparison against the data, therefore, previous theories can be modified, extended, or amended depending on the situation. Moreover, it can be used to stimulate questions for interviews or the other data collection techniques and can also be used to help direct theoretical sampling. Another reason for using technical literature is to provide a secondary source of data that can help by providing supplementary, externally sourced, validity to the research findings (Strauss and Corbin 1990).

In contrast, nontechnical literature refers to the use of other materials including reports, records, and manuscripts (Strauss and Corbin 1990). It can be used either as "primary data or to supplement interviews and field observations in Grounded Theory studies" (Strauss & Corbin, 1990, p.48). However, some researchers believe that the initial review of the literature is important as it helps in enabling readers to classify the researcher's perspective as the research begins as well as providing justification for applying the Grounded Theory study (Antle 1986).

In the study related here, a review of the relevant literature and previous theories established current thinking in the areas of mobile government and security. The main objective of this literature review was to enhance awareness of the existing knowledge and to identify the gap. In addition, technical literature was used as background material for comparison against the findings for the development of the substantive theory of this study. Nontechnical literature such as newspapers and government reports were used as well in order to support several emerging issues resulting from the empirical study.

6.2 Memos

Memos are "written records of analysis related to the formulation of theory" (Strauss and Corbin 1990, p.197). They are written continuously through the research process in order to reflect upon and explain meanings and processes, including identifying relationships between codes and categories, as well as providing a depth of understanding of the concepts (Strauss and Corbin 1990). In this study, memos were written to help describe and explain

the data analysis, as well as the relationships among concepts and categories. It further helped to explore data, and to group concepts and codes into categories. For example, during the development of the "system requirements" and "procedural issues" categories, one of the memos written stated that "Organisational and users' factors influence the identified system requirements. System requirements relate to the system itself. Procedural issues which emerged from entities factors include current and future authentication system issues that are related to the system as well". This memo helped in developing a core category - "system factors" - which combined system requirements and procedural issues along with their sub-factors.

6.3 Constant comparison

According to Charmaz (2006), constant comparison is described as being core to Grounded Theory. It refers to the process of constantly comparing data set to data set and its coding in order to refine the development of theory. Strauss and Corbin (1990) indicated that constant comparison reminds the researcher to constantly return to the data which can help in verifying the emerging categories as well as examining and comparing concepts for similarities and differences.

In this study, constant comparison was employed by comparing incoming data with the previous data to find out whether the same concepts appear and are relevant for the new cases and whether the codes were placed in correct category and were reliable and truly represent the empirical data.

6.4 Coding procedures

Strauss and Corbin (1990) defined three coding procedures in Grounded Theory which are open, axial, and selective coding.

6.4.1 Open coding

An open code refers to "the analytic process through which concepts are identified and their properties and dimensions are discovered in data" (Strauss and Corbin 1998, p. 101). In this study, open coding was considered in the initial phase of the analysis process. A total of 115 open codes were created based on 15 interviews and 311 questionnaires. During this stage, the analysis was done by using phrase-by-phrase coding. In order to capture what has been said in the interview, conceptual labels were appended to almost every phrase. These labels were mostly too close to the exact words and context of the interview. Phrases with the same idea were attached with the same open code; otherwise, a new open code was created if the existing one did not fit. As the coding process continued and the researchers became well focused and confident in the process, the codings were revisited and refined so that they were reasonably understandable and provided more meaningful concepts, taking into account that they truly represented the empirical data.

However, it is important to note that some sentences represent only one concept, while others represent more the one concept. For example, the following sentence represents the code, financial benefits: "Also, it may have financial benefits later". Whereas the next sentence represents four concepts: lack of m-government services, lack of e-government services, enquiry services, and target users: "The most current m-services as well as e-services are enquiry services for both citizens and residents".

The aim of this procedure is to begin the unrestricted labelling of all data and to allocate representational and conceptual codes for all incidents highlighted within the data.

6.4.2 Axial coding

Axial coding refers to the process of making connections and links between the categories (Strauss and Corbin 1998). In this stage, the open codes were put together in new ways by making connections and relationships between and among codes and concepts in order to develop core codes. Figure 1 below shows the emergent categories and the relationships between them; however, further developing was made as will be discussed in the following section.

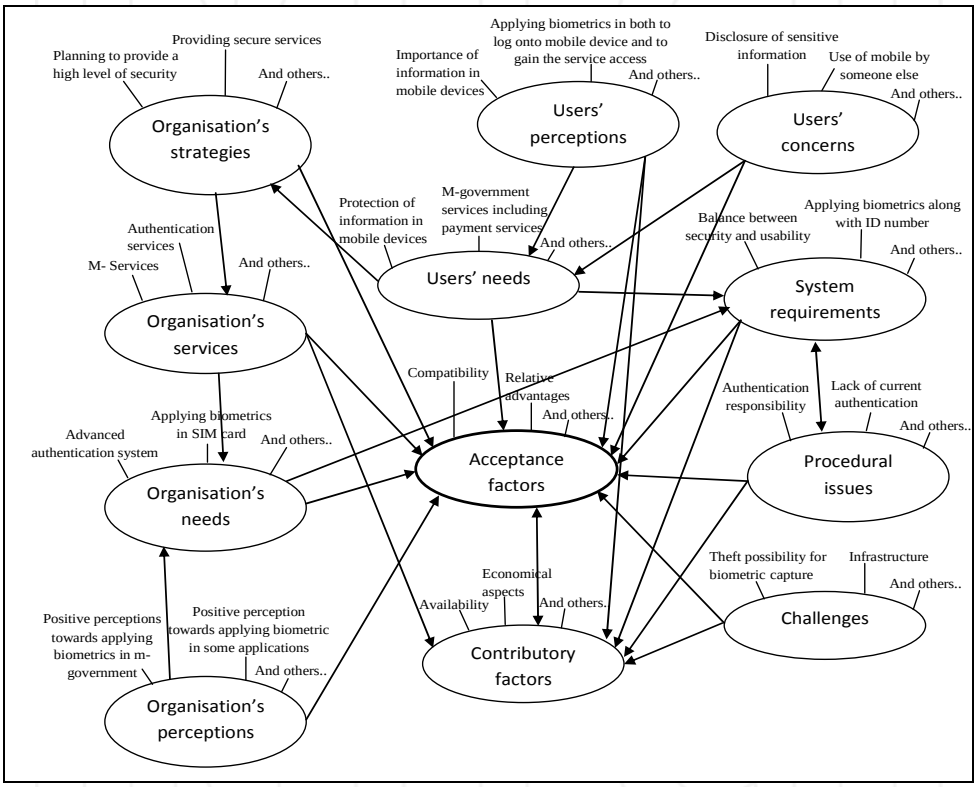


Fig. 1. Categories and relationships

The most closely interrelated open codes were aggregated under core categories. This is was done taking into account constant comparison of the open codes listed under that axial code with each other by asking questions such as: "How do these axial codes show connections and explain factors that influence the adoption of biometric authentication in m-government security?"

Through the process of axial coding, the following twelve categories were created: acceptance factors, contributory factors, challenges, system requirements, procedural issues,

users' needs, users' perceptions, users' concerns, organisation's strategies, organisation's services, organisation's needs, and organisation's perceptions. However, it is important to note that the categories of users' needs, users' perceptions, and users' concerns were developed based on the questionnaire results.

6.4.3 Selective coding

Selective coding can be identified as "the process of integrating and refining the theory" (Strauss and Corbin 1998, p.143). According to Strauss and Corbin (1990), the procedure of selective coding requires a selection of a focal core category which is the central phenomenon that has emerged from the axial codes and relating it to other categories in addition to validating those relationships. In this study, the acceptance factors code is the core category as illustrated in Figure 2.

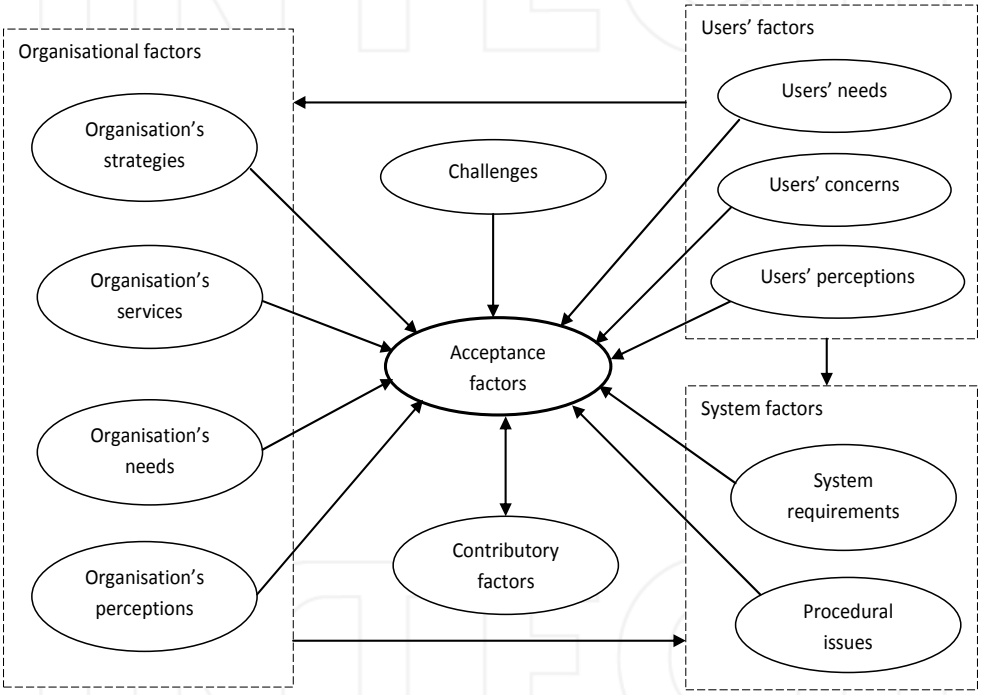


Fig. 2. Core category and relationships

The identification of the core category informs substantive theory that identifies the factors that influence the adoption of biometric authentication in m-government security. However, after becoming more familiar with the area and being well focused according to the suggestive categories, some of the categories were combined and incorporated with others, as justified in Charmaz (2006).

More specifically, system requirements and procedural issues were combined to be in the category of 'system factors', because they were all mentioned by the interviewees as part of

the system factors. Similarly, the categories of organisation's strategies, organisation's services, organisation's needs, and organisation's perceptions were combined to be 'organisational factors' as all of them related to the organisation and were mentioned as the organisation's viewpoints. Acceptance factors were also combined with contributory factors to be called 'enabling factors' as all the factors in this category were mentioned as factors that would enable the achievement of successful adoption of biometric authentication in m-government security.

It is noteworthy that the presented codes and categories in the above sections are the final set of the re-coding process. As suggested by (Miles and Huberman 1994), in order to ensure that codes and categories are applied consistently, it is significant for the researchers to verify all codes and categories that are assigned to the data. The benefit of re-coding process consisted of reconfirming and refining the codes and categories. Moreover, a comparison between newly and previously assigned codes and categories assisted us as well to check whether the codes and categories were reliable and truly represented the empirical data. The initial codes were mostly too close to the exact words of the data while the final codes provide more meaningful concepts.

As evidenced from the data analysis, one concept that was frequently stressed by the participants was the idea of acceptance. It had been introduced as a category involving: relative advantages, compatibility, ease of use, trialability, observability, trust, and privacy; and had been promoted to the "core" category. This, as known in Grounded Theory methodology, was because it linked up all of the other categories.

Another important category is the category of contributory factors which include availability, awareness, legislation, economical aspects, as well as social and cultural aspects. During the data analysis, it is found that both acceptance factors and contributory factors are involved in promoting the adoption of biometric authentication in m-government security.

Furthermore, the emerged categories show that organisational factors including organisation's strategies, services, needs, and perceptions influenced by users' factors which consist of users' needs, concerns, and perceptions. At the same time, both organisational and users' factors influence acceptance factors in different manners. For instance, applying biometric authentication along with a public key infrastructure (PKI) in m-government services is an important need of service providers due to the security relative advantage of this combination between biometrics and the PKI. This application also meets the users' need for protection of their personal and sensitive information through the use of m-government services. This combination of factors can consequently be seen to positively influence the acceptance of biometrics in m-government security among both users and service providers.

Similarly, system factors including system requirements and other related system issues such as the authentication responsibility and user registration at a website influence the acceptance factors and are at the same time influenced by users and organisational factors. This is because the majority of the system requirements, for example, have basically emerged due to organisations' and users' needs and perceptions.

It was also found that several challenges influence the adoption of biometric authentication in m-government security. These challenges include technical and related challenges such as

the biometric registration and enrolment process and the current lack of research into security and m-government in the Kingdom of Saudi Arabia. These challenges, which directly influence the acceptance factors, need to be considered before starting the implementation of biometrics in m-government in order to enhance the acceptance factors.

7. The development of the theoretical framework

Figure 3, below, illustrates the findings, focusing on the categories that have emerged from the open, axial, and selective coding phases. Based on the application of Grounded Theory, this theoretical framework, pictured, encompasses and organizes the concepts that form the factors influencing the adoption of biometric authentication.

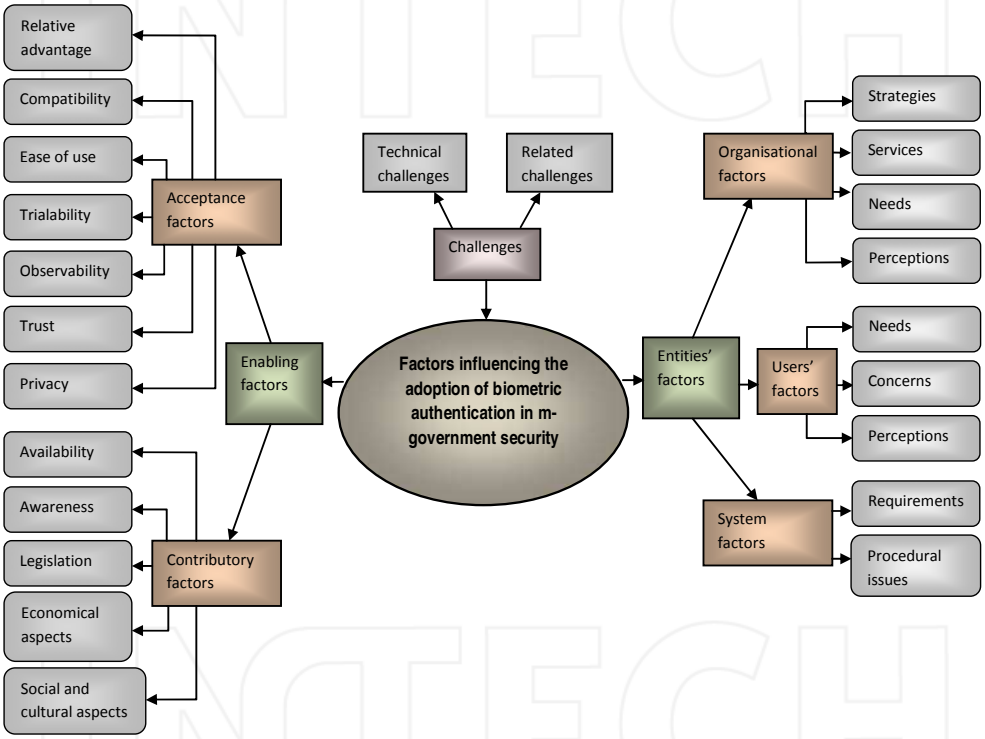


Fig. 3. Theoretical framework for the adoption of biometrics in m-government security in the KSA

Figure 3 depicts a new theoretical framework for the factors influencing adoption of biometric authentication in m-government security in Saudi Arabia, which was derived by the use of Grounded Theory as described above. Analysis and discussion of the results indicated that "entities factors", which include users', organisational, and system factors, as well as enabling factors involving acceptance and contributory factors, influence the adoption of biometric authentication in m-government security. As reported earlier in the previous section, this will also be influenced by responses to technical and non-technical challenges.

It is noteworthy that acceptance factors including relative advantage, compatibility, ease of use, trialability, observability, trust, and privacy, as well as contributory factors involving availability, awareness, legislation, economical aspects, and social and cultural aspects, are the most important factors that will enable the KSA in achieving the adoption of biometric authentication in m-government security.

The results of this study presented in this chapter are supported by a number of findings reported in literature. In particular, the findings among the acceptance factors, for example, are close to existing theories such as Diffusion of Innovation (Rogers 1995) and the Technology Acceptance Model (Davis 1989). Relative advantage, for instance, is similar to Rogers' theory of Diffusion of Innovation (1995). However, by comparing this concept with "perceived usefulness" in the Technology Acceptance Model (TAM) (Davis 1989), it seems that "relative advantage" is more accurate in representing users', service providers', and network operators' perceptions regarding the application of biometrics in m-government security. Furthermore, it is noticeable that the set of factors proposed in TAM variants and Unified Theory of Acceptance and Use of Technology (UTAUT) correspond closely with factors identified in DOI theory. While in the Technology Acceptance Model, two specific variables of perceived usefulness and perceived ease of use are hypothesized to be fundamental determinants of user acceptance (Davis 1989); the Diffusion of Innovation theory concentrates on five concepts - relative advantage, compatibility, complexity, trialability, and observability - as the five factors that affect the rate of innovation diffusion. However, the acceptance factors among the developed framework include the five concepts of DOI theory in addition to the concepts of trust and privacy as emerged from the data analysis.

Empirical studies related to the acceptance and adoption of mobile phones and electronic services via the Internet mostly indicate similar factors. For instance, Jahangir and Begum (2008) introduced a conceptual framework that considered perceived usefulness and ease of use, as well as security and privacy, as important factors that influence users' acceptance and adoption of electronic banking services. Another study by Tassabehji and Elliman (2006) highlighted trust and security as major factors in e-government adoption. AlShihi (2007) also indicated that trust has a wide impact on m-government acceptance. Kaasinen (2007) found that perceived value, ease of use, trust, and ease of adoption are important factors that influence user acceptance of mobile Internet services. However, while highly similar acceptance factors appear under various theories and models covering innovation acceptance and adoption, the developed theoretical framework in this chapter is more comprehensive. This is because it identified acceptance factors along with other factors, such as contributory and organisational and users' factors that influence adoption. Although the concepts of the developed theoretical framework in this study presented in this chapter are more comprehensive, it was created to accurately represent what different participants in Saudi Arabia including users, service providers, and network operators meant by their views, allowing it to be applied by individuals as well as organisations.

In addition, some of the identified contributory factors can be related to other findings in the literature. For example, while "availability" in this study indicates the availability of mobile devices with biometric attachment as well as m-services, Quantz (1984) identified availability of new technology as an important factor for the adoption of a new technology. Lee et al. (2002) found that social influence and self-efficacy variables significantly affect

perceived usefulness and perceived ease of use for user acceptance of the mobile Internet. Teo and Pok (2003) also found that social factors, including perceptions of relative advantage, play a significant role in influencing intentions for the adoption of Wireless Application Protocol (WAP)-enabled mobile phones amongst Internet users. Furthermore, while the developed theoretical framework in this chapter classified social and cultural aspects as contributory factors that influence the adoption of biometric authentication systems in m-government security, Myers et al. (2002) stated culture as a factor that influenced users' decision to accept and adopt a particular system.

The developed theoretical framework in this chapter identified several organisational factors as contributing to m-government acceptance. Feng (2003) and Alharbi (2006) confirmed organisational issues and culture as important factors that need to be considered when applying new technology. More specifically, Feng (2003) stated that e-government projects are not a technical issue, but rather an organisational issue. A result of the study presented in this chapter indicated a lack of organisations with clear implementation strategies, and only a few organisations following Yesser's strategies regarding the implementation of e-government applications. This supports a literature finding where Al-Shehry (2008) pointed out some doubts about transforming Yesser's ideas into reality. He mentioned that some organisations failed to follow the general standards set by Yesser. He also indicated some issues that have not been adequately addressed in Yesser's strategy, such as organisational readiness, awareness, and the re-engineering of business processes. Moreover, Sahraoui et al. (2006) indicated that there is a lack of clear vision and strategy for the deployment of e-government services in Saudi Arabia. Consideration towards applying advanced levels of authentication in electronic and mobile services were also apparent among the organisational factors; which supports the finding that reveals that successful e-government strategies have to include effective security controls for the processes and systems of the government, and to ensure privacy for personal information (OMB 2002). According to Satyanarayana (2004), an e-government strategy should identify the infrastructure needs, required process transformations within government, and the technical framework, along with an indicative timeline.

Another important category among organisational factors is addressing an organisation's needs, which in this study, represent the needs of both government organisations and mobile network companies regarding the authentication of m-government security in Saudi Arabia. A number of researchers such as (Bergstrom 1987; Putnam 1987; Roberts and Pick 2004) mentioned organisational needs as a factor that affects the adoption of new technology. According to Bergstrom (1987), organisational needs influence the decision processes involving new technologies. Putnam (1987) identified organisational needs as a critical factor that may impact the success of a modernisation project in organisations where new technology is involved. Such a determined need of advanced authentication system reflects the organisations' perceptions towards the importance of security in m-government applications, which supports the literature findings of (Al-Khamayseh et al. 2006; Chang and Kannan 2002). More specifically, Al-Khamayseh et al. (2006) indicate that the security of m-government services is considered the hallmark of successful m-government, while a study by Clarke and Furnell (2005) found that additional and advanced authentication systems are required for mobile devices. Furthermore, this result relates with the literature finding where Nanavati et al. (2002) confirmed that increased security is one of the main

benefits of adopting biometric authentication compared with traditional authentication methods such as PINs and tokens. Nanavati et al. (2002) found that the need for high levels of security frequently plays an important role in an enterprise's decision to deploy biometrics. A reliable authentication of the user accessing an agency's Website is a basic requirement, since the lack of user authentication may cause serious threats through unauthorized access (Department of Commerce 2003). Moreover, while an organisation in the developed framework indicates a need to apply biometric authentication in only some advanced m-services, Nanavati et al. (2002) emphasized that the application of biometric systems should have a limited scope. Another identified need is to store biometric capture on the SIM card, which is consistent with the literature finding that suggests storing the biometric template on the smart card of the mobile device to enable users to control their biometric pattern (Giarimi and Magnusson 2002).

The theoretical framework in this chapter indicates the importance of taking into account organisations' perceptions in order to adopt biometrics in m-government. Several studies by Putnam (1987), Ettlie (2000), and Roberts and Pick (2004) mentioned that perceptions of a specific security technology are one of the important elements in the decision to recommend the technology to an organisation. Beatty et al. (2001) stated that the more likely organisations were to perceive an innovation as consistent with their perceptions, the more likely they were to adopt it. Positive perceptions emerged, for example, towards the application of fingerprinting, which is consistent with literature findings (ORC 2002) that fingerprint scanning is the most commonly experienced technique, followed by the use of signature dynamics. This also may agree with Giesing's (2003) study where most employees pointed to fingerprint technology as their preferred biometric.

The developed theoretical framework brought to light several users' factors that influence the adoption of biometric authentication in m-government security. This framework identified users' factors including their needs, perceptions and concerns, while the most recent literature mentioned only the importance of users' factors. For example, Ashbourn (2004) stated that users can have a direct impact on the operational performance of biometric systems. They can be an essential factor in the successful implementation of biometrics (Ashbourn 2004; Giesing 2003; Scott et al. 2005). User adoption and perception problems related to the implementation of the new technology have been clarified by Giesing (2003) as a factor that would prevent an organisation from adopting biometric technology. Thus, the biometrics research community is well-advised to study the users' side regarding the use of biometrics (Bolle et al. 2004).

Wayman et al. (2005) highlighted the importance of understanding system requirements, procedures, and other related issues, including systems management and user psychology, in order to gain successful integration of biometric systems. The developed theoretical framework in this chapter identified a number of system factors including requirements and procedural issues that need to be considered to adopt biometric authentication in m-government security in Saudi Arabia. According to Kanellis and Paul (2005), in order to have a good chance of project success for such an ICT system, system requirements need to be considered before the implementation commences.

Finally, as illustrated in Figure 3, the developed theoretical framework indicates several challenges that would influence the adoption of biometric authentication in m-government

applications in Saudi Arabia. In contrast, most of the literature in the area of m-government (Al-khamayseh et al. 2006; NECCC 2001) mentioned only security and privacy as challenges of the implementation of m-government, while Lallana (2008) stated cost issues. However, there are some identified challenges that support some of the literature findings. For example, registration and enrolment processes of people's biometric credentials has been identified as one of the biggest challenges facing the adoption of biometrics in m-government, and this supports the literature finding where Hirst (2005) stated that the ease of enrolment is a determining factor for the successful implementation and use of a biometric system.

To summarise, while the developed theoretical framework (Figure 3) in this chapter supports a number of findings reported in existing theories and literature, it is unique and more comprehensive than other related existing theories such as Diffusion of Innovation (1995) and the Technology Acceptance Model (Davis 1989). It includes factors influencing the adoption of biometric authentication in m-government among mobile communication users, service providers and network operators, adding further dimensions such as contributory aspects, organisational aspects, user aspects and system aspects.

8. Considerations for the adoption of biometrics in m-government

The theoretical framework proposed in Figure 3 can be used to understand the factors influencing the adoption of biometric authentication in m-government security. Based on the findings presented in this chapter, several considerations can be suggested for those who are involved the adoption of biometrics in m-government applications.

First, the findings of this study revealed that, to be effective, there is a need to provide mobile communication users and service providers with an advanced authentication system for m-government services; therefore, government and decision makers should consider this need in order to enhance the adoption and implementation of m-government services. Based on the viewpoints of the participants, the application of biometric authentication would play an integral role in enhancing the security of m-government. However, it will be important for decision makers to take into account that such legislation needs to be carefully crafted to safeguard the rights of the involved entities, and the people involved will need to be aware of the new laws and regulations. Similarly, it will be important that legislation is enforced and that all parties involved in the application are well informed. Technical support will be required to make mobile devices with biometric attachments available around the country at a reasonable cost on the normal users' level.

It would be appropriate that the application of biometric authentication is implemented along with the use of a Public Key Infrastructure (PKI), and that service providers apply biometrics with only the advanced m-services to enhance usability and user acceptance. It is also important to consider the security of the templates and databases as well as the management of biometric data during enrolment, transmission, storage and authentication. The enrolment process, which essentially introduces the user to the authentication system, needs to be considered as it would affect the adoption of biometrics in m-government. A high level of cooperation between government agencies will be required to effectively introduce biometrics in m-government services. Biometric standards and systems evaluation could effectively take place before and during the implementation process.

Furthermore, to encourage mobile users to adopt and use biometrics in their mobile devices for government services, it would be strategically advantageous for awareness programs to take place before the technology is introduced. In fact, education programs for both mobile users and service providers will help to ensure awareness of the new technology, the purpose of its implementation, and its benefits. It is also important to note that privacy, relative advantage, ease of use; trialability, compatibility, and observability, play a significant role in promoting the adoption of biometric authentication in m-government applications.

9. Conclusions

There is a dearth of empirical studies in the adoption of biometric authentication, certainly within the context of m-government in developing countries. This chapter contributes rich insights into people's perceptions on the application of biometrics in this context, which adds weight to existing opinions on how to best apply biometrics in m-government security. The empirical data identifies several issues including the users' factors, organisational factors, system factors, acceptance factors, contributory factors, and challenges that influence the adoption of biometric authentication in m-government in the KSA context. The data also reveals that biometric authentication might best be implemented with the use of PKI in a smartcard installed in mobile devices, and preferably only for advanced government services. This is as opposed to consistently applying biometric authentication to the mobile device itself, and applying it for all online government services.

A main finding and contribution of this work is the use of Grounded Theory in the development of a new substantive theory for the adoption of biometric authentication in m-government security in the KSA. This chapter contributes to the literature by identifying and describing the factors that influence the adoption of biometric authentication in m-government applications. It further contributes to theory by providing rich insights and increased understanding of the concerns and perceptions of mobile phone users, service providers and network operators regarding the application of biometric authentication to mobile devices for government services.

This chapter adds a methodological contribution by providing a new example of the application of Grounded Theory coding procedures to develop a theoretical framework for the adoption of biometric authentication in mobile services applications in a developing country. This chapter described the application of Grounded Theory, including the development of the concepts and categories, and then the generation of the substantive theory, providing a unique insight into this qualitative information system research.

10. References

Abanumy, A and Mayhew, P 2005, M-government Implications For E-Government In Developing Countries: The Case Of Saudi Arabia, EURO mGOV 2005, Brighton, UK, pp. 1-6.

Alharbi, S 2006, *Perceptions of Faculty and Students toward the Obstacles of Implementing E-Government in Educational Institutions in Saudi Arabia*, a PhD thesis, West Virginia University, USA.

Al-khamayseh, S, Lawrence, E, and Zmijewska, A 2006, Towards Understanding Success Factors in Interactive Mobile Government, *Second European Conference on Mobile Government*, Brighton, UK.

Al-Shehry, A 2008, *Transformation towards e-government in the Kingdom of Saudi Arabia: technological and organisational perspectives*, a PhD thesis, De Montfort University, UK.

AlShihi, H 2007, M-government Services in Oman: Success and Failure Factors, viewed on 5th of January 2009 at www.csdms.in/mserve/2007/fullpapers/HafedhAlShihi.pdf

Antle, K 1986, *Writing and Evaluating the Grounded Theory Research Report. In From Practice to Grounded Theory* (Chenitz W.C. & Swanson J.M., eds), Addison-Wesley, Mill Valley, California, pp. 146–154.

Antovski, L and Gusev, M 2005, M-Government Framework, *Proceedings of the First European Conference on Mobile Government*, 10-12 July, University Sussex, Brighton, UK.

Ashbourn, J 2004, *Practical biometric from aspiration to implementation*, London: Springer.

Beatty, R, Shim, J, and Jones, M 2001, Factors influencing corporate web site adoption: A time-based assessment. *Information & Management*, vol. 38, pp. 337-354.

Bergstrom, R 1987, Critical issues in CIM implementation. *CIM Technology*, pp. 5-6.

Bolle, R, Connell, J, Pankanti, S, Ratha, N and Senior, A 2004, *Guide to Biometrics*, Springer, New York.

Bonsor, K and Johnson, R, *How Facial Recognition Systems Work, How Stuff Works*, viewed on 2nd March 2008 at available at http://computer.howstuffworks.com/facialrecognition.htm

Chang, A and Kannan, P 2002, *Preparing for Wireless and Mobile Technologies in Government*, IBM Endowment for the Business of Government.

Charmaz, K 2006, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*, Sage, Thousand Oaks, California.

Clarke, N and Furnell, S 2005, Authentication of users on mobile telephones – A survey of attitudes and practices, *Computers & Security*, vol. 24, no. 7, pp. 519-527.

Clarke, N and Furnell, S 2007, Advanced User Authentication for Mobile Devices, *Computers & Security*, vol. 26, no. 2, pp. 109-119.

Creswell, J 1998, *Qualitative inquiry and research design: Choosing among five traditions*, Thousand Oaks, Calif.: Sage Publications.

Creswell, J 2008, *Educational research: planning, conducting, and evaluating quantitative and qualitative research* (3rd ed.). Upper Saddle River, N.J., Pearson/Merrill Prentice Hall.

Dankers, J, Garefalakis, R, Schaffelhofer, R and Wright, T 2004, PKI in mobile systems, *Security for Mobility*, IEE Telecommunications 51, Mitchell, C. (ed.), The Institution of Electrical Engineers, UK, pp. 11-33, 2004.

Davis, F 1989, Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, 13(3): 319-339.

Department of Commerce (DC) 2003, *Information Security Guideline for NSW Government - Part 2 Examples of Threats and Vulnerabilities*, the Office of Information and Communications Technology, Australia.

E-government Program (Yesser) 2011, The Ministry of Communications and Information Technology, available at http://www.yesser.gov.sa

Ettlie, J 2000, *Managing technological innovation*, New York, John Wiley and Sons.

Feng, L 2003, Implementing E-government Strategy is Scotland: Current Situation and Emerging Issues, *Journal of Electronic Commerce in Organizations*, vol. 1, no. 2, pp. 44-65.

Frees, R 2008, Biometric technology improves identification security, U.S. Air Force, viewed on 3rd December 2008 at http://www.af.mil/news/story.asp?id=123084564

Giarimi, S and Magnusson, H 2002, *Investigation of User Acceptance for Biometric Verification/Identification Methods in Mobile Units*, Department of Computer and Systems Sciences, Stockholm University, Sweden.

Giesing, I 2003, *User Perceptions Related to Identification Through Biometrics within Electronic Business*, University of Pretoria.

Glaser, B 1992, *Emergence vs Forcing: Basics of Grounded Theory Analysis*, Sociology Press, Mill Valley, CA.

Glaser B and Strauss A 1967, The *Discovery of Grounded Theory: Strategies for Qualitative Research*, Aldine, Chicago.

Goulding, C 2002, *Grounded Theory: A Practical Guide for Management*, Business and Market Researchers London, Sage.

Harris, A and Yen, D 2002, Biometric authentication: Assuring access to information, *Information Management and Computer Security*, vol. 10, no. 1, pp. 12-19.

Heath, H and Cowley, S 2004, Developing a Grounded Theory approach: a comparison of Glaser and Strauss, *International Journal of Nursing Studies*, vol. 41, pp. 141-150.

Hirst, C 2005, *A Primer on Biometric Technologies*, Gartner Research.

Jahangir, N and Begum, N 2008, The role of perceived usefulness, perceived ease of use, security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking, *African Journal of Business Management*, vol. 2 (2), pp. 032-040.

Jain, A, Hong, L and Pankanti, S 2000, 'Biometric identification', *Communications of the ACM*, vol. 43, no. 2, pp. 90-98.

Kaasinen, E 2007, 'User acceptance of mobile Internet services', In Workshop on Mobile Internet User Experience, *Mobile HCI 2007 Conference*, September 9, 2007, Singapore.

Kanellis, P and Paul, R 2005, User behaving badly: Phenoma and paradoxes from an investigation into Information systems misfit, *Journal of Organisational and End-use Computing*, vol. 17, no. 2, pp. 264-291.

Kleist, V, Riley, R and Pearson, T 2005, Evaluating biometrics as internal control solutions to organizational risk, *Journal of American Academy of Business*, vol. 6, no. 2, pp. 339–343.

Lallana, E 2008, *mGovernment: Mobile/Wireless Applications in Government, eGovernment for Development Information Exchange*, University of Manchester's Institute for Development Policy and Management, UK, viewed on 2nd February 2009 at Hhttp://www.egov4dev.org

Lease, D 2005, *Factors influencing the adoption of biometric security technologies by decision making information technology and security managers*, a PhD thesis, Capella University, USA.

Lee, W, Kim, T and Chung, J 2002, *User acceptance of the mobile Internet*, In M-Business 2002, Athens, Greece.

Mansourian, Y 2006, *Adoption of Grounded Theory in LIS research*, New Library World, vol. 107, no. 9/10, pp. 386-399.

McLeod, J 1999, *Practitioner Research in Counselling*, London: Sage.

Miles, M and Huberman, A 1994, *An Expanded Sourcebook - Qualitative Data Analysis*, 2nd ed. Thousand Oaks, California, SAGE Publications, Inc.

Moore, G and Benbasat, I 1991, 'Development of an instrument to measure the perceptions of adopting an information technology innovation', *Information Systems Research*, vol. 2, no. 3, pp. 192-222.

Myers, M and Tan, F 2002, Beyond Models of National Culture in Information Systems Research, *Journal of Global Information Management*, vol. 10, no. 1, pp. 24-32.

Nanavati, S, Thieme, M, and Nanavati, R 2002, *Biometrics: Identity verification in a networked world*, New York, John Wiley and Sons, Inc.

National Electronic Commerce Coordinating Council (NECCC) 2001, *M-Government: The Convergence of Wireless Technologies and e-Government*, Research and Development Workgroup.

OMB. (2002). *E-government Strategy: Executive Office of the President Office of Management and Budget*, Washington, D. C.

ORC, Opinion Research Corporation 2002, *Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector*, Summary of Survey Findings.

Piantanida, M, Tananis, C, and Grubs, R 2002, Claiming Grounded Theory for practice-based dissertation research: A think piece, *Conference on Interdisciplinary Qualitative Studies*, Athens, Georgia.

Putnam, R 1987, *Selling modernization within your company*, Commline, 13.

Quantz, P 1984, *CIM planning: The future-factory foundation,* CIM Review, 38.

Roberts, G and Pick, J. 2004, Technology factors in corporate adoption of mobile cell phones: A case study analysis. *Proceedings of the IEEE 37th Annual Hawaii International Conference on System Sciences*, 9(9), 90287-90296.

Rogers, E 1995, *Diffusion of Innovations*, The Free Press, New York.

Sadad 2008, payments newsletter, SADAD Payment System, vol.2, issue 10, available online at http://www.sadad.com/Arabic/

Sahraoui, S, Gharaibeh, G, and Al-Jboori, A 2006, Government in Saudi Arabia can it overcome its challenges?, Brunel University, London, paper presented at Government Workshop '06 (eGOV06).

Satyanarayana, J 2004, e-Government - *The Science of the Possible*, New Delhi, Prentice-Hall of India.

Scott, M, Acton, T and Hughes, M 2005, An assessment of biometric identities as a standard for e-government services, *Services and Standards*, vol. 1, no. 3, 2005, pp. 271-286.

Strauss, A and Corbin, J 1990, *Basics of qualitative research: Grounded Theory procedures and techniques*, Newbury Park, CA: Sage Publications, Inc.

Strauss, A and Corbin, J 1994, Grounded Theory Methodology: An Overview, In Denzin, N. and Lincoln, Y (Eds.). *Handbook of Qualitative Research*. Thousand Oaks, Sage Publications.

Strauss, A and Corbin, J 1998 *Basics of Qualitative Research: Techniques and Procedures for Developing Theory*, 2nd ed., Sage, Thousand Oaks, CA.

Tassabehji, R and Elliman, T 2006, Generating Citizen Trust in E-Government Using a Trust Verification Agent: A Research Note, *European and Mediterranean Conference on Information Systems (EMCIS)*, Costa Blanca, Alicante, Spain

Teo, T and Pok, S 2003, Adoption of WAP-enabled mobile phones among Internet users. Omega: *The International Journal of Management Sciences*, vol. 31, no. 6, p. 483-498.

Urquhart, C and Fernandez, W 2006, Grounded Theory Method: The Researcher as Blank Slate and Other Myths, *In Twenty-Seventh International Conference on Information Systems*, pp 457-464, Milwaukee.

Urquhart, C Lehmann, H and Myers, M 2009, Putting the theory back into Grounded Theory: guidelines for Grounded Theory studies in information systems, *Information systems journal*, Blackwell Publishing Ltd.

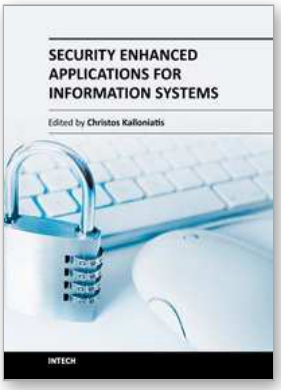
Uzoka, F.M. and Ndzinge, T 2009, An Investigation of Factors Affecting Biometric Technology Adoption in a Developing Country Context, *International Journal of Biometrics*, vol. 1, no. 3, pp. 307-328.

Venkatesh, V, Morris, M, David, G and Davis, F 2003, 'User acceptance of information technology: toward a unified view', *MIS Quarterly*, vol. 27, no. 3, pp. 425-78.

Vielhauer, C 2006, *Biometric User Authentication for IT Security: From Fundamentals to Handwriting*, Springer, New York.

Wayman, J, Jain, D, Maltoni, H and Maio, D 2005, *Biometric Systems: Technology, Design and Performance Evaluation*, Springer, New York.

World Fact Book 2011, Central Intelligence Agency, available at https://www.cia.gov/index.html



Security Enhanced Applications for Information Systems

Edited by Dr. Christos Kalloniatis

ISBN 978-953-51-0643-2
Hard cover, 224 pages
Publisher InTech
Published online 30, May, 2012
Published in print edition May, 2012

Every day, more users access services and electronically transmit information which is usually disseminated over insecure networks and processed by websites and databases, which lack proper security protection mechanisms and tools. This may have an impact on both the users' trust as well as the reputation of the system's stakeholders. Designing and implementing security enhanced systems is of vital importance. Therefore, this book aims to present a number of innovative security enhanced applications. It is titled "Security Enhanced Applications for Information Systems" and includes 11 chapters. This book is a quality guide for teaching purposes as well as for young researchers since it presents leading innovative contributions on security enhanced applications on various Information Systems. It involves cases based on the standalone, network and Cloud environments.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821