International Journal of Engineering & Technology, 7 (4.1) (2018) 51-56

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paperer

Mobile Government Applications Based on Security and Privacy: A Literature Review

Ala'a Saeb Al-Sherideh*, Roesnita Ismail, Fauziah Abdul Wahid, Norasikin Fabil, Waidah Ismail

Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia
**Corresponding author E-mail: alaa.sherideh@gmail.com*

Abstract

Mobile applications available in anytime and from anywhere. The utilizing of mobile governmental applications is significant to reduce the efforts and time that are required to accomplish the public services by citizens. The main challenges that face the acceptance and adoption of mobile governmental applications are the privacy and security issues. The users, who do not trust the security of mobile governmental applications, may reject the use of these applications which discourages the government to adopt the mobile services. This study focuses in investigating the security and privacy requirements of mobile government applications. Many related works are reviewed and discussed to understand the important security requirements of mobile government applications. The main results indicate that effective privacy and security of mobile government applications should be assured so as to enhance the level of adopting and using these applications. The security requirements involve many considerations such as the hardware characteristics, software characteristics, and communication characteristics. This article mainly gives better understanding of security requirements of mobile government applications.

Keywords: *Security, Privacy, Mobile Applications, Government Services.*

1. Introduction

Enterprises are now adopting mobile technologies for numerous applications to increase their operational efficiency by providing greater access to real-time information. They have improved their responsiveness and competitiveness by capitalizing on the mobile revolution to meet new customer demands [1,2]. This evolving mobile paradigm offers location independence and personalization for users accessing information and applications, thus enhancing user satisfaction. Mobile applications can also offer context-aware responses that consider the user's location, the time of use, or other attributes [2].

Mobile application is chiefly defined as a software application specifically developed for use on small and wireless computing devices. Mobile applications consist of software or a set of programs that run on a mobile device and perform certain tasks for the user. It is a new and fast developing segment of the global Information and Communication Technology. It is also easy, user friendly, inexpensive, downloadable and run in most of the mobile phone including inexpensive and entry level phone [3].

The significance of mobile government has increased due to ability of gathering data of citizens in the real-time location-based [4-6]. Thus, the efforts and time of accomplishing governmental services could be reduced. On the other hand, mobile government can customize new services through data integration among governmental ministries, which support several services through one window (i.e. accomplish all governmental services using one application) [7]. Ntaliani et al. [8] mentioned that the mobile application is one of the most used channels by citizens instead of other channels such as internet and face-face channels. Therefore, it is important to adopt the mobile applications to accomplish the citizens' governmental services.

One of the most important requirements of mobile applications is the security and privacy features [9-12]. The security is about the protections of services and information from attacking or damaging using several threats such as viruses and warms. The privacy is about ensuring the legal authority of private services and information accessing e.g. using passwords. The weakness of mobile applications security or privacy decreases the trust level of these applications which minimize the acceptance of using the mobile applications by users. In consequence, the adoption of mobile applications by organizations will be reduced which prevents the gained benefits from applying and using the mobile applications. The security and privacy are the main concerns in the development of m-government applications due to various variables related to the security requirements.

In this context, the security and privacy of mobile application are still an issue as the wireless connectivity is less secured than the wire connections [9-12]. The security and privacy of mobile applications are affected by many complex variables such as usefulness of security and privacy methods, processing speed of mobile devices, storage capacity of mobile devices, the sensitivity level of information and services, speed and coverage of data transferring and the volume of transferred data [13-15]. Hence, the analysis of security and privacy features of mobile applications should be carefully conducted according to various variables of mobile environment. Accordingly, the main objective of this study is to investigate the security and privacy requirements of mobile government applications.

Copyright © 2016 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Related Works

The privacy and security concerns could decrease the level of using and adopting the mobile government applications. The users may reject the using of mobile government application, for they do not trust the security of these applications. On the other hand, the government may not adopt these applications due to security concerns. This section presents some related works to the security of mobile government applications in order to understand the security and privacy requirements of mobile government applications.

2.1. Security and Privacy Factors of Mobile Government Applications

At first, several related works focused on the importance of security and privacy factors of mobile government applications. Abdelghaffar and Magdy [16] conducted a case study of mobile applications among 100 students from the Egyptian universities. The study explored the success users' intention factors of mobile governmental applications. One of the main important factors is the users' trust of mobile governmental applications. The user's beliefs of trust can be assured through effective security and privacy levels of mobile governmental applications.

On the other hand, Al-Hujran [4] mentioned that the adoption of mobile applications in governmental services in developing countries is still facing many challenges due to weak understanding of mobile application features. The researcher investigated the main requirements of mobile applications in governmental services in Jordan. The data was collected using semi-structured interview with experts from Ministry of Information and Communications Technology (MoICT). The results indicated that there is no structured or standard framework for mobile governmental services in Jordan [4]. The trust of mobile applications for the governmental services in Jordan is one of the most central issues of mobile applications development. The mobile applications should cover the security and privacy issues of governmental services and citizen's data.

Moreover, Osman [17] surveyed 103 citizens in Sudan to investigate the variables that affect the use of mobile applications in the governmental services. In addition to trust, privacy, security and infrastructure variables, there is a lot of other key variables that affect the acceptance of mobile applications such as gender, level of educations and skill level of using mobile applications.

Furthermore, Al-Thunibat et al. [5] conducted questionnaire survey on 300 Jordanian citizens to analyze the most important issues of mobile governmental services from users' perspective. The significant results show that although the mobile governmental services are perceiving usefulness, the most essential barriers of mobile applications are as follows: trust, privacy and security, law and public policy, lack of infrastructure and lack of security.

In the same context, ElSherif et al. [6] stated that there are two main criteria of m-government, namely: services satisfaction and usage analysis. Both services satisfaction and usage analysis are affected by the data transactions efficiency and service quality of mobiles applications. The efficiency of data transactions is determined by the data transaction speed, data privacy and trust and data usability. On the other hand, the services quality is determined by many variables such as users' awareness, services accuracy and services availability. This model was constructed on the survey with 127 citizens from the United Arab Emirates. Table 1 summarizes the related works of security factors of M-governmental applications.

Based on the Table 1, there are limitations in the studies conducted on the security and privacy features of mobile applications for governmental services. As for the past studies, they focused on the importance of security and privacy of mobile applications rather than the design of effective model or framework to structure the various security and privacy methods that can be utilized to improve the trust level of mobile applications for governmental services. Many researchers confirmed that there is still a gap in the development of standard models or framework to structure the various requirements of m-governmental applications such as security requirements.

2.2. Security and Privacy Methods of Mobile Government Applications

There were many related works conducted on the security and privacy of mobile applications. Huang et al. [10] focused on the privacy and security methods from mobile applications in health domain. Two main methods were suggested; (1) assuring the authority of mobiles applications users through generating random key or code and sending it as SMS to accomplish the login procedures, and (2) encrypt the data stored in the server and once the user requests data from server, this data will be decrypted by a secret decryption key stored in the user mobiles.

Bahar et al. [18] focused on the data and service encryption stored in the server side. The data and services are decrypted in the server and encrypted once it arrives to mobile device. The mobile device can decrypt the services and data by using the secret decryption key, and the received data by server are encrypted again. This method of encryption is called Symmetric Algorithm (the destination and source of data have different encryption and decryption keys).

In the same context, Qi and Gani [15] mentioned that the data gathered between mobile application and the servers could be attacked in the mid line (connection path). They recommended two solutions to avoid this problem. The first solution is speeding up the data transferring using technology such as fiber optic in order to increase the difficulty of data attacking. The second solution is the transferring of amount of data according to network and mobiles specifications in order to reduce the possibility of data waiting in the connection paths. The data waiting increases the opportunities of attacking activities. Moreover, Qi and Gani [15] argued that it is important to classify the data and services stored in server in line with its security levels that reduce the security costs (i.e. focus on the private data and services and give less attention to public data and services).

Khan et al. [14] suggested effective security methods of mobile application based on the signature matching between the server and the mobile device. All active and legal mobiles on the network have specific signatures. Once the signature of mobile device is matched with the signatures that is stored in the server, then the user of mobile application can gather the services and data with the server. Otherwise, the mobile device will be blocked and deactivated from the network. Thus, the trust level of mobile devices can be identified based on the predefined signatures.

Another work concerning mobile applications' security was conducted by Ibukun and Daramola [13], they explained that the antivirus' tools are effective to detect and prevent the illegal transactions or attacking of service and data.

However, the specifications of antivirus for mobile network (i.e. wireless) are different from the fixed wire connection. Thus, it is necessary to develop or utilize the most suitable antivirus according to mobile application specifications and environment.

Table 1: Summary of Related Works of Security Factors of M-governmental Applications

Source	Aim	Scope	Findings	Strength	Weakness
Abdelghaffar and Magdy [16]	Explore the success users' intention factors of mobile governmental applications.	Higher Ministry Education in Egypt: questionnaire survey with 100 university students.	The user's beliefs of trust can be assured through effective security and privacy levels of mobile governmental applications.	Covered several motivational variables of using mobile applications in governmental services.	-The study scope focuses on universities environment rather than focusing on core government ministries. -No focus on specific security variables. -There was no model developed to clarify the importance of levels and relationship of/among studied variables.
Al-Hujran [4]	Investigate the main requirements of mobile applications in governmental services in Jordan.	Semi-structured interview with experts from Ministry of Information and Communications Technology.	Mobile applications should address the following requirements: Security Trust - Fair Cost - Infrastructural constraints.	-Focuses on specific and important requirements of mobile applications for governmental services. -The data collected from useful sources (specialists in ICT in governmental sectors).	-The study did not cover the citizens perspective. -Not focused on specific security variables. -There was no model developed to clarify the importance levels and relationship of/between studied variables.
Osman [17]	Investigate the variables that effects on using mobile applications in governmental services.	103 citizens from Sudan country.	-Trust. -Privacy. -Security. -Infrastructure -Demographic Aspects such as gender, education level, and skill of using mobile applications.	-Focused on important requirements of mobile applications for governmental services. -The data collected from good sample of citizens.	-Not focused on specific security variables. -There was no model developed to clarify the importance levels and relationship of/between studied variables.
Althunibat et al. [5]	Analyze the most important issues of mobile governmental services from users' perspective.	Questionnaire survey with Jordanian citizens.	-Law and public policy. -Lack of infrastructure. -Lack of security.	Studied the importance of formulate structured security requirement of m-government application.	-Focused on security polices rather than specific variables. -There was no model developed to clarify the importance levels and relationship of/between studied variables.
ElSherif et al. [6]	Construct model of mobile application features for governmental services.	Questionnaire survey with 127 citizens from United Arab Emirates.	-Efficiency (speed, data privacy and trust, and data usability). -Service Quality (users' awareness, services accuracy, and services availability).	Develop structured model based on effective data collection.	The model not includes deep details about the security variables and requirements.

In the context of mobile applications' privacy, Chow et al. [19] argued that the applications or accounts accessing using the right username and password are the most effective privacy methods. Stajano et al. [20] explained that the user passwords should be provided in strong manner to increase the difficulty of illegal accessing. For examples, the passwords must mix between letters, digits and special characters, the password should contain capital letters, and the passwords should not less than 8 characters. These specifications can be assured by the system in the stage of users registration.

Rassan and Al Shaher [21] highlighted many drawbacks of accessing a mobile application by using a password such as the possibility of stealing the password by watching from other users. They argued that the accessing using physical entities belong to user itself could enhance the privacy level of accessing authority. The accessing using the fingerprint is considered as one of the most and usable accessing methods to assure the authority of mobile applications accessing. For instance, someone cannot steal the fingers of a mobile user to perform any illegal accessing.

Wang et al. [22] agreed that it is necessary to develop or adopt other privacy methods in addition to accessing by username and password. They suggested the password encryption as one of the supportive methods as it increases the difficulty of attack or stealing the users' passwords. Table 2 summarizes the related works of mobile applications security and privacy methods.

2.3. Features of Mobile Government Application Related to Security Requirements

There are many related works to the features of the security requirements for mobile government applications. Wasserman [23] listed several features that should be taken in the development consideration of mobile government applications, which may affect the security requirement of the developed applications as the following:

i. Security: the mobile applications and data may be attacked or stolen, thus these applications should be secured using effective methods in order to motivate the using of mobile applications.
ii. Interaction with other applications: the mobile application may require integration with other other applications or data sources. Therefore, it is necessary to understand the integration possibilities with other applications.
iii. Families of hardware and software: the developed application may not work on some mobile hardware or conflict with other mobile software. Therefore, it is important to understand the targeted customer mobiles and develop the mobile applications to work effectively based on targeted mobile hardware. Also, it is necessary to avoid the confliction with other applications.
iv. The mobile application should be able to work using different mobiles network such as 2G, 3G, and WiFi technologies.

v. The mobile application is preferred to work effectively using different network speeds.

vi. The mobile application would be updated continually and smoothly to enhance the application effectiveness.

Table 2: Related works of mobile applications security and privacy

Source	Aim	Scope	Findings	Strength	Weakness
Ibukun and Daramola [13]	Improve the security of mobile applications.	Mobile Data Security.	The mobile devices in central database must be protected by antivirus.	Show that the antivirus of mobiles should have special specifications.	Did not focus on the transferred data via network.
Khan et al. [14]	Improve the security of mobile applications.	Mobile Data Security.	The mobile network must identify the valid mobile devices based on secure signatures. Thus, the invalid signature will not access the network.	The suggested security solution prevents strangers from access the mobile network.	Did not cover the mobile devices security or central database security.
Stajano et al. [20] ; Chow et al. [19]	Improve the privacy of mobile applications.	Mobile Data Privacy.	The users' passwords should be strong.	Improve the password performance.	Still use text passwords which can be attacked.
Bahar et al., [18]; Huang et al. [10]	Improve the security of mobile applications.	Mobile Data Security.	The data gathered between mobile applications and users must by encrypted.	Show that the encryption is the main process of mobile security.	-Only Focus on security processes. -Did not show the encryption details.
Rassan and Al Shaher [21]	Improve the privacy of mobile. Applications	Mobile Data Privacy.	Fingerprints accessing.	Improve the passwords performance.	Need special requirements.
Qi and Gani [15]	Improve the privacy of mobile applications.	Mobile Data Privacy and Security.	-Suitable specifications of mobiles (i.e. Speed). -Speed network line (i.e. Fiber optic). -Classify the services as public or private.	Cover many privacy and security issues.	No details were provided about the specifications.
Chow et al. [19]	Improve the privacy of mobile applications.	Mobile Data Privacy.	The users must login using username and password.	Basic and mandatory process.	Traditional solution.

On the other hand, Flora et al. [1] surveyed 130 respondents including software developers, team managers, researchers and customers to analyze the most important features that should be considered by mobile application developers for various categories such as games, multimedia, education, travel, communication and utilities. The survey results revealed the following important features:

1. Characteristics related to hardware: the characteristics of mobile hardware are important to develop the mobile applications. For example, the mobile application must be developed to be suitable for mobiles of different screen sizes and in less power requirements.
2. Characteristics related to software: The software feature contains three main characteristic; (1) application interaction such as user interfaces, users experiences of using mobile applications, and error notification, (2) application development such as application purpose, localization, and reachability, and (3) application security such as encryption and privacy.
3. Characteristics related to communication: the communication features are about the network connectivity.

In the context of software engineering phases, McIver [24] explained that the analysis and design of mobile application are very important to ensure the success of installing and running the applications. McIver [24] highlighted that there are many characteristics of mobile applications to be considered in analysis and design phase. The characteristics for mobile applications are as follows: affordance perception, usage contexts, user interface design, location of information retrieval, data storage of mobiles, connection quality and bandwidth issues, device power and security issues.

Thus, the security issues of mobile government applications could be affected by many features such as the following:

- Processing speed of mobile devices: the processing speed features of the mobiles owned by citizens could be analyzed to assure effective mobile services based on these features.
- Storage capacity of mobile devices: the storage capacity features of the mobiles owned by citizens could be analyzed to assure effective mobile services based on these features.
- Sensitivity level of information and services: the governmental services could be classified according to level of security in order to classify these services as public and private services. Thus, the security efforts can be expended on the private services rather than the public services.
- Speed and coverage of data transferring: the mobile speed and coverage of mobile network used by the citizens could be analyzed in order to understand the security and privacy features based on the specifications of mobile network.
- Volume of transferred data: the volume and type of transferred data of governmental services could be analyzed to understand the required security and privacy features of mobile applications to secure the transferred data.

3. Discussion of Related Works

Based on the related works, there are three main directions of the security of mobile government applications. Firstly, the security and privacy requirements are one of the most important success factors of the mobile government applications implementation [5,6]. Secondly, it is necessary to apply useful privacy and security methods based on the environment of the mobile government applications [13,15,21]. Thirdly, there are many features such as the transferring capacity, speed and device power that affect the security issues of the mobile government applications [1,24].

Despite the fact of the complexity of the security issues of the mobile government applications, it is pertinent to propose a security framework to manage the various directions related to the security requirements. It is also due to the lack in the rules and structures of how to develop a secure mobile government applications [4,5]. There are many gaps need to be filled in order to propose

the secure framework of mobile government applications, the gaps are as the following:

a) There is lack in the studies conducted on the privacy and security methods of mobile government applications. Thus, it is necessary to investigate the security and privacy methods to enhance the security level of the mobile government applications.

b) There is lack on the models or frameworks development to structure the security and privacy requirements of mobile application for the governmental services. Therefore, it is important to identify the features that affect the security of mobile government application.

4. Recommendations

Based on the identified gaps, the researchers would like to extend this research and propose a secure framework for mobile government applications which can manage the security issues of these applications. The propose framework should include several important directions such as the following:

a. **Security methods**: the security methods aim to prevent the attackers, along with their threats to attack the services and information (i.e. damage or stole). Among the examples of security methods are the data encryption, devices signatures, and antiviruses. However, the useful security methods should be adopted or developed based on the environment of mobile applications.
b. **Privacy methods:** the privacy methods aim to assure the users authority of services and information accessing. Of the examples of privacy methods are the passwords, fingerprints and send accessing code via SMS. The methods and characteristics of privacy methods should be usefully adopted or developed according to environment of mobile applications.
c. **Communication specifications:** the commutation specifications such as connection speed, coverage and capacity play an important role in the information security of mobile applications. The environment of mobile application should be carefully analyzed in order to understand the most suitable specification of communication.
d. **Hardware specifications:** the hardware specifications such as capacity and types of mobiles devices may affect the security of mobile applications. The environment of mobile application should carefully be analyzed in order to understand the most suitable hardware specification of mobile devices.
e. **Information Specifications:** the volume and format (e.g. video and text) of transferred information via mobile applications are one of the main factors that affect the information security of mobile applications. The specification of transferred information via mobile applications should be carefully analyzed to utilize the most suitable security requirements.
f. **Services and information types:** the type of services and information (public and private) of mobile applications should be analyzed and classified so as to understand the services and information that should be protected. The public services and information do not need security requirements which reduce the efforts and costs of security processes.

5. Conclusion and Future Works

The mobile government applications are important to enhance the services provided by governmental sectors to citizens. The security of mobile government applications is one of the most important challenges in using and adopting f these mobile applications. There are various and complex factors affect the security of mobile government applications such as the privacy and security methods, the communication types, hardware and software specifications and transferring speed and volume. Consequently, it is necessary to manage all of these factors in order to assure effective security level of mobile government applications.
These security factors could be managed through effective secure framework for mobile government applications. In a nutshell, the secure framework requires some works in the future such as investigating the security trust level of mobile government applications using questionnaire with citizens, examining the most useful privacy and security methods for mobile government applications and identifying the real situation of the related security factors in the countries i.e. mobile communication coverage, speed and strength in the county.

Acknowledgments

This research was supported by the short term research grant scheme (PPP-FST-12316-00) at the Universiti Sains Islam Malaysia (USIM).

References

[1] H. K. Flora, X. Wang., & S. V. Chande, An investigation on the characteristics of mobile applications: A survey study. *International Journal of Information Technology and Computer Science (IJITCS)*, Vol. 6, No. 11, pp.21-27, 2014.
[2] B. Unhelkar, S. Murugesan, The enterprise mobile applications development framework. *IT Professional Magazine*, Vol. 12, No. 3, pp.33-39, 2010.
[3] R. Islam, R. Islam., & A. T. Mazumder, Mobile applic-ation and its global impact. *International Journal of Engineering & Technology IJET-IJENS*, Vol. 10, No. 06, pp. 72-78, 2010.
[4] O. Al-Hujran, Toward the utilization of m-government services in developing countries: a qualitative investigation. *International Journal of Business and Social Science*, Vol. 3, No. 5, pp. 155-160, 2012.
[5] A. Althunibat, T. A. Alrawashdeh., & M. Muhairat, The acceptance of using m-government services in Jordan. *Journal of Theoretical and Applied Information Technology,* Vol. 63, No.3, pp.733-740. (2014).
[6] H. M. ElSherif, K. M. Alomari, A. S. AlHaddad., & A. O. Alkatheer, Mobile Government Services Satisfa-ction and Usage Analysis: UAE Government Smart Services Case Study. *A Monthly Journal of Computer Science and Information Technology*, Vol. 5, Issue. 3, pp.291 – 302. 2016.
[7] M. H. Kuscu, I. Kushchu., & B. Yu, Introducing mobile government. In A. Anttiroiko (Ed.), *Electronic Government: Concepts, Methodologies, Tools and Applications IGI Global*, pp. 227-235, 2008.
[8] M. Ntaliani, C. Costopoulou., & S. Karetsos, Mobile government: a challenge for agriculture. *Government Information Quarterly*, Vol. 25, No. 4, pp. 699-716, 2008.
[9] H. T. Dinh, C. Lee, D. Niyato., & P. Wang, A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing*, Vol. 13, No. 18, pp.1587-1611, 2013.
[10] D. Huang, Z. Zhou, L. Xu, T. Xing., & Y. Zhong, Secure data processing framework for mobile cloud computing. *In Computer Communications Workshops (INFOCOM WKSHPS) 2011 IEEE Conference*, pp. 614-618, 2011.
[11] S. K. V. Ko, J. H. Lee., & S. W. Kim, Mobile cloud computing security considerations. *Journal of Security Engineering*, Vol. 9, No. 2, pp. 143-150, 2012.
[12] H. Zhu, H. Xiong, Y. Ge., & E. Chen, Mobile app recommendations with security and privacy awareness. *In Proceedings of the 20th ACM SIGKDD inter-national conference on Knowledge discovery and data mining*, ACM, pp. 951-960, 2014.
[13] E. Ibukun, O. Daramola, A systematic literature review of mobile cloud computing. *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 10, No. 12, pp.135-152, 2015.
[14] A. N. Khan, M. M. Kiah, S. U. Khan., & S. A. Madani, Towards secure mobile cloud computing: A survey. *Future Generation Computer Systems*, Vol. 29, No. 5, pp. 1278-1299, 2013.
[15] H. Qi, A. Gani, Research on mobile cloud computing: Review, trend and perspectives. *In Proceedings of the Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, IEEE, pp. 195-202, 2012.

[16] H. Abdelghaffar, Y. Magdy, The adoption of mobile government services in developing countries: the case of Egypt. *International Journal of Information and Communication Technology Research*, Vol. 2, No. 4, pp. 333 – 341, 2012.
[17] N. B. Osman, Extending the technology acceptance model for mobile government systems. *The International Arab Conference on Information Technology ACIT*, 2013.
[18] A. N. Bahar, M. A. Habib., & M. M. Islam, Security architecture for mobile cloud computing. *International Journal of Scientific Knowledge Computing and Information Technology*, Vol. 3, No. 3, pp.11-17, 2013.
[19] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi., & Z. Song, 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, 2010.
[20] F. Stajano, M. Spencer, G. Jenkinson., & Q. Stafford-Fraser, Password-manager friendly (PMF): Semantic annotations to improve the effectiveness of password managers. *In: Passwords. Volume 9393 of Lecture Notes in Computer Science. Springer*, pp. 61–73, 2014.
[21] I. A. Rassan, H. Al Shaher, Securing mobile cloud using finger print authentication. *International Journal of Network Security & Its Applications*, Vol. 5, No. 6, pp.41-53, 2013.
[22] Y. Wang, R. Chen., & D. C. Wang, A survey of mobile cloud computing applications: Perspectives and chall-enges, *Wireless Personal Communications*, Vol. 80, No. 4, pp. 1607-1623, 2015.
[23] A. I. Wasserman, Software engineering issues for mobile application development. *In Proceedings of the FSE/SDP workshop on Future of software engineering research*, ACM, pp. 397-400, 2010.
[24] W. McIver, Software engineering processes for mobile application development. Technical report, *Nserc Industrial Research Chair in Mobile First Technology*. New Brunswick Community College, Canada, 2015.