Overview Of Security Issues In Mobile Cloud Computing

Ms. Prafulla Kumbhar
Assistant Professor, Tilak Maharashtra Vidyapeeth

Abstract
The evolution of cloud computing has a great effect on software designing. With the development of mobile internet and cloud computing, concept of mobile cloud computing is emerging. Nowadays, storage capacity is being tremendously increasing with the use of cloud computing. As development continues, security issues as well as privacy risks exists due to data outsourcing over the Internet. Those threats should be identified to protect the sensitive information of users. In this paper, we will discuss some of the security issues related to mobile cloud computing systems in order to reduce them.

Keywords: Cloud computing, Cloud security, Mobile cloud computing, Privacy, Wireless communications security.

Introduction
Mobile cloud computing is explain as the service of cloud offer to the mobile users with a variety of applications, irrespective of connectivity strength, operating system and memory capacity. Huge amount of user access software with the help of cloud through data centres which are places world wide. In last decade cloud computingwas developed. Which is having various advantages. MCC (Mobile Cloud Computing) is having many benefits. Using MCC research programmers and research industry get benefited. whichincludesthe processing power and battery life of mobile devices. Now a days user accesses various applications and searches data which is stored on cloud. By using existing resources in cloud infrastructures and increasing the resource sharing on the Internet based applications and services. MCC can overcome from its existing limitations of the mobile devices which are now a days get used, with help of future cloud based network and mobile enabled service.

But there are so many risks and challenges which are get faced by MCC applications. This paper focuses on security problems and its solutions. [1]

Cloud Computing
The IT services is more flexible on internet with the help of Cloud computing. With the help of third party it provides important sources of a business, which causes a risk to the security and privacy of data.

It can be well-defined as Common Location Independent Online Utility on Demand. Mostly cloud computing is get used to increase the capacity and capability of client devices by retrieving the infrastructure and software applications without purchasing them. [2]

Cloud Services
Following are three general categories of cloud services:

Platform as a service (PaaS): Most of the software for developers, IT managers or end-users are get benefited of various platforms and services without installing or downloading of computing platforms. To test and implement on the application PaaS provides a platform with a high level of integration.

The user notable to supervise the infrastructure (such as operating systems and storage, network, servers). user now controls deploy applications and, probably, their configurations. E.g. Windows Azure, Magento Commerce Cloud.

Infrastructure as a Service (IaaS): with the help of virtualization technology the hardware resources are get shared to use some infrastructure and to use various services. Its objective is to make resources available such as servers, network and storage. Which are more easily accessed by applications and operating systems. That’s why it provides Application Programming Interface (API) to interact with hosts, switches, and routers. Addition of new equipment with help of IaaS is very simple and it get added in transparent manner. E.g. Amazon Web Services, Google Compute Service.
Software as a Service (SaaS): SaaS is explained as different software applications over the Internet. It provides the facility to the customer that without installing software or operating system on their own computer make use of various services. It provides support of various software systems. It removes the continuous operations of software also maintenance of it. [2]

**Cloud Service Models**

- **SaaS**: Software as a Service
- **PaaS**: Platform as a Service
- **IaaS**: Infrastructure as a Service

**Application Deployment Models**

- **Private Cloud**: The organization owns the physical structure and also manages the security with the extension of the management of organization.

- **Public Cloud**: The computing resources are dynamically circulated over the Internet via Web applications or services from the third party provider. Third party runs public cloud. On the cloud’s server different applications used by different customer are mixed together using storage systems, and networks.

- **Community Cloud**: This model of Cloud computing is used by a group of an organization or individuals. This cloud used by a group of entities who have sharing resources.

- **Hybrid Cloud**: It is a combination of two or more clouds i.e. public or private. Which are get bounded together but still act as a separate entities. It is a standardized technology that permits data and applications portably. [4]

**Mobile Cloud Computing**

The data transfer, media transfer is done by using computer or any wireless enabled device is known as mobile computing technology. The mobile communication is the concept of mobile hardware and mobile software together. Mobile computing is not only limited to Mobile Phones, but also get used in other devices like PDAs (Personal Digital Assistant), Smart phones, Tablets, I-Pad etc.

Mobile Cloud Computing (MCC) is a part of mobile computing technology. Processing of data is done on cloud, and data get stored on the servers over the cloud. Whereas mobile are act as an output device. Various services are provided by Mobile Cloud Computing (MCC) using wireless networks. Which mobile model is get used by user accordingly services of wireless network is get used. [6]
Mobile Computing Security issues

Computing environment is a part of mobile computing where mobile devices or any other devices are not restricted in a particular place or areas. All devices are having a facility to communicate when it’s moving. Without creating any physical connection data gets transferred between source and computing device using wireless networks. This kind of networks includes wireless LAN, wireless access point, and cellular networks. Whenever any new security related issues are generated in mobile computing, they are mostly originated from both the wireless networks and distributed computing systems. [8]

There is a two security aspects:

Wireless Security Issues

When hackers interrupt radio signals then only security related issues are generated. Also it happens because of not proper management of the network by user. Because a private network manages most of the wireless networks which are dependent on it and get managed by others. Hence there is very less control of security. Using wireless network most commonly observed security issues of mobile computing are:

A. Denial of Service (DOS) attacks: It is a very common attack that occurs in most kinds of networks. It means attacker attacks on communicating server and prevents the users by sending large amount of data using wireless network services. Which get resulted into slow down of network, because of it user not get benefit over the use of its services. [9]

B. Traffic analysis: This is mostly done to check which type of network packets are getting flowed with the networks deeply. Analysis of network traffic is monitored using network bandwidth monitoring software. Attackers mostly use Bandwidth monitoring software for analysing patterns of network software. Also used to identify susceptible patterns to interruption in or to recover complex data. [10]

C. Eavesdropping: Attackers tries to steal data or information which is being transmitted using machine through network is known as a sniffing or snooping attack. Due to insecure communication network its easy to access the data which is get to be send or received, this is an advantages of eavesdropping attack. These kind of attacks are not easy to identify because they do not interrupt network transmissions which appear to be operating strangely. [11]

D. Session interception and message modification: Sessions are get interrupted and modified by attackers over a transmitted data. When sender and receiver both are working on data that time system is cases by the attacker is called as man in middle attack. It’s a kind of insertion of attacker. [9]

E. Spoofing: These kind of attacks are done from most reliable sources such as emails, websites. This kind of communication is also applicable for phone calls. Also occasionally applicable to technical things like ARP packets (Address Resolution Protocol), IP address,.. [12]

Privacy

Privacy is mostly hiding data. That the unauthorised person should not able to access any ones data. Share private information with only authorised person. It helps to protect data. Make use of good encryption system or algorithm to encrypt confidential information. So if the device is physically lost, then also data will be secure. [13]

Data Ownership

Store a data like videos, e-books, audio, e data these are the kind of e-materials we can able to store and access this kind of facilities are provided by cloud computing. User can faces so many kind of risks such as lose of data, not able to use purchased authorised data. To overcome from these kind of risks, we should aware of purchased media. Also terms and conditions of that purchased media. Information which user uses such as user profile, locations shared by user, device capacity all is get operated or used by Mobile Cloud Computing. Above information is get stored on mobile cloud server which can utilize the information such as locations and capacity of devices and user profiles, which can be get accessed by management. [4]

Role of Malware in Security

The inventors of malware keep on eye that which kind of mobile applications are get used. There is a wide range of variety in mobile applications. By
focusing on mostly used mobile application malwares are get created. With the help of this unauthorized users tries to access unauthorized data, and then issues are get raised. All this happen because user they itself allows to install malware on their mobile devices, which causes to transfer a data also leaks all personal information to the malware creators. [1]

**Data Security**

Mobile devices are susceptible for malicious code. There are so many chances to lose of the data, because mobile devices are mostly insecure. It easily causes to unauthorized user who can easily access the information which is stored on the mobile devices. Following are the top most mobile threats:

1. OS and third-party applications, Susceptibilities within devices.
2. Information get stolen by mobile virus.
3. third party applications are poorly designed which causes to an data leakage.
4. Data get to be loosen from lost or stolen devices.
5. Access of insecure or unreliable network and use of unreliable or insecure access points.
6. Not secure marketplaces.
7. No sufficient management tools and access of APIs. [4]

**Integrity**

Integrity assurances that only authorized parties or users are allowed to modify or access the information or messages. It also gives guarantees that a message which being transmitted is never get changed. There is an application of privacy, integrity get to a stream of messages, which applicable to a single message or selected portion within a message. But, there is amost useful approach is total stream protection of given message. A connection-oriented integrity service, assures you about the data which is contains with a stream of messages, who guarantees that messages are get to be received, with there is no duplication of data, no insertion, no modification, no deletion, or replays of data. The data corruption is also enclosed under integrity service. Thus it addresses to flow of message which having modification and also rejection of services.

**Conclusion**

In this paper mostly try to cover security issues of mobile devices, mobile networks and are discussed to an extent of scope. Still there is a necessity to find more innovative approaches which can to be put an end to the threats, and issues which are continued as a never ending processes.

**References**


[7] https://ars.els-cdn.com/content/image/1-s2.0-S1319157817300642-gr1.jpg


