ISSN No. 0976-5697

Volume 8, No. 4, May 2017 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Security Vulnerability in Mobile Cloud Computing (MCC)

Er. Amandeep Singh Walia
Assistant Professor, Dept. of CSE
Sant Baba Bhag Singh University
Khiala, Jalandhar, India
er.amanwalia@hotmail.com

Abstract--- Mobile Cloud computing is promising technology showing consistent growth in the field of computing. Cloud computing frameworks like, Google App Engine, Windows Azure, Amazon Web Services and Rackspace have become increasingly popular among practitioners. The advent of Smartphone and the widespread use of other mobile devices such as tablets have introduced a new dimension to cloud computing, offering a higher degree of flexibility in data access, and with it has increased the need for security standards. Mobile cloud computing promotes use of cloud based applications and services in a mobile environment. It support virtualization, resource management and provide services to IaaS, PaaS, SaaS levels. While cloud computing provides many features but still it has some short comings like providing security in cloud environment. Mobile devices are unable to make effective use of resources and results in communication delay, and unexpected mobile attacks or vulnerabilities. These challenges have great effect in the improvement of service qualities of mobile cloud. This paper reviews the concept of mobile cloud computing as well as the security issues inherent within the context of mobile application and cloud computing environment.

Keywords---Mobile Cloud Computing, IaaS, PaaS, SaaS, Cloud Security, Encryption.

I. INTRODUCTION

In the past few years, the smartphone has become integral part of human life and come out as a new computing paradigm that offers a wide scope of useful applications, powerful operating systems and multifunctional sensors. Mobile Cloud Computing provides mobile users with all resource-intensive computing to be performed in clouds, without having the need to have powerful hardware components (such as CPU, Memory capacity, power supply etc.).Mobile Cloud computing (MCC) refers to an infrastructure where both the storage of data and processing happens in environment outside of the mobile device into powerful and centralized computing platforms located in cloud infrastructure, which is then accessed over the wireless access point or satellite link.[3]Unlike the traditional Mobile Computing, the Mobile Cloud Computing resources are virtualized and executed with numerous distributed computers or server rather than local computers or servers [1]. Countless applications are developed on Mobile Cloud platform basis and served to users, such as Google's Gmail, Maps and Navigation system for mobile, Google's Voice search on Android Platform, MobileMe from Apple, One Drive from Microsoft, Amazon's Web Browser Silk etc. SaaS (Software-as-a-Service): The Software as services is high product of a quality model. Software services hosted on the cloud venders are rented to the end users, which helps in the replacement of the applications running on local computer. Central organization of resources helps in reduction of the cost. In this strategy, the sales force, Microsoft, yahoo, Google is offered by companies. They include customer relationship management (CRM) as a service; email, logistics service etc. PaaS (Platform-as-a-service): The platform as services is referred to the software deployment framework, runtime environment and the element on to pay to alter the direct readying of application level assets or internet application. It is environment in which the package deployment, testing and development are done. They are resources of entire life cycle and can be operated on a PAAS level.[2] For example: Microsoft Azure, IBM Smart cloud, Google app engine, and Amazon EC2etc.[2] Platform as a service allows the users to create their own application. The cloud application supports a set of applications program interface. It is the middle connection between application and hardware management software. The major goal of MCC is to enhance the functionality derived from mobile devices by investing on the strengths of mobile cloud computing. It is still a relatively new favorable area of research, where ample of problems are yet to be resolved. The Cloud however is liable to be many privacy and security attacks. The biggest obstacle hindering the adoption and progress of the Cloud is the privacy and security problems related with it. Evidently, ample of privacy and security attacks occur from inside the Cloud. Cloud providers usually have direct access to data stored and steal the data to sell to third parties in order to target ads and gain profit.[3]Critics argue that cloud computing is not secure enough because data leaves companies local area networks. The major goal of the paper is to finds out the problems associated with mobile cloud security. Paper extracts the issues and concentrates on securing the user's data and privacy during communication on the clouds.

II. ARCHITECTURE

Mobile Cloud Computing (MCC) is basically the interconnection and combination of cloud resources, mobile computing and wireless networks to make powerful processing environment to mobile users, network operators, as well as providers of cloud computing. This availability of environment enables mobile users to use the cloud infrastructure to overcome the drawbacks of mobile technology. The major goal of MCC is to enable processing of rich mobile applications on a environment of mobile devices, with a rich user interface experience. MCC provides business related opportunities both for mobile network operators and cloud providers. Moreover MCC can be defined as "a rich and high end mobile computing technology

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

that maintains integrity and connectivity between resources of different clouds and network technologies.[4] It also provides unlimited storage, and mobility to gain a multitude of mobile devices from any location. The major architectural design is composed from these components: mobile users, mobile operators, internet service providers (lSP), and cloud service providers such as Google and Azure respectively.[5]

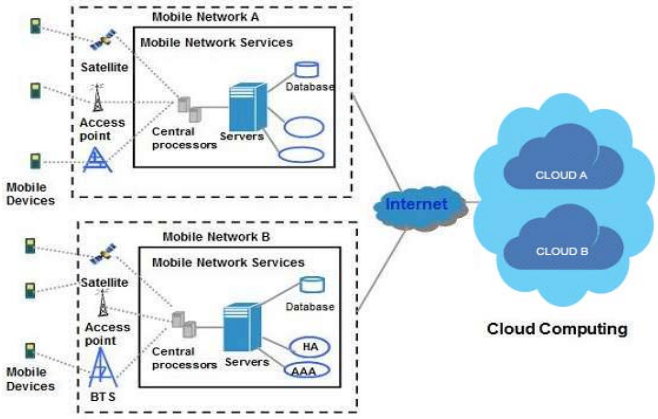

Figure 1: Mobile Cloud Computing [2]

III. MCC SERVICE MODELS

1) Infrastructure as a Service (IaaS): It includes the outsourcing of the devices used to support functions, including data storage, hardware, and servers and routing and networking components .Virtualization is mainly used in IaaS cloud order to combine or split physical devices. Users are able to deploy and execute arbitrary programs or software, which includes operating systems and applications. The user doesn't manage or directly control the cloud hardware and resources but the software and operating systems; storage, deployed applications and possibility limited control of selected networking components can be controlled by user. Instances of IaaS include Amazon Elastic Compute Cloud (EC2), IBM Computing on Demand, Joyent, and Rackspace.[6]

2) Platform as a Service (PaaS):PaaS is a type of development that allows users to develop cloud services and applications directly on the resources of PaaS cloud. PaaS offers development environment that hosts both completed under development cloud applications. An example of PaaS can be Google App Engine.[6]

3) Software as a Service (SaaS): Generally the client launches their application on a hosting environment that can be executed through network from various clients by the users of the application. The client does not manage or fully control the cloud environment. But some limited settings of user-specific application can be configured. Its instances include Google Apps and Microsoft Office 365.[7]

Figure 2: Mobile Cloud Computing Layers.[8]

IV. MCC DEPLOYMENT MODELS

A. Private cloud

Private cloud describes the infrastructure operated mainly for a single organization. It can be managed internally or by a third-party company and they can be hosted internally or externally by the organization.

B. Public cloud

Public cloud models describes cloud computing in the traditional style, where the hardware and resources are dynamically handled to the general public or users on a fine-grained and self-service basis over the Internet, by using web applications or web services from different or third-party organization who charges on a fine-grained utility processing basis.

C. Community cloud

Community cloud models are those which shares resources between different organizations that is from a specific community with common characteristics such as compliance, jurisdiction, security etc., which can be managed internally or by a third-party organization and hosted internally or externally by some organization.

D. Hybrid cloud

Hybrid cloud consists of combination of multiple clouds that can be private, community, or public that remains unique model but is bound together by offering the features of multiple deployment models. Some Cloud Computing Service Providers are Microsoft windows Azure, Google AppEngine, Amazon, VMware cloud, Rack space, Verizon, Go grid, AppNexus[9]

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

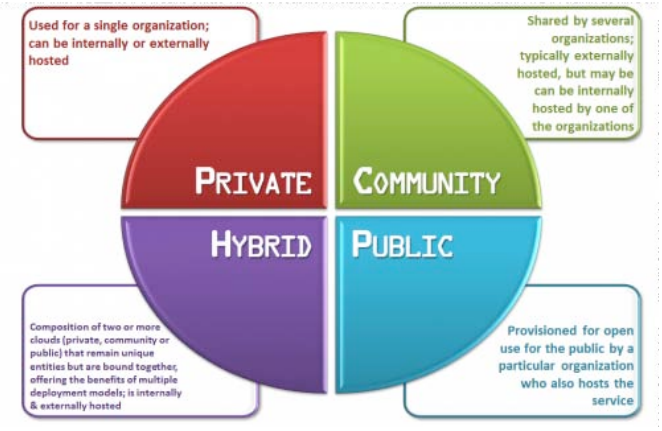

Figure 3: MCC DEPLOYMENT MODELS[5]

V. SECURITY THREATS

Mobile Cloud computing technology is facing number of issues. These issues which are encountered in the system are listed as the following: data breaches, data loss, malicious insiders, insecure interfaces and APIs, account or Service hijacking, data location, and denial of Service.

A. Data Breaches:
A mobile cloud environment has large number of users and organizations, whose data is stored in the same environment. Any type of breach to this mobile cloud computing would expose all users' and organizations' crucial data to the hackers. As there is multi-tenancy, users using different applications on cloud virtual machines could access and share the same set of database and any corruption to the database will affect other users sharing the same database set. Moreover, SaaS cloud providers have made a claim that they can provide more security to user's data than traditional cloud providers. Any user which is inside the cloud environment can access the data but by using different techniques or methods; that is they can access the user's data by indirect method by accessing vital information in their cloud environment and this illegal access could make the mobile cloud environment. It has been seen that that hacking and malware are the common causes of important data breaches, with 50% hacking attacks and 49% malware.

B. Data Loss:
Companies are outsourcing their entire data to cloud service providers. Because of the low cost rate that the cloud offers, the customers should make sure not to expose their important data to risks because of the many ways to compromise their data. In cloud computing, the risks are there because it is faced in the cloud and did not happen to traditional old computing, and there are major challenges taken to avoid those risks.[3]. There are many possibilities of losing data due to a malicious attack and sometimes due to server crashes or unintentional deletion by the provider without having backups. Catastrophic events like an earthquake and fire could be the causes of loss. Also, any event that leads to harming the encryption keys could lead to data loss to[7]. In order to avoid losing the data, there are many solutions proposed [9]:

- Strong API for access control should be used
- While should be encrypted in transit, ensuring its integrity.
- Analyze data protection at design time& run time..
- Using practices such as strong key generation, storage, destruction, and management.
- Requiring the provider to erase the persistent media data before releasing it to the pool.
- Specifying strategies for back up and retention.

C. Malicious Insiders:
Malicious insiders are the people who are authorized to manage the database such as administrators or employees of the company offering cloud services partners, and contractors who have access to its data.[12].Hackers can steal or corrupt the crucial data because they are getting paid by other organizations or to just to make loss to a company. Even the cloud organization may not be aware of attack because of not managing their employees properly. There are many solutions proposed:

- Conducting a comprehensive assessment of supplier and making supply chain management ID stricter
- Defining human resources requirements as it is part of the legal contract.
- Implementing transparency in information security and all cloud service practices.
- Notify instantly, when data breaches occur.

D. Insecure interfaces and APIs:
The communication between the cloud service provider and the client is through the API through which the clients can manage and control their data [7]. Therefore, those interfaces should be secure to prevent any unauthorized access. If they are weak and security mechanism cannot defend them, this could lead to accessing resources even as privileged user. There are many solutions proposed to avoid insecure interfaces and APIs:[8]

- Analyzing the security model for interfaces of the cloud provider
- Making a strong access control and authentication when data is transmitted
- Understanding dependencies in API

E. Account or Service Hijacking:
Users are using passwords to access the cloud service resources so when their accounts are hijacked and stolen, the passwords are misused and altered unsurprisingly [6]. An unauthorized user who has a password can access the data of clients by stealing it, altering it, or deleting it, or for the benefit of selling it to others. There are many solutions proposed to avoid account or service hijacking:[8]

- Preventing users from sharing their credentials
- Using a two-factor authentication system
- Monitoring all activities to detect unauthorized access
- Understanding security policies and SLAs

F. Data Location:
Cloud providers mainly have distributed centers widespread over several places. Data location is major issue in cloud computing since the users of clouds need to know the location where their vital data is stored. Some of the countries according to law, require their organization to store their data in their respective country only. Moreover, there are regulations in some countries where the company can have their data centre. Also, the data location matters when the user data is stored in allocation that is prone to wars and disasters.

G. Denial of Service:
Some organizations need their systems to be highly up time because availability is crucial to them due to the critical services they provide to users. The mobile cloud services provider offers various hardware and software resources that are shared among several users. If a hacker occupy all available resources, others users will have shortage of the resources, which will lead to denial of service and could slowdown accessing those resources. Also, users, who are using cloud service and affected by botnet, could work to affect availability of other providers.

VI. SECURITY MEASURES

The vital data on cloud can thus be secured by following:-

A) *Authentication* - The process of identifying user is usually based on a username and password. In security systems, authentication is different from authorization, which is the process of giving individuals access to system resources based on their identity.[8] Authentication merely ensures what the individual claims to be, but says nothing about the access rights of the user.

B) *Authorization* - Authorization is the process of providing permission to someone to access resources. In multiuser computer systems, generally a system administrator defines users are allowed to access cloud or system and what roles of use (such as access to Read/Write files, time of access, amount of allocated memory space, and so on).[9]

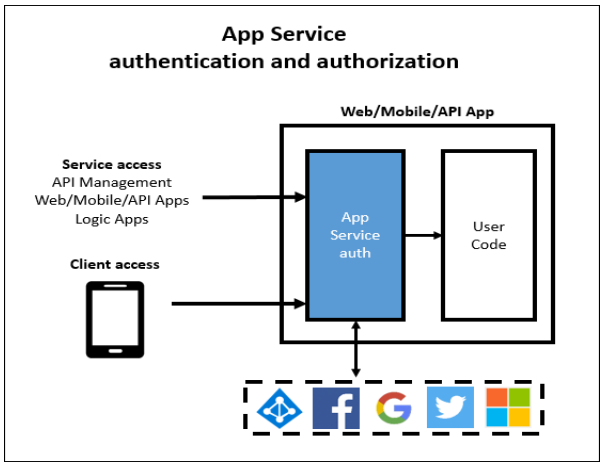

Figure 3: Authentication & Authorization in Cloud [10]

C) *Encryption*–Encryption defines the process which takes input of the plaintext and encoded into unreadable format or scramble text using mathematical calculations and algorithms, effectively making the data in unreadable form unless a cryptographic key is used to convert it into the readable form. Encryption method ensures data security and integrity, even if the data is accessed by an unauthorized user, provided that encryption keys have not been compromised.[11] Encryption can protect data during transmission or storage. Encryption is performed at multiple levels of a system, appropriate to the context of use and other system components. As shown in figure below, it translate the data into a secret code and is most effective way to achieve data security.

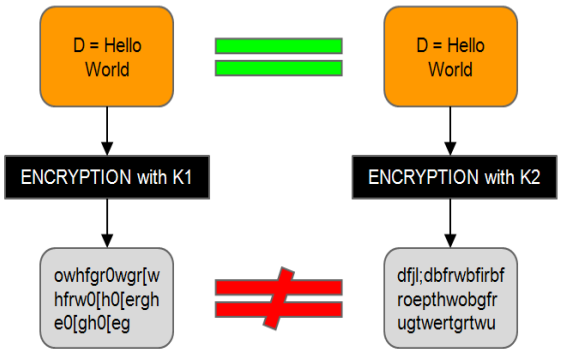

Figure 4: Encryption of data with keys [11]

D) Integrity- Every user in mobile must ensure the integrity of their data present on the cloud. Every access should be verified and authenticated. To preserving integrity for user's information present in cloud different approaches are being proposed. [10] For instance, data saved by each user or enterprise in the cloud is tagged or initialized to them to have access or perform operation on data. Every access must be authenticated assuring that it is their data and thus verifying its integrity.

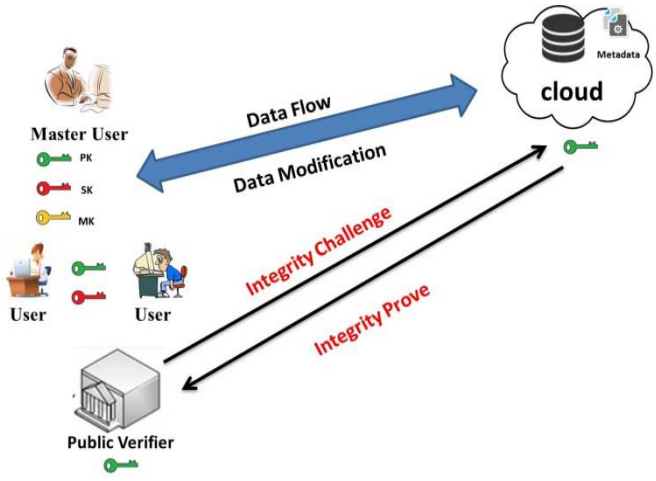

Figure 5: Integrity of data

E) Legal Provision- Sharing, distributing and piracy of digital media such as image, video, audio, and e-books, software should be criticized.[12] The effective method to protect these contents from piracy and illegal access are applied such as paid access or encryption and decryption keys to access these contents.

CONCLUSION

Mobile Cloud Computing is an enticing technology that will receive more attention in the future from industry and researchers. The cost of this technology is very minimal when it is compared to building the infrastructure for local servers. But with mobile cloud computing customers can't trust commitments or policies made by these cloud organizations. This leads to many security issues with data storage such as privacy, confidentiality, availability and integrity. In this paper we focused on data storage security issues in mobile cloud computing. It also describes the measures to be taken for the prevention of the security related issues.

REFERENCES

[1] Han Qi, Abdullah Gani, "Research on Mobile Cloud Computing: Review,Trend and Perspectives" in Proceedings of Conference-2011

[2] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing,"in System Sciences (HICSS), 2011 44th Hawaii International Conference on.IEEE, 2011, pp. 1–10.

[3] N. Gonzalez, C. Miers, F. Red´ıgolo, M. Simplicio, T. Carvalho, M. Naslund, ¨and M. Pourzandi, "A quantitative analysis of current security concerns andsolutions for cloud computing," Journal of Cloud Computing, vol. 1, no. 1,pp. 1–18, 2012. [32] N. Gonzalez, C. Mie

[4] Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, "Mobile cloud computing: A survey", Elsevier, pp.84-106,2012.

[5] Pragya Gupta, Sudha Gupta, "Mobile Cloud Computing: The Future of Cloud", International Journal of Advanced

[6] Priyanka Asrani, "Mobile Cloud Computing", International Journal of Engineering and Advanced Technology,Volume-2April 2013.

[7] Ahmed Dheyaa Basha, Irfan Naufal Umar, and Merza Abbas, "Mobile Applications as Cloud Computing:

[8] Implementation and Challenge", International Journal of Information and Electronics Engineering, Volume-4, No. 1,January 2014.

[9] M. Rajendra Prasad, Jayadev Gyani, P. R. K. Murti, "Mobile Cloud Computing: Implications and Challenges"

[10] Shantanu Deshmukh, Prof. Rinku Shah, "ComputationOffloading Frameworks in Mobile Cloud Computing : ASurvey", Vidyalankar Institute of Technology,Mumbai,India, 2016.

[11] Journal of Information Engineering and Applications, Volume-2, No.7, 2012.https://www.cs.purdue.edu/homes/bb/cloud/MCC.pptx.

[12] Wassim Itani Ayman Kayssi Ali Chehab,"EnergyEfficient Incremental Integrity for Securing Storage in Mobile Cloud Computing", Department of Electricaland Computer Engineering American University of BeirutBeirut, Lebanon.