Biometric Authentication for Mobile Government Security

An Application of Grounded Theory

Thamer Alhussain, Steve Drew, Osama Alfarraj
School of ICT, Griffith University
Gold Coast, Australia
t.alhussain, s.drew, o.alfarraj, @griffith.edu.au

Abstract—**Mobile government provides unique opportunities to utilize mobile technology to receive government services and information literally from any place, at any time, using varieties of wireless networks. However, mobile devices are using wireless network broadcasts which are vulnerable as they send signals over the public airwaves. With the rapid growth of mobile devices and Internet services, there is a growing need for user and government authentication for the protection of data and services, and to promote public trust. This paper presents the process of the grounded theory application to information system security research to develop a substantive theory for the successful implementation of biometric authentication in m-government security. It concludes by presenting the findings in the form of categories with their relationships. These emerging categories indicate the factors that influence the adoption of biometrics in m-government security.**

Keywords: biometric; authentication; grounded theory; m-government.

I. Introduction

With the valuable advantage of using mobile phones easily anywhere and at any time, several governments have started looking to offer their services via these devices in order to provide an efficient service delivery. Mobile government (or m-government) is a new delivery channel of e-government which provides unique opportunities to utilize mobile technology to receive government services and information literally from any place, at any time, and using a variety of wireless networks [1]. However, the increased use of mobile phones to store large amounts of data carries the risk of loss or theft which can compromise the security of information, especially with the inclusion of sensitive personal information. Similarly, there are implications for ensuring and enhancing the security of data using wireless communications. Hence, a high level of authentication needs to be achieved for data, device and service access in order to provide a secure channel for m-government applications and to meet the security requirements for users, service providers, and network operators. As a result, biometric authentication might be used to provide a stronger solution for m-government security as it depends on something the user is, which is the highest level of authentication.

Specifically, biometric technology is an automated method which is used to measure and analyze a person's physiological and behavioral characteristics [2; 4]. It involves the use of physiological images common to most people, such as fingerprints, faces, and irises. Thus, biometrics can be used to provide reliable identification of individuals as well as improved ability to control and protect the integrity of sensitive data stored in information systems. It also can be used to improve the performance of security applications [3].

This paper discusses the use of grounded theory for the development of a substantive theory for the successful implementation of biometric authentication in m-government security. The work is a part of a research project that aims to explore how biometric authentication can play an integral role in providing secure m-government services. Data includes users', service providers', and network operators' concerns and perceptions regarding the application of biometric authentication into mobile devices for government services. This paper provides an explanation of the authentication systems currently in use for m-government followed by a proposed model for an authentication system employing biometrics in m-government. Finally a description of the grounded theory study involving a survey and interviews of mobile communication users, service providers, and network operators is provided.

II. Authentication and Mobile government

A. *Current Authentication System in M-Government*

The current security method in mobile phone based m-government applications is based on the use of 4-8 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 [5]. The PIN is a secret-knowledge authentication method and consequently relies upon knowledge that the authorized user has. Unfortunately, secret-knowledge approaches have long-established problems, with weaknesses often being introduced as a result of the authorized users themselves [5]. Moreover, the PIN is an approach providing low level of authentication which based on something the user knows, while other advanced and combined authentication approaches involve something the user has, like a credit card, and something the user is, like biometric characteristics [2].

Providers of 2G and 3G mobile networks deliver smartcards with pre-installed symmetric keys which are used by the network to authenticate the mobile device and, in 3G, for the mobile device to authenticate to the access network.

978-1-4244-6585-9/10/$26.00 ©2010 IEEE

The authentication mechanism is based on the trust relationship that exists between the network access 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 air are derived during the authentication process. However, data confidentiality and integrity extending over the whole path between the communicating parties is not provided by network access security of second and third generation systems, which has to be provided on the network at application levels to provide end-to-end security [6]. Therefore, Public Key Infrastructure (PKI) combined with biometric authentication may provide an effective means to achieve strong end-to-end m-government security.

B. Authentication System for Biometrics in M-Government

Applying biometric authentication in m-government applications might work as illustrated in Figure I. When a user initiates a mobile government application or service, the mobile device should request the user to register his/her biometric pattern on an integrated sensor. The device would then compare it to the one already stored in the device and a backup also stored on a server of a trusted third party. The device would then send the service request and the result of the biometric authentication comparison to the service provider for approval to perform the service. The service provider will authenticate the user by a third party and accordingly will give the approval. However, the process of the approval and authentication should be done through a PKI hierarchy and Certification Authorities (CA).

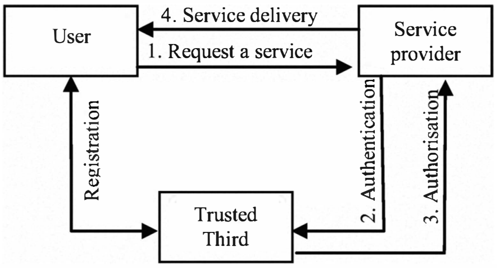

Figure 1. An authentication system for m-government

The key benefits of this scenario are to:

- provide a device with proven security for basic authentication;
- personalize these devices for individual users and identities;
- provide two-factor authentication of possession and knowledge;
- protect sensitive and personal data against stealth and misuse; and
- enable service providers to accurately and reliably authenticate their users.

However, several issues such as speed of system, key management, network congestion, availability, and error rate need to be considered to effectively apply this system.

III. Research Methodology

A. Saudi Arabia as a Focus Example for this Study

The Kingdom of Saudi Arabia (KSA) is located in the South-eastern part of the Asian continent. It occupies 2,240,000 sq km [7]. The total population reached 26 million in mid-2005, compared with 24 million in mid-2004, reflecting an annual growth rate of 2.9 percent; however, about 5 million of the population is non-Saudi [8].

With Information Technology in Saudi Arabia, the national e-government program was launched in early 2005 under the name Yesser, which is an Arabic word meaning "simplify". This national e-government program plays the role of the enabler and facilitator of the implementation of e-government in the country [9]. However, Saudi Arabia has started the use of biometrics in e-government applications a couple of years ago and it is trying to widely implement this technology. One year ago, the Ministry of Interior started to require citizens submit their biometric data when they issue or renew their ID national card as well as residents' biometrics when they issue or renew their residential cards.

B. Research Paradigm

The research paradigm adopted for this study is the interpretive paradigm which is based on the philosophical view that reality is socially constructed by people [10, 11]. The interpretive research tends to rely upon the "participants' views of the situation being studied" [12] (p.8). Thus, this interpretive research assumes that people generate their own subjective and intersubjective meanings about the world as they interact with the social world around them [13].

C. Grounded Theory

Grounded theory was initially developed by Barney Glaser and Anselm Strauss in 1967 for the purpose of generating theories. They defined grounded theory as "the discovery of theory from data – systematically obtained and analysed in social research" [14] (p. 1). In subsequent years, two different approaches of grounded theory have appeared, one by Glaser and the other by Strauss and they became more noticeable after the publication of Strauss and Corbin's book in 1990. According to Strauss and Corbin [15], grounded theory 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 [16] clarified that "grounded theory is based on the systematic generating of theory from data, that itself is systematically obtained from social research" (p. 2).

Grounded theory, according to Strauss and Corbin [15], should be inductively derived from the phenomena being represented and discovered and verified through systematic data collection and analysis. While Glaser [16] believed that the theory should be allowed to emerge during the observation of the codes and data analysis by allowing the data to tell its story, Strauss and Corbin's [15] approach is considerably more prescriptive in determining the steps to be taken during the data coding and analysis.

Furthermore, Glaser [16] and Strauss and Corbin [15] differed on the role of the literature review. Glaser [16] 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. Conversely, Strauss and Corbin [15] believed that the researchers 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. They believe that some understanding of the study area through the literature review will enhance the theoretical sensitivity of the researchers when generating theory.

D. *Application of grounded theory*

This study employed the grounded theory methodology as it is likely to provide insight, increase understanding, and offer a meaningful guidance to action as derived from data, as mentioned by Strauss and Corbin [17]. Furthermore, the main purpose of the grounded theory approach is to generate or develop a theory that is grounded in data systematically gathered and analysed [18]. Thus, the grounded theory approach fits the purpose of this study, which is to develop a theoretical framework for successful implementation of biometric authentication in m-government security in KSA. Through the interviews and questionnaires, we can explore the factors influencing the successful implementation of biometrics in m-government through the users', service providers', and network operators' concerns and perceptions regarding applying biometric authentication into mobile devices for government services. More specifically, this study followed Strauss and Corbin's approach as it allows researchers to take into consideration previous relevant literatures and theories in order to help get insights into the data. It also provides extensive guidance for researchers, while Glaser's approach is much less structured.

E. *Data Collection*

In this study, eleven face-to-face semi-structured interviews were conducted in 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. The purpose of these interviews was to explore how biometric authentication might help government agencies to provide secure services and whether its application would enhance their services.

Similarly, four interviews were conducted with managers and IT security providers in mobile communication network services including the Saudi Telecom Company and Etihad Etisalat. The purpose of these interviews was to determine their specific views and requirements of applying biometric authentication in m-government security.

As a third data capture mechanism a research questionnaire was designed for the purpose of this study as well. It was designed to explore mobile communications users' concerns regarding applying biometric authentication in their mobile devices for government services. Participants were chosen from both genders with 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". We distributed 420 questionnaires and 330 were returned from the participants. Nineteen of the 330 were excluded from the study as they were deemed incomplete. Hence, a total sample of 311 questionnaires was included in the data analysis.

IV. Data Analysis

Data were analysed following Strauss and Corbin's [15] approach as follows:

A. *The Use of Literature*

According to Strauss and Corbin [15], there are two types of literature which are technical and nontechnical literature and both are of equal usefulness and can be used at the same points in grounded theory analysis procedures. Technical literature which includes theoretical and philosophical papers as well as other empirical studies can be used as background resources for comparison against the results of grounded theory [15]. Nontechnical literature includes other resources such as reports, manuscripts, and diaries and can be used to supplement the gathered data or as primary data [15].

In this study, previous literatures including theories and empirical studies relating to mobile government and security reviewed current thinking in this area of research. Although, the review of the previous literature did not lead to any hypotheses, it helped to gain insights into the data which makes the grounded theory methodology the appropriate approach for this study. Moreover, technical literature was used as background resources for comparison against the results. Nontechnical literature was used as well for the purpose of supporting several emerging issues resulting from the empirical study.

B. *Memos*

Strauss and Corbin [15] identified memos as "written records of analysis related to the formulation of theory" (p.197). During all research processes including analysis process, memos should be recorded and written constantly in order to assist in explaining the data as well as classifying the group categories which can provide depth understanding of concepts [15]. Consequently, this study adopted the same process by recording and writing memos constantly in order to extensively describe and provide sufficient explanation of the data analysis as well as categories and their relationships.

C. *Constant Comparison*

According to Charmaz [19], constant comparison is described as a core to grounded theory. It basically can be identified as the process of comparing incidents to concepts and their coding in order to refine the theory development [19]. Constant comparison helps researchers to verify the emerging categories and comparing the identified concepts for similarities and differences [15]. In this study, constant comparison was employed for the purpose of comparing the previous collected data with incoming data in order to examine whether the same concepts were still appearing or becoming relevant for the new cases and to also examine whether the codes were placed correctly in the right category and accurately represent the empirical data.

D. *Coding*

The three coding procedures, from Strauss and Corbin's [15] approach, were applied as follows:

1) Open coding: Open coding is "the analytic process through which concepts are identified and their properties and dimensions are discovered in data" [17] (p.101). Open coding is the first analysis process that aims to represent all central ideas from the collected data and allocate all conceptual and representational codes for all occurrences highlighted in the data. In this study, a phase by phase coding was done for this coding process and a total of 116 open codes were generated and emerged based on 15 interviews. However, it is important to note that some sentences represent more than one concept, while others represent only one sentence. For example, the following sentence represents the code 'financial benefits': "Also, it may have financial benefits later". However, 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".

2) Axial coding: Axial coding concentates on making links and connections between categories [17]. In this process, all open codes were put together in new modes by creating connections and relationships between concepts and codes for the purpose of developing core categories. Core categories contained the most interrelated open codes and this was done taking into consideration constant comparison between open codes aggregated under axial code. This entailed asking how these axial codes show connections to, and explaining factors that influence the successful implementation of biometric authentication in m-government security? Through the axial coding process, the following ten categories were created: "acceptance factors", "authentication and procedure factors", "challenges", "network operators' aspects", "organisation's services", "organistion's objectives and strategies", "service providers' aspects", "critical factors", "system requirements", and "users' factors". Table I below illustrates the ten categories provided with some instances of the open codes.

TABLE I. AXIAL CODING

Categories	Examples of open codes
Acceptance factors	Trust, privacy, relative advantage, compatibility
Authentication and procedure factors	PIN and Password, face-to-face authentication with ID, registration and authentication offices
Challenges	Theft possibility for biometric capture, lack of m-government services, infrastructure
Critical factors	Availability, technical issues, financial issues
Network operators' aspects	Applying biometrics in SIM card, positive perception towards applying biometric in some applications
Organisation's services	Provide secure network access, push messages, enquiry services
Organisation's objectives and strategies	Automation of processes, regulation and legislation, utilising the available resources and technologies
Service providers' aspects	Positive perceptions towards applying biometrics in m-government, negative perceptions towards applying biometric in each m-service
System requirements	Appling biometrics along with ID number, balance between security and usability, applying biometrics along with PKI
Users' factors	Biometrics meets the need for protection sensitive information in mobile devices, Positive perceptions towards the acceptance of biometrics in m-government

3) Selective coding: Selective coding is "the process of integrating and refining the theory" [17] (p. 143). According to Strauss and Corbin [15], Selective coding aims to find out the main core category that can represent the central phenomena that has emerged from the axial codes and has relationships with others categories. In this study, the "critical factors code" is the core category and the identification of the core category informs substantive theory that identifies the factors that influence the successful implementation of biometric authentication in m-government security. However, after becoming more familiar with the area and being able to collect the data selectively, being well focused according to the suggestive categories, some of the categories' names were changed and some of them were combined and incorporated with others, as outlined in Charmaz [19]. More specifically, "system requirements", "challenges" and "authentication and procedure factors" 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 "network operators' aspects", "service providers' aspects", "organisation's services", and "organisation's objectives and strategies" were combined to be 'organisational factors' as all of them related to the organistion and were mentioned as the organisation's viewpoints. "Acceptance factors" were also combined with "critical factors" to be called 'critical factors' as all the factors in this category were mentioned as critical factors for the implementation of biometric authentication in m-government security to be successful.

V. FINDINGS AND DISCUSSION

Among the preliminary findings of this study, we could identify "acceptance factors" and "critical factors" as the most important factors that influence the successful implementation of biometric authentication in m-government security. In interviews and questionnaire responses, participants had frequently mentioned, for example, relative advantage, privacy, compatibility, and availability as essential factors to accept and use biometrics to access government services via their mobile phones. However, it is noticed from Figure 2 that the emerging categories and relationships indicated that “system factors”, “organisational factors” and “users’ factors” influence “critical factors”. Moreover, these four categories influence implementation of biometric authentication in m-government security which can lead to the improvement of m-government efficiency.

The results further demonstrate that government organisations and network operators have positive perceptions towards applying biometrics in m-government, especially for the services required high level of security. In parallel, applying biometrics in mobile device meet users’ need for protection of their sensitive information. However, several issues such as enrolment and registration processes as well as the balance between security and usability need to be considered to effectively apply this system.

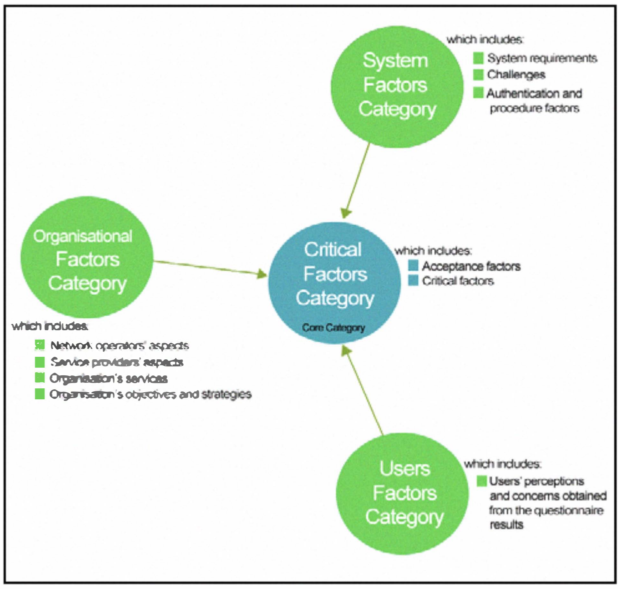
System Factors Category
which includes:
🟩 System requirements
🟩 Challenges
🟩 Authentication and procedure factors
Organisational Factors Category
which includes:
🟩 Network operators' aspects
🟩 Service providers' aspects
🟩 Organisation's services
🟩 Organisation's objectives and strategies
Critical Factors Category
Core Category
which includes:
🟦 Acceptance factors
🟦 Critical factors
Users Factors Category
which includes:
🟩 Users' perceptions and concerns obtained from the questionnaire results

Figure 2. Categories and relationships

VI. Conclusion

The main purpose of this paper was to explore and show the process of the emergence of grounded theory for developing a theoretical framework for the successful implementation of biometric authentication in m-government security. In this paper, justification for the use of grounded theory methodology in this research project has been given. Through the analysis of interviews and questionnaires via Strauss and Corbin’s [15] approach, we explored the factors that influence the implementation 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. We have presented the process of analysis and coding and how the research categories have emerged. Based on these findings, the next phase of this research project will consist of developing a substantive theory for the use of biometric authentication in m-government security as well as comparing these findings with the literature and previous theories and then providing guidelines and practical information on how biometrics can be applied to enhance the security of m-government.

References

[1] Rossel, P, Finger, M and Misuraca, G 2006, ‘“Mobile” e-Government Options: Between Technology-driven and Usercentric’, *The Electronic Journal of e-Government*, vol. 4, issue 2, pp. 79-86.

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

[3] McLindin, B 2005, *Improving the Performance of Two Dimensional Facial Recognition Systems*, University of South Australia.

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

[5] 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.

[6] 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.

[7] The Saudi Network, available online at http://www.the-saudi.net/, viewed on 14 May 2010.

[8] Central Department of Statistics & Information (CDSI), (2009), available at http://www.cdsi.gov.sa, The Kingdom of Saudi Arabia.

[9] E-government Program (Yesser), The Ministry of Communications and Information Technology (2009), available at http://www.yesser.gov.sa.

[10] Schwandt, T 1994, Constructivist, interpretivist approaches to human inquiry. In Denzin NK and Lincoln YS, ed., *Handbook of Qualitative Research*, Thousand Oaks, CA: Sage, pp. 118-137.

[11] Mertens, DM 1997, *Research Methods in Education and Psychology: Integrating Diversity with Quantitative and Qualitative Approaches*, Thousand Oaks: Sage Publications.

[12] Creswell, J 2003, *Research design: Qualitative, quantitative, and mixed methods approaches,* 2nd ed., Thousand Oaks, Sage.

[13] Orlikowski, WJ and Baroudi, JJ 1991, "Studying information technology in organizations: research approaches and assumptions", *Information Systems Research*, vol. 2, no. 1, pp. 1-28.

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

[15] Strauss A and Corbin J 1990, *Basics of Qualitative Research: Grounded theory Procedures and Techniques*, Sage Publications, London.

[16] Glaser B 1992, *Emergence vs Forcing: Basics of Grounded Theory Analysis*, Sociological Press, Mill Valley, California.

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

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

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