International Journal on Emerging Technologies 11(5): 558-566(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Motivating Path between Security and Privacy Factors on the Actual use of Mobile Government Applications in Jordan

Ala'a Saeb Al-Sherideh[1] and Roesnita Ismail[2]

[1]PhD Candidate, Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia.

[2]Senior Lecturer, Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia.

(Corresponding author: Ala'a Saeb Al-Sherideh)

(Received 16 September 2020, Revised 20 October 2020, Accepted 14 November 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Mobile Government (MG) applications provide services anytime from anywhere at less time, lower costs, and efforts. However, the security and privacy concerns of MG applications might influence the acceptance level of these applications by the citizens. MG applications acceptance by users has several challenges such as security and privacy. This study investigates the mediating effect of the motivation of use on the relationship between security and privacy, and the actual use of MG applications. Security and privacy are independent factors in this study. The data in this study is collected using questionnaires among 513 Jordanian citizens. The questionnaires are constructed based on Technology Acceptance Model (TAM) to investigate the mediation role of motivation factors (usefulness and ease of use) in the relationship between security and privacy and intention and attitudes of using the MG applications. The data are analyzed using AMOS in terms of Structured Equation Model (SEM). The results show that privacy concerns affect the motivation to use M-government applications. This paper contributes in expanding the acceptance factors of MG applications with the inclusion of security and privacy factors. The results show that related to the privacy affects to use MG applications that should be assured to enhance the acceptance of M-government applications. Although security is important, the citizens do not believe that security has some effects on the acceptance level of the M-government application. The research fills the gap of study on the motivation to use MG application based on the security and privacy toward the actual use of MG applications.

Keywords: Mobile applications, Mobile government, Government services, security, privacy, acceptance.

Abbreviations: MG, Mobile Government; TAM, Technology Acceptance Model; SEM, Structured Equation Model; CFA, Confirmatory Factor Analysis.

I. INTRODUCTION

Mobile applications are easy, user-friendly, inexpensive, downloadable and run on most of the mobile phones including inexpensive and entry-level phones [30, 44]. Mobile Government (MG) has the potential of delivering real-time location-based information on demand, performing transactions, and most importantly use the mobile network to reach citizens and provide new customized services [33]. M-government is considered as a subset of e-government comparing another channel to provide government information and services [17, 20, 24, 37]. This helps in reducing the time and efforts required to achieve governmental services. [37] showed that citizens now regard the mobile application as one of the favorite channels in preference to other channels such as the World Wide Web and face-face. And so, adopting the concept of mobile applications turns to be a key step to attain the various governmental services related to the life of citizens.

Several studies have recently found that the mobile applications' key components lie in the privacy and security features [18, 27, 29, 32, 34, 45]. The concept of security encompasses all related to the protective processes of information and services from damaging and attacking the authority structure of the services and information accessing such as the use of passwords in several processes by the users. The mobile applications' concerns resulting from security and privacy can reduce the aforesaid applications' trust level, affecting the process of approval of the use of mobile applications by various citizens. The research focuses on investigating the role of security and privacy in the acceptance of MG applications in Jordan. The following section presents the theoretical considerations of the study, section 3 clarifies the research methodology, section 4 discusses the study results based on the collected data, and section 5 provides the study conclusion and future works.

II. THEORETICAL CONSIDERATIONS

The use of technology acceptance models. i.e. the TAM model is strongly used to measure the MG applications' acceptance. During the 1970s, several organizations have adopted these systems sue to the increasing boom of information technology. The organizations notice that the information system adoption fails due to users' rejection of the use of the new system. In 1985, Fred Dav develops TAM to measure the users' acceptance of use the technology systems to assure the success of the adoption of the system [15]. Fig. 1 presents the TAM structure that would be adopted to measure the motivation levels of using technology systems and evaluated the actual use of the systems.

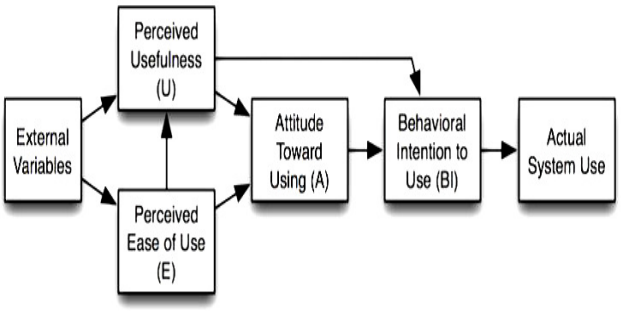

Fig. 1. TAM Main Structure.

The core conceptual model of TAM structured as four layers as follows: (1) The external variables that could affect the using of the systems such as technology skills; (2) The motivation of using the technology systems that consists of the usefulness and the ease of using the technology system. The usefulness "the degree to which an individual believes that using a particular system would enhance his or her job performance.", while the ease of use "the degree to which an individual believes that using a particular system would be free of physical and mental efforts" [12]; (3) the attitudes toward the user of the systems; and (4) the intention of using the technology system.

Based on the TAM structure, there are many external factors effects on the motivation of using the M-government applications. Security is considered as an independent acceptance factor of MG applications. One of the main conditions to use the M-movement applications by the users is that they need to trust that the data used is strongly protected. Another important factor the privacy is that this factor is also an independent acceptance factor of M-government applications [4, 5, 8, 14, 29, 34, 36, 39]. The users need to trust that there are no strange persons who can access their services accounts through illegal capturing of accessing data.

The security of mobile applications can be defined as the protection of data, information, and services from attacked or damaged. The attacker tries to steal or damage the information and services using many threats like viruses and illegal deception. On the other hand, the privacy of mobile applications can be defined as to prevent the illegal authority of users' accounts or information. Some users can steal or damage other users' information by stealing their accessing authority (e.g. passwords and access cards).

In terms of MG applications, the flow of experience external factor is related to the security and privacy of M-government applications [5, 19]. The users are provided with the advantage of using the M-government application's security and privacy performance level because of the high level of skills and experience. Thus, they can apply the security and privacy procurers in a useful manner. Also, the characteristic of M-government applications such as accessibility and availability another external factor that related to security and privacy of these applications [7, 21]. Security and privacy performance should agree with the characteristics of M-government applications. For example, users should have secure connections and adequate mobile features to use M-government services anytime and from anywhere.

The above external factors could affect the motivation of using MG applications by the citizens. Based on the TAM acceptance model, two motivational factors could measure the user's acceptance of MG applications. These motivational factors are the usefulness and ease of using the applications. The usefulness a motivational factor that measures the degree to which users believe that using M-government applications would enhance the provided services [2, 4], while the factor of easy use helps in measuring the degree of users' insight that the application of M-government has zero mental and physical efforts [2, 4].

The motivation of using the MG application led to the actual use of these applications. The actual use of the M–government applications by the users represents the real action of the user's acceptance of these applications. According to the TAM model, the actual use of the applications can be measured using two important factors which are the attitudes and the intention. The attitude dependent acceptance factor to measure the actual use of M-government applications. The attitudes reflect the positive/negative stand of the users toward the use of M-government applications [2, 6]. On the other hand, the intention factor is dependent (actual use), along with the attitude factor. The intention of use aims to measure the future real actions of the users toward the use of M-government applications [2, 42].

Furthermore, security and privacy factors affect motivation factors, usefulness, and ease of use. The motivation factors are considered as mediation factors on the relationship between the independent factors (i.e. security) and the dependent factors which the actual use of M-government applications. The actual use factors include two main dimensions which are the attitudes toward the M-government application and the intention to use these applications.

Simply put, the theoretical model in the research intends to investigate the role of security and privacy factors in the motivation of acceptance of using M-government applications and the impact of the role on the actual use of these applications. Two external factors are identified (Flow of experience, and Application characteristics) that are related to the security of M-government applications. The users are required to acquire the skills and knowledge related to the use of mobile applications to attain a full understanding of the level of the privacy and security features related to the M-government applications and be more familiar with the use of methods of privacy and security properly. Also, the characteristics of M-government applications are such as accessibility and availability of M-government applications external factors of security and privacy. For example, the users may not have adequate mobile pieces of equipment such as internet connection and devices to use the M-government applications, thus, the security and privacy performance will not motivate them to use these applications due to low owned mobile requirements.

Based on the TAM, The independent factors could affect the motivation factors of M-government applications which are the usefulness and the ease of use. Security and privacy should improve the usefulness

of M-government applications through a high-performance level of security. The low security and privacy level could harm the usefulness of the M-government applications. Conversely, various complex steps related to the concepts of privacy and security play a key role in affecting the easy use of the M-applications.

Concerning TAM, the connection between the independent factors (security and privacy) and the meditating factors (usefulness and ease of use) could have an important impact on the actual use of M-government applications. The actual use factors are considered as dependent factors, whereby the acceptance of the M-government application is reflected by the users' attitudes and intentions to use the M-government applications. Without the positive altitudes and real intention to use the applications, the acceptance of M-government applications will fail. Figure 2 illustrates the connection between the various research factors. Take into account that there are two external factors (experience of flow, and application characteristics) that could affect the security and privacy.

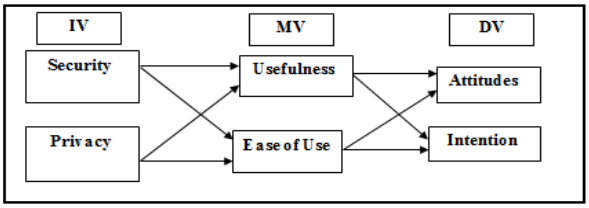

Fig. 2. Connections among the Various Research Factors.

In light of the above discussion in one context of the theoretical model of M-government applications acceptance, the research focuses on the trust in services of security and privacy of M-government applications in connection with the users' acceptance of these applications (Fig. 3). By assuring the external factors and security and privacy, the users would be encouraged to accept and use M-government applications. These assumptions require to test the seven main research hypotheses, which are as the following:

H1: The security is an important factor for the acceptance of M-government applications.

— H1a: There is positive relationship between the M-government characteristics (availability and accessibility) and the security of the M-government application.

— H1b: There is a positive relationship between the flow of experience and the security of the M-government application.

H2: The privacy is an important factor for the acceptance of M-government applications.

— H2a: There is a positive relationship between the M-government characteristics (availability and accessibility) and the privacy of the M-government application.

— H2b: There is a positive relationship between the flow of experience and the privacy of the M-government application.

H3: There is a positive relationship between H1 (H1a and H1b) and the usefulness of the M-governments applications.

H4: There is a positive relationship between H1 (H1a and H1b) and the ease of using the M-governments applications.

H5: There is a positive relationship between H2 (H2a and H2b) and the usefulness of the M-governments applications.

H6: There is a positive relationship between H2 (H2a and H2b) and the ease of using the M-governments applications.

H7: There are the mediating effects of the motivation of using the M-government applications (usefulness and ease of use) on the relationship between the independent factors and the actual use of the M-government applications (attitudes and intention).

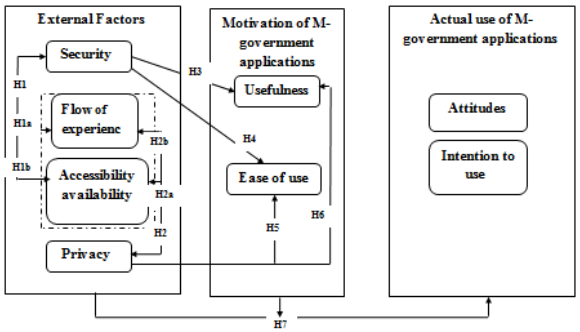

Fig. 3. Research Model.

III. RESEARCH METHODOLOGY

This section gives an insight into the method adopted in this study together with the techniques, method of analysis, data collection setting, study population, and study sample. Various sources are used to prepare the questionnaire adopted in this study so that the acceptance of using the M-government applications by the citizens in the Hashemite Kingdom of Jordan in terms of the variables of security and privacy. To achieve the objective of the questionnaire, the 5-level Likert scale is factored in as follows: 1 for Strongly Disagree (SD), 2 for Disagree (D), 3 for Neutral (N), 4 for Agree (A), and 5 for Strongly Agree (SA) [1, 3, 13, 28, 35, 40]. Due to its high level of focus and capability of producing relative response averages more than the lower and higher scales, the 5-level Likert scale is strongly adopted in this study [16].

The validity of the adapted questionnaire is judged by five Jordanian experts. The final questionnaire draft is prepared according to the collated feedback from the experts to assure the questionnaire validity. Another important part of the questionnaire is that because the respondents' mother language is Arabic, the questionnaire is translated into the Arabic language. Then, it is distributed to the respondents in Jordan. Later on, the questionnaire is collated from the Jordanian respondents to complete the procedures related to the analysis of the responses. For testing the total hypotheses of this study because of the theoretical model's the mediating structure, the Structured Equation Modeling (SEM) using AMOS software is used. The links between constructs of a structural equation model

may be estimated with independent regression equations or through more involved approaches.

IV. DISCUSSION OF THE RESULTS

The section presents the discussion of the results including the demographic analysis, confirmatory Factor Analysis (CFA), descriptive Analysis, and the Structural Equation Model (SEM).

There are 8 demographic variables analyzed to ensure that the collected data useful to address the research aim. The demographic variables are; (1) gender, (2) age, (3) education level, (4) occupation, (5) Experiences of using mobile applications, (6) marriage status, (7) using of mobile per-week, and (8) living province. The gender variable analysis shows that 69% of all respondents (352 respondents) are male, while 31% of the respondents (161) are female. On the other hand, the analysis of the age variable shows that the age of most respondents is between 20-40 years. Moreover, the analyses of the education level variable show that most respondents (53% of all respondents) have a university degree, followed by the respondents that have medium college qualification (18% of all respondents), then the respondents that have a postgraduate qualification (18% of all respondents). Furthermore, the analysis of the occupation variable shows that 42% of all respondents (218 respondents) are governmental employees. The business sector employees represent 32 % of the respondents' total (162 respondents).

The fifth demographic variable is the experience of using mobile applications. The analysis of the variables shows that all respondents are using mobile applications. The sixth demographic variable the marriage status. The analysis of the variables shows that most of the respondents are married (64% of all respondents), while 36% of the respondents are single. The seventh demographic variable the time of using mobile applications per week. According to the analysis of the variable, most of the respondents (48%) are using mobile applications for less than 12 hours per week. 30% of all respondents are using mobile applications for 12-24 hours per week. 22% of respondents' total using mobile applications for more than 24 hours per week. The last demographic data the living province of the citizens. The analysis of the variables shows that most of the respondents (41% of all respondents) are living in Amman (the capital of Jordan). 18% of all respondents are living in Irbid city, 14% are living in Zarqa city, 5% are living in Mafraq city, 4% are living in Balqa city, 3% are living in Tafila, 3% are living in Aqaba, 3% are living in Karak, 3% are living in Ma'an, 2% are living in Madaba, 2% are living in Jarash, and 2% are living in Ajloun.

V. CONFIRMATORY FACTOR ANALYSIS AND DESCRIPTIVE ANALYSIS

The section presents the Confirmatory Factor Analysis (CFA) to test the accuracy of the collected data (model fit). First of all the three data screening processes are conducted to assure the model validity; (1) missing value, (2) remove outlier, and (3) assessment of data normality. All of these analyses confirm the validity of the model data. [43]Mentioned that accepted missing values 0.05 for each first order variable in the questionnaire. As a result, 513 responses out of 548 returned questionnaires are acceptable to involve the data analysis in the research.

Furthermore, the data normality is another conducted analysis to confirm the data validity. The data normality aims to estimate the normal distribution of the questionnaire responses. The normal distribution of the data indicates the good relationship between the item responses to support the validity of the study variables. By using AMOS, two normality assessments are conducted; (1) Skewness, whereby the average of the data normal distribution should fall in the range -3 to 3; and the Kurtos, whereby the average of the data normal distribution must fall in the range -7 to 7. Both Skewness and Kurtos tests are accomplished using the AMOS tool. The normality test shows that all responses belong to the normal distribution of the applied tests. Hence, the collected data are interrelated to support the modeling of the study variables, which allow the next analysis steps such as CFA.

Based on the data screening tests, the CFA model for performed depend on 37 items is distributed on eight main variables of first-order construction; There are many CFA analyses are conducted to assure the reliability and validity of the model data such as the factor loading, goodness of fit indices, reliability, and convergent validity, and discriminant validity.

Based on all 37 items included in the overall CFA model analysis, the validity test (factor loading test) is applied to determine the correspondence level among the items in each factor. It is maintained that the factor of loading related to the acceptance level (validity) is required to be more than 0.5 [38]. According to the factors loading, 30 items can effectively represent the eight first-order construction in the model.

There are 7 items are eliminated from the final model. However, the entire 30 items stay represent all factors in the study. The flow experience factors represent 3 items (FE1, FE2, and FE3), the application characteristics are represented by 3 items (AC1, AC2, and AC3). On the other hand, security is represented by 3 items (ST1, ST3, and ST4). The privacy is represented by 4 items (PT2, PT3, PT4, and PT5). Moreover, the ease of use of mobile applications is represented by four items (EU1, EU2, EU3, and EU4). The usefulness of using the mobile application is represented by four items (UF1, UF2, UF3, and UF4). Furthermore, the attitude toward using M-government applications is represented by four items (AT1, AT2, AT3, and AT4). The intention of using the mobile application is represented by five items (IN1, IN3, IN6, IN7, and IN9).

In light of the whole thirty items factored in the amended model, the reliability and convergent validity tests are conducted. The reliability coefficients (Cronbach alpha) are 0.921 for the intention dimension, 0.952 for the attitudes dimension, 0.944 for the usefulness dimension, 0.951 for the ease of use dimension, 0.916 for the flow experience dimension, 0.937 for the dimension of application characteristics, 0.84 for the privacy, and 0.824 for the security. Hence, the reliability acceptable for all included dimensions in the modified model. Furthermore, the composite reliability of each dimension strong (> 0.7) based on the related path with other dimensions. In conclusion, the reliability of the modified

model very good and indicates careful data filling by the respondents. On the other hand, the coregent validity based on the AVE test shows that all dimensions are above the acceptable cut point of the valid relationships between the dimensions (> 0.5). The AVE test records 0.702 for the intention dimension, 0.831 for the attitudes dimension, 0.81 for the usefulness dimension, 0.83 for the ease of use dimension, 0.784 for the flow experience dimension, 0.833 for the dimension of application characteristics, 0.595 for the privacy, and 0.611 for the security. The indicates the good interrelation between the items of all dimensions.

To measure the model's fit side, the study adopts using the RMSEA test as the data threshold's value is required to be less than 10%. RMSEA working on finding the errors of the correspondence between the data. Thus, the smaller RMSEA coefficient indicates the high corresponding between the model data. Other important indices that can test the model fit are the GFI, AGFI, CFI, TLI, IFI, and χ2/df.

The good interrelationships among the data of the entire thirty items related to the final form of the model are confirmed by the results representing the fit indices' goodness. As put by [26], the GFI coefficient is found 0.872 while the acceptable cut value of the GFI shall be more than 0. As for the cut value of the Adjusted GFI, it reaches 084. As indicated by [11], this cut value is considered an acceptable fit indicator (i.e. > 0.8). Still, the CFI, TLI, and IFI indices' acceptable values shall be more than 0.9 [9], [25]. The entire aforesaid tests reach acceptable fit values, being 0.947 for the CFI coefficient, 0.938 for the TLI coefficient, and 0.949 for the IFI coefficient 0.947 respectively. Furthermore, the RMSEA one of the most important tests to assure the fitness of the BPM model, and the coefficient of RMSEA must below 0.1 [41].

As for the RMSEA test, it reaches 0.065 making it an acceptable coefficient to the study as it shows the fitness feature among the whole model items. The results representing the entire tests are parallel with the degree of the adequacy of the X2/df (3.159), which is considered less than the cut value of 5. Accordingly, the amended CFA model is regarded as fit.

To test the relationship between the model factors, the discriminant validity is conducted on the overall model. The discriminant validity test is regarded as a central element to verify the interrelation among the modified model's dimensions. The discriminant validity is different from the correlation test; it estimates the relationship between the dimensions and the square root of the average variance extracted for each dimension [22]. Kline [31] mentioned that the accepted discriminant correlations among the dimensions should below 0.85, and the discriminant correlations among the items in the same dimension should near to 1. The discriminant test shows that the inter-correlations are valid in/among all dimensions in the modified model, which indicates a strong interrelation level between the model factors. The inter-correlation is less than the r2 of the average variance extracted from each dimension (0.838, 0.912, 0.9, 0.911, 0.886, 0.913, 0.771, and 0.782 respectively for intention, attitude, usefulness, ease of use, the flow of experience, application characteristics, privacy, and security), whereby the discriminant validity of the modified model confirmed. Figure 4 illustrates the CFA of the overall model in the study. [Intention=IN, Attitude=AT, Usefulness=UF, Ease of use=EU, Flow of experience=FE, Application Charactertics=AC, Privacy =PT, and Security=ST]

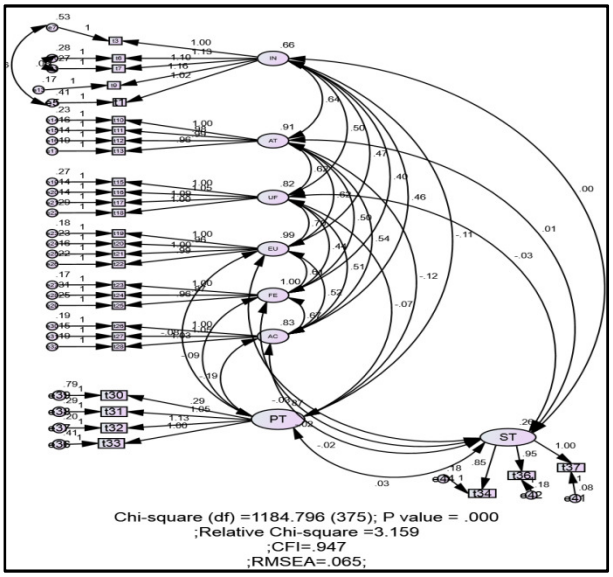

Fig. 4. CFA of overall model.

Based on the modified model, the descriptive analysis is conducted using 30 items that are distributed on eight main variables that are related to the using of M-government applications; the flow of experience, application characteristics, security, privacy, usefulness, ease of use, attitudes, and intention. The main aim of the descriptive analysis to understand the directions of the respondents' opinions about the study variables. The items are analyzed based on the 5-Likert scale; 1 for Strongly Degree (SD), 2 for Degree (D), 3 for Neutral (N), 4 for Agree (A), and 5 for Strongly Agree (SA).

In terms of the experience of a flow variable, the respondents have good experience in using mobile applications. The respondents have good skills in using mobile applications (FE1). They do not face critical challenges in using mobile applications (FE2). The respondents prefer to use mobile applications to accomplish their services (FE3). These results indicate that citizens prefer the use of m-government applications in their daily life, and the citizens have the required skills to use mobile applications.

The results of mobile application characteristics show that the respondents prefer using mobile applications due to many reasons such as accomplishing the services at any time and from anywhere. The respondents see that the M-government applications provide access to the services at any time (AC1 and AC3). On the other, the respondents see that the M-government applications are effective to accomplish the services from anywhere and at any time (AC2). Hence, the characteristics of M-government applications motivate citizens to use these applications in their daily life services.

The descriptive analysis of the security variable shows that the respondents have several concerns about the security of M-government applications. The respondents

see that the security-critical requirement to accept M-government applications (ST1). The respondents see that their information may hack or steal when they use the M-government application (ST3). Yet, the study's respondents believe that it is one of the safest matters is to the utilization of the M-government services (ST4) in several fields related to their life. Hence, it is necessary to provide a high level of M-government applications to assure the user's acceptance of these applications.

The descriptive analysis of the privacy variable shows that the respondents have any concerns about the privacy of M-government applications. The respondents see that the services' privacy is an important requirement for the use of M-government applications (PT2). The respondents are afraid of snatch their personal information by strangers (PT3). The respondents' concerns about sharing their personal information with third-party organizations (PT4). Another concern is the unintended use of personal information by governmental agencies. In summary, the respondents need to assure the high-level privacy of the M-government applications to trust the use of these applications.

In terms of the usefulness of using the M-government applications, the respondents are motivated to use the M-government applications due to the usefulness of these applications. The respondents see that the M-government application could save the time of accomplishing the services (UF2). Thus, these applications can improve various M-government services (UF1). Besides, mobile services are an enjoyable experience (UF4), which motivates the use of M-government services by the citizen. In total, the respondents see that the M-government application would add many benefits to their life (UF3).

The descriptive analysis of the ease of use of the M-government applications shows that the respondents are motivated to use the M-government applications due to the ease of using these applications. The respondents see that it will be easy to use M-government applications (EU1 and EU2). It is easy to become skillful at using mobile government applications (EU3). Altogether, the respondents find the use of M-government applications helpful and simple to use (EU4).

Concerning the attitudes toward the use of M-government applications, the respondents provide positive attitudes toward the use of M-government services. The respondents see that M-government applications are a good idea (AT1). They believe that the use of mobile applications fashionable (AT3). Furthermore, the respondents see that the use of M-government applications would save the time and efforts of accomplishing governmental services (AT2 and AT4). The results show the Jordanian citizens' positive beliefs concerning the adoption of M-government applications because of the beneficial gains attained from putting these applications into action in real-life situations.

In the context of the intention of using the M-government applications, the respondents in total intend to use the M-government applications for many services such as civil services (i.e. passport producing and renewing), civil defense services (i.e. investigation of phone bills), and police services (i.e. notice of traffic accidents). The respondents intend to recommend others to use M-government applications. These results represent the importance of the M-government services for the citizens, whereby there high intention to use the M-government applications by the citizens.

VI. STRUCTURAL EQUATION MODEL AND HYPOTHESES TESTING

The structural equation model is ranked second as a significant process in the SEM statistical analysis. Also, the relationships amongst the variables are evaluated once the validation process of the measurement model is completed. Importantly, the structural model presents a great amount of related data on the relationship between dependent or endogenous variables and the independent or exogenous variables. First, it centers on the total fit model, alongside the direction, size, importance of the hypothesized parameter estimates. The one-headed path diagram explains this in detail, while the final phase encompasses the structural model's confirmation. To achieve this in the study, there shall be an analysis of the suggested relationship between the assessed and identified variables.

Redrawing the paths among the variables in the amended model is strongly required to make an effective SEM test. Having the model items' correlations retested assists the model fit in decreasing the degree of the indirect or hidden relationship among the items i.e. improve the x2 value. Precise records are provided by the entire CFA tests for the final model, namely: factors loading, reliability, and fit indices. From this time, making the SEM model adopted in this study is based on the entire 30 items in the amended model. Figure 5 demonstrates the final SEM model, and the hypotheses can be also tested in the current study. [Intention=IN, Attitude=AT, Usefulness=UF, Ease of use=EU, Flow of experience=FE, Application Charactertics =AC, Privacy =PT, and Security =ST]

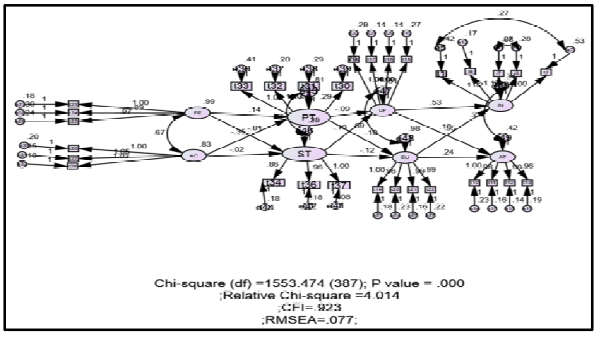

Fig. 5. Structural Equation Model.

Based on the above Figure 5, it can be noticed that all factor loading is above the acceptable cut point (> 0.5). For example, the factors loading of the flow of experience is 0.92, 0.85, and 0.89 for items FE1, FE2, and FE3 respectively. Also, the factors loading of the attitudes is 0.90, 0.93, 0.93, and 0.89 for items AT1, AT2, AT3, and AT4 respectively. As for the RMSEA test, it reaches 0.077 making it an acceptable coefficient to the study as it shows the fitness among the model items. The degree of adequacy of X2/df (4.014) is considered less than the cut value of 5. Accordingly, the model data are found as effective and operative to test the study's research hypotheses.

This study is labeled as one of the directional relationships as it uses a significance level p-value of 0.05 to test the effect of the relationship's possibility in one/direct direction. The relationship of P-value that <= 0.05 represents the acceptance of using the research hypotheses, while the P-value that > 0.05 represents the research hypotheses' rejection.

Table 1 summarizes the judgment on the direct hypotheses test based on the SEM analysis. The direct research hypotheses show that all hypotheses related to the security are rejected. Therefore, security does not affect the users' acceptance of M-government applications. On the other hand, all hypotheses related to privacy are partially supported, which presents the importance of privacy in the users' acceptance of M-government applications. These results are helpful to update the research focuses. The privacy should be assured to enhance the users' acceptance of M-government applications.

Table 1: Judgment on the direct hypotheses test.

Hypotheses	P-value	Supporting
H1	H1a: >0.05 H1b: >0.05	Rejected
H2	H2a: not significant H2b: <0.05	Partially supported
H3	> 0.05	Rejected
H4	> 0.05	Rejected
H5	<0.05	Partially supported
H6	<0.05	Partially supported

According to [10, 23], as an approach, SEM is more applicable to regression techniques for testing the mediation effect because the SEM technique allows modeling of both measurement and structural relationship and generates overall fit indices. The study used a bootstrapping approach as recommended by [9] to test the research hypothesis H7. Table 2 summarizes the paths analysis of the mediating effects between the study variables, which reflect the test of research hypothesis #7. The paths analysis shows that all mediating paths related to the security are not significant (P-value < 0.05), while all the paths that are related to the privacy are significant (p-value <0.05). This represents the partial support of H7.

Table 2: Paths test for H7 research hypothesis.

Specific Indirect effect	Estimate	Lower	Upper	P-value
Privacy-> Usefulness-> Intention	-.047	-.095	-.004	.054
Privacy-> Ease of use-> Intention	-.010	-.029	.000	.049
Privacy-> Usefulness->Attitude	-.050	-.101	-.004	.044
Privacy-> Ease of use-> Attitude	-.024	-.053	-.001	.046
Security -> Usefulness-> Intention	-.050	-.137	.026	.264
Security -> Ease of use-> Intention	-.012	-.036	.005	.253
Security -> Usefulness-> Attitude	-.053	-.142	.027	.264
Security -> Ease of use-> Attitude	-.029	-.074	.010	.221

Based on the above Table 2, the P-value 0.264 shows the mediating effect of the usefulness on the relationship between the security and the intention of using the M-government applications. On the other hand, the P-value 0.243 for the mediating effect of the ease of use on the relationship between the security and the intention of using the M-government applications. Moreover, the P-value 0.264 for the mediating effect of the usefulness on the relationship between the security and the attitudes toward the use of the M-government applications. Furthermore, the P-value 0.221 for the mediating effect of the ease of use on the relationship between the security and the attitudes toward the use of the M-government applications. The entire security paths have not shown any significant results because of the effect of the weak significance of the P-value (> 0.05). Thus, the security has no effects on the users' acceptance of M-government applications.

In the context of the paths of privacy, the P-value 0.054 for the mediating effect of the usefulness on the relationship between the privacy and the intention of using the M-government applications. On the other hand, the P-value 0.049 for the mediating effect of the ease of use on the relationship between the privacy and the intention of using the M-government applications. Moreover, the P-value 0.044 for the mediating effect of the usefulness on the relationship between the privacy and the attitudes toward the use of the M-government applications. Furthermore, the P-value 0.046 for the mediating effect of the ease of use on the relationship between the privacy and the attitudes toward the use of the M-government applications. All of the privacy paths are provide significant results due to significant P-value (< 0.05). Therefore, the privacy effects on the users' acceptance of M-government applications.

Consequently, the research hypothesis H7 partially supported, and the result matched with the direct hypotheses that explained in the previous section. As a conclusion of the research hypotheses, the users' acceptance of M-government applications affected by the privacy trust, while the security trust does not affect users' acceptance of these applications. These results may due to many reasons such as the following:

1. The privacy methods such as passwords are intangible for the users, while the security methods like encryption are not intangible for the users. Thus, users provide more attention to privacy.
2. The security methods are surrounded by many technical sues and cannot be understood easily by traditional users while the traditional users can understand the privacy methods (i.e. provide strong passwords).
3. The M-government applications in Jordan are still in the earlier stages and these applications just provide information rather than real actions such as payments. Hence, the users are afraid of illegal access to their accounts (privacy) more than their concerns of damage or stealing their data (attacks related to the security).

VII. CONCLUSION AND FUTURE WORK

In a nutshell, the main focus of the study lies in the effect of motivation on the relationship between the

attitudes and difficulties using the M-government applications. The study constructs the conceptual model adopted in this study by using standard TAM. The method of the questionnaire is used to collect the required data. 513 Jordanian citizens have been the main source to collect the data needed for this study. In this study, the SEM analysis is used to test seven related research hypotheses using the AMOS tool. The results attained show that the concerns related to the privacy and security features affect the concept and feeling of motivation to use M-government applications. Privacy should be assured to enhance the acceptance of M-government applications. Although security is important, the citizens do not believe that security has some effects on the acceptance level of the M-government application. This is due to a weak understanding of technical security uses by traditional users. In the future, quantitative data could be collected from experts to propose the technical privacy model of M-government applications.

REFERENCES

[1]. Abdelghaffar, H., & Magdy, Y. (2012). The adoption of mobile government services in developing countries: The case of Egypt. *International Journal of Information and Communication Technology Research, 2*(4), 333 - 341.

[2]. Al-Hujran, O. (2012). Toward the utilization of m-Government services in developing countries: a qualitative investigation. *International Journal of Business and Social Science, 3*(5), 155-160.

[3]. Alhussain, T. O. (2012). Factors Influencing the Adoption of Biometric Authentication in Mobile Government Security. Griffith University.

[4]. Almarashdeh, I., & Alsmadi, M. K. (2017). How to make them use it? Citizens acceptance of M-government. *Applied Computing and Informatics, 13*(2), 194-199.

[5]. Almuraqab, N. S., & Jasimuddin, S. M. (2016). A literature survey of m-government services adoption: Lessons for a smart city Success. In *GCC Smart government & Smart cities conference, At Dubai, UAE,* 22, 1-12.

[6]. Alotaibi, S., & Roussinov. D. (2016). Developing and Validating an Instrument for Measuring Mobile Government Adoption in Saudi Arabia. *International Journal of Economics and Management Engineering, 10*(3).

[7]. Althunibat, A., Alrawashdeh, T. A., & Muhairat, M. (2014). The Acceptance of Using M-Government Services In Jordan. *Journal of Theoretical and Applied Information Technology, 63*(3), 733-740.

[8]. Althunibat. A, Azan. M., & Sahari. N. (2011). Modelling the factors that influence mobile government services acceptance. *African Journal of Business Management, 5*(34), 13030-13043.

[9]. Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the academy of marketing science, 16*(1), 74-94.

[10]. Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. Sage focus editions, 154, 136-162.

[11]. Chau, P.Y. and Hu, P.J.H., 2001. Information technology acceptance by individual professionals: A model comparison approach. *Decision sciences, 32*(4), pp.699-719.

[12]. Chuttur, M. Y. (2009). Overview of the technology acceptance model: Origins, developments and future directions. WorkingPapers on Information Systems, *9*(37),pp.9-37.

[13]. Colesca, S. E. (2009). Understanding trust in e-government. *Engineering Economics, 63(*4).

[14]. Dahi, M., & Ezziane, Z. (2015). Measuring e-government adoption in Abu Dhabi with technology acceptance model (TAM). *International Journal of Electronic Governance, 7*(3), 206-231.

[15]. Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

[16]. Dawes, J., 2008. Do data characteristics change according to the number of scale points used? An experiment using 5-point, 7-point and 10-point scales. *International journal of market research, 50*(1), pp.61-104.

[17]. Derindag, O. F., Canakci, M., & Tsarev, R. (2019). Information and communication technologies in e-commerce and e-governance. *In Journal of Physics: Conference Series, 1399*, No. 3, p. 033110). IOP Publishing.

[18]. Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing, 13*(18), 1587-1611.

[19]. Dwivedi, Y. K., Rana, N. P., Tajvidi, M., Lal, B., Sahu, G. P., & Gupta, A. (2017). Exploring the role of social media in e-government: an analysis of emerging literature. In Proceedings of the *10th International Conference on Theory and Practice of Electronic Governance*, 97-106. ACM.

[20]. El-Kiki, T., Lawrence, E., & Steele, R. (2005). A management framework for mobile government services. Proceedings of CollECTeR, Sydney, Australia, 2009-4.

[21]. 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.

[22]. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 18*(1), 39-50.

[23]. Garver, M. S., & Mentzer, J. T. (1999). Logistics research methods: employing structural equation modeling to test for construct validity. *Journal of business logistics, 20*(1), 33.

[24]. Gottschalk, P. (2020). E-government interoperability and information resource integration: Frameworks for aligned development. *Information Systems, 193*.

[25]. Hair, J.F. Jr., Anderson, R.E., Tatham, R.L., & Black, W.C. (1998). Multivariate Data Analysis, (fith Edition). Upper Saddle River, NJ: Prentice Hall.

[26]. Hoyle, R.H., 1995. The structural equation modeling approach: Basic concepts and fundamental issues.

[27]. Huang, D., Zhou, Z., Xu, L., Xing, T., & Zhong, Y. (2011). Secure data processing framework for mobile

cloud computing. In *2011 IEEE Conference on Computer Communications Workshops* (INFOCOM WKSHPS) (pp. 614-618). IEEE.
[28]. Hung, S. Y., Chang, C. M., & Kuo, S. R. (2013). User acceptance of mobile e-government services: An empirical study. *Government Information Quarterly, 30*(1), 33-44.
[29]. Isagah, T., & Wimmer, M. A. (2019). Recommendations for M-G Implementation in Developing Countries: Lessons Learned from the Practitioners. In *International Conference on Social Implications of Computers in Developing Countries*, 544-555).
[30]. Islam, R., Islam, R., & Mazumder, T. (2010). Mobile application and its global impact. *International Journal of Engineering & Technology, IJEST*, 10(6), 72-78.
[31]. Kline, R. B. (2011). Principles and practice of structural equation modeling. 3rd Ed. United states, New York, Inc. ISBN 1462523358.
[32]. Ko, S. K. V., Lee, J. H., & Kim, S. W. (2012). Mobile cloud computing security considerations. *Journal of Security Engineering, 9*(2), 143-150.
[33]. Kuscu, M. H., Kushchu, I., & Yu, B. (2008). Introducing mobile government. In Electronic Government: Concepts, Methodologies, *Tools, and Applications,* 227-235). Igi Global.
[34]. 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, 31*(2), 290-310.
[35]. Lin, F., Fofanah, S. S., & Liang, D. (2011). Assessing citizen adoption of e-Government initiatives in Gambia: A validation of the technology acceptance model in information systems success. *Government Information Quarterly, 28*(2), 271-279.
[36]. Mouakket, S. (2010). Extending the technology acceptance model to investigate the utilization of ERP systems. *International Journal of Enterprise Information Systems (IJEIS), 6*(4), 38-54.
[37]. Ntaliani, M., Costopoulou, C., & Karetsos, S. (2008). Mobile government: A challenge for agriculture. *Government Information Quarterly, 25*(4), 699-716.
[38]. Nunnally, J. C., and Bernstein, I. H. (1994). Psychometric theory (3rd ed.). New York: McGraw-Hill. ISBN 1847879500.
[39]. Ovais Ahmad, M., Markkula, J., & Oivo, M. (2013). Factors affecting e-government adoption in Pakistan: a citizen's perspective. Transforming Government: *People, Process and Policy, 7*(2), 225-239.
[40]. Qi, J., Li, L., Li, Y., & Shu, H. (2009). An extension of technology acceptance model: Analysis of the adoption of mobile data services in China. Systems Research and Behavioral Science: The Official *Journal of the International Federation for Systems Research, 26*(3), 391-407.
[41]. Schumacker, R., & Lomax, R. G. (2010). A beginner's guide to Structural Equation Modeling (Third ed.). New York: Routledge: Taylor & Francis Group. ISBN 978-1-84169-890-8.
[42]. Sheila, M., Faizal, M. A., & Shahrin, S. (2015). Dimension of mobile security model: mobile user security threats and awareness. *International Journal of Mobile Learning and Organization, 9*(1):66–85.
[43]. Tabachnick, B. G., & Fidell, L. S. (2007). Using multivariate statistics (6th ed.). Boston, MA: Allyn & Bacon. ISBN 0205849571.
[44].Vetter, B. J., Gopi, R. P., & Arrieta, G. (2019). U.S. Patent No. 10,459,772. Washington, DC: U.S. Patent and Trademark Office.
[45]. Zhu, H., Xiong, H., Ge, Y., & Chen, E. (2014, August). Mobile app recommendations with security and privacy awareness. In Proceedings of the *20th ACM SIGKDD international conference on Knowledge discovery and data mining*, 951-960.

How to cite this article: Ala'a Saeb Al-Sherideh and Roesnita Ismail (2020). Motivating Path between Security and Privacy Factors on the Actual use of Mobile Government Applications in Jordan. *International Journal on Emerging Technologies, 11*(5): 558–566.