Towards Secure M-Government Applications: A survey study in the Kingdom of Saudi Arabia

Towards Secure M-Government Applications

A survey study in the Kingdom of Saudi Arabia

Thamer Alhussain, Steve Drew
School of ICT
Griffith University
Gold Coast, Australia
Email: t.alhussain@griffith.edu.au; s.drew@griffith.edu.au

***Abstract*—This paper discusses a survey study of mobile communication users' perceptions regarding the security of m-government applications in the Kingdom of Saudi Arabia (KSA). We suggest that studying their perceptions will help to determine the preferred authentication technique among mobile users and therefore help ease the adoption of m-government. This paper presents questionnaire results that indicate the need for introducing an advanced authentication method for m-government. It became apparent that applying biometric technology can meet the users' requirements by providing secure m-government services.**

Keywords-m-government; security; authentication; mobile users; Saudi Arabia

I. INTRODUCTION

Recently, several governments have started to provide their services via mobile devices to take advantage of using these devices easily anywhere and at any time. As a complement to current e-government, mobile government (m-government) is using mobile and wireless technologies to deliver and improve government services [1]. However, the security of information being handled by device becomes more important, especially with the rapid growth of mobile devices to store large amounts of data.

This paper discusses the results of a questionnaire distributed to mobile communication users in the Kingdom of Saudi Arabia (KSA) regarding the security of m-government services. The aim is to gain an understanding of the preferred authentication system by mobile users in order to provide secure m-government services and promote public trust so as to successfully apply m-government. Firstly, the relevant literature is reviewed, followed by a description of the empirical research along with the results and conclusions.

II. NEED FOR SECURITY IN M-GOVERNMENT

Security is the most important issue facing m-government implementation [2, 3, 4]. It has been found that the security of m-government services is considered the hallmark of successful m-government [2]. Wireless networks are used to broadcast to mobile devices, which is vulnerable as this sends signals over the public airwaves [4]. Hence, the original specifications for security in the third generation (3G) networks identified the importance of the provision of advanced authentication approach for users [5]. Moreover, adequate levels of security and privacy must be ensured before implementing such wireless government applications [6].

Consequently, the increased use of mobile devices for storage of personal and sensitive data makes the need for a more advanced authentication approach essential. The current method of m-government security depends on a PIN to verify the user. This method has several weaknesses, especially in the relation to user authentication. Therefore, it is important for mobile services that require a higher level of security to implement a reliable authentication system to ensure that the users are who they claim to be.

III. ICT IN SAUDI ARABIA

A. *E-government in Saudi Arabia*

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 strict 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" or "simplify". 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 [7].

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 the most successful e-government service is the payment system called "Sadad" which has been implemented by the Saudi Arabian Monetary Agency in order to facilitate and streamline the bill payment transactions of end consumers via all banking channels, available including bank branches, ATMs, telephone banking, and Internet banking. In 2008, the

number of transactions conducted by Sadad has exceeded 5 million transactions per month, with a monthly growth rate of 22% [8].

B. M-government in Saudi Arabia

The use of mobile phones is rapidly increasing among the people in the KSA. According to the latest statistics in 2008, there were 36 million telephones (cellular mobiles), with only 7.7 million internet users of a total population of about 26 million [9]. Hence, as the number of mobile phone users is very high, delivering government services via mobile devices became the intention of the Saudi government. 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 as anyone who knows a student's number can get that student's results without their permission [10].

The Ministry of Interior also started to provide several services via mobile devices through its different sectors. For instance, 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 receive a text message containing the response.

However, while the majority of current m-government services in the KSA are based on the use of SMS, several government organisations are planning to introduce advanced applications.

IV. METHOD OF THE STUDY

Since the questionnaire is an effective method to explore people's attitudes and opinions regarding particular issues [11], it was used to gather the required data related to mobile communication users' perceptions of the security and authentication in m-government applications. In particular, the questionnaire was a printed document seeking responses to a selection of choices, with the participants having the opportunity to add their comments after each question. The literature on the security and authentication was used to help design the questionnaire. The method of sampling was purposive as it is a strategy in which "particular settings, persons, or activities are selected deliberately in order to provide information that can't be gotten as well from other choices" [12] (p.88).

Consequently, mobile communication users were approached in a range of public settings in the KSA. Users from both genders were sought from a range of relevant age groups and occupations to ensure that a representative sample of the user population was surveyed. A total of 420 questionnaires were distributed and 330 were returned; however, nineteen were excluded, because they were deemed incomplete. Thus, a total of 311 questionnaires were included in the data analysis.

V. DATA ANALYSIS

The Statistical Package for Social Sciences (SPSS) software was used to accomplish the statistical analysis of the 311 questionnaires. However, missing values were eliminated from the analysis. In this section, only those survey questions will be presented which are relevant to detecting problems in this context and seeking solutions for m-government security by understanding the perceptions of mobile communication users. The analysis includes the frequency and the percentage of the responses for each question, the Chi square value and its level of significance. This analysis took gender differences into account in order to examine whether there are differences between the responses of both genders or not.

A. Willingness to Use M-Government Services

This question explored the mobile users' willingness to use their device to get more government services.

TABLE I. CHI-SQUARE TEST FOR THE WILLINGNESS OF M-GOVERNMENT

Are willing to use your mobile phone to get more government services?	**Gender**				**Total**	
	Male		***Female***			
	No.	***%***	***No.***	***%***	***No.***	***%***
Yes	167	88.4	82	74.5	249	83.3
No	22	11.6	28	25.5	50	16.7
Total	189	100.0	110	100.0	299	100.0
Chi-square	9.528					
P-Value	0.002					

Table I indicates the results for the question, "Are you willing to use your mobile phone to get more government services?" The chi-square value (9.528) [P-value = 0.002] indicates statistical significance at the 0.01 level for the willingness of m-government services due to different genders. A high percentage of males (88.4%) and females (74.5%) are willing to use their mobile devices to get more government services, while only 16.7% of both genders are not willing.

B. Types of M-Government Services

This question sought to determine the preferred type of m-government service that participants would like to get from the government.

TABLE II. CHI-SQUARE TEST FOR TYPES OF M-GOVERNMENT SERVICES

Do you have a PIN or password to log onto your mobile device?	**Gender**				**Total**	
	Male		***Female***			
	No.	***%***	***No.***	***%***	***No.***	***%***
Only information inquiry	31	16.4	27	25.2	58	19.6
Any service not involving a payment	49	25.9	33	30.8	82	27.7
Services including payment	105	55.6	43	40.2	148	50.0
Special services	4	2.1	4	3.7	8	2.7
Total	189	100.0	107	100.0	296	100.0
Chi-square	7.208					
P-Value	0.066					

Table II shows the results for the question, "What kinds of service do you want to get from the government via your mobile phone?" The chi-square value (7.208) [P-value = 0.066] indicates no statistical significance. The highest percentage (50%) indicated 'Services including payment', with the majority of males (55.6%) and females (40.2%) choosing this option. The next was 'Any service not involving a payment' at 25.9% for males and 30.8% for females. The third option was 'Only information inquiry' for females (25.2%), which is more than the males (16.4%). However, only 2.7% of the participants indicated special services.

C. Lending the PIN and Password of a Mobile Device

This question investigated whether the users have lent the PIN or password of their mobile devices to somebody else.

TABLE III. CHI-SQUARE TEST FOR LENDING THE PASSWORD OF A MOBILE DEVICE

Have you ever lent the PIN or password of your mobile device to somebody else?	**Gender**				**Total**	
	Male		***Female***			
	No.	***%***	***No.***	***%***	***No.***	***%***
Yes	66	44.6	48	64.0	114	51.1
No	82	55.4	27	36.0	109	48.9
Total	148	100.0	75	100.0	223	100.0
Chi-square	7.501					
P-Value	0.006					

Table III indicates the results for the question, "Have you ever lent the PIN or password of your mobile device to somebody else?" The chi-square value (7.501) [P-value = 0.006] showed high statistical significance at the 0.01 level, which indicates that there is a gender difference among the participants for lending the password of their mobile device to somebody else. A majority (64%) of the females have lent the PIN or password of their mobile devices to somebody else, while the majority (55.4%) of males has not. The percentages of the total participants for both answers were close together, with a slightly higher percentage (51.1%) for those who have lent their password from both genders.

D. Required Level of Information Protection in Mobile Devices

This question explored the level of protection for privacy of information that the users require in their mobile devices.

TABLE IV. CHI-SQUARE TEST FOR THE REQUIRED LEVEL OF INFORMATION PROTECTION IN THE MOBILE DEVICE

What level of protection of privacy do you require for the information in your mobile device?	**Gender**				**Total**	
	Male		***Female***			
	No.	***%***	***No.***	***%***	***No.***	***%***
High protection	83	43.7	62	52.5	145	47.1
Moderate protection	76	40.0	40	33.9	116	37.7
Low protection	24	12.6	12	10.2	36	11.7
No protection	7	3.7	4	3.4	11	3.6
Total	190	100.0	118	100.0	308	100.0
Chi-square	2.326					
P-Value	0.507					

Table IV shows the results for the question, "What level of protection of privacy do you require for the information in your mobile device?" The chi-square value (2.326) [P-value = 0.507] indicated no statistical significance. 'High protection' was an important level at 47.1% (43.7% for males and 52.5% for females). The second most important protection level was 'Moderate protection' at 40% for males and 33.9% for females. 'Low protection' ranked second last (12.6% for males and 10.2% for females), while only 3.6% of the participants from both genders indicated no need for protection.

E. The Preferred Authentication Method

This question tried to determine the most preferred authentication method for mobile users for the information security of their mobile device.

TABLE V. CHI-SQUARE TEST FOR THE PREFERRED AUTHENTICATION METHOD FOR MOBILE DEVICES

Which authentication method would you like to have to protect the important information in your mobile device?	**Gender**				**Total**	
	Male		***Female***			
	No.	***%***	***No.***	***%***	***No.***	***%***
PIN or password	82	42.7	41	36.6	123	40.5
Biometric	106	55.2	69	61.6	175	57.6
Other	4	2.1	2	1.8	6	2.0
Total	192	100.0	112	100.0	304	100.0
Chi-square	1.186					
P-Value	0.553					

Table V shows the results for the question, "Based on information about authentication that was provided, which authentication method would you like to have to protect the important information in your mobile device?" The chi-square value (1.186) [P-value = 0.553] indicates no statistical significance, which points out that there is no gender difference between the participants in the preference authentication method for a mobile device. The biometric method (57.6%) was the preferred authentication method (55.2% of males and 61.6% of females), followed by the PIN or password (42.7% for males and 36.6% for females).

F. Confidence of Biometrics in M-Government

This question investigated whether applying biometric authentication in m-government will provide users with the confidence to perform more government services via their mobile devices.

TABLE VI. CHI-SQUARE TEST FOR CONFIDENCE IN USING BIOMETRICS IN M-GOVERNMENT

Will the use of biometrics give you confidence to perform more government services via your mobile device?	**Gender**				**Total**	
	Male		***Female***			
	No.	***%***	***No.***	***%***	***No.***	***%***
Yes	176	91.2	106	89.8	282	90.7
No	17	8.8	12	10.2	29	9.3
Total	193	100.0	118	100.0	311	100.0
Chi-square	0.160					
P-Value	0.689					

Table VI shows the results for the question, "Will the use of biometric authentication give you confidence to perform more government services via your mobile device?" The chi-square value (0.160) [P-value = 0.689] showed no statistical significance, which indicates that there is no gender difference between participants regarding the confidence of using biometrics in m-government. The highest percentage (90.7%) of the participants from both genders indicated that the use of biometric authentication in m-government will give them the confidence to perform more m-government services. Only 9.3% of the participants (8.8% of males and 10.2% of females) answered 'No'.

G. Correlation Between the Risk of Disclosure of Personal Information and the Preferred Authentication Method of M-Government

This question explored whether the preference of an authentication method for m-government services is related to the experience of facing a risk of disclosure of sensitive or personal information when a mobile device has been lost. Table VII below reveals the percentage of each category of the responses, the chi-square value and its level of significance.

TABLE VII. CHI-SQUARE TEST FOR THE RISK OF DISCLOSURE OF PERSONAL INFORMATION AND THE PREFERRED AUTHENTICATION METHOD OF M-GOVERNMENT

If you are conducting a government service transaction via your mobile device, which authentication method would you prefer to use?	**Have you been in a situation where there is a risk of disclosure of sensitive or personal information?**				**Total**	
	Yes		***No***			
	No.	***%***	***No.***	***%***	***No.***	***%***
PIN or password	20	39.2	35	51.5	55	46.2
Smart cards	7	13.7	12	17.6	19	16.0
Biometric (e.g. fingerprint scan)	24	47.1	17	25.0	41	34.5
Other	0	0.0	4	5.9	4	3.4
Total	51	100.0	68	100.0	119	100.0
Chi-square	8.344					
P-Value	0.039					

Table VII shows the chi-square value (8.344) [P-value = 0.039] that indicates statistical significance at the 0.05 level. This points out that there is a difference between participants in the preferred authentication method related to their experience of facing a risk of disclosure of their sensitive or personal information when their mobile devices have been lost. The percentage was 51.5% for the participants who were not concerned about the risk of disclosure of sensitive information when their mobiles had been lost and preferred to use a PIN or password when conducting a government service transaction via a mobile device. Conversely, 25% of the participants who were not concerned about the risk of disclosure of sensitive information preferred the biometric method to be the authentication method for m-government services. However, 39.2% of the participants were concerned about the risk of disclosure of sensitive information and preferred to use a PIN or password as the authentication method, while 47.1% of the participants who were concerned about risk of disclosure of sensitive information preferred the biometric method as an authentication method. It can be concluded that the participants concerned about the risk of disclosure of sensitive information had a high percentage in preferring the biometric method as an authentication method. Therefore, there is a positive relationship between the risk of disclosure of sensitive information and the preference for the biometric method as an authentication method.

H. Correlation Between the Trust in Biometrics in M-Government Security and the Reasons for not Conducting any Government Service via a Mobile Device

This question explored whether applying biometric authentication in m-government security would increase trust in conducting m-government services. Table VIII below reveals the percentage of the responses to each category, the chi-square value and its level of significance.

TABLE VIII. FREQUENCY FOR THE TRUST IN BIOMETRICS IN M-GOVERNMENT SECURITY AND THE REASONS FOR NOT CONDUCTING ANY GOVERNMENT SERVICE VIA A MOBILE DEVICE

Why have you not conducted any government service transaction via your mobile device?	**Would the use of biometric authentication increase your trust in the conduct m-government services?**				**Total**	
	Yes		***No***			
	No.	***%***	***No.***	***%***	***No.***	***%***
Cost reasons	26	83.9	5	16.1	31	100.0
Service availability reasons	90	90.9	9	9.1	99	100.0
Security reasons	19	82.6	4	17.4	23	100.0
Issues of mistrust	43	86.0	7	14.0	50	100.0
Other	23	95.8	1	4.2	24	100.0
No. of Cases	168		20		188	

Table VIII shows whether applying biometrics in m-government would increase trust in conducting m-government services for those who mentioned security and mistrust as reasons for not conducting previous m-government services. For the participants who gave security reasons for not conducting government service transactions on a mobile device, 82.6% said that biometric authentication would increase their trust in these transactions, while 17.4% said that biometric authentication would not increase their trust in these transactions. For the participants who gave mistrust reasons for not conducting government service transactions on a mobile device, 86% said that biometric authentication would increase their trust in these transactions, while only 14% said that biometric authentication would not increase their trust in these transactions.

VI. DISCUSSION

It is firstly noteworthy that the analysed questions reveal no statistical differences between both genders among their responses. However, the results indicated that a majority (83.3%) of the participants are willing to use their mobile devices to get government services. This result might be understood in terms of the perceived benefits of conducting m-government applications, especially with the advantage of using mobile devices easily anywhere and at any time. This concurs with [13] who stated that m-government provides a

unique opportunity to deliver personalized services to citizens, and the individual citizens can reach the service wherever they are and whenever they need it.

However, a small majority (51.1%) of the respondents have lent the PIN or password of their mobile devices to somebody else, which relates to the literature finding by [14] who found that 26% had shared their PIN with someone else. This result indicates that the PIN and password face important challenges in terms of correct usage.

The results further demonstrate that a majority of the participants indicated that they require a high level of protection of privacy for the information in their mobile device, while 57.6% placed biometrics as the most preferred authentication method to protect the important information in their mobile device. These results reflect two of the literature findings [15] and [16] which negate the concern regarding the lack of the citizens' information privacy and fear of information leakage as one of the challenges for implementing e-government in the Kingdom of Saudi Arabia. In particular, [17] and [18] emphasized that privacy and security concerns play a significant role in the adoption of e-government.

Moreover, the highest percentage (90.7%) of the participants indicated that the use of biometric authentication in m-government would give them the confidence to perform more m-government services; however, the participants concerned about the risk of disclosure of sensitive information had a high percentage in preferring the biometric method as an authentication method. In addition, 82.6% of the participants who gave security reasons for not conducting government service transactions on a mobile device said that biometric authentication would increase their trust in these transactions. This agrees with the literature where security was determined as the most important issue facing m-government implementation [2, 3, 4] and the finding that biometric technology can be used to improve the performance of security applications [19].

VII. CONCLUSION

A study was undertaken to investigate mobile communication users' perceptions and concerns about the security and authentication of m-government applications. This was done to determine the preferred authentication method by users to get their acceptance and gain successful implementation of m-government services in a secure manner. The results supported a number of findings reported in the literature regarding the security and authentication of mobile devices and government services. Analysis of the results shows that mobile users are concerned about their personal and sensitive information stored in their mobile devices. It further confirmed their need for an advanced authentication system such as biometrics to protect the important information in mobile devices and for conducting m-government services. Based on the results, we suggest that biometric authentication should take place in m-government applications to enhance security and meet the users' requirements. However, this should take into account the factors influencing the implementation of biometrics in m-government security, which we will try to determine by completing this ongoing research project.

REFERENCES

[1] 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.

[2] 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.

[3] Sandy, GA and McMillan, S 2005, A Success Factors Model For M-Government, EURO mGOV 2005, Brighton, UK, pp. 349-358.

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

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

[7] E-government Program (Yesser), The Ministry of Communications and Information Technology (2010), available at http://www.yesser.gov.sa.

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

[9] World Fact Book 2010, Central Intelligence Agency, available at https://www.cia.gov/index.html.

[10] 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.

[11] Fraenkel, J and Wallen, N 2000, How to design & evaluate research in education, McGraw-Hill, New York.

[12] Maxwell, J 2005, Qualitative Research Design: An Interactive Approach (2nd Ed). Thousand Oaks, Sage Publication.

[13] Snellen, I and Thaens, M 2008, From e-government to m-government: towards a new paradigm in public administration, viewed on 12th January 2009 at http://unpan1.un.org/intradoc/groups/public/documents/CAIMED/UNPAN028992.pdfH.

[14] Clarke N, Furnell S, Rodwell P, and Reynolds P, 2002, Acceptance of subscriber authentication methods for mobile telephony devices, Computers and Security, Vol. 21, No. 3, pp. 220-228.

[15] Alsuwail, M. 2001, Directions and local experiences, Foundations and Requirements of E-Government, E-Government Conference, Institute of Public Administration, the Kingdom of Saudi Arabia.

[16] Alshareef, T 2003, E-Government in the Kingdom of Saudi Arabia, Applicational Study on the governmental mainframes in Riyadh City, King Saud University.

[17] Alharbi, S 2006, Perceptions of Faculty and Students toward the Obstacles of Implementing E-Government in Educational Institutions in Saudi Arabia, West Virginia University.

[18] Conklin, W 2007, Barriers to Adoption of e-Government, Proceedings of the 40th Hawaii International Conference on System Sciences.

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