International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Special Issue No. 01, September 2015
www.ijates.com
ijates
ISSN 2348 - 7550

MOBILE CLOUD COMPUTING: A REVIEW OF ARCHITECTURE, APPLICATIONS, PRIVACY AND SECURITY ISSUES

Usman Isah Rabiu[1] , Vivek Dimri[2] , Aliyu Ashiru[3]

[1, 2, 3] *Department of Computer Science and Engineering, Sharda University (India)*

ABSTRACT

Mobile Cloud Computing has emerged as a promising technology and its application is expected to expand its features in storing personal health information, e-governance and others. Although data security and privacy have been the major concern to the users. These issues originated from the fact that the cloud is a semi-trusted environment and the sensitive information stored in the cloud can be accessed by any unauthorized person. Thus, new methods and models are needed to solve the problem of privacy and security of data owner.

In this paper, we attempt to address the concern of privacy and security of data owner. A survey is carried on existing models of security and the models were assessed on their security and privacy impact

This paper is divided into five sections where by section I introduces the topic mobile cloud computing, section II explains the architecture of mobile cloud computing, section III discusses the applications of mobile cloud computing while section IV takes a review on proposed models that deals with security and user privacy in mobile cloud computing, finally section V gives the conclusion.

Keywords: Authentication, Encryption, Mobile Cloud Computing, Privacy, Security,

I. INTRODUCTION

Mobile cloud computing is emerging technology. The number of mobile cloud computing subscribers is grown rapidly in last five years and it's going to extend multiple times in future years. According to the latest study & Research, Cloud based mobile market will generate annual revenue of $9.5 billion in 2014 from $400 million in 2009, at an average annual increase of 88%.It appears that in the near future, there will be more growth for both traditional, device-based apps and mobile cloud-based apps.[16]

Mobile devices (e.g., smartphone, tablet pcs, etc.) are increasingly becoming an essential part of human life as the most effective and convenient communication tools not bounded by time and place. Mobile users accumulate rich experience of various services from mobile applications (e.g., iPhone apps, Google apps, etc.), which run on the devices and/or on remote servers via wireless networks. The rapid progress of mobile computing (MC) becomes a powerful trend in the development of IT as well as commerce and industry fields. However, the mobile devices are facing many challenges in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., mobility and security) [1]

The limited resources significantly impede the improvement of service qualities. Cloud computing (CC) has been widely recognized as the next generation's computing infrastructure. CC offers some advantages by

allowing users to use infrastructure (e.g., servers, networks, and storages), platforms (e.g., middleware services and OS), and software's (e.g., application programs) provided by cloud providers (e.g., Google, Amazon, and Salesforce) at low cost. [1]

The Mobile Cloud Computing Forum defines MCC as follows [2]:

"Mobile Cloud Computing at its simplest, refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smartphone users but a much broader range of mobile subscribers"

Buyya et al also describe MCC as "Is a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle". [3]

II. MOBILE CLOUD COMPUTING ARCHITECTURE

From the concept of MCC, the general architecture of MCC can be shown in Fig.1. Below.

In Fig.1. Mobile devices are connected to the mobile networks via base stations (e.g., base transceiver station (BTS), access point, or satellite) that establish and control the connections (air links) and functional interfaces between the networks and mobile devices. Mobile users' requests and information (e.g., ID and location) are transmitted to the central processors that are connected to servers providing mobile network services. Here, mobile network operators can provide services to mobile users as AAA (for authentication, authorization, and accounting) based on the home agent (HA) and subscribers' data stored in databases. After that, the subscribers' requests are delivered to a cloud through the Internet. In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services. These services are developed with the concepts of utility computing, virtualization, and service-oriented architecture (e.g. web, application, and database servers). [1]

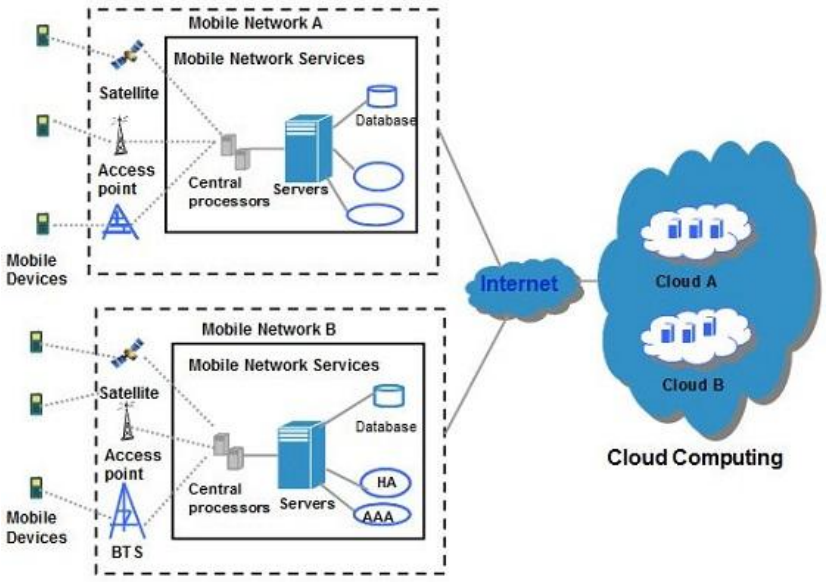

Fig. 1. Mobile Cloud Computing (MCC) Architecture

III. MOBILE CLOUD COMPUTING APPLICATIONS

3.1 Mobile Commerce

Mobile devices are being used extensively in business and commerce for a wide range of purpose. [13] Mobile commerce (m-commerce) is a business model for commerce using mobile devices. The m-commerce applications generally fulfil some tasks that require mobility (e.g., mobile transactions and payments, mobile messaging, and mobile ticketing). The m-commerce applications can be classified into a few classes including finance, advertising and shopping. The m-commerce applications have to face various challenges (e.g., low network bandwidth, high complexity of mobile device configurations, and security). Therefore, m-commerce applications are integrated into cloud computing environment to address these issues.[1]

3.3 Mobile Learning

Mobile learning (m-learning) is designed based on electronic learning (e-learning) and mobility. However, traditional m-learning applications have restrictions in terms of high cost of devices and network, low network transmission rate, and limited educational resources [8]. Cloud-based m-learning applications are introduced to solve these restrictions. For example, utilizing a cloud with the high storage capacity and powerful processing ability, the applications provide learners with much richer services in terms of data (information) size, better processing speed, and long lasting battery life.

[1] Presents benefits of combining m-learning and cloud computing to enhance the communication quality between students and teachers. In this case, a smartphone software based on the open source JavaME UI framework and Jaber for clients is used.

3.4 Mobile Healthcare

The intention of applying MCC in medical applications is to minimize the limitations of traditional medical treatment (e.g., small physical storage, security and privacy, and medical errors [1]). m-healthcare provides mobile users with convenient helps to access resources (e.g., patient health records) easily and quickly. Besides, m-healthcare offers hospitals and healthcare organizations a variety of on-demand services on clouds rather than owning standalone applications on local servers. There are a few schemes of MCC applications in healthcare. For example, [4] presents five main mobile healthcare applications in the pervasive environment.

i. Comprehensive health monitoring services enable patients to be monitored at anytime and anywhere through broadband wireless communications.
ii. Intelligent emergency management system can manage and coordinate the fleet of emergency vehicles effectively and in time when receiving calls from accidents or incidents.
iii. Health-aware mobile devices detect pulse-rate, blood pressure, and level of alcohol to alert healthcare emergency system.
iv. Pervasive access to healthcare information allows patients or healthcare providers to access the current and past medical information.
v. Pervasive lifestyle incentive management can be used to pay healthcare expenses and manage other related charges automatically.

3.5 Mobile Gaming

Mobile game (m-game) is a potential market generating revenues for service providers. M-game can completely offload game engine requiring large computing resource (e.g., graphic rendering) to the server in the cloud, and gamers only interact with the screen interface on their devices.[1]

3.6 Other Applications

A cloud becomes a useful tool to help mobile users share photos and video clips efficiently and tag their friends in popular social networks as Twitter and Facebook. MeLog is an MCC application that enables mobile users to share real-time experience (e.g., travel, shopping, and event) over clouds through an automatic blogging [1]. The mobile users (e.g., travellers) are supported by several cloud services such as guiding their trip, showing maps, recording itinerary, and storing images and video.

IV. MOBILE CLOUD COMPUTING PRIVACY AND SECURITY ISSUES

One of the key concerns for people about using a mobile cloud is that their personal data on mobile device could be stored on, or accessed by the cloud. A mobile device contains contact lists, text messages, personal photos and videos, calendars, location information, and these data can reveal many things about someone's personal life. However

With the rapid adoption of mobile computing, and immediate connection to cloud computing, the CSA established the Top Threats to Mobile Computing research discipline, in addition to the current Top Threats to Cloud Computing

"Personally owned mobile devices are increasingly being used to access employers' systems and cloud-hosted data, both via browser-based and native mobile applications. This without a doubt is a tremendous concern for enterprises worldwide, "said John Yeoh, Research Analyst for the Cloud Security Alliance. "The results of this research will play an important role as we set out to develop much needed guidance on where time, talent and money should be placed when it comes to addressing mobile security threats." [15]

i. Data loss from lost, stolen or decommissioned devices
ii. Information-stealing mobile malware
iii. Data loss and data leakage through poorly written third-party applications
iv. Vulnerabilities within devices, OS, design and third-party applications. Insecure Wi-Fi network or rogue access points
v. Insecure Wi-Fi, network access and rogue access points.
vi. Insecure or rogue marketplaces
vii. Insufficient management tools, capabilities and access to APIs (includes personas).
viii. NFC and proximity-based hacking.

The security concern for the mobile devices make the issues of security and privacy of great concern, as such several models for secure mobile cloud computing were developed

[7] Here files are encrypted with DES algorithm in which keys are generated randomly by the system. Two servers, means distributed server concepts are used here for ensuring high security. In this model also El Gamal algorithm is used for secured communication between the users and the companies' servers. The advantage of

this model is the user data is secure from theft when transferred through the internet to the cloud and between cloud server and database server. The disadvantage is that the integrity and privacy of data can be tempered with in between the successive encryption and decryption

[8] Propose a method that combines the secure multiparty computation protocol of Goldreich et al. and the garbled circuit design of Beaver et al. with the cryptographically secure pseudorandom number generation method of Blum et al. User communicate with (N+2) servers to perform garble circuit and generate encryption key and data encryption. The system has high encryption strength but the technique can incur traffic overload and delay due to multiple connections.

[9] In this paper a new mechanism is proposed and implemented to authenticate mobile cloud computing by using fingerprint recognition as part of the security solution. Improving the mechanism of protecting access to the mobile cloud leads to improving the security. Cloud access can only be allowed when the data matched the stored data. The technique make access to user data secured as impersonation of user will be difficult. Although the technique add security to authentication the variation in time for image capturing and camera resolution can make access to legitimate users denied, also the captured image is stored together with the database which makes user data vulnerable to attacks.

[10] Uses biometric data such as image, encrypt the image using Malakooti algorithm and distribute the resulting image to many servers. This method encrypt user data with the biometric and the data can only be decrypted with that image. The advantage of this model is the access to user data will be difficult even if the database server is hacked as the encryption key is stored in different servers. But the disadvantage is the model will be costly and may incur delay as the image parts which is the key to decrypt the data are stored in different servers

[11] Propose a mobile-government (m-government) platform that will take into consideration of all security aspects in mobile cloud to be taken care of in the mobile device. The system will take into consideration of security and privacy of cloud user, considering limitations of mobile devices the propose model will be complex to implement.

[12] Propose two models thus mobile node model and centralized owner model, both models use IBE to encrypt user data and authenticate data sharing between data owner and mobile user, data owner provides access of cloud data to mobile client via proxy server without revealing its identity. The advantage of this model is able to secure the communication between data owner and mobile user, the trusted leader and data sharer to authenticate and protect the privacy of both the parties.

[13] Designed an archive mechanism that integrates cloud storage, hybrid cryptography, and digital signatures to provide security requirements for data storage of mobile phones. This model is able to protect the integrity of the data in the device and also the authenticity of origin of the data The model incur so much delay and computational overload at the stages of encryption while transferring large data.

The user privacy and security of data is of great concern as such there is a need to build models that are safe to be use by peoples and organizations knowing that their secrets are safe with the cloud service providers.

V. CONCLUSIONS

Mobile Cloud Computing has been integrated into daily life activities, the use of mobile devices to access corporate networks or clouds from remote location poses threat to the security of the network or cloud as mobile devices have so many limitations such as power, processing and storage that makes its security a major concern. This paper reviewed the mobile cloud computing environment through security and privacy of user data. From the papers surveyed it has been observed that so many security models have been put in place and research need to be carried to convert the current security challenges in the mobile cloud computing environment.

VI. ACKNOWLEDGMENT

We wishes to acknowledge the love and support of our parents may Allah reward them with best of his rewards. Our sincere appreciation goes to all the faculties in the department of Computer Science and Engineering, Sharda University. Special appreciation to our families, friends and colleagues that helps and support us in our daily activities and during this research.

REFERENCES

[1] Dinh, Hoang T., Chonho Lee, Dusit Niyato, and Ping Wang. "A survey of mobile cloud computing: architecture, applications, and approaches." Wireless communications and mobile computing 13, no. 18 (2013): 1587-1611.

[2] www.mobilecloudcomputingforum.com

[3] Sanaei, Zohreh, Saeid Abolfazli, Abdullah Gani, and Rajkumar Buyya. "Heterogeneity in mobile cloud computing: taxonomy and open challenges. “Communications Surveys & Tutorials, IEEE 16, no. 1 (2014): 369-392.

[4] Doukas, Charalampos, Thomas Pliakas, and Ilias Maglogiannis. "Mobile healthcare information management utilizing Cloud Computing and Android OS." In Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE, pp. 1037-1040. IEEE, 2010.

[5] Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. "A survey on security issues and solutions at different layers of Cloud computing." The Journal of Supercomputing 63, no. 2 (2013): 561-592.

[6] Suo, Hui, Zhuohua Liu, Jiafu Wan, and Keliang Zhou. "Security and privacy in mobile cloud computing." In Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International, pp. 655-659. IEEE, 2013.

[7] Kar, Tonny Shekha, MA Parvez Mahmud, Shahjadi Hisan Farjana, Kawser Wazed Nafi, and Bikash Chandra Karmokar. "A Newer Secure Communication, File Encryption and User Identification based Cloud Security Architecture."International Journal of Computer Applications 52, no. 4 (2012).

[8] Premnath, Sriram N., and Zygmunt J. Haas. "A Practical, Secure, and Verifiable Cloud Computing for Mobile Systems." Procedia Computer Science34 (2014): 474-483.

[9] Rassan, Iehab AL, and Hanan AlShaher. "Securing Mobile Cloud Computing Using Biometric Authentication (SMCBA)." In 2014 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 157-161. IEEE, 2014.

[10] Mhammad v. Malakooti, Nilafor Mansourzadeh, "A two level-security model for cloud computing based on the biometric features and multi-level encryption" The Proceedings of the International Conference on Digital Information Processing, Data Mining, and Wireless Communications, Dubai, UAE, 2015 pp. 100-112

[11] Singh, Teg. "Privacy & Security of Mobile Cloud Computing." Asian J. of Adv. Basic Sci 2, no. 3: 75-82.

[12] Mehrotra, Parul, and S. Venkatesan. "An efficient model for privacy and security in Mobile Cloud Computing." In Recent Trends in Information Technology (ICRTIT), 2014 International Conference on, pp. 1-6. IEEE, 2014.

[13] Rahimi, M. Reza, Jian Ren, Chi Harold Liu, Athanasios V. Vasilakos, and Nalini Venkatasubramanian. "Mobile cloud computing: A survey, state of art and future directions." Mobile Networks and Applications 19, no. 2 (2014): 133-143.

[14] Fernando, Niroshinie, Seng W. Loke, and Wenny Rahayu. "Mobile cloud computing: A survey." Future Generation Computer Systems 29, no. 1 (2013): 84-106.

[15] Data Loss from Missing Mobile Devices Ranks as Top Mobile Device Threat by Enterprises. (2012, October 4). Retrieved May 5, 2015, from https://cloudsecurityalliance.org/media/news/data-loss-mobile-ranks-top-threat-enterprises

[16] Amar, Deep Gorai , Birendra, Goswami "New Trends on Mobile Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 10,(2014) pp 291-300