Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of Information Technology and Networking

Article

Examining the Impact of Privacy, Security and Legal Framework on Trust in Mobile Computing in Business Environment: An Exploratory Study

*Qais Hammouri *,Emad Abu-Shanab , Ahmad Manasrah*
IT College, Yarmouk University, Irbid, Jordan

Article info

Article history:

Accepted Jan, 2016

Keywords:

Security

Privacy

Trust

Law

Mobile computing expert opinion

Abstract

With the vast and rapid growing of information technologies, the use of mobile computing has increased dramatically. This led to the emergence of concerns related to information security, customers' privacy, guiding laws, and lack of trust in using mobile services. This study will investigate the issues related to trust in mobile computing and its impact on users of mobile devices. The results demonstrated that both privacy and security are essential issues that affect users' trust and hence, the adoption process. Results also indicated that an adequate legal framework that governs security issues needs to be developed and enforced in mobile computing and business environments. The detailed results of this study are reported with conclusions at the end.

* Corresponding author: Qais Hammouri
E-mail address: hammouriqais@yahoo.com

1. Introduction

Mobile technology has grown significantly over the past few years. A wide range of mobile technologies became available for users like smart phones, tablets (PCs), notebooks and laptops. Two important phenomena emerged: First, great computing power of Smart phones along with its place convenience. Such feature encourages the development of many new mobile applications offered to users online via the app store. The second phenomenon is the spread of malware, which is increasingly deployed to extracting users' data. Nevertheless, effective mechanisms of defense are developed against malware because of the complexity of m-applications and their operating system (Santos, 2013). Using open networks such as the Internet environment, issues concerning trust and security become critical. The physical view of the network vs. the distributed nature and the user authentication concept to the domain is becoming more important. Kagal (2001) asserted that with the growing complexity of mobile devices in the modern era, the security of such devices (in the presence of countless attacks) is becoming the main issue. The majority of mobile phones are still not guaranteed against the existing and emerging security threats. Regardless of its nature, security attacks on mobile devices aim mainly at causing a system malfunction or leak of personal information (Mal-Sarkar & Bhunia, 2010).

Mobile computing provides users with a platform of information management system that is free from temporal and spatial constraints. Freedom from these restrictions allows users to access and process required information from any place and at any state (mobile or static). PCSs are connected to the Public Switched Telephone Network (PSTN) to provide access to wired phones (Kumar, 2004). Users of smart environment demanded solutions to be trustworthy, private, and secure. Security defines the techniques of cryptography utilized to secure required data and communication channels. Privacy is related to the risks involved in exposing personal information when interacting with ISs. Based on that, users' trust is defined in terms of users' allowed level of control on the quantity of information that could be disclosed, and the calculated risks or anticipated benefits that would stimulate users to share their information during such interactions (Nixon et al., 2004).

The general theory of confidence in computers and humans networks should be built on computational trust theory or behavioral trust theory. These theories depend on the increased people participation in the protocols of socio-economic and social networking. The effective participation of users in the protocols depends mainly on trust. Strict on-line protocol compliance verification is often not practical, where verification can cause user's inconvenience. Confidence is captured through the preferences of participants (such as betrayal aversion or risk), and their beliefs in the credibility of the participants in another protocol (Gligor, 2011).

2. Literature Review

The convergence between mobile computing and the Internet allows personalized access to online services anytime and anywhere. Such feature creates great opportunities for new business models that stimulate rapid innovation and vigorous investment. Unfortunately, such innovation produces also new threats and vulnerabilities, and the new business models also generate incentives for more attacks. The growth in mobile service and use of the Internet would face painful setbacks due to the unequal security measures and new emerging threats. The main factors to identity management sustainable development in online communities and markets were trust and security (Josang, 2013).

2.1 Mobile Computing Environment

Handheld devices, such as smart phones, are becoming an increasingly essential part of human lives for communication, where their most convenient and effective benefit is that they are not bounded by place and time. Mobile users can benefit from diverse mobile applications like: Google Apps, iPhone apps, etc. With the rapid advancements in Mobile Computing (MC), there is a strong tendency to benefit from such phenomenon when joined by information technology. But, mobile devices face many challenges like its storage, bandwidth, battery life, and communication issues like security and mobility (Dinh et al, 2011).

At present, most of institutions utilized mobile devices at work to facilitate the services they provide and products they sell. Mobility enables employees to take their work with them wherever they go, including company proprietary information, sensitive customer data and intellectual capital data. Mobile devices enable employees to perform what they need to do, wherever and whenever they want. People could cooperate and collaborate in the field with business partners, customers, patients or students. Employees working in the field require data support for their transactions and processes like documents, Internet, or applications (Archer et al., 2012). Employees can access corporate resources using their mobile devices to increase their productivity and flexibility. But if their mobile devices are exploited or vulnerable, they become a source for leaking or corrupting crucial business information. Such benefit (company mobility initiatives) comes with cost; mainly risking the resources needed to manage the devices that contain the data and secure corporate data (Ro, 2012).

Data availability and increased connectivity provide new models for conducting business, but create new security risks. For instance, to simplify financial transactions, the organization may want to allow business partners or customers some accessibility to certain local resources. The institution should develop company policies outlining the privileges of extranet accessibility. Such relationship brings trust to the front page. Trust requires a repetitive detection of credentials among the two parties in order to build the needed level of confidence to complete any transaction (Wins-

lett & Yu, 2001). Finally, improvements in MC device storage and power capabilities make the physical damage much more harmful to the organization. Additionally, they become attractive to profit-motivated cyber criminals (Robb, 2009).

Mobile phone users are divulging more information on their behavior and location on the basis of site data created when using their mobile devices. In criminal cases, law enforcement parties can access site data to help solve crimes; this confirms how data can be revealed in identifying patterns of individuals' behavior (Syme, 2009).

Mobility causes unplanned interactions among computer systems that are used by people to reach services in diverse environments. Before any transaction between two systems, systems must trust each other and satisfy the requirements of privacy and security (Caceres & Sailer, 2006). Mobile payment (M-payment) allows easy payment, thus, it has received considerable attention and became an important complement to the traditional payment methods. Nevertheless, m-payment via open networks makes security challenges more potent (Alafeef et al., 2013). Although much research has addressed security issues, still some security problems are not well resolved. An example is the problems of platform integrity and the protection of user's privacy. Authors have proposed public wage structure with trusted computing (TC) technologies to secure the m-payment transactions. Using simple infrastructure of mobile payment, a study presented a solution to protect the integrity of the platform, secure the payment software download, secure payment transactions, and protect application initialization (Zhong et al, 2009).

Huge market for mobile applications to serve e-commerce across the world is booming. Nevertheless, the demand for these services was challenged by privacy and security concerns of end users. The limited memory, limited processing of mobile devices, and its dependence on wireless channels made it inherently unreliable and left a little room for a layer of reliable security measures (Chaturvedi et al., 2013).

2.2 Trust and mobile computing

The risks associated with mobile computing are increasing, where mechanisms, policies, and models are developed to assess the credibility of such service to each involved party. Trust formation depends on the reputation of the other party involved, recommendations from other users, or previous experience. Trust management allows for the recommendation of a service provider who is most probably to offer the necessary service whenever users are faced with a number of service providers who are not previously known (Seigneur, 2005).

People are increasingly saving more personal information on their mobile devices which increases the risk of losing such data or exposing it to unwanted people. The concerns of privacy and security in MC environment could be seen from different views including applications, user interfaces, databases, networks, operating systems and hardware (Khiabani et al., 2009). Threats against

mobile devices are much more severe than conventional malware; mobile devices usually carry personal data more than desktop computers. Users may think that because they are carrying their mobiles constantly, they are securing them. But the physical control over the device does not necessarily guarantee the safe control of its content. Users have false security sense, which would lead them to a misleading confidence in such devices (Dagon et al., 2004). Mobile devices were developed to be lightweight and small, making it highly portable. Thus, they were susceptible to theft and loss. Mobile Devices could be protected through the use of smart cards and passwords. The types of trust in mobile devices reported in the literature are: trust of undercover-agent, trust of captured-agent, and trust of personal-agent (Mavridis & Pangalos, 2002).

Trust is an important factors influencing people's adoption of any technology (Yan et al. 2009; Abu-Shanab, 2014; Khasawneh et al., 2013). Trust is the affirmative belief around the reliability, dependability and confidence in the process, object and persons related to MC services. When users are conducting transactions through mobile networks they are not likely to know the identity of service providers. In addition, mobile services collect information about users and their use behavior. Such process is bounded with ethical dimensions that require more attention, particularly ensuring user's privacy (Kaasinen, 2005).

Trust in electronic transactions is developed by the "Trusted Computing Group" (TCG), which aims at imposing trustworthy conduct over computing platforms. The software chain consists of 'good software' like scanners for viruses. Such applications try to eliminate and identify harmful programs. The techniques suggested by "Trusted Computing Group" are concentrated around "Trusted Platform Module" (TPM). The TPM chip is connected to the Central Processing Unit-CPU and offers isolated storage for the keys of encryption and the 16 PCR "Platform Configuration Registers" (Lyle & Martin, 2010). When people use their computers they tacitly assume that their machines don't include malware, like keystroke logger, and are not manipulated with. Such assumption is realistic because the unauthorized physical access to device is prohibited. For the vision of ISR (Internet Suspend/Resume), users should be capable of rapidly establish identical level of confidence in devices that do not manage or own. To tackle this problem, the Trust-Sniffer is created; a tool that assists users to gradually gain trust in un-trusted machines (Surie et al., 2007).

There are many behavioral and technical factors that influence the deployment and design of mobile applications. Trust is one of the main factors. In a study on confidence in an assortment of technology-based subjects like virtual teams and e-business, evidence is found that there is a need to ample trust for deployment of different computing environments. Consequently, it is also likely that confidence will be an important element in achieving successful deployment of computing

environments everywhere (Valacich, 2003). Trust management or trust models within mobile environment need to extract standards for user's trust in various contexts, user's decision, feedback dissemination, and user's experience in trust or distrust. Nevertheless heterogeneity, uncertainty, and mobility of the mobile computing environment makes confidence management more complex, where users are becoming more undetermined, volatile, and mobile. The study suggested the model of distributed trust in the environment of mobile computing based on a range of useful notes about conduct of user (Wu, 2013).

2.3 Solutions for trust issues

Trusted computing is expected to behave as expected by users. TCG promotes open standards to hardware enabled security technologies and trusted computing including software interfaces and across multiple devices, peripherals and platforms. It deploys a specified technology that enables computing environments to become more secure without affecting individual rights, functional privacy or integrity (Yan, 2007).

Kagal et al. (2002), suggested a solution for trust issues based on the management of distributed trust which includes thinking about the access rights of users, revoking rights, delegating trust to other parties, and developing security policy. The study depicted the infrastructure that supplement the existing features of security such as "Role Based Access Control" and "Public Key Infrastructure" (PKI) augmented by management of distributed trust to supply a high degree of flexibility for security in a widespread computing environment.

Security and trust issues were main factors in the deployment of cloudlet. The thick "Virtual Machine" VM boundary isolates a cloudlet from programs implemented by malicious or careless users. Nevertheless, a user's trust in the integrity of the infrastructure Cloudlet rests on assumptions that are more fragile. For instance, a malicious VMM can skillfully implement distortion of translation within the VM and consequently subvert a significant business deal without user being aware of harm (Satyanarayanan et al., 2009). The advent of deployed computing systems like Internet Resume/Suspend has facilitated the access to the personalized computing field of users through layers of "Virtual Machine" technology at the head of distributed storage. This model suffered from several challenges like establishing trust in unmanaged devices that users can access, and eventually migrating "Virtual Machine" (VM) state through networks of low-bandwidth (Surie, 2007).

2.4 Privacy issues in mobile computing

Social networks are becoming more and more important as a popular platform for social interaction and communication between millions of users. Nevertheless, these systems pay little attention to the concerns of privacy and security associated with revealing friendship information and personal social networking behaviors (Beach et al., 2009). The protection of privacy through techniques of automatic anonymity is not bearable in

which data richness and research value can be maintained at the same time. Trusted researchers are allowed to work with Lausanne Data Collection Campaign (LDCC) after accepting in written format to respect privacy and anonymity of the participants volunteering in LDCC (Laurila et al, 2012).

Policies related to privacy are confidence-based mechanisms that prescribe specific uses from location information. While regulations intend to provide group-based and global privacy guarantees, privacy policies intend to provide privacy protection that is elastic enough to adapt to the individual user's requirements and individual transactions. There are three key initiatives currently underway that described few methods to handle privacy issues and they are: Internet Engineering Task Force (IETF), GeoPriv, World Wide Web Consortium (W3C), Privacy Preferences Project (P3P), and Personal Digital Rights Management (PDRM) (Duckham & Kulik, 2005). In successful attacks on privacy, certain party gets unauthorized information. Persons can consent that certain information about them can be available for others, and other information should remain private. The key concern of privacy with respect to ubiquitous computing is that several vectors of automated attack become possible (Brandi & Rosteck, 2006).

2.5 Security issues in mobile computing

Privacy and security are explored in most cases together when dealing with their importance to users and in mobile environment (Abu-Shanab & Ghaleb, 2012). Mobile cloud is combining cloud computing and mobile networks concepts. In mobile cloud computing the main challenges facing cloud services are performance, availability and security. Security of cloud computing is always the major factor and is ranked as a top priority for users and developers (Bahar et al., 2013; Sinjilawi et al. 2014). Cloud providers, mobile user, and other parties were all concerned about confidence. Basically confidence propensity is a personal trait. The reputation of service provider influences the level of confidence between the cloud and its clients. Standards required in the establishment of trust are the following: Security, privacy, robustness, stability, reliability, and elasticity (Sanaei et al, 2012).

Mobile cloud computing brings many advantages to hardware with minimum resources; benefits that lead to developing applications with rich functionality. Security issues in mobile cloud computing could be categorized into two major categories: cloud threats and mobile threats. The key purpose of these threats is to exploit the resources of mobile device or steal personal data (like location, calendar, contact database and passwords) (Popa et al, 2013).

Establishing applications on customized infrastructure rather than establishing applications on rigid and fixed infrastructure is offered by cloud computing. By tapping into the cloud, organizations benefit from adequate infrastructure resources and business applications with reduced capital expenditure (CAPEX). The cloud carries

large size of information from enterprises and individuals, where security becomes more important (Ko et al, 2012). Security is associated with distribution, scale, concurrency, and multi-tenancy. Direct concerns originate from aspects like lack of control on code and data distribution at distributed infrastructures, and the loss of potential data. Also, the indirect issues originating from offering unlimited computational resources virtually to users raise the issue of trust by users (Kovachev, 2010).

3. Research Methodology and Results

3.1 Research model and hypotheses

This research explored the research queries using two samples. The first sample filled a questionnaire exploring the descriptive of the items of survey. The second sample was used for the purpose of testing the model. The aim of the second sample is to investigate the main factors that influence the level of trust in mobile computing. Research model shown in Figure 1 depicts our premise in this study, where we hypothesize that security, privacy and legal framework will influence users trust in mobile computing. Similar premise was proposed by Al-sharafi et al., (2015), but in Internet banking area.

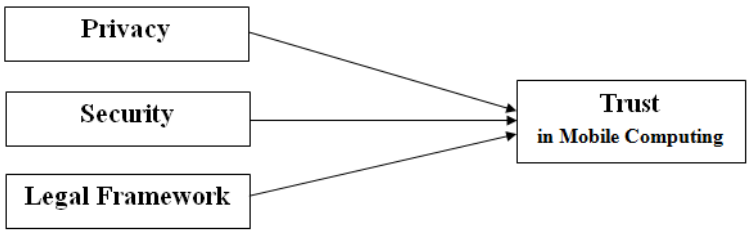

Figure 1: *The research model*

The third factor proposed in this study is the legal framework, where previous research emphasized on the role of legal framework in defining the risks associated with technology (Abu-Shanab, 2012). This factor is not well researched and is considered a major contribution of this area. The following hypothesis is stated:

H3: Legal framework existence will have a significant influence on Trust in Mobile computing.

The first sample: The developed survey was distributed to students in a public university in the Northern part of Jordan. The questionnaire focused on issues like: the existence of effective programs that cover privacy and trust in mobile computing, the effect of raising awareness to electronic security in mobile computing, and the existence of laws that protect privacy issues related mobile computing.

The questionnaire used utilized a 5 point Likert scale where 1 indicated a total disagreement, and 5 indicated a total agreement with the statements posted. The items covering the influence of privacy on trust were 5 as shown in Table 1. Similarly, 5 items measured security, 5 items measured legal framework, and 5 items measured the level of

trust. The total sample size was 30, which is not adequate for relational statistical analysis, but benefited from the high awareness of graduate students where they might be considered experts in the domain. Research indicated that education level is a strong influencer of such domain (Abu-Shanab, 2011).

The second sample: The same items were used in a second survey distributed after 6 months (based on the inadequacy of the first sample) but utilizing a 7 point Likert scale where 1 indicated a total disagreement and 7 indicated a total agreement with the statements posted. The total second sample size was 99 students, with 68 females (68.7%) and 31 males (31.3%).

Table 1: *Survey items*

Privacy items	
P1	The use of mobile computing could reduce privacy.
P2	Information exchanged among mobile computing devices has the necessary privacy.
P3	The existence of effective programs that provide privacy when using mobile computing increases trust
P4	Supplying users with the methods necessary to protect privacy increases trust in mobile computing.
P5	The most important reasons for distrust in mobile computing is the lack of privacy
Security items	
S1	The exchange of expertise in scientific and technological knowledge related to information security increases trust in mobile computing.
S2	The use of mobile computing might reduce information security.
S3	Providing the means of protection necessary to maintain security of information increases trust in mobile computing.
S4	The most important reason for distrust in mobile computing is the lack of security
S5	The awareness of electronic security could reduce IT crimes and increase trust in mobile computing .
Legal framework items	
L1	The existence of adequate legal framework protects privacy and increases trust in mobile computing.
L2	The existence of adequate legal framework supports security and increases trust in mobile computing.
L3	The existence of adequate legal framework that punishes people who use mobile computing illegally will increase trust in mobile computing.
L4	Trust in mobile computing is related to adequate legal framework
L5	Legal framework has significant influence on mobile computing privacy and security issues
Trust items	
T1	Awareness of mobile computing threats and how to avoid them increases confidence in mobile computing
T2	Trust in mobile computing is affected by privacy degree.
T3	Trust in mobile computing is affected by security
T4	Trust in mobile computing is affected by legal issues
T5	Trust in mobile computing leads to increasing its use.

3.2 Data results and hypotheses testing

This study depended on experts opinion regarding issues related to mobile computing security. In The previously mentioned questionnaire was distributed to 30 graduate students studying in a public university in Jordan. 53.3% of respondents were males, while 46.7% were females. Table 2 lists the frequencies of each item and the distribution of items in relation to the survey items mentioned in Table 1.

Table 2: *Distribution of responses according to all survey items*

Privacy Scale	**Privacy item 1**		**Privacy item 2**		**Privacy item 3**		**Privacy item 4**		**Privacy item 5**	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
Strongly Disagree	1	3.3	3	10	4	13.3	1	3.3	5	16.7
Disagree	6	20	9	30	4	13.3	2	6.7	3	10
Neutral	7	23.3	4	13.3	4	13.3	3	10	4	13.3
Agree	14	46.7	11	36.7	9	30	11	36.7	12	40
Strongly Agree	2	6.7	3	10	9	30	13	43.3	6	20
Total	30	100	30	100	30	100	30	100	30	100
Security Scale	**Security item 1**		**Security item 2**		**Security item 3**		**Security item 4**		**Security item 5**	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
Strongly Disagree	0	0	2	6.7	2	6.7	4	13.3	1	3.3
Disagree	4	13.3	4	13.3	7	23.3	4	13.3	2	6.7
Neutral	3	10	3	10	0	0	0	13.3	1	3.3
Agree	15	50	11	36.7	10	33.3	13	43.3	12	40
Strongly Agree	8	26.7	10	33.3	11	36.7	9	30	14	46.7
Total	30	100	30	100	30	100	30	100	30	100
Legal Scale	**Legal item 1**		**Legal item 2**		**Legal item 3**		**Legal item 4**		**Legal item 5**	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
Strongly Disagree	0	0	0	0	2	6.7	2	6.7	1	3.3
Disagree	2	6.7	1	3.3	1	3.3	1	3.3	1	3.3
Neutral	2	6.7	2	6.7	2	6.7	0	0	3	10
Agree	15	50	15	50	15	50	13	43.3	12	40
Strongly Agree	11	36.7	12	40	10	33.3	14	46.7	13	43.33
Total	30	100	30	100	30	100	30	100	30	100
Trust Scale	**Trust item 1**		**Trust item 2**		**Trust item 3**		**Trust item 4**		**Trust item 5**	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
Strongly Disagree	0	0	2	6.7	1	3.3	0	0	3	10
Disagree	1	3.3	1	3.3	1	3.3	1	3.3	2	6.7
Neutral	4	13.3	8	26.7	7	23.3	5	23.3	8	26.7
Agree	13	43.3	12	40	15	50	15	50	15	50
Strongly Agree	12	40	7	23.3	6	20	9	30	2	6.7
Total	30	100	30	100	30	100	30	100	30	100

The first step done on the second sample was to estimate the bivariate correlations between the variables and the means and standard deviation of each variable. Results are shown in Table 3 below. The results indicated a high perceived mean of each variable (all above 5). Also, a significant correlation was estimated between the variables and with an alpha value < 0.01. Finally, such result indicates that all three variables are important in influencing trust.

Table 3: *Bivariate Pearson's correlations and the means and standard deviations*

	Privacy	Security	Legal	Trust	Mean	Stand. Dev.
Privacy	1				6.2843	1.01568
Security	.661**	1			5.8530	0.98470
Legal	.520**	.553**	1		5.7455	1.18729
Trust in Mobile Computing	**.579****	**.565****	**.606****	1	5.6051	1.26145

**. Correlation is significant at the 0.01 level (2-tailed).

To test the hypotheses and the proposed research model we conducted a multiple regression test that regressed the three independent variables on trust in mobile computing. Based on that, the results indicated a significant model with an R^2 =

0.481, with an $F_{3,95}$ = 29.332, p<0.001. Such result indicates that the model explains 48.1% of the variance in trust in mobile computing. Finally, to know the influence of each variable on trust, the regression coefficient table shows such result. The results shown in Table 4 indicate a significant influence by privacy and legal framework, but not security.

Table 4: *The regression coefficient table*

Variables	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-0.100	0.637		-0.157	0.876
Privacy	0.330	0.126	0.266	2.615	**0.010**
Security	0.240	0.133	0.187	1.799	0.075
Legal	0.387	0.097	0.365	3.982	**0.000**

Dependent Variable: Trust

4. Conclusion and Future Works

This research aimed at investigating the factors affecting user's trust in mobile computing environment. Two samples were used to explore the issues related to the research model proposed. A survey covering four dimensions was distributed among 30 graduate students (experts). The dimensions are: privacy, security, legal framework, and trust. Results demonstrated that both privacy and security are essential issues that affect users' trust to adopt and use mobile computing.

The use of mobile computing may also result in decreasing the security level for the transferred data; so users must be aware of the probable risks and threats that may occur in this environment. There must be also an adequate legal framework governing security issues to reliably transfer data in mobile computing environments. It can be also concluded that the exchange of the experiences between concerned authorities will result in improving the level of security and thus increase trust and the adoption of this technology. Future work is required to comprehensively explore the four dimensions and expand the sample size.

Furthermore, the same items but utilizing a wider scale (7 points Likert scale) and a different sample (99 bachelor students) was used to explore the relationships shown in the research model. Results indicated that 48.1% of the variance in trust can be explained by the data collected and by using privacy and the legal framework. The security factor did not predict trust as hypothesized. This result supports hypotheses H1 & H3, and failed to support H2.

This study drives researchers' attention to explore more the dimensions of security to understand why they did not compete well in the model. Also, our model supported the importance of the legal framework that covers mobile computing issues. This study suffered from the sample size in the first stage, where statistical analysis was not valid.

Also, using students in the second sample risks the generalizability of our conclusions.

References

[1] Abu-Shanab, E. (2011). Education Level as a Technology Adoption Moderator.Proceedings of the 3rd IEEE International Conference on Computer Research and Development (IC-CRD 2011). Shanghai, China, March 11-13, 2011, V0l 1, pp. 324-328.

[2] Abu-Shanab, E. (2014). Antecedents of Trust in E-government Services: An empirical Test in Jordan. Transforming Government: People, Process and Policy, Vol. 8(4), pp. 480-499.

[3] Abu-Shanab, E. &Ghaleb, O. (2012). Adoption of Mobile Commerce Technology: An Involvement of Trust and Risk Concerns. International Journal of Technology Diffusion, Vol. 3(2), April-June, 2012, pp. 36-49.

[4] Alafeef, M., Singh, D., Ahmad, K., Abu-Shanab, E. (2013).Usability Testing for Mobile Banking Prototype in Jordan.*Proceedings of the 2nd International Conference on Computer Engineering &Mathematical Sciences (ICCEMS 2013),* 5-6 December 2013, Kuala Lumpur, Malaysia, pp. 48-54.

[5] Al-Sharafi, M., Arshah, R., Abu-Shanab, E., Fakhreldin, M. &Elayah, N. The Effect Of Security And Privacy Perceptions On Customers' Trust To Accept Internet Banking Services: An Extension Of TAM. *COMSCET 2016,* Kuala Lumpur, Malaysia, 23-24 January, 2016, pp. 1-9.

[6] Archer, J. Boehme, A. Cullinane, D. PuhlmanN, N. Kurtz, P. and Reavis, J. (2012).Mobile Working Group Security Guidance for Critical Areas of Mobile Computing.Cloud Security Alliance, 2012.

[7] Bahar, A. Habib, A. and Islam, M. (2013).Security Architecture for Mobile Cloud Computing. International Journal of Scientific Knowledge, Vol. 3(3), PP, 11-17.

[8] Beach, A. Gartrell, M. &Han, R.L. (2009).Solutions to Security and Privacy Issues in Mobile Social Networking.In Computational Science and Engineering, 2009.CSE'09.International Conference on (Vol. 4, pp. 1036-1042). IEEE.

[9] Brandi, H.&Rosteck, T. (2004).Technology, Implementation and Application of the Trusted Computing Group Standard (TCG).Secure platforms provide new levels of security. Infineon White Paper.Datenschutz und Datensicherheit.Viewag.

[10] Caceres, R. &Sailer, R. (2006).Trusted Mobile Computing.In Proc. of IFIP Workshop on Security and Privacy in Mobile and Wireless Networks, Coimbra, Portugal.

[11] Chaturvedi, M. Malik, S. Aggarwal, P. and Bahl, S. (2013). Privacy & Security of Mobile Cloud Computing.Ansal University, Sector 55, Gurgaon-122011, India.

[12] Dagon, D. Martin, T. and Starner, T. (2004). Mobile Phones as Computing Devices: The Viruses are Coming! Pervasive Computing, IEEE, Vol. 3(4), PP, 11-15.

[13] Dinh, H. Lee, C. Niyato, D. & Wang, P. (2011). A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches .Journal of Wireless Communications and Mobile Computing, Vol. 13(18), PP, 1587-1611.

[14] Duckham, M. &Kulik, L. (2006).Location Privacy and Location-Aware Computing.Investigation in Change and Time.Dynamic & mobile GIS: investigating change in space and time, Vol. 3(1), PP, 35-51.

[15] Gligor, V. & Wing, J. (2011).Towards a Theory of Trust in Networks of Humans and Computers. In Security Protocols XIX (pp. 223-242).Springer Berlin Heidelberg.

[16] Josang, A. (2013). Identity Management and Trusted Interaction in Internet and Mobile Computing. IET Information Security, Vol. 8(2), PP, 67-79.

[17] Kaasinen, E. (2005). User acceptance of mobile services– value, ease of use, trust and ease of adoption. Behavior and Information Technology, Vol. 24(1), PP, 37-49.

[18] Kagal, L. Finin, T. & Joshi, A. (2001). Moving from Security to Distributed Trust in Ubiquitous Computing Environments, IEEE Computer, Vol. 34(12), PP, 154-157.

[19] Kagal, L. Undercoffer, J. Perich, F. Joshi, A. &Finin, T. (2002).A Security Architecture Based on Trust Management for Pervasive Computing Systems.Maryland Univ Baltimore Dept of Computer Science and Electrical Engineering.

[20] Khasawneh, R., Rabayah, W. & Abu-Shanab, E. (2013). E-Government Acceptance Factors: Trust And Risk. *The 6th International Conference on Information Technology (ICIT 2013),* 8-10 May, 2013, Amman, Jordan, pp.1-8.

[21] Khiabani, H. Sidek, Z. and Manan, J. (2009). A Study of Trust and Privacy Models in Pervasive Computing Approach to Trusted Computing Platforms. In proceedings of the International Conference for Technical Postgraduates (TECHPOS '09), PP, 1–5, Kuala Lumpur, Malaysia, December 2009.

[22] Ko, S. Lee, J. and Kim, S. (2012). Mobile Cloud Computing Security Considerations. Journal of Security Engineering, Vol. 9(2), PP, 143-150.

[23] Kovachev, D. Cao, Y. and Klamma, R. (2010). Mobile Cloud Computing: A Comparison of Application Models. Journal of Arxiv preprint arXiv: 1107.4940.

[24] Kumar, S. (2004).Mobile communications: global trends in the 21st century. International Journal of Mobile Communications, Vol. 2(1), PP, 67-86.

[25] Laurila, J. Perez, G. Aad, I. Blom, O. Do, T. Dousse, O. Eberle, J. &Miettinen, M. (2012). The Mobile Data Challenge: Big Data for Mobile Computing Research. In Pervasive Computing (No.EPFL-CONF-192489).

[26] Lyle, J and Martin, A. (2010). Trusted Computing and Provenance: Better Together. In TaPP'10: Proceedings of the second USENIX Workshop on Theory and Practice of Provenance. 2010: San Jose, CA, USA.

[27] Mal-Sarkar, T &Bhunia, S. (2010). Collaborative Trust: A Novel Paradigm of Trusted Mobile Computing. arXiv preprint arXiv:1010.2447.

[28] Mavridis, I. and Pangalos, G. (2002).Security Issues in a Mobile Computing Paradigm.

[29] Nixon, P. Wagella, W. English, C. and Terzis, S. (2004). Security, Privacy and Trust Issues in Smart Environments: Technology, Protocols and Applications. Wiley, London, UK, pp. 220-240. ISBN 978-0-471-54448-7

[30] Poppa, D. Boudaoud, K. CremenE, M. and Borda, M. (2013).Overview on Mobile Cloud Computing Security Issues.RoEduNet 11th International Conference: Networking in Education and Research, Sinaia, Romania, January 17- 19, 2013.

[31] Ro, W. (2012).Report of Basic Principles for Increasing Security in a Mobile Computing Program. HTC Media Relations, htcpr@waggeneredstrom.com

[32] Robb, C. (2009). Security at the Edge — Protecting Mobile Computing Devices. NASCIO: Representing Chief Information Officers of the States.

[33] Sanaei, Z. Abolfazli, S. Gani, A. &Khokhar, R. (2012).Tripod of Requirements in Horizontal Heterogeneous Mobile Cloud Computing.arXiv preprint arXiv:1205.3247.I*nternational Conference on Computing, Information Systems and Communications.*

[34] Santos, N. (2013). Improving Trust in Cloud, Enterprise, and Mobile Computing Platforms, (Doctoral dissertation, Saarbrücken, Universität des Saarlandes, Diss., 2013).

[35] Satyanarayanan, M. Bahl, P. Caceres, R. and Davies, N. (2009).The Case for VM-Based Cloudlets in Mobile Computing.Pervasive Computing, IEEE, Vol. 8(4), PP, 14-23.

[36] Seigneur, J. (2005).Trust, Security and Privacy in Global Computing.Trinity College Dublin PhD thesis, technical report TCD-CS-2006-02. Retrieved from https://www.cs.tcd.ie/publications/tech-reports/reports.06/TCD-CS-2006-02.pdf

[37] Sinjilawi, Y., AL-Nabhan, M. & Abu-Shanab, E. (2014). Addressing Security and Privacy Issues in Cloud Computing. Journal of Emerging Technologies in Web Intelligence, Vol. 6(2), May 2014, pp. 192-199.

[38] Surie, A, Perrig, A. Satyanarayanan, M. and Farber, D. (2007).Rapid Trust Establishment for Pervasive Personal Computing. IEEE Pervasive Computing, Vol. 6(4), PP, 24-30.

[39] Surie, A. (2007). Improving Mobile Infrastructure for Pervasive Personal Computing (No.CMU-CS-07-163).Carnegie-

mellonunivpittsburgh pa school of computer science.

[40] Syme,R. (2009). Privacy of a mobile phone user in a rapidly evolving technological framework. Research Report, School of Mathematical and Geospatial Sciences, RMIT University.

[41] Valacich, J. (2003). Ubiquitous Trust: Evolving Trust into Ubiquitous Computing Environments.Presented at Workshop on Ubiquitous Computing Environments, Washington State University.

[42] Winslett, M. Yu, T. Seamons, K. Hess, A. Jacobson, J. Jarvis, R. Smith, B. and Yu, L. (2001). Negotiating Trust on the Web.In: IEEE Internet Computing, Vol. 6(6), PP, 30-37.

[43] Wu, X, (2013).Research on Light-weight Trust Management Approach in Mobile Computing Environments. Journal of Communications, Vol. 8(12), PP, 877-882.

[44] Yan, A., Md-Nor, K., Abu-Shanab, E. &Sutanonpaiboon, J. (2009).Factors that Affect Mobile Telephone Users to Use Mobile Payment Solution, Int. Journal of Economics and Management, Vol. 3(1), pp. 37-49.

[45] Yan, Z. (2007). Trust Management for Mobile Computing Platforms. (Doctoral dissertation).Helsinki Univ.Of Technology, Helsinki, Finland.

[46] Zhang, C. Seifert, J. and Zhong, H. (2009). Secure Mobile Payment via Trusted Computing.In Proceedings of APTC 08 of third Asia-Pacific Trusted Infrastructure Technologies Conference, PP, 98-100.