IJRSET 2015 SPL Volume 2, Issue 9 Pages: 42-45

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

Security Threats in Mobile Cloud Computing

[1] M. Usha, [2] P.Malathi, [3] Dr. M. PushpaRani
[1,2] M.Phil.Scholars, [3]Professor and Head,
[1, 2, 3] Department of Computer Science,
[1, 2, 3] Mother Teresa Women's University,
[1, 2, 3] Kodaikanal.

Abstract:-

Mobile Cloud Computing (MCC) is a huge revolution in the field of mobile world. It refers to the combination of Cloud Computing services in the mobile environment. In the sense, it incorporates the elements of mobile networks and cloud computing. MCC guarantees reduced Capital Expenditure (CAPEX) to an organization by simply tapping into the cloud. As it attracts many business organization and individual, they started to place more and more information into the cloud. So, the different security issues arise about how safe MCC environment is and what are the preventive measures has to be done.

Keywords: - Mobile cloud computing (MCC), security threats, cloud computing

1. INTRODUCTION

Mobile Cloud computing is based on three major notions named as hardware, software and communication. The hardware refers to mobile devices and the software refers to mobile applications in that devices. The communication refers to mobile networks, protocols, services, data delivery etc... Mobile Cloud Computing (MCC) refers to availability of cloud computing services in a mobile environment with mobile devices such as smart Phones, iPod, Tablets, PDAs, Laptops and so on. MCC architecture divided into two layers. They are cloud service provider (CSP) and mobile link layer. Resources in MCC are virtualized and assigned in a group of numerous distributed computers to form 'the cloud' and are provided to mobile devices. The cloud provider has Saas (software as a service), Paas (Platform as a service),Iaas (Infrastructure as a service)[1,2,3]. The mobile users send service request to the cloud through a browser or desktop applications. The two main parts of Mobile Cloud Computing (MCC) are separated as cloud computing and mobile computing. The working pattern of MCC is shown below [1,2]

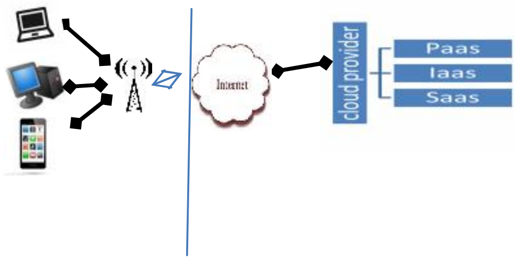
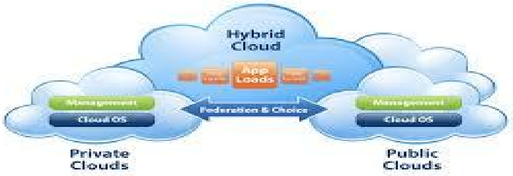


Figure1. Mobile computing Cloud computing

2. CLOUD DEPLOYMENT MODELS

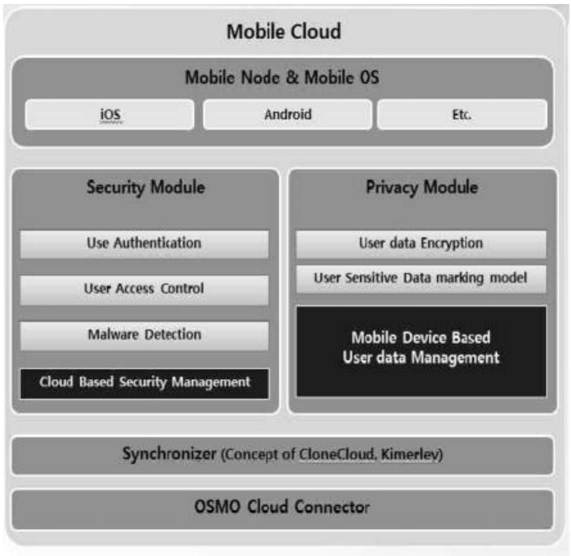


There are three types of cloud application deployment models with each has own benefits and usages. They are [2,3]

- **Private Clouds:** They are owned and managed by an organization for its own users. It offers more security for its data and quality of service is greater
- **Public Clouds:** They are for external users through Internet whoever can register in the cloud and use its resources. It offers less security than private clouds.
- **Hybrid Clouds:** It is the mix up of private and public clouds.
- **Community Clouds:** It is established for specific purposes, such as for government, healthcare, finance and so on.

3. SECURITY ARCHITECTURE OF MCC

The overview of Mobile Cloud Computing Security Architecture is shown below [2],



As we know from above, applications are run on a remote server and then sent to the user, two major concerns in MCC which is impossible between different cloud computing service providers (CCSP) is Portability and Interoperability[1,2]

♦ **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 there by realizing portability among heterogeneous CCSPs.

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

4. MOBILE CLOUD COMPUTING SECURITY

The key issue that most of the cloud gives attention to securing MCC is User's privacy and Integrity of data or applications. From the words above, MCC is a combination of mobile network and cloud computing, so the security issues are classified into two types [1, 2, and 3].

1. Mobile network user's security
2. Cloud security

4.1 Mobile network user's security: Different mobile devices such as smart phones, PDAs, Laptops, etc... has various security vulnerabilities and threats. Some applications to these devices can cause privacy issue for users. There are two main issues concerning subscriber's security.

▪ **Security in mobile application**

The simplest way to detect security threats will be installing and running security software and antivirus programs on mobile devices. Several approaches have been developed to transfer threat detection and security mechanisms to the cloud. It will be better that mobile devices performs only light weight activities

- **Privacy**

The presenting of private information and user's data creates problems for privacy. These types of threats are minimized through selecting and analyzing the enterprise needs and require only specified services to be needed and moved to the cloud.

Cloud Security:

Individuals and Enterprises store large amount of data or application on the cloud. In consequence of this benefit brings issues on Integrity, Authentication and Legal Provisions.

➢ **Integrity**: Every user must be guarantee that every access they make should be valid and verified. But different methods are proposed to preserve user's information on the cloud.

➢ **Authentication**: Various authentication techniques are accessed using cloud computing to secure the data access suitable for mobile environment. Some of uses open standards and even supports the integration of various authentication methods.

➢ **Legal provisions**: Nowadays, variety of digital content such as video, image, audio and e-book programs are pirated. Some solutions to protect this content from illegal access are established by encryption and decryption keys to the access contents. In other words, coding or decoding platform must be done before any mobile user can have access to digital contents.

5. IMPLEMENTATION ISSUES IN MCC

The main obstacle for the user to movetheir data to the cloud, some common threats in clouds [3] and data security and privacy issues are

- ♦ Data theft risk
- ♦ Violation of privacy
- ♦ Loss of physical security
- ♦ Lack of standard to ensure data integrity
- ♦ Services incompatibility

Some of these threats are excluded by transmitting the data between the components of homogenous mobile applications, some dynamic intrusion detection systems and methods are installed during runtime in network domain systems and so on. There by we offer more effective methods to maximize the user's data security and satisfaction towards MCC.

Also, the data life cycle in cloud computing are need to be standardized if the user adopts the cloud data services [3]

- ✓ Generating Data
- ✓ TransferingData
- ✓ Using and Sharing of Data
- ✓ Storage
- ✓ Archival and Destruction

These steps are done so that we can provide good and valid Authorization, Accounting and Authentication at different levels during runtime in user's mobile devices. In addition to that , offloading techniques are used and even clone of the device is accessed by the network.

Similarly, some warnings are also found in user's mobile devices such as [3]

- ❖ Device theft
- ❖ Virus attacks via Wireless device
- ❖ Misuse of Access rights
- ❖ Limited resources
- ❖ Low Bandwidth

In user's mobile device security, we can install a legal and well developed anti-virus application that suits our mobile environment and check the authentication of the transaction at different levels with high networking speed and so on.

Some of the benefits in implementation of MCC are [3]

a. **Data reliability**: Since data stored and backed up on different servers in the cloud. It gets less chance of losing data and applications on user's mobile device.

b. **Scalability**: Cloud service providers (CSP) can possibly add any number of applications and services without any concern about resource usage.

c. **Multi-tenancy**: CSP and data center owner shares the same cloud resources for different applications and avails services to the end users. They divide their cost between them.

d. **Flexible Integration**: Each mobile user has different request and demands. CSP can integrate different services through cloud and internet without much effort.

CONCLUSION

Mobile Cloud Computing is an emerging future technology because of variety of advantages it offers to mobile subscribers. It provides an easy way for small developers to secure their services. Here, MCC is a combination of mobile computing and cloud computing, the security related issues are divided into mobile network user's security and mobile cloud security. This paper shows that in MCC data storage and data processing done on Internet, but not on individual devices. Thus providing on demand services. In order to overcome security threats, we need to improve security technologies and mechanisms for cloud services and minimize mobile user's security problems.

REFERENCES

[1] Jasleen .Lovely Professional University, Phagwara,India. “Security Issues in Mobile Cloud Computing”. International Journal of Computer Science & Engineering Technology(IJCSET). Vol.4No.07 Jul 2013.

[2] Soeung-Kon(Victor) Ko, Jung-Hoon Lee, Sung Woo Kim. “Mobile Cloud Computing Security Considerations”.www.sersc.org /Journals/jse/vol9/no2/2012. Journals of Security Engineering(JSE) vol9.no.2-2012

[3] AbidShahzad and MureedHussain. “Security Issues and Challenges of Mobile Cloud Computing”. International Journal of Grid and Distributed Computing, vol.6. no.6 (2013) ppno37-50[4][

[4] S.O. Kuyoro,F.Ibikunle and O. Awodele, “Cloud Computing Security Issues and Challenges”, International Journala of Computer Networks(IJCN), vol3,Issue 5,(2011)

[5] S.S.Qureshi, T.Ahmad, K. Rafique and Shuja-ul-islam, “Mobile cloud computing as future for mobile applications-Implementation methods and challenging issues”, IEEE International Conference on Cloud Computing and Intelligence Systems(CCIS),(2011)September15-17.

[6]http://www.smartdevelopments.org//p=84

[7]https://wiki.cloudsecurityalliance.org/guidance/index.php/cloudcomputing-Architectural-Framework.