VOL 1 (2017) NO 4

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

A Security Perspective on Adoption and Migration to Mobile Cloud Technology

Mohammad Bin Ghudayyer [#], Yasir Javed [*], Mamdouh Alenezi [#]

[#] *CCIS, Prince Sultan University, Riyadh, KSA.*

[*] *Network Security Research Group, FIT, UNIMAS, Sarawak, Malaysia*

E-mail: mohammad.alghudayyer@oracle.com, yjaved@psu.edu.sa, malenezi@psu.edu.sa

Abstract— **Security is one of the main concerns of those who want to adopt and migrate to cloud computing technology. Security issues raised by cloud technology reveals that mobile cloud computing is raising the privacy and security issues such as identification and authentication issue, as sometimes the identity and the authentication of the owner of the device or the owner of the data contained in the cloud was not strictly remote. These are some examples that could be considered as major setbacks to the mobile cloud computing adaptation and the reason why some entities are still reluctant of embracing, adopting and migrating to this technology. This research reviews the phenomenon of mobile cloud computing, and the security and privacy issues intrinsic within the area of mobile application and cloud computing with more emphasis on the security and privacy considerations to embrace and migrate to Mobile Cloud Computing.**

Keywords— **Security, Mobile Cloud Technology**

I. Introduction

Nowadays, the market of mobile phones is increasing at a very high pace. International Data Corporation (IDC) report shows that 44% of the world's population around 3.2 billion people, will have access to the Internet in 2016. While more than 2 billion will be using mobile devices to access the internet with $32 billion is calculated to be spent on cloud IT infrastructure per year. This accounts for 33% of the total IT infrastructure spending. In 2019 cloud infrastructure spending is expected to reach $52 billion, which is considered as 45% of the total IT expenditure (IDC 2015). Along with the explosive increase of mobile applications and the emergence and needs of cloud computing phenomenon, the concept of mobile cloud computing has been launched to be the likelihood technology for mobile devices and services, according to (Krishnan, 2017) and when the servers of such application want to migrate to cloud structure, the main concern would be security that is often heard in news.

Mobile Cloud Computing (MCC) incorporates the cloud-computing concept into the mobile milieu or environment and overcomes the issues linked to the environment and performance. Regardless of the incredible evolution and significant benefits realized by Mobile Cloud Computing, its mobile users are still unsatisfied, due to the related privacy and security risks (Gasparis, 2017). These threats are playing an important role in discouraging organizations and single users to adopt and migrate to Mobile Cloud Computing milieu and environment. According to data from IDC, Saudi Arabia remains one of the top spenders on IT services in the Middle East and Africa region. In 2014, cloud services investment in the country totalled $50.4m and is estimated to reach $77.4m in 2015. A survey conducted by "Dun & Bradstreet" has revealed the Saudi public sector is increasing use of "cloud computing", during the forum entitled "Reshaping Information Technology Future Features" held recently in Jeddah, Saudi Arabia. The survey provided expectations for a rise in spending on information technology in transformative industries sector in the Kingdom at a CAGR of 7.5 percent from 2013 to 2018, according to a report issued by "IDC". The kingdom would prefer that public cloud is managed in the region at least, not overseas to overcome security and privacy issues. Much of this growth is driven by spending on public cloud services such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The types of cloud computing technology can be viewed from two different ways. The first way is based on access and the second way based on capability. Mobile Cloud Computing (MCC) has emerged from two hot tendencies, cloud and mobility. MCC brings many advantages to the devices; advantages that result to the development of rich operational applications. Nevertheless, while this technology presents several advantages and enables mobile users to have access to reliable and powerful computing applications and resources anytime and anywhere, there is a need to consider some noteworthy issues that its presents, namely privacy and security issues. This research primarily discusses the security of mobile cloud computing. This study will, therefore enable to eradicate the doubt and the concerns that stop users at all levels to adopt and migrate to this technology.

MCC or even the cloud computing technology CC is a new pattern in the IT sector and has prominently changed the way information technology is delivered and utilized. Therefore, relying on these facts, there has been little research work that has been carried out in this field. The present research will be conducted in the surroundings of Public sector, financial services Industry in Saudi.

II. Literature Review

Cloud Computing (CC) has been fostering itself as an evolving and emerging technology in the world of Information Technology (IT), which offers a new approach model for companies and individuals to use of software, hardware resources, and applications. MCC provides the mobile users a platform to allow them to use cloud services on their mobile devices. Regardless of the amazing emergence and evolution realized by mobile cloud computing, its users are still below expectations due to the linked risks, mainly mobile privacy and security that are becoming increasingly important. These risks had significantly stopped organizations to embrace mobile cloud computing environment (Jones, Irani & Sivarajah, 2017). Mollah, Azad & Vasilakos (2017) have presented a general overview of mobile cloud security architecture. Gupta, Gupta & Chaudhary (2017), evaluated the mobile browser security and figured out the attacks mostly in form of cross-site scripting, they provided a framework for cloud based browser security. Gupta & Gupta (2017) showed that almost all applications are vulnerable to security threats. The authors found out that PhP and Java based applications account for most threats. Amrutkar, Traynor & Van (2012) evaluated mobile browsers security and conclude that most of the browsers are subjected to Man-in-the-Middle attack. It presented an approach to prove user location identification is easy by using timing attack, which is sniffing, on the user browser cache. Hosmer, Jeffcoat, Davis & McGibbon (2011) that showed the similar results of attacking user browser cache to collect critical information about history, proposed a similar approach. Dinh, Niyato & Wang (2013) has proposed a framework together with a survey and explained MCC. It presented all existing proposed solutions with details to how to secure mobile cloud infrastructure and also identified all the possible issues in mobile cloud computing. In addition, the authors proposed a new framework for mobile cloud computing. The proposed framework is mainly focused on trust, risk management and routing security that will enhance the working of mobile and ad-hoc networks. Jouini, & Rabai (2016) presented an evaluator framework for detection of cloud related security threats. They used mean cost failure analysis considering multiple parameters and did quantitative analysis for detection of threats. De (2016) and Alizadeh, Hassan, Behboodian & Karamizadeh (2013) in the research they come up with a definition for mobile cloud computing which is a mixture of cloud computing and mobile web; which is the most well-known instrument for mobile users to have access to different services and applications offered on the cloud thru the Internet. Many surveys and researches of potential cloud advocates show that security and privacy are the main and number one concern deferring its adoption to migrate to this technology (Abolfazli, Sanaei, Ahmed, Gani & Buyya, 2011). There is a huge number of obstacles existing in the field of MCC, including information replication, availability, scalability, security, integration, and business continuity of cloud resources because of lack of cloud infrastructure standard. According to the survey that conducted by Subashini & Kavitha (2011), 74% of IT Executives and Chief Information Officers are not encouraged to migrate their existing technology to be on top of cloud because of the associated risks especially security and privacy. Several researchers are demonstrating their interest in this new technology; nevertheless, there are several challenges and issues in MCC because of several restrictions or limitations of the mobile devices in the like of restricted storage capacities, limited bandwidth and low battery power, and the like. Yet, security is the major issue in MCC. In order to establish and maintain the trust of consumers in the mobile platform. Yang, Pan & Shen (2010), have argued that this can only be achieved by the protection of their application and data from adversary; and he proposed a 3G E-commerce platform that combines the advantages of both 3G network and cloud computing to increase data processing speed and security level. This platform uses an encryption-based access control PKI (public key infrastructure) to ensure the privacy of user's access to the outsourced data.

Security for mobile users

The mobile devices in the like of smartphones, cellular phones, and personal digital assistants are exposed to several security menaces such as malicious codes (in the like of Trojan horses, worm and virus) and their vulnerability and weaknesses. Additionally, with mobile devices incorporated global positioning system (GPS) equipment, they can generate security issues for users (Fernando, Loke & Rahayu, 2013). Two main issues or challenges are as follow:

Security for mobile applications

The security of application model or mobile application is quite important because these applications offer a better service to clients by using cloud resources; these mobile applications utilize the services of the cloud to augment the ability of a mobile equipment. The installation and the functioning of security software in the like of AVG, Kaspersky and McAfee antivirus software on mobile phones are the easiest ways to identify security menaces on the devices, such as malicious codes, worms, and virus. Nevertheless, mobile phones or devices are inhibited in their power and processing, consequently, protecting effectively from the menaces and security threats is harder compare to resourceful devices in the like of laptops. For instance, it is quite impossible to keep functioning the virus discovery software on mobile phones and devices. Dai & Zhou, (2010) proposed an approach to shift or move the menace detection abilities to clouds. This approach is an expansion of the current Cloud Anti-Virus (CAV) platform that offers an in-cloud service for virus detection.

Securing Data on Clouds

The major challenge in utilizing MCC is protecting the data of the mobile subscriber stored within the mobile cloud. The file or data of a mobile client is very important and sensitive, and need to be secured adequately since any unauthorized individual or intruder can do changes in it to affect the data or corrupt the data. Consequently, the major concern of cloud service providers is to offer the security of file or data created and managed on a cloud server or mobile device. The file or data security is quite important and essential for the proprietor of the file or data, because they can contain some sensitive and confidential information of the mobile user (Khan, Kiah, Khan & Madani, 2013). However, both the application developers and the mobile users take advantage from storing a significant amount of data and applications on a cloud, they have to be mindful of dealing with applications and data regarding their authentication, digital rights and integrity (Morrow, 2012). Consequently, the data linked concerns in mobile cloud computing are as follow:

a. Integrity

Sometimes mobile users show concerns regarding their data integrity within the cloud. Many solutions are available to overcome these concerns (Wang, Li, Owens & Bhargava 2009). Nevertheless, these solutions do take into account the energy consumption of mobile users. Itani, Kayssi & Chehab (2011), have taken into consideration the energy consumption; their paradigm includes three major elements: a cloud storage service, a mobile client and a trusted third party. The paradigm executes three stages: initialization, update, and verification. In the prime stage, files (Fx) that require being transferred to the cloud will be charged with a message authentication code (MACFx). These messages authentication will be locally stored, while the files will be transferred and stored in the cloud. For the update stage, a case when a mobile user desires to input the data into the file is considered. In this case, the cloud sends the file to this specific user. In the meantime, the cloud also sends a demand to the trusted crypto coprocessor (TCC) to yield (MAC'Fx). TCC then directs (MAC'Fx) to the user to check (Fx) by contrasting it with (MACFx). In the case everything is adequately verified, the user can input or delete data. Finally, the user or mobile client can demand the integrity checking of a file, whole file system or collection of files stored in the cloud. This stage begins when the mobile client sends a demand to check the integrity of files on the TCC; then TCC retrieves the files that require being verified from the cloud and yields (MAC'Fx) to send to the mobile user. The user only contrasts the received (MAC'Fx) and (MACFx) that are stored within its device to check the integrity of these files. This scheme does not only check the integrity of data but additionally saves energy and the bandwidth for the network communication. The reason is that verification and checking are processed within TCC and the user just operates a simple code for contrasting. The outcome demonstrates that this solution can spare up to 90 percent processing requirements, consequently saving considerable energy for a mobile device.

b. Authentication

Chow et.al. (2010) have presented an authentication approach utilizing cloud computing to protect the data access adequate for mobile environments. This approach mixes according to Song et.al. (2009) TrustCube and hidden authentication to validate the mobile users. TrustCube is cloud authentication platform policy based that uses the open standards and it accepts the integration of diverse authentication approaches and techniques. The authors construct a hidden authentication system utilizing mobile data, such as SMS, calling logs, website accesses, location and messages, for existing mobile setting. The system demands input restrictions that make it hard for mobile clients to utilize hard passwords. As an outcome, this sometimes results in the utilization of short and simple passwords. In the case where a web server gets a demand from a mobile user, the web server reorients the demand to the integrated authenticated (IA) service with the details of the demand. The IA then retrieves the policy for the access demand, excerpts the information that requires to be gathered, and send an inquest to the IA server via a dedicated trusted network connect (TNC) protocol. The IA server gets the inquest, yields a report and directs it back to the IA service. Following that, the IA service implements the authentication norm in the policy, identifies the authentication outcome (whether or not the user is authenticated for the access inquest successfully), and transfers the authentication outcome back to the web server.

Intrusion detection and prevention

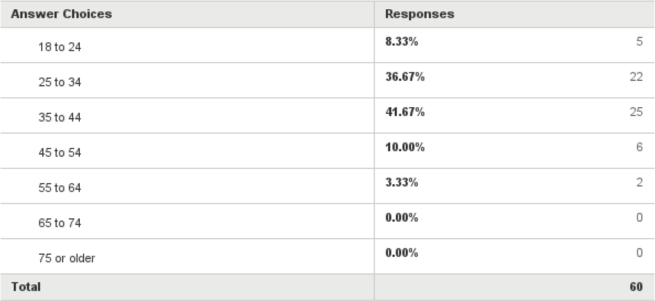
Mobile devices' growing popularity entices intruders in intruding to these platforms by taking advantage diverse weaknesses of mobile devices, such as malware and mobile network security weaknesses. For example, mobile device security survey conducted by Catteddu & Hogben (2009), revealed that Trojans utilized for robbing confidential information that are talked via mobile devices by taking advantage and using voice recognition algorithms. There are many networks based and on-device intrusion detection and answer techniques already suggested in the literature to tackle mobile device security issues (Taylor, Young, Kumar & Macaulay, 2011), (Takabi, Joshi & Ahn, 2010). Most of them suggested on-device solutions were not adequate because of their large limitations such as computational resources, battery power and memory capacity. In addition to that, most of the suggested solutions detect misbehaving users or malwares relying on the signatures that they acquired from a central database but having small storageto keep signatures. Moreover, signatures linked detection could be evaded with ease by launching zero-day threats. Network related solutions tackle the resource restrictions of on-device solutions, but because of the lack of feedback and knowledge from the mobile device's inner behavior, their performance and accuracy are intensively impacted. The much-needed stage after detecting and attack is an automated response to the attack and a recovery of the former state, which is not tackled by neither of the previously suggested network related nor on-device solutions (Brunette & Mogull 2009).

III. Methodology

This research is mainly based on the deductive research approach, as the results will be about verifying or measuring the relationship between the existing variables or theories; and to prove that the existing theories developed within the literature review are in line with the results and findings of the research. In addition to that, in the recommendation part the research will embrace the inductive approach, as some new orientations will be given to result in new theories of realities. In this research, different questions and potential solutions are discussed with different stakeholders such as (Mobile end users, IT Specialist and Companies) during the research, to enhance both the researchers and the mobile cloud providers' knowledge in the field. In addition to that, the research will adopt qualitative and quantitative approach; as the data collected will be quantified and they will also be qualitative in nature. This research will adopt survey as data collection instrument and precisely survey through a questionnaire of some respondents as it permits to collect data regarding situations, practices or phenomenon at one point of time through interviews or questionnaires. For the purpose of this research, 59 individuals will constitute the sample size, and they will all be selected among the students and personnel, which have a background in IT and are located in Saudi Arabia.

IV. Results and Findings

There was a total of 60 individuals who took part in the survey, and based on the table above, out of the 60, 51 were male and the remaining 8 were female.



Answer Choices	Responses	
18 to 24	8.33%	5
25 to 34	36.67%	22
35 to 44	41.67%	25
45 to 54	10.00%	6
55 to 64	3.33%	2
65 to 74	0.00%	0
75 or older	0.00%	0
Total		60

Fig.1 Showing the age of participants

Out of the 60 respondents, 8.33% were aged from 18 to 24 years old; 36.67% were aged from 25 to 34 years old; 41.67% were aged from 35 to 44 years old; 10% were aged from 54 to 54 years old; and only 3.33% were aged from 55 to 64 years old.

Knowledge of Mobile Cloud Computer

Familiarity with the term mobile cloud computing

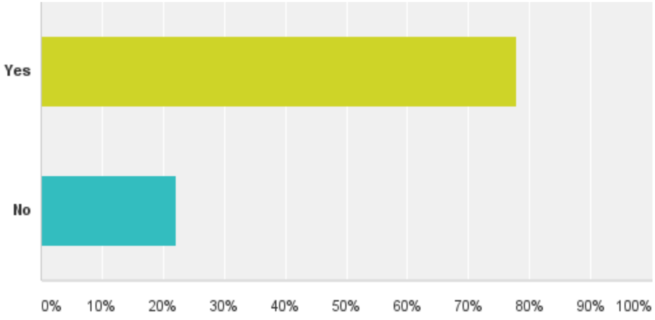


Fig. 1 Shows the participants' familiarity with the Mobile Cloud Computing

Most of the respondents 77.97% of the questionnaires were familiar with the concept of mobile cloud computing as most of them where individuals with IT backgrounds; so this new IT concept was well known for most of them, and known from the rest. The vast majority of the respondents had a positive point of view regarding mobile cloud computing, as most of them agreed that this technology has revolutionized the technology area for mobile devices; as this concept was making the use of mobile devices easy and granting the access to a wide range of data and information contained in the cloud. The respondents revealed that, mobile cloud computing offers to mobile users with the storage services and data processing in clouds. There is no need for the mobile devices to have a powerful configuration such as central processor unit speed and huge memory capacity; considering the fact that all the sophisticated computing tasks can be executed in the clouds, and not on the mobile, where the efficacy of this concept.

Storing sensitive information/documents on mobile cloud apps

Regarding the storing sensitive information/documents on mobile cloud apps, the vast majority of the respondents either agreed (31.03% of the respondents), Neutral (29.31% of the respondents) or totally agree (20.69%) that their storing sensitive information/document on mobile cloud apps, while only 10.34% and 8.62% did not encounter such fate.

Information about Sensitive and Secure Data

The vast majority of the respondent revealed that can't guarantee that their information stored on the cloud is nor secure; 39% of the respondents disagree 22% totally disagreed. 17% agree and 5% Totally agree of the respondents believed that data stored in cloud is secure, and the remaining 17% were neutral.

Table I. Showing People perception about Sensitive information on Cloud and Should be keep information secure

	Can you store Sensitive Information on Cloud	Can you Guarantee that information on Cloud is secure	Personal Data Should be Kept Confidential
Totally Disagree	10	22	0
Disagree	9	39	2
Neutral	29	17	11
Agree	31	17	19
Totally Agree	21	5	68

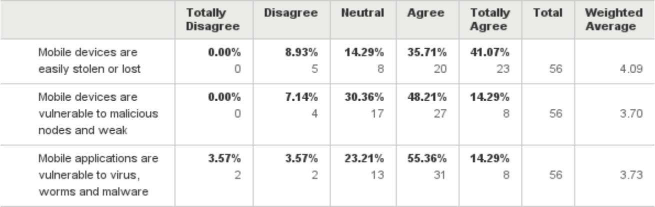
Out of the 60 respondents, (68%) of respondent totally agreed and agreed (19%) that personal data should be kept confidential and secret in the cloud; they were denouncing the fact that there is a lack of privacy in data on the cloud; only (2%) disagreed and (11%) were neutral.

Security Challenges

Security challenges of mobile cloud computing

The common security challenges that the respondents have risen regarding mobile cloud computing and devices associated are; the loss or stolen of the mobile device, the vulnerability of the mobile devices to malicious threats, the vulnerability to the mobile applications to worms, virus and the like

Table II: Showing perception about mobile devices whether they are security vulnerable



	Totally Disagree	Disagree	Neutral	Agree	Totally Agree	Total	Weighted Average
Mobile devices are easily stolen or lost	0.00% 0	8.93% 5	14.29% 8	35.71% 20	41.07% 23	56	4.09
Mobile devices are vulnerable to malicious nodes and weak	0.00% 0	7.14% 4	30.36% 17	48.21% 27	14.29% 8	56	3.70
Mobile applications are vulnerable to virus, worms and malware	3.57% 2	3.57% 2	23.21% 13	55.36% 31	14.29% 8	56	3.73

Table II shows answers collected from the respondents, the mobile devices are easily stolen or lost, as 23% of the respondents totally agreed and 46% agreed that the mobile device is either stolen or lost on a frequent basic and mainly among the female respondents. Only 12% disagreed with that, while the remaining 19% were neutral. The intrusion of malicious nodes is another security breach that the mobiles devices are exposed to on the cloud, as 14% of the respondents totally agreed and 48% agreed on the fact that they have been victims of malicious nodes on the mobile cloud and the remaining 14% were skeptic on this aspect. The mobile applications downloaded on the cloud have been recognized as vulnerable to virus, worms and Trojan horses by the majority of the participants to the survey, as 15% totally agreed and 57% agreed, so 4% of them were for the fact that the security of applications was threatened by worms, virus, and Trojan horses; 24% were neutral and 4% disagreed.

Some solutions Considered by participants

You believe that solutions could be implemented to overcome security and privacy issues in mobile cloud computing.

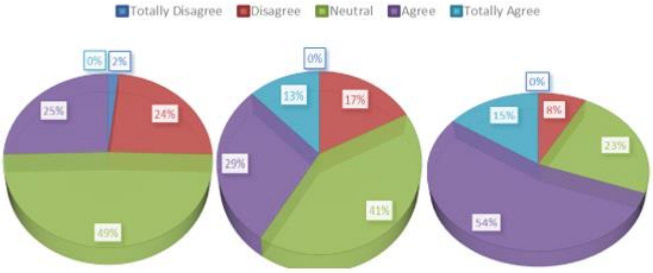


Fig. 3 (A) You Believe That Solutions Could Be Implemented To Overcome Security And Privacy Issues In Mobile Cloud Computing. (B) Mobile Security Software Such As AVG And Kaspersky Could Solve Security Threats (C) Mobile Users Should Have Unique Access In Their Data In Mobile Cloud Computing

Figure 3 (a) shows a chart above, 25% of the respondents asserted that there is a need for solutions to meet the privacy and security issues in mobile cloud computing, as they believe that these were among the factors that were still refraining people to embrace this new concept. Only 24% disagreed and 49% were neutral. (b) Based on the data collected from the participants of the survey, 29% agreed on the fact that mobile security software in the like of Kaspersky and AVG could be used to solve the security threats in mobile cloud computing. 17% of the respondents did not see in that software the solutions for the security issues in mobile cloud computing and 41% of them were neutral. (c) 54% agreed and 15% totally agreed of the respondents asserted that there should be a unique access to their data in mobile cloud computing, so that third parties should not have access to these data and therefore, keep the privacy to the data confidential. 8% of the respondents disagreed as they believed that some data which are not sensitive could be accessed by third parties, and 23% were neutral.

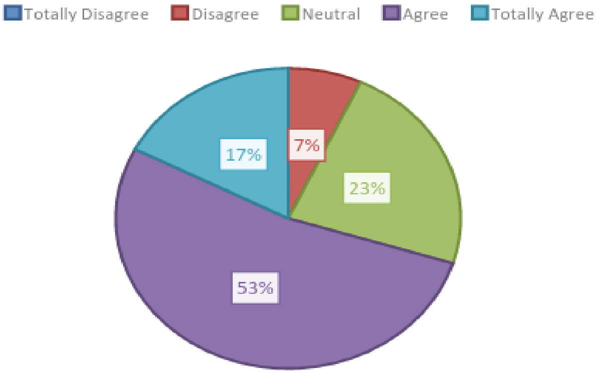


Fig. 4 Shows Bio information could be used to grant access to data or mobile device such as fingerprint or voice tone.

Figure 4 shows 53% of the respondents agreed and 17% totally agreed that the use of bio information cloud be used to control the access to data or mobile device, considering the fact that this information, such as fingerprints are unique to each user and therefore could not be copied or duplicated by another person. This appears to them as an effective way to control the access to data.

Mobile application developers

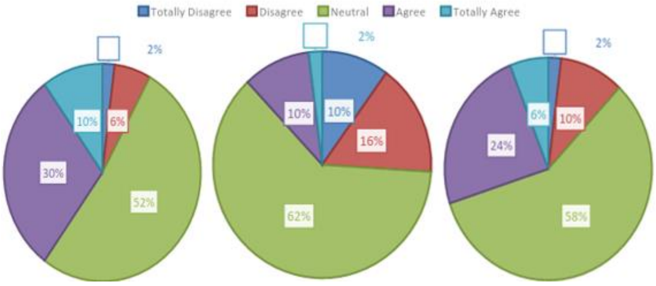


Fig. 5 (a) showing the result of "Do the apps you or your outside agency develops follow best practices for security?" (b) Showing the result of" Do you have visibility into the security of the mobile devices impacting your organization?" (c) Showing the result for the question "Is mobile security testing built into your app development lifecycle?"

Figure 5(a) shows that out of the 60 respondents, (30%) of respondent agreed and (10%) Totally agreed that they are following best practices when they develop a new app. While 6% disagree and 2% totally disagree that they are not following best practices when they develop a new application. 52% were Neutral. Figure 5(b) the respondent revealed that they do a visibility into the security of the mobile devices impacting their organization 10% agreed and 2% totally agreed. Only 10% totally disagree and 16% disagree that they don't have a visibility into the security of the mobile devices impacting their organization were 62% Neutral. Figure 5(c) the question revealed that security testing is at very low scale

Only 24% agree and 6% Totally agree that they do have a security testing built in during development lifecycle while 10% disagree and 2% totally disagree that they don't have while 58% were Natural.

V. Discussions

The respondents of the selected groups, which were all IT experts, provided some interesting answers that have significantly contributed to the completion of the present research. Though the concept of MCC is quite new, they were all familiar with this technology. They all agreed or revealed that MCC was just an extension, utilization, or access to the cloud computing services through mobile devices. The main difference between cloud computing and mobile cloud computing is the mobility of the user and the device that is used to have access to the services or applications from the cloud. The respondents revealed that mobile cloud computing was raising the following privacy and security issues: identification and authentication issue, as sometimes the identity and the authentication of the owner of the device or the owner of the data contained in the cloud was not strictly remoted. In the same line, they have also raised the access control issue; implying that there should be a way to regulate or to control who access what and ensure that people only access to services, data and applications for which they are eligible or for which they are owners. It was also recommended that users must have privacy in their access to the cloud, and access to content should be only that belong to them in order to keep their confidentiality and secrecy and in the meantime ensure that the data they load into the cloud is protected and cannot be accessed by any other entity. As for what they believe could be the solutions to some of the raised security and privacy challenges in mobile cloud computing, and to ensure that this technology is widely embraced and adopted, they have suggested some solutions, such as the use of antivirus for mobile devices in order to hamper the intrusion of viruses and malware in the mobile device. They have also suggested the implementation of personal recognition to have access to the cloud and to data, with encryption keys.

VI. Conclusion

This research has mainly elaborated on the security of data stored in the cloud and the significance of data security. Whilst mobile cloud computing has the considerable potential to allow the mobile servers to have access to reliable and powerful resources and applications anytime and anywhere, one must take into consideration many challenges comprising security and privacy, and also reliability in implementing mobile cloud computing. We have identified singular privacy and security issues of mobile cloud computing and have discussed the diverse mechanisms to tackle these issues. This research has elaborated a number of ways to provide data security, access control, confidentiality as well as the integrity of data and mobile users, so that great number of mobile users in the future could widely adopt mobile cloud computing. Finally, the researcher will provide some research areas and the aspects that future studies need to tackle to improve the popularity and acceptance of mobile cloud computing and its environment.

When discussing mobile cloud security threats, the primary concern is threats to smartphones and tablet platforms. These threats can be divided into three categories:

- Physical threats
- Threats to mobile network security
- The threat of malware

One recommendation is each service providers must take in consideration to implement a solution that maximizes the security in order to protect end-users' information by implementing the evaluation scheme for analysis of security and data analysis. Then doing the prevention using encryption and key control while there should be a mechanism for detection to perform these two options.

References

[1] IDC 2015 International Data Corporation, report 2015 available at http://www.idc.com/research/Predictions15/index.jsp

[2] Krishnan, R. (2017). Security and Privacy in Cloud Computing.

[3] Gasparis, I. (2017). Ensuring Users' Privacy and Security on Mobile Devices(Doctoral dissertation, University of California, Riverside).

[4] Jones, S., Irani, Z., Sivarajah, U., & Love, P. E. (2017). Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. Information Systems Frontiers, 1-24.

[5] Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications.

[6] Gupta, B. B., Gupta, S., & Chaudhary, P. (2017). Enhancing the Browser-Side Context-Aware Sanitization of Suspicious HTML5 Code for Halting the DOM-Based XSS Vulnerabilities in Cloud. International Journal of Cloud Applications and Computing (IJCAC), 7(1), 1-31.

[7] Gupta, S., & Gupta, B. B. (2017). Detection, Avoidance, and Attack Pattern Mechanisms in Modern Web Application Vulnerabilities: Present and Future Challenges. International Journal of Cloud Applications and Computing (IJCAC), 7(3), 1-43.

[8] Amrutkar, C., Traynor, P., & Van Oorschot, P. C. (2012, September). Measuring SSL indicators on mobile browsers: Extended life, or end of the road?. In International Conference on Information Security (pp. 86-103). Springer, Berlin, Heidelberg.

[9] Hosmer, C., Jeffcoat, C., Davis, M., & McGibbon, T. (2011). Use of mobile technology for information collection and dissemination. Data & Analysis Center for Software, 77.

[10] 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.

[11] Jouini, M., & Rabai, L. B. A. (2016). A Security Framework for Secure Cloud Computing Environments. International Journal of Cloud Applications and Computing (IJCAC), 6(3), 32-44.

[12] De, D. (2016). Mobile cloud computing: architectures, algorithms and applications. CRC Press.

[13] Alizadeh, M., Hassan, W. H., Behboodian, N., & Karamizadeh, S. (2013). A brief review of mobile cloud computing opportunities. Research Notes in Information Science, 12, 155-160.

[14] Abolfazli, S., Sanaei, Z., Ahmed, E., Gani, A., & Buyya, R. (2014). Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. IEEE Communications Surveys & Tutorials, 16(1), 337-368.

[15] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[16] Yang, X., Pan, T., & Shen, J. (2010, July). On 3G mobile e-commerce platform based on cloud computing. In Ubi-media Computing (U-Media), 2010 3rd IEEE International Conference on (pp. 198-201). IEEE.

[17] Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. Future generation computer systems, 29(1), 84-106.

[18] Dai, J., & Zhou, Q. (2010, May). A PKI-based mechanism for secure and efficient access to outsourced data. In Networking and Digital Society (ICNDS), 2010 2nd International Conference on (Vol. 1, pp. 640-643). IEEE.

[19] Khan, A. N., Kiah, M. M., Khan, S. U., & Madani, S. A. (2013). Towards secure mobile cloud computing: A survey. Future Generation Computer Systems, 29(5), 1278-1299.

[20] Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. Network Security, 2012(12), 5-8.

[21] Wang, W., Li, Z., Owens, R., & Bhargava, B. (2009, November). Secure and efficient access to outsourced data. In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 55-66). Acm.

[22] Itani, W., Kayssi, A., & Chehab, A. (2010, December). Energy-efficient incremental integrity for securing storage in mobile cloud computing. In Energy Aware Computing (ICEAC), 2010 International Conference on (pp. 1-2). IEEE.

[23] Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E., & Song, Z. (2010, October). Authentication in the clouds: a framework and its application to mobile users. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop (pp. 1-6). ACM.

[24] Song, Z., Molina, J., Lee, S., Lee, H., Kotani, S., & Masuoka, R. (2009). Trustcube: An infrastructure that builds trust in client. In Future of Trust in Computing (pp. 68-79). Vieweg+ Teubner.

[25] Catteddu, D., & Hogben, G. (2009). Cloud computing. Benefits, Risks and Recommendations for Information Security/European Network and Information Security Agency, ENISA (November 2009).

[26] Taylor, S., Young, A., Kumar, N., & Macaulay, J. (2011). The mobile cloud: When two explosive markets collide. Cisco Internet Business Solutions Group Tech. Rep.

[27] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.

[28] Brunette, G., & Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing v2. 1. Cloud Security Alliance, 1-76.