

Investigating Security Technology Requirements for Mobile Cloud Computing Applications/Services Users.

Ibrahim, M. & Ibrahim, M.I.

Jigawa State Institute of Information Technology
Kazaure, Jigawa State, Nigeria
ibrahimmuktar26@yahoo.com, Ibrahimq7@gmail.com
08065334410, 08137167587

ABSTRACT

Mobile Cloud Computing as a term was introduced not long after the emergence of Cloud Computing model in 2007, and the term Cloud Computing exists when tasks and data are kept on the internet instead on individual mobile devices. This paper investigates mobile device user's security technology requirements for mobile cloud computing applications and services; for the purpose of protecting their personal information, business information and messages from various attacks or unauthorized access. This is because companies and individual user's information are stored in service provider's servers and information security is the most important issues in any system that needs to be properly secured.

Keywords: Mobile Device, Mobile Cloud Computing, Cloud Computing, Email/Mobile Devices Encryption.

Aims Research Journal Reference Format:

Ibrahim, M. & Ibrahim, M.I. (2015): Investigating Security Technology Requirements for Mobile Cloud Computing Applications/Services Users. *Advances in Multidisciplinary Research Journal*. Vol 1, No. 2 Pp 115-122

1. BACKGROUND TO THE STUDY

The success of modern technologies is highly dependent on its standardization, user-interface simplicity, and its ease of use by end users /customers, and most importantly its level of information security and control (Ramgovind S, Eloff MM, Smith E., 2010). Mobile devices are now in such scale that can easily fit in our pockets and can connect us to varieties of information sources, and enable communication nearly everywhere we go. Nowadays, current mobile devices have all the functionalities of a standard computer and are being used by almost everyone on the planet (Pragya Gupta, and Sudha Gupta, 2012). In addition Mobile devices have changed from simple device that enabled voice calls communication only such as calling or sending text messages communication a few years back to smart devices with value added services such as browsing or accessing internet, receiving or sending emails, storing and/or retrieving documents anytime, anywhere. As a result of this, not only phone numbers and addresses are stored in the mobile devices but also sensitive financial information and business information that must to be kept privately are also stored (Aman Jain, and Shilpa Mehta., 2013).

Mobile Cloud Computing was introduced after Cloud Computing. In brief, Cloud Computing is a technique which provides services and data to the users or customers on demand basis through the web. The data is stored at service provider's servers rather than individual devices. In mobile cloud computing, the issue of data/information security is of primary important. This is because the information and data have become one of organization's greatest assets. The information and data that have been used by individual's mobile device over the cloud are stored in services provider's premises which make the information highly unsecured (Rajesh et al., 2012).

2. STATEMENT OF PROBLEM

The most recent technology in the IT world has now been the potential growth of Mobile Cloud Computing. As mentioned earlier, the security is the main challenge and problem associated with both mainstream cloud computing and Mobile Cloud Computing. Securing data, such as business information, personal information or messages in Mobile Cloud Computing have become more important nowadays, this is because of the increasing usage of mobile devices with internet (A. Cecil Donald, S. Arul Oli, L. Arockiam, 2013). besides, the major problem in implementing successful cloud computing or mobile cloud computing technology is managing the connectivity, performance and security (Ali Newaz Bahar, Md. Ahsan Habib, and Md. Manowarul Islam, 2013).

In addition, most of the applications that run on mobile devices store user's information on service providers premises which raised a concern in user's mind that their private or confidential business information can be use without their permission. Lastly companies are still worried about security issues when using cloud computing applications or services. Users are also worried about the vulnerability to attacks, when information and critical IT resources are outside the firewall (M. Rajendra Prasad, Jayadev Gyani, P.R.K. Murti, 2012).

3. OBJECTIVE

The main objective of the research is to investigate the security requirements for mobile cloud computing applications and services users which they prefer to have in their mobile devices and cloud computing applications. This is because the major problem area for mobile cloud computing is in securing the users data or business information, which is stored in cloud service providers servers.

The research intends to cover security requirement areas such as: Mobile devices security, Data and information security, Network security and applications security. Based on our findings, we aim to give suggestions on which security requirements are much needed by mobile device users. Since user's data can be store in mobile devices or in the cloud server, which can be accessed by applications running on the mobile device or in the cloud thereby disseminating information between series of different computing devices over a network. As such, user's personal information is in the process exposed to different security risks (D. Popa, K. Boudaoud, M. Cremene, M. Borda, 2013).

4. METHODOLOGY

4.1 The Research Design

Research methods are the various procedures, techniques and algorithms that are used for conducting Research Project. In other words, all the methods or techniques that can be used by the researchers during a research project operation. Research methodology is the way to systematically solve the research problem by logically adopting various steps. It is a science of studying how research is done scientifically. In addition, it defines the way data is collected in a research project (S. Rajasekar, P. Philominathan, and V. Chinnathambi, 2013). In order to achieve all the objectives of the research; Mixed method approach was adopted. In mixed methods Project or Research, both qualitative and quantitative data are collected and analyzed. Creswell, (2003) and Ivankova et al., (2006), defined mixed methods, as a process or procedure for collecting, analyzing, and mixing or integrating both quantitative and qualitative data in many stages of the research process within a single study for the purpose of gaining a better understanding of the research problem.

In addition, the main idea of using mixed methods approach is that the use of quantitative and qualitative data approach in combination provides a better understanding of research problems than either approach alone (Creswell, 2006). Quantitative research methods will be used to quantify the findings, survey questionnaire will also be use to obtain the statistical data for analysis as it is more objective and number based which makes it reliable and valid. Followed by qualitative research methods that will be use to collect non statistical information that will support the quantitative data analysis.

5. DATA PRESENTATION

The students, Lecturers and IT staff of Jigawa State Institute of Information Technology Kazaure, Jigawa State College of Education Gumel and Hussaini Adamu Federal Polytechnic Kazaure form the Sample population of the research. As mentioned earlier, both quantitative and qualitative data will be analyzed, to obtain the desired results on investigating security requirements for mobile cloud computing users. After successful completion of questionnaires and interviews, the data collected from questionnaires, interviews and secondary sources were summarized according to the research themes. Moreover, data obtained from respondents were analyzed to make sure all invalid as well as inaccurate questionnaires are removed by looking at the way questions are answered. This is because data analysis is extremely important in every research. Besides, Data analysis has great advantage which allows us to be more accurate in our interpretations of the data obtained. Data analysis sometimes seems very difficult, but it is a vital component in research project.

6. DISCUSSION OF FINDINGS

Figure 1: Questions Number (4) of the survey asked the respondents to indicate the type of their mobile device they are currently using. The aim of this question is to justify the types of mobile devices being used for mobile cloud computing applications and services. The figure below shows the result of the finding:

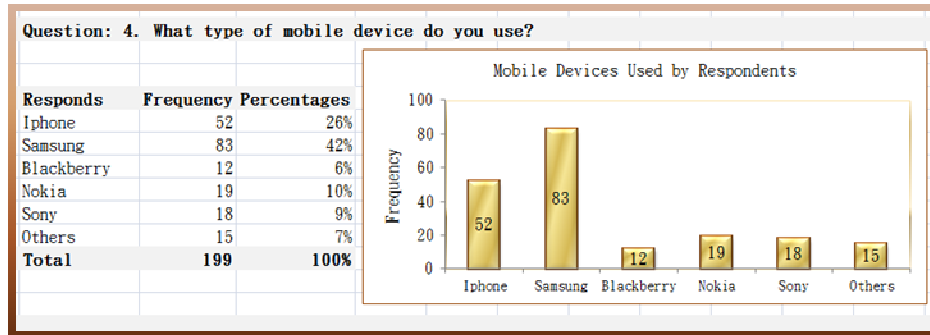


Figure 1: Respondents Mobile Devices

The results indicated that “Samsung” takes the highest percentage with 42% of the respondents, followed by “Iphone” with 26%, “Nokia” with 10%, “Sony” with 9%, while “Others” with 7%, and also “Blackberry” with only 6% respectively. From the stated results, majority of the respondents are using “Samsung” mobile devices among others.

Figure 2: In this regard, respondents were asked about the usage of cloud computing applications and/or services in their organizations. The main target of the question is to find out whether respondents are using cloud computing applications and/or services. The figure below shows the results of the findings.

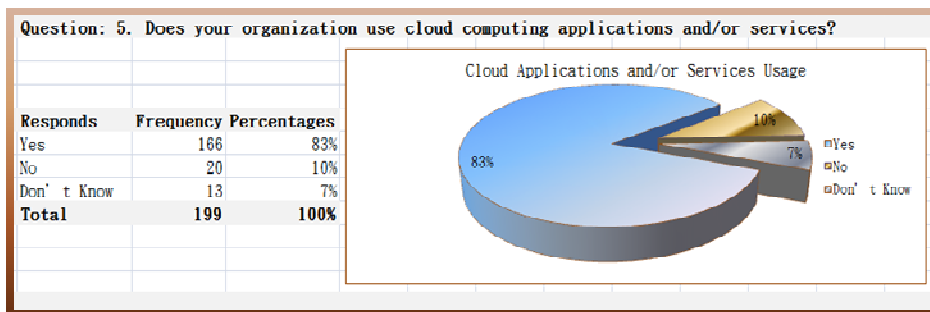


Figure 2: Cloud Computing Applications and/or Services Usage

The above data analysis shows that, 83% of the respondents indicated “Yes”, followed by 10% with “No”, and the remaining 7% “Don't Know”. This means that, the majority of the respondents' organizations are currently using cloud computing applications and/or services with (83%). Figure 3, Question number (6) of the survey asked the respondents to indicate the kind of activities they are performing with their mobile devices. The purpose of the question is to find whether the respondents are using mobile cloud computing applications. The figure below interprets the results:-

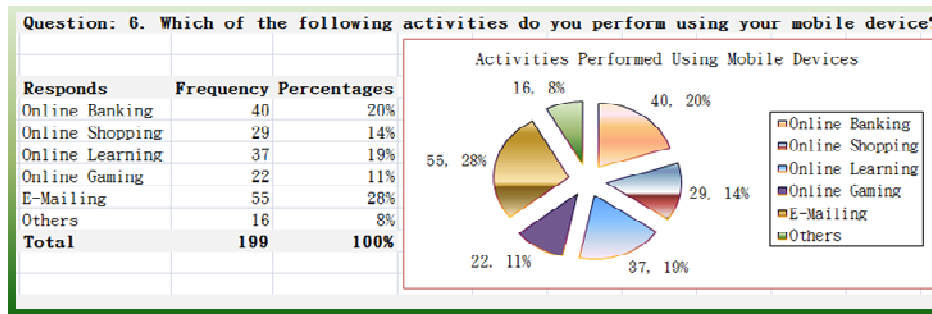


Figure 3: Activities Performed Using Mobile Device

The above result proved that, 28% of the respondents indicated “E - Mailing” as the major activities they are performing with their mobile devices, 20% indicated “Online Banking”, followed closely by 19% with “Online Learning”. Then 14% are performing “Online Shopping”, 11% with “Online Gaming”, and only 8% with “Others”. The result proved that, the majority of the respondents indicated “E-Mailing” as their major activities with their mobile devices.

Figure 4: Question Number 7 of the survey asked the respondents to indicate the cloud computing service they are currently using. The purpose of the question is to find whether all respondents of the sample population are using cloud computing applications or services. The response of this question is represented in the figure below.

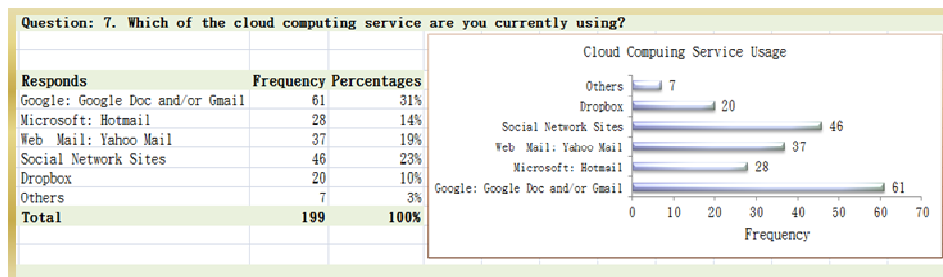


Figure 4: Cloud Computing Services Usage

As shown above, the result indicated that, 100% of the respondents of the sample population are currently using varieties of cloud computing applications and services. Out of the population, 31% are currently using “Google: Google Doc and/or Gmail”, 23% are using “Social Network Sites”, 19% are using “Web Mail: Yahoo Mail”, and 14% are using “Microsoft: Hotmail”, and then 10% of the respondents indicated “Dropbox” and only 3% indicated “Others” cloud computing services.

Figure 5: The respondents were asked to indicate their main concerns associated to mobile cloud computing applications/services. The objective of the question is to find whether the respondents has a major concern associated to mobile cloud computing applications. As shown in the figure below:-

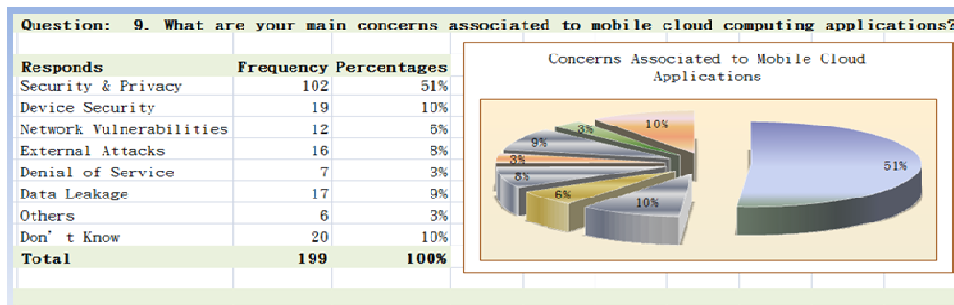


Figure 5: Concerns Associated to Mobile Cloud Applications

From the result, 51% of the respondents indicated that “Security & Privacy” is their main concerns, which is the highest majority, 10% indicated “Devices Security” as their concerns, followed by another 10% with “Don’t Know” and 9% opined “Data Leakage”. Then 8% Indicated “External Attacks” and 6% indicated “Network Vulnerabilities”, 3% indicated “Denial of Service”, followed by another 3% with “Other” opinions. The result clearly proved that majority of them considered “Security & Privacy” as their main concern.

Figure 6: This question asked the respondent to indicate or rank the most important based on their opinion between Data Security, Network Security and Applications Security. The purpose of the question is to find out which one that needs to be more secured in mobile cloud computing environment. As it is shown below, 57% among them indicated “Data Security”, then 25% indicated “Network Security”, while 11% indicated “Applications Security” and only 7% with “Don’t Know” as their opinion. The findings proves that majority of them with (57%) indicated “Data Security” is the most important.

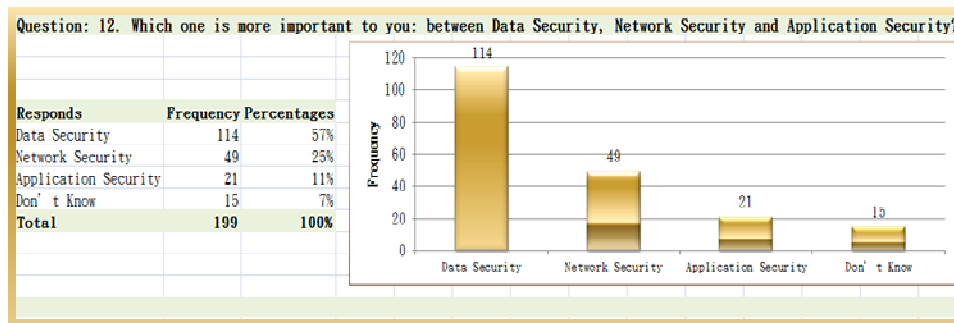


Figure 6: Data, Network and Application Security

Figure 7: Respondents here were asked to indicate their satisfaction with the security provision by the cloud service providers. The purpose of the question is to find out whether the respondents are satisfied with the security provision by their service providers. As shown in figure below, 47% of the respondents are in a “Neutral” position, whereas 25% are “Satisfied”, and 16% are “Unsatisfied”, followed by 7% with “Very Satisfied” opinion. But 5% of them indicated “Very Unsatisfied”. From the result analysis, it is clearly proves that “Neutral”, takes the highest percentage with (47%) of the respondents.

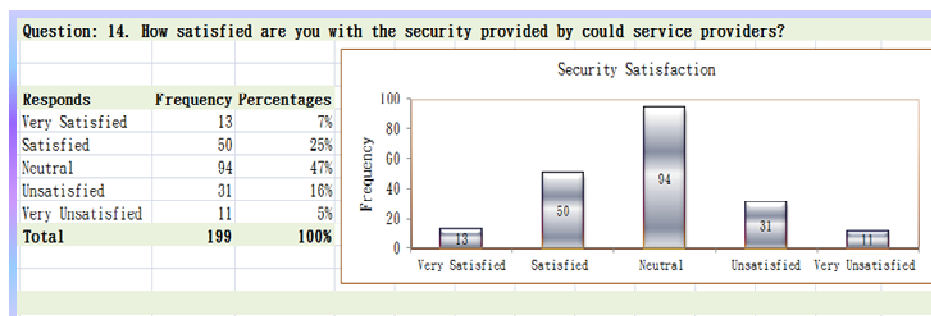


Figure 7: Cloud Service Security Satisfaction

Figure 8: Respondents were asked to indicate what type of security technology they prefer to use “in mobile cloud computing environment” now or in future. The objective of the question is to find out the security technology, that the users prefer to be using in order to protect their information. The figure below shows that, 38% of the respondents prefer to use “Mobile Device Encryption”, whereas 30% preferred “E-Mail Encryption”, and 13% preferred “Multi Factor Authentication”. Another 13% indicated “Network Monitoring”, 4% clearly indicated “Don’t Know”, whereas 2% indicated “Other” opinions. The results show that, the most preferred technology is “Mobile Device Encryption” followed by “E-Mail Encryption” in mobile cloud computing environment.

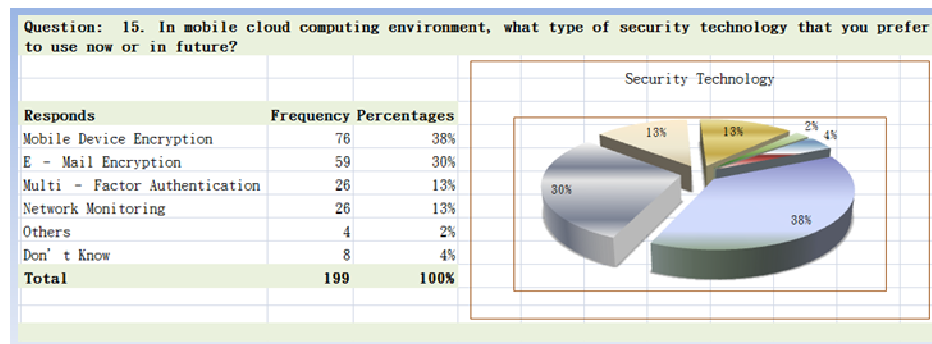


Figure 8: Security Technology

Figure 9: In this part, the respondents were asked to rank “Encryption” in mobile cloud computing based on their opinion, with multiple options provided. The objective of the question is to find out how important “Encryption” is, in mobile cloud computing environment. From the result, 44% of the respondents indicated “Encryption” as “Important” to them, 37% indicated “Very Important”, whereas 10% indicated “Not Very Important”. Then 8% indicated “Don’t Know” but only 1% indicated “Not Important At All”. It can be concluded that, majority of the respondents (44%) considered “Encryption” as important in mobile cloud computing environment.

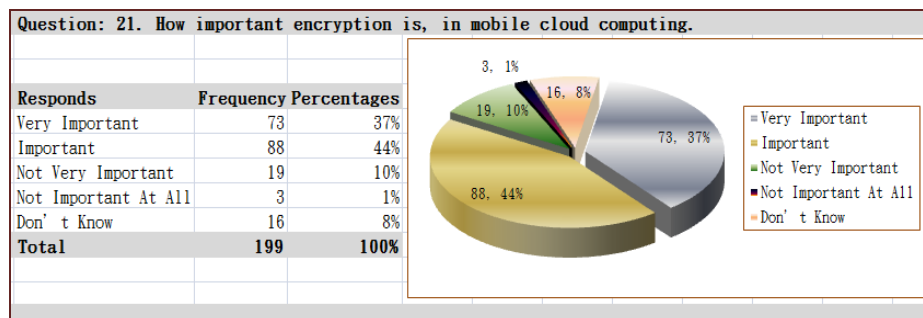


Figure 9: Important of Encryption

7. CONCLUDING REMARKS

The general conclusion is about security technology requirement and user’s main concern associated to mobile cloud computing applications security. The conclusion in this section was presented in short, but can only properly be understood in combination with the information presented in the previous parts of the research. On the security technology requirements of mobile cloud computing applications, the users prefer to use encryption technology, such as mobile device encryption and email encryption. With regard to the user’s main concern associated to mobile cloud computing applications/services, the majority considered security and privacy as their main concern related to mobile cloud computing applications/services.

8. CONTRIBUTIONS TO KNOWLEDGE

Based on the review of the related literature, findings and analysis presented in this paper, the following recommendations were suggested to the cloud services providers, mobile devices companies and mobile applications developers.

- It is from the purpose and significant of this study to investigate the concern of the mobile device users, therefore it is recommended that Security and privacy confirmation statements should always be displayed to the users while using mobile cloud computing applications for them to be satisfied, this is because, in the findings of this research, it has been proved that, Mobile Cloud Computing applications users are worried and unsatisfied with the security and privacy of their data stored in the services provider’s premises.
- In addition, it is part of the significance of this work, as a results of it is findings, Mobile devices companies should come up with encryption technology in their new products, in such a way that, data will be more secured from the hand of unauthorized users, because it has been proved from the findings that, mobile

devices users are more interested in using new security technology, such as mobile device encryption and email encryption.

- Mobile applications developers should develop another application that can support all types of encryption technology for both sides' users.
- Another significance derived from this study is that mobile device users preferred to use email services among others, therefore, Cloud computing applications and services providers should add more security to upgrade their security services, this is because, users preferred email applications service than the other services.

9. FUTURE RESEARCH

This research has only achieved in investigating the required security technology by mobile devices users, and also proved that majority preferred to use Encryption security technology. Therefore, the future research we would consider this findings and come up with the prototype of this technology in mobile cloud computing application and services.

REFERENCES

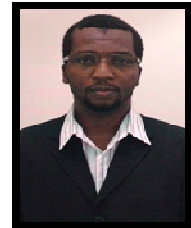
1. Pragma Gupta, Sudha Gupta, (2012), Mobile Cloud Computing: The Future of Cloud, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 1, Issue 3, September 2012 , ISSN 2278 – 8875, http://www.ijareeie.com/upload/september/4_Mobile%20Cloud%20Computing.pdf, [Accessed Date: 27 – December – 2013].
2. D. Popa, K. Boudaoud, M. Cremene, M. Borda, (2013), Overview on Mobile Cloud Computing Security Issues. http://shannon.etc.upt.ro/bulletin/2013/vol58_72_1/pdf/58_1_4.pdf, [Accessed Date: 22 – January – 2014].
3. Ali Newaz Bahar, Md. Ahsan Habib, and Md. Manowarul Islam, (2013), Security Architecture for Mobile Cloud Computing, International Journal of Scientific Knowledge Computing and Information Technology, July 2013. Vol. 3, No.3 ISSN 2305-1493. http://www.ijsk.org/uploads/3/1/1/7/3117743/2_mobile_cloud_computing.pdf, [Accessed Date: 24 – December – 2013].
4. Aman Jain and Shilpa Mehta, (2013), International Journal of Emerging Trends in Electrical and Electronics (IJETEE) Vol. 1, Issue. 3, March-2013., Mobile Devices and Social Networking Security Solution, <http://iieee.co.in/Docs/Volume%201/Issue3/16%20Mobile%20Devices%20and%20Social%20Networking%20Security%20Solution.pdf>, [Accessed: 20 – December - 2013].
5. A. Cecil Donald, S. Arul Oli, L. Arockiam, (2013), Mobile Cloud Security Issues and Challenges: A Perspective, International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013, ISSN: 2277-3754, http://ijeit.com/Vol%203/Issue%201/IJEIT1412201307_73.pdf, [Accessed Date: 24 – January - 2013].
6. Ramgovind S, Elof MM, Smith E., (2010), The Management of Security in Cloud Computing, <http://umkn-dsp01.unisa.ac.za/xmlui/bitstream/handle/10500/3883/ramgovind.pdf?sequence=1>, [Accessed Date: 24 – October - 2013].
7. M.Rajendra Prasad, Jayadev Gyani, P.R.K.Murti, (2012), Mobile Cloud Computing: Implications and Challenges, Journal of Information Engineering and Applications , ISSN 2224-5782 (print) ISSN 2225-0506 (online), Vol 2, No.7, 2012, <http://iiste.org/Journals/index.php/JIEA/article/viewFile/2571/2587>, [Accessed Date: 12 – February - 2013].
8. Rajesh et al, (2012), An Overview and Study of Security Issues & Challenges in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012 ISSN: 2277 128X, http://www.ijarcsse.com/docs/papers/9_September2012/Volume_2_issue_9/V2I900174.pdf, [Accessed Date: 30 – December – 2013].
9. Ivankova et al., (2006), Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice, *Field Methods*, Vol. 18, No. 1, February 2006 3–20, DOI: 10.1177/1525822X05282260 http://wtgrantmixedmethods.com/sites/default/files/literature/Ivankova%20etal_2006_mixed%20methods%20sequential%20design.pdf, [Accessed date: 21 – May – 2014].
10. S. Rajasekar, P. Philominathan, and V. Chinnathambi, (2013), Research Methodology, <http://arxiv.org/pdf/physics/0601009.pdf>, [Accessed date: 28 – June – 2014].

11. Creswell, J. W. (2003) Research design: Quantitative, qualitative, and mixed method approaches, Thousand Oaks, CA, Sage Publications, [Accessed date: 07 – May – 2014].
12. Creswell, (2006), Understanding Mixed Methods Research, http://www.sagepub.com/upm-data/10981_Chapter_1.pdf, [Accessed date: 06 – May - 2014].

Authors' Profiles



Engr. Ibrahim, M.I obtained his B.Sc. in Computing and Software Engineering from Oxford Brookes University in 2007, M.Sc. Mobile & Satellite Communications from Bradford University in 2009, his research interest areas are emerging mobile technologies multimedia services, data mining and machine learning in healthcare industry.



Ibrahim Muktar was born on 3rd October, 1985 in Gagarawa, Jigawa State. He studied at the Informatics Institute Singapore, graduated with a B.Sc (Hons) in Business Computing and Information Technology (2005 - 2008). He obtained a Master Degree in Information Technology in (2014) at the SEGi University Malaysia. His research areas includes cloud computing, mobile wireless security technologies.
