Journal of Statistics Applications & Probability
An International Journal

http://dx.doi.org/10.18576/jsap/130110

Development of a Secure Model for Mobile Government Applications in Jordan

Ala'a Saeb Al-Sherideh[1,], Roesnita Ismail[2], Mohammad Rasmi Al-Mousa[1], Khaled Al-Qawasmi[1], Ala'a Al-Shaikh[1], Hebatullah Awwad[1], Khaled Maabreh[3] and Mohammad Alauthman[4]*

[1]Department of Cyber Security, Faculty of Information Technology, Zarqa University, Zarqa, Jordan
[2]Department of Information Security and Assurance, Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai, Malaysia
[3]Department of Data Science and Artificial Intelligences, Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan
[4]Department of Information Security, Faculty of Information Technology, University of Petra, Amman, Jordan

Received: 17 May 2023, Revised: 20 Aug. 2023, Accepted: 7 Sep. 2023.
Published online: 1 Jan. 2024.

Abstract: This paper develops a secure model for mobile government (M-G) applications using effective privacy methods and validates the model through semi-structured interviews with eight Jordanian e-government experts. The experts emphasized the importance of M-G applications in enhancing services such as bill payments, civil services, civil defense, and police services. To improve privacy, the experts suggested methods such as strong textual passwords, data encryption, login tracking, SMS login confirmation, and signup confirmation. Based on these suggestions, a prototype with suggested privacy features was developed using Android programming, and a questionnaire was administered to 150 Jordanian citizens who confirmed the ease of use and usefulness of the proposed privacy model. This paper expands the acceptance of M-G applications and recommends privacy methods to improve their security. The study highlights the importance of security and privacy as acceptance factors for M-G applications in developing countries and suggests that further studies can investigate advanced privacy and suitable security methods for M-G applications in other developing countries.

Keywords: Mobile Government (MG), Mobile Applications, Security, Privacy, Government Services.

1 Introduction

In recent years, mobile technologies and applications have become more important in every aspect of our personal and professional lives [1-2]. Mobile technologies have been adopted by businesses for a variety of applications in order to increase operational efficiency by providing greater access to real-time information. They have increased their responsiveness and competitiveness by taking advantage of the mobile revolution to meet new customer demands [3-4-5-6-7]. This evolving mobile paradigm provides users with location independence and personalization when accessing information and applications, improving user satisfaction. Mobile applications can also provide context-aware responses based on the user's location, time of use, or other factors. [1-8].

A mobile application is a software application designed specifically for use on small and wireless computing devices [9]. Mobile applications are programs or software that run on a mobile device and perform specific tasks for the user [10]. The mobile application is a new and fast-developing segment of the global information and communication technology. The mobile application is easy, user-friendly, inexpensive, and downloadable, and is run in most mobile phones including inexpensive and entry-level phones [11].

The e-government applications can be defined as the government services that conducted using technology platforms such as online websites using computers, pads or laptops [11]. The next-generation e-government service development, which is sometimes referred to as M-G (or mobile government), is the extension of e-government to mobile platforms as well as the strategic use of government services and applications which are only possible using wireless computing devices and wireless internet infrastructure [12-13].

The importance of M-G has grown due to its ability to collect real-time and location-based data from citizens [13-14-15]. As a result, the effort and time required to use government services could be reduced. On the other hand, m-government can be customized as a new service through data integration among government ministries, allowing many services to be accessed through a single window.

Security and privacy features are critical requirements for mobile applications [16-17-18-19-20-21-43-44]. Security is concerned with preventing threats such as viruses and worms from attacking or damaging services and information. The purpose of privacy is to ensure legal access to services and information, such as through the use of passwords. The inadequacy of a mobile application's security and privacy affects the motivation to use it [14], this reduces user acceptance of using mobile applications. As a result, the adoption of mobile applications by organizations will be reduced, preventing the benefits gained from using mobile applications from being realized. Because of variables related to security requirements, security and privacy are major concerns in the development of M-G applications [18-19-20-21-46].

In this context, the researchers defined two main concepts of M-G security. Firstly, mobile security is defined as the authentication and confidentiality of mobile applications [18-19]. The security represented by protocols includes cross-platform communications with encryption, signature, and authentication to improve mobile application development capabilities by establishing a secure communication

*Corresponding author e-mail: asherideh@zu.edu.jo

system among networks. Secondly, the privacy of mobile applications can be defined as the permissions in the usage of resources assigned to different actors of a wide mobile network [20-21-45]. Two subjects are important: the data holders and the data collectors. Data holders must be able to feed data collectors only with the data regarding a specific target. At the same time, data collectors must be able to identify or authenticate users as legitimate data holders where the information is collected.

In this paper suggesting suitable privacy methods to improve the motivation level of use the M-G applications by the citizens. The paper is organized as follows: section II presents the related works. Section III Research Methodology. Results and Discussion are presented in section IV. Finally, section V Conclusion and Future Works.

2 Related Work

This paper aims to suggest the practical methods that could enhance the privacy levels of the M-G applications. Hence, this section reviewed the methods that can be used to improve M-G security and privacy.

This section presents the security methods of mobile applications in general due to the lack of practical evidence of the security methods that could enhance the security performance of the M-G application. One of the most basic security models that can be adopted for mobile applications is known as the C-I-A triangle. This model is designed from three principles: confidentiality, integrity, and availability [22]. Confidentiality refers to the requirement that unauthorized parties be prevented from reading the data. Data integrity safeguards data against changes during storage or transmission. The availability of data and information services ensures that authorized parties can access them when they need.

The McCumber Information Systems Security (INFOSEC) model proposed in 1991. Figure 1 depicts the McCumber INFOSEC model, and INFOSEC is defined as “Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats”.

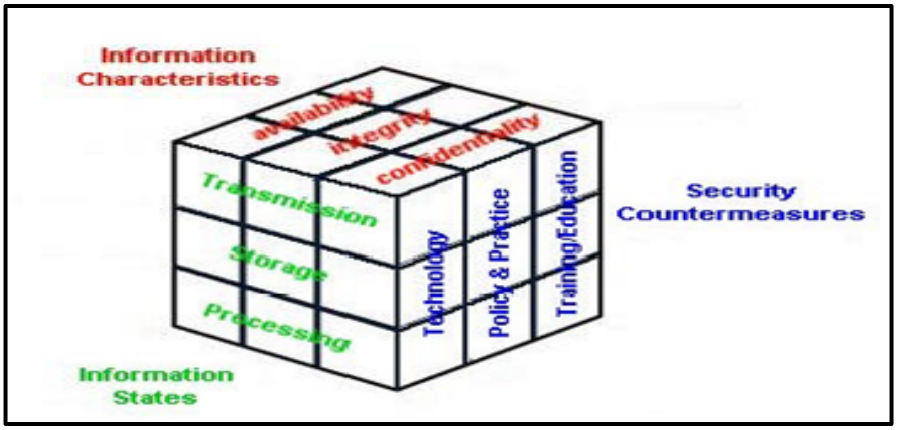

Fig. 1: McCumber INFOSEC Model

The McCumber model has three components for analyzing all aspects of information security. The first area is concerned with information characteristics including confidentiality, integrity, and availability, which are simply referred to as the C-I-A triangle. The second component of this model is the information states, which are concerned with the state in which the information exists. Information can be in one of three states (transmission, storage, or processing), each with its own set of security concerns. The third component of the McCumber INFOSEC model addresses security countermeasures related to information system defense. Technology, policy, and practice, as well as training and education, are all part of the security countermeasures. Technology encompasses all of the components, including hardware and software that the system employs to ensure its security. Policies and practices have an impact on an organization's overall security. However, system user training and education are important security countermeasures because users have a large impact on the success of such information security systems.

To summarize, two security features need to be considered for M-G applications:

- Authentication (privacy): Ensuring that parties with access to a service or device are trusted and not imposters.
- Protection (security): Preventing strangers from taking any action on services or data.

Many studies on the security and privacy of mobile applications have been conducted. Huang et al. [16] concentrated on the privacy and security methods used by mobile health applications. Two main methods were proposed: (1) ensuring the authority of mobile application users by generating a random key or code and sending it as an SMS to use the login procedures, and (2) encrypting the data stored in the server and decrypting the data once the user requests data from the server using a secret decryption key stored in the users' mobiles.

Many researchers have concentrated on data and service encryption stored in mobile application servers [23-24-25-26]. The data and services are encrypted in the server and are decrypted once they arrive at a mobile device. Then, using a secret decryption key, the mobile device can decrypt the services and data, and the data received by the server is encrypted again. This type of encryption is known as an asymmetric algorithm (the destination and source of data have different encryption and decryption keys).

In the same context, Qi and Gani [27] referred to the possibility of a midline assault on the data collected between the mobile application and the servers (connection path). They suggested two remedies to get around this issue. The first option is to boost data transport speed utilizing modern technology like fiber optics to make data attacks more challenging. To lessen the probability of data waiting in the connection channels, the second method is to transfer the amount of data in accordance with network and mobile specifications. The options

for attacking operations rise as a result of the data waiting. Qi and Gani [27] claimed that in order to lower security requirements, it is crucial to categorize the data and services housed on the server according to its security levels (i.e. focus on the private data and services and give less attention to public data and services).
Many academics have proposed efficient security measures for mobile applications based on server and client signature matching [28-29-30]. On the network, every legitimate, active cellphone has a unique signature. The user of the mobile application can access the server's services and data once the server's signature and the signature on the mobile device have been verified. Otherwise, the network will ban and disable the mobile device. As a result, the predetermined signatures can be used to determine the trust level of mobile devices.
In another work of mobile application security conducted by Ibukun and Daramola [31], According to the researchers, antiviral software is useful for identifying and stopping unauthorized transactions and attacks on services and data. However, antivirus software requirements for wireless (mobile) networks differ from those for conventional wire connections [32]. As a result, it's essential to create or employ the best antivirus software based on the requirements and environment of mobile applications.
In the context of mobile application privacy, Chow et al. [33] and Khamis et al. [34] claimed that one of the earliest and most reliable privacy measures is accessing programs or accounts with the correct login and password. Strong passwords should be used by users to make unauthorized access more difficult [35-36-42].
Rassan and Al Shaher [37] mentioned that mobile application access using passwords is necessary. However, this method has many drawbacks such as the possibility of stealing the password by watching from other users. Rassan and Al Shaher [37] argued that accessing utilizing tangible objects connected to the user themselves might increase the level of accessing authority's privacy. One of the most practical accessing methods to confirm the legitimacy of mobile applications access is using a user's fingerprints [38].
Also, Wang et al. [39] agreed that in addition to using a login and password, extra privacy measures must be created or adopted. And suggested password encryption as a supportive method to enhance the privacy level of the mobile application accessing. Password encryption increases the difficulty of attacks or stealing users' passwords.
Based on the conducted works and studies of the mobile applications, security and privacy methods can be classified into three layers:
Mobile services layer: the mobile services and information stored in the central database can be secured using many activities such as data encryption and antiviruses. Another important activity of mobile services security is the classification of services as public or private services. Public services (such as public alerts for all citizens) are not important to be secured which reduces the cost of security processes.
Mobile devices (users) layer: this layer can be secured through many methods such as assigning usernames and passwords for each connected device with mobile services, encrypting the password of the mobile when it is gathered with the service's server, and installing an antivirus to protect the mobiles from attacks.
Connection layer: the connection between mobile devices and mobile services can be secured using several activities such as defining the mobile signature on the network to prevent the strange mobile from accessing this network, assuring the speed of data transfer via network to increase the difficulty of data attack, and assure compatibility between mobile specification (i.e. processor) and transferred data styles and capacity.
In developing countries, there are restrictions on the models development that are used to structure the security and privacy or methods of M-G applications. In order to raise the security level of M-G applications, this study intends to provide a novel model that offers useful privacy solutions.

3 Research Methodology

The interview is an important method to collect useful data by experts to support research development. The interview can be defined as a method to collect qualitative data depending on open questions to analyze useful variables or methods according to a research case study [40].
A qualitative method was applied in this research in order to gain rich understanding of such reasons. The employed data collection method was semi-structured interviews with public and private sector employees. The interviews were done based on in-person discussions with specialists in order to validate the contents of the interview in relation to the associated purpose. In order to satisfy the associated objectives, any necessary modifications to the interview questions, clarification of any unclear portions or items, and addition of any necessary information were done so directly with the experts. In other words, the experts are crucial in validating the interview's contents in light of the stated goals.
All experts were leaders in the Jordanian institutions, whereby the quality of the collected responses was high due to the respondents' understanding of M-G services and its requirements in Jordan. Furthermore, all experts selected had extensive experience in governmental services. Hence, they were able to provide rich and useful information about the requirements of the M-G application in Jordan.
The responses from the interview transcripts were analyzed using the content analysis method. Any endeavor to reduce and make sense of qualitative data after gathering a large amount of qualitative material can be referred to as a content analysis method [41]. In other words, the qualitative content analysis items often include texts that have been carefully chosen to contribute to and address the study topics. When there are few responses to be analyzed, content analysis is a useful technique.

4 Results and Discussion

This section provides the required qualitative data analysis with experts in order to determine the most suitable privacy features for M-G applications. Based on the qualitative data analysis, the development and validation of the privacy model for the M-G applications are explained.

A. Qualitative Data Analysis

The qualitative data was collected using interviews with eight experts in electronic government services in Jordan. The main aim of the interview is to determine the privacy features and methods that could improve the acceptance in M-G services. The interview data was collected based on four parts: (1) personal information, (2) overview of M-G applications, (3) services of M-G applications, and (4) privacy

of M-G applications.

The first part of the interview (personal information) aims to assure the characteristics validity of the respondents to confirm the data's usefulness. The most significant items in this part are the organization of respondent, working position, years of working experience and expert domain. Table 1 summarizes the personal information of the experts.

Table 1: Experts' Personal Information

Expert	Working position	Experience years	Experience domain
Expert #1	Information security manager	Six years	Information security
Expert #2	Chief technical officer	Nine years	IT security
Expert #3	Project manager	More than 11 years	Information technology
Expert #4	Analyst	15 years	Information technology
Expert #5	System engineer	5 years	System security
Expert #6	Security administrator	Eight years	System security
Expert #7	Information security specialist	12 years	Information security
Expert #8	Director of E-services	25 years	IT applications

The above Table 1 shows that all experts have more than five years' experiences in the information technology domain. Most of them are specialists in information technology security. On the other hand, the experts' positions (i.e. analyst, system engineer, project managers and security administrator) are effective to enrich this research by providing useful information about the privacy of M-G applications. Furthermore, the experts working in organizations are directly related with electronic government services. All these justifications qualify the involved experts to provide useful information to construct the proposed privacy model of M-G applications.

The second part of the interview represents the main interview codes, and this part presents the overview of M-G applications and the benefits and challenges of M-G applications in Jordan. Table 2 summarizes the feedback of the experts on this part.

Table 2: Summary of M-G Applications

Expert	Usability of M-G applications in Jordan	Benefits	Challenges
Expert #1	✓	Speed up the governmental services.	Acceptance in using the applications by the users.
Expert #2	✓	Reduce the services mistakes.	Acceptance of using the applications.
Expert #3	✓	Reduce the efforts of conduct the services.	Ability to use the applications by all citizens due to mobile and communication requirements.
Expert #4	✓	Improve the public services (i.e. reduce costs and time)	Communication requirements.
Expert #5	✓	Accessibility and availability of the services.	Experience in using the applications by the citizens.
Expert #6	✓	Reduce the operational costs.	Security and privacy.
Expert #7	✓	-Real time services. - Reduce the operational costs.	Privacy of the applications.
Expert #8	✓	Accessibility and availability of the services.	Awareness of using the M-G applications.

In total, the experts encourage using of M-G applications in Jordan due to many reasons, for example, reducing the time of services, reducing the efforts, reducing the operational costs and the services availability and accessibility. However, many issues need to be resolved in order to ensure the success in adopting M-G applications. Security and privacy is the most important issue in using the M-G applications by the citizens. Other issues are the technology requirements of M-G applications and the users' skills in using these applications.

The third interview part focuses on the second interview code, which are the services that could benefit from the M-G applications. Table 3 summarizes the experts' responses about the third interview part.

Table 3: Services Based on M-G Applications

Expert	Service Type	Current Services	Service in Plan	Expected Services
Expert #1	Bill Payment (i.e. Water, electricity, telecommunication).	Investigation about bills through WhatsApp. - Pay using third party application	Simplify the direct payment through pay cards.	Read the online records, calculate payment, and conduct payment (full electronic services).
Expert #2	-Bill Payment. -Civil (produce and renew passport and identity cards).	-Pay using third party application - Send SMS when the civil services are complete by government side	-Simplify the direct payment through pay cards. -One online window for all civil services.	- Full M-G applications without face to face utilization of services.
Expert #3	-Bill Payment. -Citizens' complaints.	-Pay using third party application - Receive the citizens' complaints about some services.	-Simplify the direct payment through pay cards. - Allow the citizens to present their complaints about all services.	- Full M-G applications that managed by the government departments. - analyze the huge citizen's complaints using artificial methods.
Expert #4	- Bill Payment. -Police services (traffic violation and notice of traffic accident).	- Pay using third party application - Send SMS about road traffic	- Avoid the third party payment of bills. - No planned services for police services.	- Full M-G applications that managed by the government departments. - Utilize the police services using M-G applications.
Expert #5	- Civil Services. - Civil defense (i.e. fires and Ambulances).	Send SMS when the civil services are complete by government side. - no services for civil defense services	Send the online locations (using WhatsApp) for civil defense services	- Full M-G applications without face to face utilization of services. - Online M-G services for civil defense cervices.
Expert #6	- Civil Services. -Police services.	-Pay using third party application	Avoid the third party payment of bills.	Full M-G applications without face to face utilization of services.
Expert #7	- Bill Payment.	Send SMS when the civil services is complete by government side	One online window for all civil services.	Full M-G applications that managed by the government departments.
Expert #8	- Bill Payment. - Civil defense.	-Pay using third party application	Use adopted services by the government without third party supporting	Full M-G applications without face to face utilization of services.

Based on the above Table 3, the experts encourage the use of M-G applications in various public services in Jordan. The experts mentioned that partial M-G services are applied in Jordan, and it is expected to apply the full online M-G application to operate full public services. The challenges explained in the previous interview parts need to be resolved prior to applying full M-G services in the future.
The fourth interview part is designed to discuss the privacy methods and features that could improve the privacy level of M-G applications in order to enhance the citizens' acceptance of M-G applications. Table 4 summarizes the experts' responses about the privacy features and methods of M-G applications.

Table 4: Privacy Features and Methods of M-G Applications

Expert	Privacy Method	Privacy Features
Expert #1	Data Encryption	The Encryption of username and password could increase the privacy level of M-G applications.
Expert #2	Strong password	The privacy level of M-G applications would be improved through login using strong passwords (minimum 8 letters, mixed letters numbers and special characters, and include capital letter)
Expert #3	- Data encryption -Track login places and devices	- Encrypt password in database. - Inform the users about the login history such as the used devices IP and login places.
Expert #4	-Login confirmation - Strong password	At login process, the security code is sent as an SMS to complete the login processes. - The user should provide private password of specific features.
Expert #5	-Confirm the signup	- At signup, the user should provide security code that is sent to an Email.
Expert #6	- Data Encryption	Encrypt the username and password in database.
Expert #7	-Login confirmation - Data encryption	Encrypt the username and password in database.
Expert #8	- Data encryption - Strong password	- At login process, the security code is sent as an SMS to complete the login processes.

Based on the above Table 4, the experts confirm that the privacy of M-G application is necessary to improve the privacy of M-G applications. The experts proposed many privacy methods and features to improve the privacy level of M-G applications.
In summary, the experts propose five main privacy methods for M-G applications: (1) encrypt the username and password in the database, (2) have strong textual passwords, (3) track the login history, (4) have a security code for every sign-in, and (5) get a signup confirmation. The next section explains the design and development of privacy M-G model based on the proposed methods by experts.

B. Design and Development of Privacy Model for M-G Applications

According to the interview analysis, the design of the privacy model for M-G application should contain five main privacy methods; data encryption, strong textual password, login confirmation, signup confirmation, and track the login history. Figure 2 illustrates the design of the proposed privacy model for M-G applications.

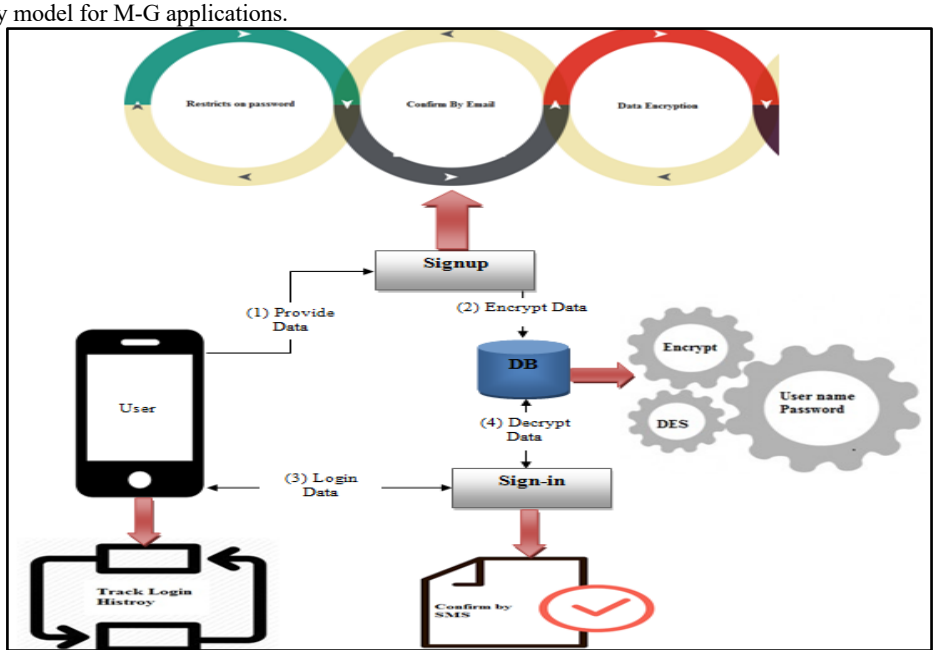

Fig. 2: Design of the Proposed Privacy Model for M-G Applications

The above Figure 2 clarifies the design of the proposed privacy model for M-G applications. Firstly, the users need to sign up using sufficient data. At signup process, the user needs to provide effective textual password forms that contain a minimum of eight letters, mixed letters (characters, numbers, capital characters, and special characters), and the password is not allowed to contain parts of the username. When the success data is registered, the users need to confirm the registration through entering a security code sent to the user's email. Having succeeded in entering the confirmation code, the username and password are encrypted and stored in the database.
Secondly, the database (usernames and passwords) needs to be encrypted using an effective encryption approach. The Data Encryption

Standard (DES) approach could be selected for data encryption due to its effectiveness in encrypting textual data. DES is a symmetric-key algorithm for the encryption of electronic data. Despite its short key length of 56 bits, it is secure for most textual applications, and it is highly influential in the advancement of modern cryptography. Thirdly, the users need to provide a security code of four numbers to access their profiles. This code is sent in an SMS for the users' mobiles at every login process. The successful login using the username, password, and security code leads to decrypting the user database in order to benefit from the government services. Fourthly, the users can track the history of account login places and devices in order to ensure that no illegal accessing has happened by strange places or devices.

Based on the design of the proposed privacy model of M-G applications, a prototype is developed as an Android application to present the privacy methods and features. The Android Studio programme was used to utilize the proposed prototyping due to its integration with most mobile platforms and features. Android Studio is the official integrated development environment (IDE) for Google's Android operating system built by JetBrains' IntelliJ IDEA software and designed specifically for Android development. It is available for downloading on Windows, Mac OS and Linux-based operating systems. It is a replacement for the Eclipse Android Development Tools (ADT) as the primary IDE for native Android application development.

C. Model Validation

The previous section explains the design and prototyping of the proposed privacy model for M-G applications. This section discusses the validation of the proposed privacy model based on the conducted prototype.

The ease of use and usefulness of the proposed prototype was validated by 150 Jordanian citizens who use the privacy methods. The main aim of the validation was to ensure that the proposed privacy model of M-G applications is accepted by the Jordanian citizens in order to judge the acceptance in the proposed privacy model.

The questionnaire was collected directly from the citizens and analyzed using SPSS tool version 23.0. The SPSS tool is effective to analyze the quantitative data collected from a large sample. In order to assure the usefulness of questionnaire responses, the demographic data of the respondents were analyzed based on six demographic variables: (1) gender, (2) age, (3) education level, (4) marriage status, (5) province, and (6) experience of using the mobile applications. Table 5 summarizes the analysis of the demographic variables.

Table 5: Analysis of the Demographic Variables

Variable		Frequency	Percentage
Gender	Male	97	65%
	Female	53	35%
Age (years)	20-30	28	19%
	31-40	83	54%
	41-50	19	13%
	51-60	10	7%
	More than 60	10	7%
Education Level	School	0	0%
	Medium College	46	31%
	University degree	91	61%
	Postgraduate degree	13	8%
Marriage status	Married	88	59%
	Single	62	41%
The province where you live	Amman	38	25.3%
	Balqa	5	3.3%
	Madaba	5	3.3%
	Irbid	35	23.3%
	Jarash	5	3.3%
	Ajloun	5	3.3%
	Mafraq	5	3.3%
	Zarqa	32	21.3%
	Tafila	5	3.3%
	Aqaba	5	3.3%
	Karak	5	3.3%
	Ma'an	5	3.3%
Experiences of using mobile applications	Never	4	3%
	< 6 months	22	15%
	6-12 months	12	8%
	1-2 years	53	35%
	Above 2 years	59	39%

Based on the above Table 5, the data were collected from both genders, male (65% of all respondents) and female (35% of all respondents),

whereby the collected responses represent the citizens' opinions of both genders. On the other hand, the majority of respondents' ages were from 20 to 50 years. The citizens in this age understood the governmental services because as they used these services in their daily lives. Hence, the responses could be useful to support the citizens' vision of M-G services.
Moreover, all respondents were educated i.e. medium college, undergraduate, and postgraduate. Thus, the respondents were able to provide their responses based on a good understanding of the questionnaire factors due to their education levels. Furthermore, the respondents' social statuses were mixed (married and single). This enriches the study of the acceptance of M-G application based on different social perspectives.

Additionally, the collected responses represent the various geographic regions of Jordan based on the normal distribution of the citizens on the Jordanian province. The largest responses were collected from Amman, Irbid, and Zarqa (25.3% from Amman city, 23.3% from Irbid city, and 21.3% from Zarqa city) due to the large number of citizens in these three cities. The number of citizens in other cities were near, whereby the collected responses from these cities were same (3.3%). Lastly, the majority of respondents had experience in using mobile applications for more than one year (74% of all respondents), which support the understanding of M-G applications. In total, the characteristics of the respondents were effective to present useful data to validate the proposed model of M-G applications. Table 6 presents the frequency analysis of the responses on the ease of use and usefulness of the proposed privacy prototyping for M-G applications.

Table 6: Validation Frequency Analysis of Proposed Privacy Prototyping

Ease of Use						
Items		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	Overall privacy functions are simple to be conducted.	2 (1%)	2 (1%)	14 (9%)	72 (48%)	60 (41%)
2.	Overall privacy methods and feature are clear.	4 (3%)	9 (6%)	29 (19%)	91 (61%)	17 (11%)
3.	The privacy methods and features are conducted in short time.	0 (0%)	0 (0%)	3 (2%)	54 (36%)	93 (62%)
Usefulness						
Items		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
4.	The privacy features and methods are useful to prevent the illegal accessing by strangers.	3 (2%)	5 (3%)	13 (9%)	50 (33%)	79 (53%)
5.	I prefer to use the M-G application that includes privacy methods and feature such as the presented.	3 (2%)	6 (4%)	29 (19%)	85 (57%)	27 (18%)
6.	The proposed privacy methods and features motivate me to use the M-G applications.	0 (0%)	3 (2%)	47 (31%)	61 (41%)	39 (26%)
7.	In total, I accept the M-G applications of privacy level based on the presented methods and feature.	2 (1%)	4 (3%)	17 (11%)	73 (49%)	54 (36%)

Based on the validation frequency analysis of the proposed privacy methods of M-G applications, Table 7 presents the validation descriptive analysis of the proposed privacy methods. The mean level indicates the high agreement with all validation items of the proposed privacy methods of M-G applications.

Table 7: Validation Descriptive Analysis of Proposed Privacy Prototyping

No.	**Items**	**Mean**	**Agreement Level**
1	Overall privacy functions are simple to be conducted.	4.24	High
2	Overall privacy methods and feature are clear.	3.72	High
3	The privacy methods and features are conducted in short time.	4.60	High
4	The privacy features and methods are useful to prevent the illegal accessing by strangers.	4.31	High
5	I prefer to use the M-G application that includes privacy methods and feature such as	3.85	High

	the presented.		
6	The proposed privacy methods and features motivate me to use the M-G applications.	3.91	High
7	In total, I accept the M-G applications of privacy level based on the presented methods and feature.	4.15	High

Based on the above Table 7, the respondents agreed that the proposed privacy methods and features of the M-G applications are useful and are easy to be used. The respondents agreed with all questionnaire items, indicating the privacy acceptance of the M-G applications based on the proposed privacy model.

The respondents agreed that privacy functions are simple to be conducted (item #1). Overall privacy methods and features are clear (Item #2). The privacy methods and features are conducted in a short time (item #3). These two items represent the ease of use of the proposed privacy functions of M-G applications, which represent important motivation factors for citizens to adopt these applications. On the other hand, the respondents agreed that the privacy features and methods are useful to prevent illegal access by strangers (item #4). The respondents preferred to use the M-G application including privacy methods and features such as what was presented (item #5). The proposed privacy methods and features motivate the citizens to use the M-G applications (item #6). These items represent the usefulness of the proposed privacy functions of the M-G applications, which represent another important motivation factor for citizens to adopt these applications.

In total, the respondents agreed that they accept the M-G applications of privacy level based on the presented methods and features (item #7). Hence the analyses of the questionnaire responses confirm the validity of the proposed privacy model for M-G applications.

5 Conclusion and Future Works

The M-G applications offer many benefits for citizens such as saving time, effort, and being able to utilize the services anytime and from anywhere. However, the acceptance of the M-G applications is still an issue due to many factors such as weakness of security and privacy, flow of experience, and the characteristics of mobile applications. Users may refuse to use M-G applications if they feel that these applications are not protected or are difficult to be used. Thus, this paper tries to examine the mediating effect of the motivation of using M-G applications on the relationship between security and privacy, and the actual use of these applications. The privacy practical model of M-G application was developed. Many privacy features were suggested in the privacy model such as password encryption, login confirmation, login tracking, and strong password. The proposed privacy model was prototyped and validated by 150 Jordanian citizens. The respondents confirmed that the proposed model is useful and easy to use, which motivates them to use M-G applications based on the proposed model. The results of this research show that the proposed model is useful to improve the privacy trust of using M-G applications in developing counties. However, many works could be conducted in the future based on the outcome of this research. In the future, it is important to study the effects of security in the acceptance of M-G applications. This future work requires hard effort to give the citizens effective knowledge about the technical feature of systems security and security methods. Also, the practical model of M-G security could be developed based on effective security methods.

Acknowledgment

This research is funded by the Deanship of Research and Graduate Studies at Zarqa University /Jordan.

References

[1] Alsouda, Y. (2019). An IoT Solution for Urban Noise Identification in Smart Cities: Noise Measurement and Classification.
[2] Al-Sherideh, A. S., Ismail, R., Wahid, F. A., Fabil, N., & Ismail, W. (2018). Mobile government applications based on security and privacy: a literature review. International Journal of Engineering and Technology (UAE).
[3] Al-Turjman, F. (2019). 5G-enabled devices and smart-spaces in social-IoT: an overview. Future Generation Computer Systems, 92, 732-744.
[4] Flora, H. K., Wang, X., & Chande, S. V. (2014). An investigation on the characteristics of mobile applications: A survey study.
[5] Rohan, E. A., Slotman, B., Goettsche Tristani, E., Townsend, J. S., White, D. E., Fultz-Butts, K., & Gardner, A. (2019). Evaluating the Feasibility of Using a Mobile App to Track Oncology Patient Navigation Activities and Outcomes. Journal of Oncology Navigation & Survivorship, 10(3).
[6] Al-Sherideh, A. S., Ismail, R. (2020). Motivating path between security and privacy factors on the actual use of mobile government applications in Jordan. International Journal on Emerging Technologies.
[7] Almajali, D. A., Omar, F., Alsokkar, A., Alsherideh, A. A. S., Masa'Deh, R. E., & Dahalin, Z. (2022). Enterprise resource planning success in Jordan from the perspective of IT-Business strategic alignment. Cogent Social Sciences, 8(1), 2062095.
[8] Liu, X., Li, J., Wu, Y., & Kang, H. (2019, December). A Deployment Scheme Based on Game Theory in 3D Heterogeneous Wireless Sensor Networks. In 2019 International Conference on Big Data, Electronics and Communication Engineering (BDECE 2019) (pp. 115-118). Atlantis Press.
[9] Choudhary, S. R., Fazzini, M., & Orso, A. (2019). U.S. Patent No. 10,296,444. Washington, DC: U.S. Patent and Trademark Office.
[10] Raj, H., Santos, N., England, P., Saroiu, S., & Wolman, A. (2019). U.S. Patent No. 10,496,824. Washington, DC: U.S. Patent and Trademark Office.
[11] Islam, R., Islam, R., & Mazumder, T. (2010). Mobile application and its global impact. International Journal of Engineering & Technology (IJEST), 10(6), 72-78.

[12] Gottschalk, P. (2020). E-government interoperability and information resource integration: Frameworks for aligned development. Information Systems, 193.
[13] Derindag, O. F., Canakci, M., & Tsarev, R. (2019, December). Information and communication technologies in e-commerce and e-governance. In Journal of Physics: Conference Series (Vol. 1399, No. 3, p. 033110). IOP Publishing.
[14] Althunibat, A., Alrawashdeh, T. A., & Muhairat, M. (2014). The Acceptance of Using M-G Services in Jordan. Journal of Theoretical and Applied Information Technology, Vol. 63, No.3, pp.733-740.
[15] ElSherif, H. M., Alomari, K. M., AlHaddad, A. S., & Alkatheeri, A. O. (2016). Mobile Government Services Satisfaction and Usage Analysis: UAE Government Smart Services Case Study. International Journal of Computer Science and Mobile Computing, 5(3), 291-302.
[16] Huang, D., Zhou, Z., Xu, L., Xing, T., & Zhong, Y. (2011, April). Secure data processing framework for mobile cloud computing. In 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 614-618). IEEE.
[17] Al-Mousa, M. R., Al Zaqebah, M., Al-Sherideh, A. S., Al-Gghanim, Mohammed., Samara, G., Al-Matarneh, S., Asassfeh, M, R. (2022). Examining Digital Forensic Evidence for Android Applications. In 2022 23nd International Arab Conference on Information Technology (ACIT).
[18] Li, K. C., Lee, L. Y. K., Wong, S. L., Yau, I. S. Y., & Wong, B. T. M. (2019). Evaluation of mobile learning for the clinical practicum in nursing education: application of the FRAME model. Journal of Computing in Higher Education, 1-21.
[19] Isagah, T., & Wimmer, M. A. (2019, May). Recommendations for M-G Implementation in Developing Countries: Lessons Learned from the Practitioners. In International Conference on Social Implications of Computers in Developing Countries (pp. 544-555). Springer, Cham.
[20] Kureerung, P., & Ramingwong, L. (2019, October). A Framework for Usability Design to Promote Awareness of Information Disseminated via Mobile Government Applications. In 2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST) (pp. 1-6). IEEE.
[21] Munyoka, W., & Maharaj, M. S. (2019). Privacy, security, trust, risk and optimism bias in e-government use: The case of two Southern African Development Community countries. South African Journal of Information Management, 21(1), 1-9.
[22] Parker, D. B. (1981). Computer security management (p. 308). Reston, VA: Reston Publishing Company.
[23] Onashoga, A., Ogunjobi, A., Ibharalu, T., & Lawal, O. (2016). A secure framework for SMS-based service delivery in M-G using a multicast encryption scheme. African Journal of Science, Technology, Innovation and Development, 8(3), 247-255.
[24] Bahar, A. N., Habib, M. A., & Islam, M. M. (2013). Security architecture for mobile cloud computing. International Journal, 3(3), 2305-1493.
[25] Marković, M., & Đorđević, G. (2019). Mobile Government Systems in Cross-Border Environments. MeTTeG14, 67.
[26] Al-juaifari, M. K. R. (2016). Secure SMS Mobile Transaction with Peer-to-Peer Authentication Design for Mobile Government. American Journal of Engineering Research (AJER), 4(11), 143-149.
[27] Qi, H., & Gani, A. (2012, May). Research on mobile cloud computing: Review, trend and perspectives. In 2012 Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP) (pp. 195-202). IEEE
[28] Qin, Z., Sun, J., Wahaballa, A., Zheng, W., Xiong, H., & Qin, Z. (2017). A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing. Computer Standards & Interfaces, 54, 55-60.
[29] Hassan, R. G., & Khalifa, O. O. (2016). E-Government-an Information Security Perspective. International Journal of Computer Trends and Technology (IJCTT), 36(1), 1-9.
[30] Khan, A. N., Kiah, M. M., Khan, S. U., & Madani, S. A. (2013). Towards secure mobile cloud computing: A survey. Future Generation Computer Systems, 29(5), 1278-1299.
[31] Ibukun, E., & Daramola, O. (2015). A systematic literature review of mobile cloud computing. International Journal of Multimedia and Ubiquitous Engineering, 10(12), 135-152.
[32] Cheng, B. C. (2017). Exploring Mobile Data Security with Energy Awareness. In Adaptive Mobile Computing (pp. 203-215). Academic Press.
[33] Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E., & Song, Z. (2010, October). Authentication in the clouds: a framework and its application to mobile users. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop (pp. 1-6). ACM.
[34] Khamis, M., Hasholzner, R., Bulling, A., & Alt, F. (2017, June). GTmoPass: two-factor authentication on public displays using gaze-touch passwords and personal mobile devices. In Proceedings of the 6th ACM International Symposium on Pervasive Displays (p. 8). ACM.
[35] Stajano, F., Spencer, M., Jenkinson, G., & Stafford-Fraser, Q. (2014, December). Password-manager friendly (PMF): Semantic annotations to improve the effectiveness of password managers. In International Conference on Passwords (pp. 61-73). Springer, Cham.
[36] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2018). Incorporating touch biometrics to mobile one-time passwords: Exploration of digits. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 471-478).
[37] Rassan, I. A., & Al Shaher, H. (2013). Securing mobile cloud using finger print authentication. International Journal of Network Security & Its Applications, 5(6), 41.
[38] Yang, C., Zhang, J., Guo, J., Zheng, Y., Yang, L., & Ma, J. (2019). Fingerprint Protected Password Authentication Protocol. Security and Communication Networks, 2019.
[39] Wang, Y., Chen, R., & Wang, D. C. (2015). A survey of mobile cloud computing applications: Perspectives and challenges. Wireless Personal Communications, 80(4), 1607-1623.
[40] Jassim, O. A., Mahmoud, M. A., & Ahmad, M. S. (2015). A multi-agent framework for research supervision management. In Distributed Computing and Artificial Intelligence, 12th International Conference (pp. 129-136). Springer, Cham

[41] Patton, M.Q., 2002. Qualitative Research & Evaluation Methods (Thousands Oaks, Sage).
[42] Al-Slais, Y., & El-Medany, W. M. (2022). User-centric adaptive password policies to combat password fatigue. Int. Arab J. Inf. Technol., 19(1), 55-62.
[43] Kasım, Ö. (2022). An Efficient Ensemble Architecture for Privacy and Security of Electronic Medical Records. Int. Arab J. Inf. Technol., 19(2).
[44] Al-Khateeb, M., Al-Mousa, M., Al-Sherideh, A., Almajali, D., Asassfeha, M., & Khafajeh, H. (2023). Awareness model for minimizing the effects of social engineering attacks in web applications. International Journal of Data and Network Science, 7(2), 791-800.
[45] Alqawasmi, K.E., Alsmadi, A.M. Estimation of ARMA Model Order Using Artificial Neural Networks. Circuits Syst Signal Process (2023). https://doi.org/10.1007/s00034-023-02305-6.
[46] Al-Sherideh, A. S, Maabreh, K., Maabreh, M., Al-Mousa, M. R, Asassfeha, M. (2023). Assessing the Impact and Effectiveness of Cybersecurity Measures in e-Learning on Students and Educators: A Case Study. International Journal of Advanced Computer Science and Applications, Vol. 14, No. 5.