Study on Mobile Cloud Computing Security Issues, Challenges and Preventive Measures

Prof. Deepali Shah[1], Prof. Seema Bhuvan[2], Ganesh Thite[3], Tejnarayan Chaudhary[4]

Assistant Professor, Dept. of MCA, NCRD's Sterling Institute of Management Studies, Navi Mumbai, India[1]

Assistant Professor, Dept. of MCA, NCRD's Sterling Institute of Management Studies, Navi Mumbai, India[2]

PG Student, Dept. of MCA, NCRD's Sterling Institute of Management Studies, Navi Mumbai, India[3]

PG Student, Dept. of MCA, NCRD's Sterling Institute of Management Studies, Navi Mumbai, India[4]

ABSTRACT: Cloud Computing is from one of the most widely and popularly technologies that are used Today. Mobile Cloud Computing (MCC) is in favour of a new system in the field of the mobile world. In Recent Years mobile applications and mobile devices are developing rapidly. With the growth of the mobile applications and cloud computing concepts, cloud computing has to become a potential technology for mobile services. Mobile cloud computing is the combination of cloud computing and Wireless Networks to bring benefits for mobile users, network operators, as well as providers of cloud computing. The uses of the computational resources on pay per use models a lot of business is growing. The major issues which hamper the growth of cloud are the only one which is Security becomes a big issue to be answered [1]. The security issues and challenges focusing on the computing types and the service delivery types concerns are shown in this paper and also presents the various ways of preventing the security issues.

KEYWORDS: Mobile Cloud Computing (MCC); Cloud Computing (CC); Private; Public; Hybrid Cloud; Security

I. INTRODUCTION

Cloud computing is a produced through which we can integrate the technologies we need and create a model which provides on-demand services to the users. Cloud computing user can get the exact amount of computing typically use a "pay as you go" model. Like Amazon Drive, Box, Google Drive, Dropbox etc. It refers to the use of networked infrastructure software and capacity to provide resources to users in an on-demand environment. Cloud Provider provides the next generation of internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The market of Smartphones has been increased day by day according to the IDC a global market intelligence firm a total of 347.4 million and shipments grew 4.3%, which was slightly higher than IDC's previous forecast of 3.6% growth worldwide in the first quarter of 2017 [2].Mobile devices as been increased an essential part of human life as the most effective and convenient communication tools not bounded by time and place. Mobile users acquire an increasing number rich experience of various services from mobile applications, which run on the devices and/or on remote servers via wireless networks. The rapidly increasing progress of mobile cloud computing (MCC) becomes a powerful trend in the development of IT technology industry fields [3]. 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).

II. BASICS OF CLOUD COMPUTING

Cloud computing means an Easy way of storing and accessing data and programs over the Internet without using up your own device internal data. Cloud is just for enhancing the usability of the Internet. In Simple cloud computing means typically the Internet, it is the use of software and hardware to deliver a service over a network. It is a process of delivering/enabling scalable, expandable and almost perfectly elastic software services to an organization's computers and devices through the Internet technologies.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

2.1 Characteristics of Cloud Computing:-

Cloud computing have five essential characteristics defined by NIST (National Institute of Standard And Technology) [4][11].

1. On-demand self-service: A consumer can use cloud self-service such as Network Storage and server time etc. as needed automatically without requiring human interaction through the internet.
2. Broad network access: Capabilities available on the network and accessed through standard mechanisms that promote use by heterogeneous client platforms on over the world.
3. Resource pooling: A pool of resources are represented from which are allocated and deallocated resources to the user according to their demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a high level of abstraction is used.
4. Rapid elasticity: Capabilities should be provisioned rapidly and elastically. With no impact to applications or users.
5. Measured service: Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
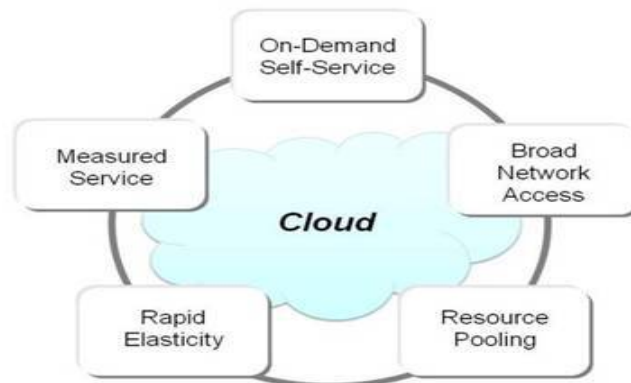

Fig.2.1Characteristics of Cloud Computing
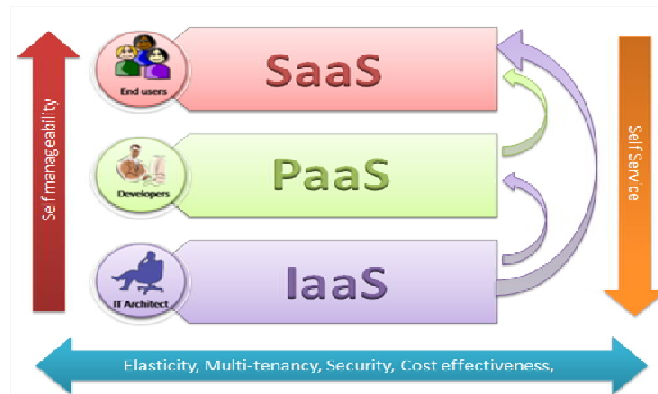
2.2 Service Models:

1. Software as a Service: This service provides a consumer an application as a service to run on the cloud infrastructure. The Consumer does manage the cloud infrastructure like network, servers and Operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
2. Platform as a Service (PaaS): Platform as a service is known as PaaS. This service provides platform independent allowing to its own Consumer to develop, run, and handle the applications without the complexity of building, developing and maintaining the infrastructures typically associated with developing and launch the app and create an environment for the application which gives programming language, libraries, services and tools supported by its provider. This service provides a computing platform for the application and creates an environment for the application which gives programming language, libraries, services, and tools. The user does not have the control over the network Storage and operating system but has the control of the deployed application and the configuration settings for the application-hosting environment. The consumer does not have to manage cloud infrastructure including network, servers, operating systems, or storage, but has managed over the deployed applications and configuration settings for the application-hosting environment.
3. Infrastructure as a Service (IaaS): This service gives to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The cloud infrastructure is not controlled by the consumer but has it has control over storage, operating systems, and deployed applications.

Fig 2.2 Service Models.

2.3 Deployment Models:

1. Private Cloud: Private cloud is a type of cloud computing that delivers similar advantages The cloud infrastructure is provisioned by the single organization which has all the control to operate it and that company may have multiple users and it may be managed by a single organization which keeps all the information confidential and exists on the premises of that single organization only. Private cloud is a type of cloud computing that delivers similar advantages to a public cloud, including scalability and self-service, but through a proprietary architecture. But public clouds are not delivered services to multiple organizations, a private cloud is dedicated to a single organization.

2. Public Cloud: Public cloud is based on the standard cloud computing model, in which such as applications and storage, available to the general public over the Internet. The cloud infrastructure is provisioned for open use by general public. It May is owned managed by some business, academic or government organization .it exist on the premises of the cloud provider. Public cloud services sometimes free or maybe offered on a pay-per-usage model.

3. Hybrid Cloud: Hybrid Cloud uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms. This cloud is the combination of both private and public cloud where an organization owns the Cloud and the Cloud is deployed in its premises. A part of the Cloud is dedicated to the organization. Private usage and some are open for general public. Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms.

4. Community Cloud: A Community Cloud computing is a collaborative computing effort which is shared some infrastructure between several organizations from a specific community with common concerns like security, compliance, jurisdiction, etc., which is managed by internally or third-party user and hosted by both internally or externally. The cloud infrastructure provisioned by the specific community of users from the organizations of similar type It may be managed and operated by one or many of the organizations, third party, else few combinations them, and it may exist on or off Premises.
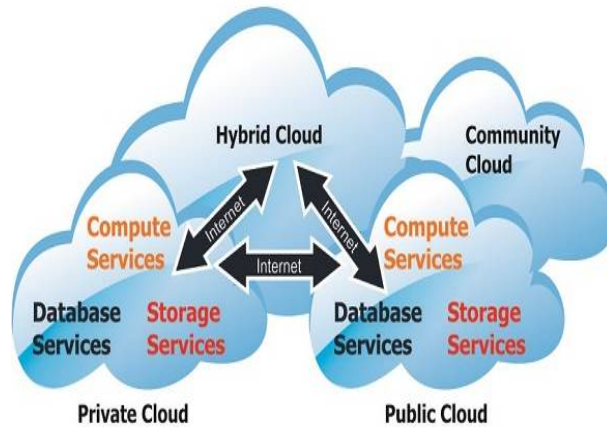
Fig 2.3Deployment Models

III. ARCHITECTURE OF MOBILE CLOUD COMPUTING

Mobile cloud computing refers to the combination between of cloud computing and wireless networks to bring the rich computational resource to mobile users, network operator as well as cloud computing providers. For the use of cloud computing in combination with mobile devices [5].The application runs on mainframe server and then send to the user.
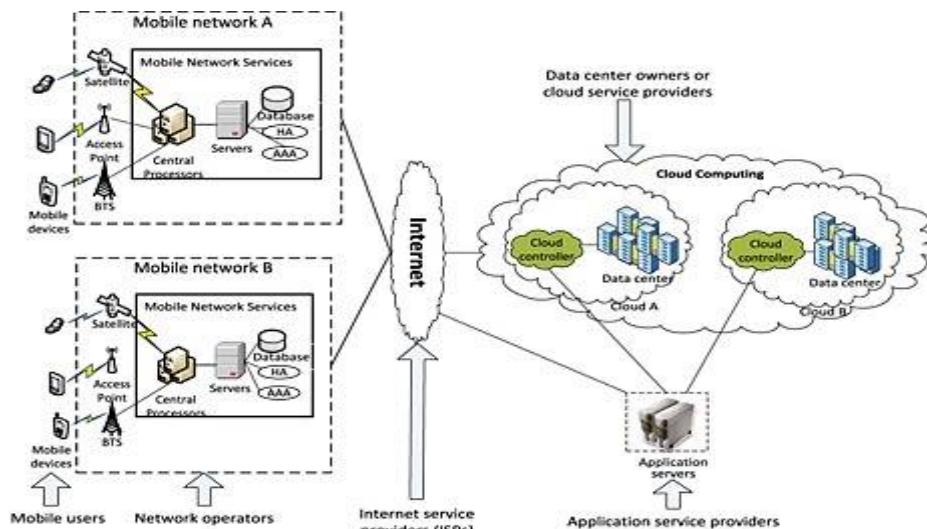
IV. SECURITY ISSUES

4.1 Privacy and Confidentiality: If any client upload data on the cloud then there should be some guarantee that only authorized user can access it. Unauthorized access to customer sensitive data by cloud provider is another risk that potential threat to cloud data. It is Important to provide assurity to the clients and proper practices, privacy policies

and procedure to be follow in place to assure data safety on the cloud. The cloud seeker should be assured that data hosted on the cloud will be confidential and privacy has been maintained.

4.1.1   Data Integrity: Data integrity is a major security issue in which it is important to ensure that stored information is uncorrupted and can only accessible by authorize access. It means cloud service providers should implement mechanisms to ensure data integrity and answerable to client what happened to data at any point. The cloud provider must make his client aware of what particular data is hosted on the cloud and mechanisms introduced by them to protect it

4.1.2   Data Location and Relocation: Mobile Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. When an enterprise has confidential data which is stored on cloud, they may want to know the location of it. They may also wish to specify a preferred location for that cloud provider must have contractual agreement between client and them to keep data on particular location or reside on a given known server. Cloud providers should take responsibility for security of data and provide authentication to keep safe customers information. The transferring data from one location to another location is another major issue in cloud computing. Data is stored at a location decide by the Cloud provider, it is rare situation to move from one place to another. For data transfer cloud providers has contract between then to use each other's resources.

4.1.3   Data Availability: Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

4.1.4   Portability: All mobile agent runs on a place on the virtual machines called Mobile Agent Place (MAP). Mobile agents carry the application code that move from one MAP to another MAP independent of the CCSP (Cloud Computing Service Provider) there by realizing portability among heterogeneous CCSPs.

4.1.5   Interoperability: Interoperability problem is condensed to the conciliation and association among agents which can be affected using agent interoperability standards.

4.1.6   Mobile network security: Although mobile networks have a different design than traditional enterprise networks, they do share many common characteristics.[9] Therefore, traditional denial-of-service attacks designed to misuse the lower protocol layers, such as IP, TCP and UDP are also relevant to mobile networks using these protocols.

4.1.7   Mobile Application Security: Simple way to check security of mobile device is by installing various Antivirus and security applications. Mobile devices having limitation with its processing and power, it's more difficult to protect them from these threads as compare to computer. Several techniques have been introduced for transferring threat detection and security mechanisms to the cloud. Before mobile users could use an application, it should go through varies steps for threat evaluation. All file activities that are done on mobile devices will be verified if it is malicious or not.

4.2 Security Issues in the Service Delivery Model :

The security issues in the service delivery model are classified broadly into three sections as follows [5]:

4.2.1   IaaSIssues :In both private and public cloud keep under systematic review very closely that data is stored in an IaaS infrastructure [13]. The effective deployment of IaaS demands comprehensive logging and reporting in place. Robust authentication and authorization help to get effective Data Loss Prevention (DLP) solution [14]. "Golden-image" VM and VM templates need to been made hard and make clean [15].

4.2.2   PaaS Issue: The PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks.

4.2.3   SaaS Security Issues: Maintaining security of data is shared responsibility of mobile cloud provider and other service providers i.e. software vendors [10]. The security issues discussed in the previous two models also inherits as it is built on top of both of them including data security management i.e. data locality, integrity, segregation, access, confidentiality, backup [7] and network security.

V. PREVENTIVE MEASURES

5.1   Security for mobile applications: Running software's such as Kaspersky, McAfee, and AVG antivirus programs on mobile devices are the best and simple way to detect security threats on the devices and protect them.

5.2   Refactoring Data: Simply performing the encryption methods does not ensure security in Data Transmission. In case of data transmission, the biggest risk is associated with the encryption technology that is being used. Instead of using encryption and decryption technique data can be broken into small packets and then those packets can be transferred through different paths to the receiver. This practice will reduce the chance of being captured by the unauthorized person. Data is not meaningful unless all the part of the data is received. [6]

5.3   Lockbox Approach: Many storage devices are available these days which has built-in encryption and decryption process, but still security is at risk if the encryption and decryption keys are caught by malicious user. In such a case, a user will be provided a key based on identity management technique corresponding to the COI (community of interest) that he belongs to so that he can have access to the lockbox. To access the data the user needs to acquire the COI key to the lockbox and then he can get appropriate access to the meaningful data. [7]

5.4   Homomorphic encryption technique: Homomorphic encryption techniques are a form of encryption technique which is capable of processing the encrypted data and then bringing back the data into its original form. [8]

5.5   A Hierarchal Proposed System: A hierarchical reputation system [12] has been proposed in the managing trust in a mobile cloud environment.

5.6   Virtualization:Attacks such as denial-of-service can be reduced by Virtualization In virtualization, a single machine is divided into many virtual machines. This technique thus provides better data isolation and safety against denial of service attacks.

5.7   Proxy based architecture [8]: SQL injection attacks are defined as those in which a malicious code is inserted into a standard SQL code. The attackers gain access to a database and are able to access some important and sensitive information. Different techniques like: preventing the usage of dynamically generated SQL in the code, using different filtering techniques to filter the input from the user are used to check the SQL injection attacks. A proxy based architecture to prevent SQL Injection attacks which dynamically detects and extracts users' inputs for suspected SQL control sequences has been proposed in the research paper [6].

5.8   Proper SLA: Proper SLAs defining the security requirements such as what level of encryption data should have, when it is sent over the internet and what are the penalties in case the service provider fails to do so.

5.9   Single Sign-On: Single Sign-On In a cloud computing environment, workers log in to multiple applications and services. Because of this reason, it is tedious to implement strong authentication at the user level. To overcome this problem, it is suggested that, to streamline security management and to implement strong authentication within the cloud, organizations should implement Single Sign-On for cloud users. This enables user to access multiple applications and services in the cloud computing environment through a single login, thus enabling strong authentication at the user level.

VI. CONCLUSION AND FUTURE WORK

Mobile cloud computing contains two factors by the combination of which this model works mobile network and cloud computing. Through the mobile network all the data or computation is being transferred to the cloud and cloud stores that data in its storage and if any computation task arrives which smartphones is not capable of executing due to lack of battery power and resources in mobile phones then it is transferred to resourceful cloud which does the execution. Mobile cloud computing is platform which is have largest scope in the future because it combines the advantages of both Mobile Cloud (MC) and Cloud Computing (CC), thereby providing optimal services for mobile users. In the field of computing, Mobile Cloud Computing (MCC) has brought a new dimension to Networking Service. The main moto of this service is interconnected Mobile Cloud (MC) where application providers and enterprises will be able to access

valuable network and billing capabilities across multiple networks, making it easy for them to enrich their services whether these applications run on a mobile device, in the web, in a SaaS Cloud, on the desktop or an enterprise server. In this article an overview on mobile cloud computing (MCC) in which its definitions, architecture, and advantages have been presented. This paper have discussed security issues and preventive measures concerning mobile cloud computing (MCC). Which help us to study and analyse various Security issues and their preventive measures in mobile cloud computing (MCC).

REFERENCES

1. LipikaGoel and Vivek Jain Assistant Professor, IMS Engineering College Ghaziabad "A Review on Security Issues and Challenges of Mobile Cloud Computing and Preventive Measures".
2. http://www.idc.com/getdoc.jsp?containerId=prUS42507917.
3. Hoang T. Dinh, Chonho Lee, Dusit Niyato* and Ping Wang," A survey of mobile cloud computing: architecture, applications, and approaches", Wiley Online Library (wileyonlinelibrary.com), 11 October 2011, DOI: 10.1002/wcm.1203.
4. Mell Peter, Grance Timothy "The NIST Definition of Cloud Computing" NIST Special Publication 800-145 in September 2011.
5. Mohamed Al Morsy, John Grundy and Ingo Müller," An Analysis of The Cloud Computing Security Problem", Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.
6. Gupta Pragya, Gupta Sudha" Mobile Cloud Computing: The Future of Cloud" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 3, September 2012, pp. 134145.
7. Seny Kamara, Kristin Lauter, "Cryptographic cloud storage", Lecture Notes in Computer Science, Financial Cryptography and Data Security, pp. 136-149, vol. 60 54, 2010.
8. A. Liu, Y. Yuan, A Stavrou, "SQLProb: A Proxy based Architecture towards Preventing SQL Injection Attacks", SAC March 8-12, 2009, Honolulu, Hawaii, U.S.A.
9. YanivBalmas"Mobile Network Security Availability risks in mobile networks" , ERT Lab Security Researcher November 2013.
10. White Paper. Mobile Cloud Computing Solution Brief. AEPONA, 2010.
11. BhavyaSareen, Sugandha Sharma and MayankArora Department of CSE CGC, Gharuan Chandigarh, India "Mobile Cloud Computing Security as a Service using Android".
12. D. Gollmann, "Securing Web Applications",Information Security Technical Report, vol. 13, issue. 1, 2008, Elsevier Advanced Technology Publications Oxford, UK.
13. Cloud security alliance: Security guidance for critical areas of focus in cloud computing v2.1, Dec 2009.
14. E. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source Cloud-Computing System," Cluster Computing and the Grid, IEEE International Symposium on, vol. 0, pp. 124–131, 2009.
15. T. Garfinkel and M. Rosenblum, "When virtual is harder than real:security challenges in virtual machine based computing environments," Proceedings of the 10th conference on Hot Topics in Operating Systems –Volume 10, 2005.

BIOGRAPHY

Prof. Deepali Shah working as a Asst. Prof in MCA dept. having 10yrs of academic experience. Presented 5 research papers till now including international and National. Research area will be in the field of testing in cloud based.

Prof.Seema Bhuvan working as Asst. Prof in MCA dept. having 13 years of academic experience .Presented 4 research papers in National and International conference. She is passionate to undertake research in the field of testing and cloud computing.

Ganesh Thiteis a Post Graduate student of Master of Computer Application (MCA), College of NCRD's Sterling Institute of Management Studies, Mumbai University.

Tejnarayan Chaudhary is a Post Graduate student of Master of Computer Application (MCA), College of NCRD's Sterling Institute of Management Studies, Mumbai University.