International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - TeLMISR 2015, ISSN : 2348-2273
Available Online at www.ijeecse.com

# Mobile Cloud Computing - Challenges and Security Issues

Indu Sahu
Research Scholar, Mewar University, Rajasthan

***Abstract: Mobility has changed the way the world has been looking at mobile phones. Mobile phones have become smart and mobile applications more intelligent and complex. These applications require heavy computations, data mining, searching and multimedia processing. This is where Cloud services can help greatly by enhancing the computing capability of otherwise not so competent mobile devices. Mobile Cloud Computing is cloud computing extended by mobility and a new ad-hoc infrastructure based on mobile devices. The potential growth of mobile cloud computing seems to have taken the world by storm. In the current scenario security of data on the Mobile Cloud has become more important because of the increasing usage of mobile devices with internet. This paper therefore discusses the security issues involved in mobile cloud computing and the solutions that have been proposed till now.***

***Keywords: Mobile Cloud Computing, security, threats, architecture.***

## 1. INTRODUCTION

The hottest wave in the IT world these days is the potential growth of mobile cloud computing. Securing data in the Mobile Cloud has become more important in the recent days because of the increasing usage of mobile devices with internet. Nowadays, Smart phones are on the top of the invention list as they are built on a mobile OS, which is capable for advanced computing and faster in connectivity than ordinary mobile phones. Mobile cloud has the ability to change the life of both enterprise and users today. With the increase in usage, the threat of information /data being stolen from the mobile cloud has increased manifolds. We therefore, summarize all the possible security threats and available solutions in this paper.

This paper is organized as follows: Section II explains the basic concepts, Section III provides all the challenges and security issues. Section IV describes mobile security layers and related security issues. Section V discusses available solutions to the security problems discussed in section III and IV followed by conclusion and future scope (Section VI)

## II. MOBILE CLOUD AND ITS ARCHITECTURE

*1. Service Models in Cloud:* According to NIST [4], Cloud Computing services can be readily broken down into three layered service models. It is also known as the SPI model where SPI stands for Software, Platform and Infrastructure.

- Software as a Service [SaaS]
- Platform as a Service [PaaS]
- Infrastructure as a Service [IaaS]

*Software as a Service (SaaS):* This service is commonly used by business users. This service provides the complete applications to the user which is customizable within the limits. It is mainly used for achieving specific business task with the focus on end- user requirements.

*Platform as a Service (PaaS):* This service provides pre-built application components such as Application Programmable Interface (API). It is commonly used by developers and deployers for building the higher level applications. The developers create and deploy applications services for the users. It is not necessary to manage the OS and Databases manually.

*Infrastructure as a service (IaaS):* This service is mainly used by the system managers. The main advantage is that there is no need to purchase a server or manage physical data center equipment such as storage, networking, etc. Managers create platforms for service. Other than these service models, there are several service models such as *Business Process as a Service (BPaaS), Network as a Service (NaaS), Anything as a Service (XaaS), Disaster Recovery as a Service (DRaaS).*

2. *Mobile Cloud and Mobile Cloud Computing:* Mobile Cloud services can greatly enhance the computing capability of mobile devices. Mobile users can rely on the cloud to perform computationally intensive operations such as searching, data mining, and multimedia processing. In addition to providing traditional computation services, mobile cloud computing also enhances the operation of the ad hoc network itself by treating mobile devices as service nodes. Mobile Cloud Computing is defined as cloud computing extended by mobility and a new ad-hoc infrastructure based on mobile devices. This can be interpreted as an infrastructure where storage of data and its processing could happen somewhere outside of the mobile device, thus enabling not only powerful smart phones users, but a large number of less competent mobile phones equipped with internet, have access to a wide range of smart mobile applications.

Mobile Cloud Computing has integrated cloud computing into the mobile environment and therefore MCC has been able to prevail over the obstacles related to the performance of the mobile devices for e.g., its short battery life, limited storage space and bandwidth, and security for e.g., reliability and privacy that are there in mobile computing. Mobile devices access centralized applications over the wireless connection based on a web browser or a thin native client. Researchers have outlined that because all the complex computing is done in the cloud, mobile cloud computing does not need any powerful mobile configuration. [2]

*3. Mobile Cloud Computing Architecture:*

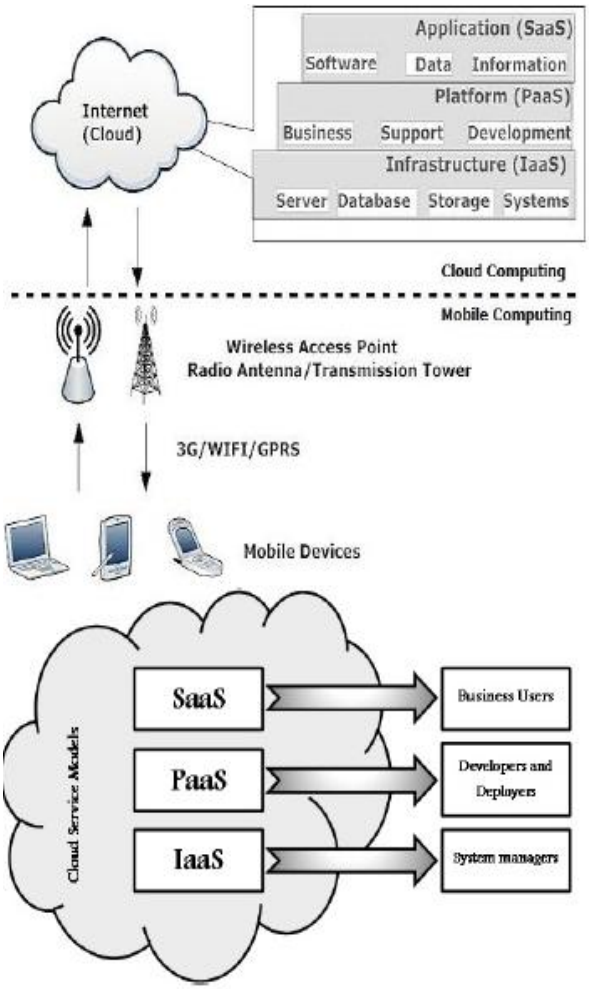


Figure 1: Mobile Cloud Computing Architecture [9]

The Figure 1[9] above shows the mobile cloud computing architecture. According to the figure, mobile cloud computing can be divided into cloud computing and mobile computing. The mobile devices used could be laptops, smart phones, or any other wireless device that is connected with a hotspot or a base station by 3G, Wi - Fi, or GPRS. Since the computing and major data processing phases are shifted to the 'cloud', every mobile device irrespective of its smartness is capable of accessing the cloud through the use of a cross-platform mid-ware. The service requests from the mobile devices are sent to the cloud through a web browser or desktop application. The management component of the cloud then allocates resources to the request for establishing a connection, while the monitoring and calculating functions of mobile cloud computing will be implemented to ensure the Quality of Service until the connection is completed. Authentication, Authorization and Accounting services may be provided to the users based on Home Agent and subscriber data that is stored in the databases. The subscriber requests are then delivered to a cloud through internet. These requests are processed by the cloud controllers present in the cloud in order to provide the desired service to the mobile users. These services are developed based on the concepts of utility computing, virtualization and service-oriented architecture [8]

## III. SECURITY ISSUES IN MOBILE CLOUD COMPUTING

Even as mobile cloud computing provides immense benefits, like, using cloud servers for data storage, platforms and software services, there are less than expected number of cloud users ,this can be attributed to the risk involved in terms of privacy and security of the data and services on the cloud. A survey conducted by a research firm Portio and published by another research firm Colt points that 68% of chief information officers (CIOs) have serious concerns about the security of cloud computing[3]

In MCC, a lot of investigations are being carried out to eradicate the issues to make it more reliable and secure because precious data are stored on the cloud. As the Internet-enabled mobile devices including smart phones and tablets continue to grow, web-based malicious threats will continue to increase in number.

1. *Mobile Security Service Layers:* The security services in mobile ecosystem are divided into three different layers.

- Backbone layer
- Infrastructure layer
- Application and Platform layer

The backbone layer constitutes the security surveillance on cloud physical systems. This helps in monitoring the servers and machines in the cloud infrastructure. The

infrastructure layer monitors the virtual machines in the cloud. Various activities such as Storage verification, VM migration, Cloud Service Monitoring, VM Isolation, Risk Evaluation and Audits are carried out in this layer to secure cloud host services. Application layer performs activities such as user management, key management, authentication, authorization; encryption and data integration. According to a recent survey, 73% of IT Executives and Chief Executive Officers are unwilling to adopt cloud services due to the associated risks with privacy and security. To attract consumers, the cloud service provider (CSP) has to target all the security issues to provide a highly secure environment.

2. *Security Issues and their Solutions:* Though there are several advantages in mobile cloud ecosystem, there are some issues and challenges in mobile cloud computing. Some of the major issues in security are Data Ownership, Privacy, Data Security and other Security issues. [6]

*2.1. Data Ownership:* Cloud computing facilitates storage of data and purchased digital media such as e-books, video and audio files, of the users, remotely. The users have a great risk of losing access to their purchased media data. For avoiding such risks, the user must be aware of the different rights regarding the purchased media. For a mobile device user security remains a major concern. All types of mobile devices are susceptible to a number of security threats like malicious codes for e.g., virus, worm, and Trojan horses. Important data may be compromised if a device is lost or stolen. Misuse of data lost from stolen/ misplaced devices can be avoided by wiping of mobile device remotely. This feature is generally provided by most of the mobile manufacturers and wireless carriers [12].

A lot many privacy issues can be raised by the Global Positioning System (GPS) of mobile devices. To detect security threats for e.g., virus, worms, and other malicious codes in the mobile devices, security software like Kaspersky, McAfee, and AVG antivirus programs may be installed and executed. However, due to the limitations of processing power and battery life in mobile devices, they are more susceptible to such threats compared to their wired counterparts eg desktop PC. It is therefore required that policies regarding access control, authentication procedures, account and user management, encryption, content assurance, and general communications security are developed and it is ensured that these policy measures are enforced[10]. It is very important that user privacy and data/application secrecy is provided to establish and maintain consumers' trust on the mobile platform. These threat detecting capabilities can be shifted to clouds. This paradigm is an extension of the existing Cloud AV platform that provides an in-cloud service for malware detection. This malware detection on the cloud enables us to use multiple antivirus engines in parallel by hosting them in virtualized containers. In this case we are also able to improve the improve malware detection and also the battery lifetime of the mobile device by almost 30%. Although it is a great advantage to store a voluminous of data and large applications on the cloud, but it is very important that we also take into consideration problems related to integrity of the data stored, user authentication problems and the digital rights of data/applications.[13]

*2.2. Privacy:* Privacy is one of the biggest challenges in the mobile cloud computing environment. Researchers have expressed that there are various policies being proposed which require rigorous controls and procedures to protect the privacy of individuals. Organizations that collect data/information must have some policies and procedures in order to handle, store, and dispose them securely and must be implemented to maintain the privacy. Risk of privacy exposure, identity theft and fraud can be reduced by implementing enhanced protection measures for sharing data in interconnected systems, implementing monitoring capabilities and protocols, and by educating users about proper social media safe-surfing. By establishing policies regarding use of social media and implementing processes to protect their infrastructures from unauthorized use of social media an organization can protect themselves from serious legal and security-related problems. Otherwise their information infrastructure and reputation both will be irreparably damaged [7].

For maintaining the integrity and confidentiality of information encryption is the most effective way. Encryption favors data storage and transport but it fundamentally prevents data processing. Therefore, initially it was quite useless to send encrypted data to cloud providers for processing. But this challenge has been met by homomorphic cryptography (HC) which ensures that operations performed on an encrypted text results in an encrypted version of the processed text [14].

The problem is that, when applications hire cloud computing for remote storage of user's data, some third party companies might sell out the information to some agencies without user permission.[7]

Location based services can be used with the help of GPS. These Location based Services, though, raise a serious privacy issue when mobile users provide private information such as their current location. On top of it, if some more private information about the user is also known, the privacy concern is raised manifolds. Location trusted server (LTS) provides solution to this issue [15].

*2.3. Other Security Issues: Malicious Attacks:* All networks are susceptible to one or more malicious attacks. As more as external Web sites are being accessed malicious actors will have more opportunities to access the network and operational data of that organization. Implementing security controls across all Web 2.0 servers and verifying these rigorous security controls can reduce the threats to internal networks and operational data. Additionally, separating Web 2.0 servers from other internal servers may further mitigate the threat of unauthorized access to information through social media tools and Web sites [10]. Some of the potential attack vectors criminals may attempt include:

*2.3.1. Denial of Service (DoS) attacks*: It has been argued that a cloud is more susceptible to a DoS attack; because more than one client can access cloud simultaneously, which makes DoS attacks much more damaging. Twitter has suffered a devastating DoS attack in 2009 and then again in 2011.

*2.3.2. Side Channel attacks***:** In this kind of attack a malicious virtual machine is placed in close proximity of a target cloud server to compromise the cloud security and then a side channel attack is launched.

*2.3.3. Authentication attacks:* Authentication is one of the weak points in case of hosted and virtual services and is generally been targeted. A user can be authenticated in number of ways and these mechanisms and methods which are used to secure the authentication process are frequently been targeted by the attackers.

*2.3.4. Man-in-the-middle cryptographic attacks:* This attack is carried out when an attacker places himself between two users. In this kind of attack attacker places himself in the communication path and after that it is up to him what to do, he can intercept and modify communication [17].

## IV. CONCLUSION

Mobile Cloud Computing has taken the world of mobile users by storm. The increase in the use of mobile cloud by the mobile users has immensely increased the risk involved in storing the data on the cloud and there are authentication issues as well. Many organizations have come up with solutions for the foreseen threats to instill confidence in the mobile cloud users' mind. It is the users' trust in the security policies that, gives strength to MCC. In this paper, we have tried to summarize the challenges faced by mobile cloud computing in terms of data security, privacy and authentication. Apart from the security issues we have also summarized available solutions that have been proposed by researchers and academicians.

## V. REFERENCES

[1]. RNewswire.org, http://www.reportlinker.com/, 2012.

[2]. Preston A. Coz, "Mobile Cloud Computing: Devices, trends, issues & enabling technologies", 2012.

[3]. Dr. Mani Sarma Vittapu, Atoyoseph Abate and Dr. Venkateswarlu. Sunkari , "A Proposed Solution to Secure MCC Uprising Issue and Challenges in the Domain of Cyber Security", International Journal of Engineering Research and Development, e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.comVolume 10, Issue 11 (November 2014), PP.16-27

[4]. P. Mell and T. Grance, "The NIST definition of cloud computing," 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/ 800-145/SP800-145.

[5]. M. Padma et al , "Mobile Cloud Computing: Issues from a Security Perspective", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 972-977

[6]. Schneider, "Essential characteristics of Mobile Cloud Computing", Marquette University, United States, 2012.

[7]. P. Mell and T. Grance, "The NIST definition of cloud computing," 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/ 800-145/SP800-145.

[8]. Pragya Gupta1 , Sudha Gupta2, "Mobile Cloud Computing: The Future of Cloud", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 3, September 2012 Copyright to IJAREEIE www.ijareeie.com 134

[9]. Han Qi, Faculty of Computer Science and Information Technology University of Malaya Kuala Lumpur, Malaysia hanqi@siswa.um.edu.my and Abdullah Gani, Faculty of Computer Science and Information Technology University of Malaya Kuala Lumpur, Malaysia abdullah@um.edu.my , "Research on Mobile Cloud Computing: Review, Trend and Perspective"

[10]. IA newsletter Vol 13 No 2 Spring 2010. "Cloud Computing: Silver Lining or Storm Ahead" http://iac.dtic.mil/iatac 11

[11]. Le Guan, Xu Ke, Meina Song, Junde Song. 2011. 10th IEEE/ACIS International Conference on Computer and Information Science. "A Survey of Research on mobile cloud computing".

[12]. Roger Collings, "Mobile Cloud Adoption Challenges in the Enterprise"; http://cloudcomputingtopics.com/2012/04/mobile-cloud-adoption-challenges-in-theenterprise/

[13]. "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches". Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. http://onlinelibrary.wiley.com/doi/10.1002/wcm.1203/abstract

[14]. Peter Schoo, et.al. "Challenges for Cloud Networking Security", http://www.hpl.hp.com/techreports/2010/HPL-2010-137.pdf

[15]. H. Zhangwei and X. Mingjun, "A Distributed Spatial Cloaking Protocol for Location Privacy," in Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468, June 2010.

[16]. P. Zou, C. Wang, Z. Liu, and D. Bao, "Phosphor: A Cloud Based DRM Scheme with Sim Card," in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), pp. 459, June 2010

[17]. Michael Gregg, "Security Concerns for Cloud Computing", http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf