IN 3900-Independent Study
Final Report

Level 03

Security in Mobile Cloud Computing

A.R.M.Rifkhan
Reg no: 154101N

Supervisor : Mr.M.F.M.Firdhous

Faculty of Information Technology
University of Moratuwa
2018

Security in Mobile Cloud Computing

A.R.M.Rifkhan
Faculty of Information Technology
University of Moratuwa
rifkhanabdullah@gmail.com

***Abstract*—Nowadays Mobile Cloud Computing (MCC) become a very important technology in the world. Cloud computing (CC) allow to storing and accessing data through the internet. Nowadays smart phone users are increasing through the wireless technology increase. So CC become necessary thing to cloud applications and services for mobile users. These Mobile Cloud Computing help to remotely store data and demand applications you can purchase and you can maintain in your local hardware and your own software without any limitations. However, data security is a big thing in the MCC. Because this data security concern arise from the sensitive data stored people. This paper will discuss about the cloud computing concept , description of the MCC and different security issues suitable to the MCC atmosphere.**

Keywords—Cloud Computing (CC); Mobile Cloud Computing (MCC).

I. INTRODUCTION

Mobile devices are becoming a essential thing of human life. New technologies are growing in this new era. For example speech synthesis, augmented reality, image processing etc. Mobile devices need more memory capacity for include these technologies in to the mobile devices. But this is impossible because mobile device is a small device so researchers introduced a new thing that is called cloud computing. Cloud computing technology is changing the concept of converting the computer through the internet. Cloud computing services include highly valuable data centers. Varies resources are provided for use to needed by data centers.

Nowadays many users are using cloud computing through the mobile devices and world mobile data traffic grew 81 percent in 2013[6]. TechNavio's analysts prophet, the Company MCC market in North America increase at a Compound Annual Growth Rate(CAGR) of 18.12 percent in 2011-2015. One key factor contributing the demand for enterprise mobility[1]. Many mobile users download applications through the data centers like Play Store, App Store, iTunes and others.

Nowadays many mobile users using mobile computing. Many business firms and IT industries also using cloud computing. These business firms think about security of the cloud computing. Because these firm's data are highly secure data and hackers are increasing in the technology world.

Mobile cloud computing has 3 different components. Every components have security requirements. That 3 components are mobile terminal , mobile network and cloud service provider(CSP). Mobile terminal has many security issues for example SW Vulnerabilities , Malware etc. Mobile network component also has security issue , Malicious attack is the major threat in network component.

In this paper we will discuss about security analysis of mobile cloud computing. First we describe about mobile cloud computing. Then we will describe about mobile cloud computing security issues. In section 4 we will discuss about possible approaches for security problems in mobile cloud computing and solution of the security problems. Section 5 talk about the issues and finally talk about the conclusion in this paper.

II. MOBILE CLOUD COMPUTING

You need all organizations to change business needs require investing time with a high level IT budget. Such as accessories, applications and services. However, with IT's structural building structures may be slow and organizations often can't achieve the best use of IT infrastructure.

Cloud computing technology is changing the concept of converting the computer through the internet. Cloud computing services include highly valuable data centers. The provide varies resources for use to needed.

Business firms can only be connected to cloud and can find available resources to pay for the basis of use.

This is help for stop the capital expenditure and increase the infrastructure resources and decrease the business requirements.

Nowadays people have very busy work schedule so mobile devices came for reduce people work load. Now current world trend is customer getting mobile and CC services than enterprises. MCC has three different service models.

- Software as a Service (SaaS)

  SaaS is a software service provider. This service provider give through the internet to customers many software, software component and some other services. Gmail and Salesforce.com are provide this SaaS service to customers.

- Infrastructure as a Service (IaaS)

  Organizations get access to infrastructure such as storage capacity and computing power. Here the organization has control through host setting and application. This is included data bases , servers , storage devices. This is based layer in the cloud computing.

- Platform as a Service (PaaS)

  PaaS is providing development sites as a service. This software can be used for application software design , application software development or development testing , installation and hosting services. It also provide team connectivity , data saving integration , security , measurement , storage and many other services.

Several factors can present to the conclusion to introduce MCC. This MCC include excellence cloud computing, infrastructure, mobile internet, wireless and more etc. The MCC has enabled users to posses unlimited energy and online storage. MCC has come to be a model for the absolute elastic expansion of available features in mobile devices, everywhere wireless network access for cloud storage and compute resources, as well as dynamic contextual adaptation offset that varies with operating conditions. Sadly, mobile devices are functional, with limited memory, problematic connectivity, processing power, and low power consumption[3].

Mobile devices still have a problem that are need compute ability and need high storage. We want to increase the storage capacity need to be transferred to the cloud. most important thing is data security. In section 1 we talk about the MCC components. MCC has 3 different components one is mobile terminal next one is mobile network other one is cloud service provider. These three components will face the security issues. Recently many users using mobile cloud application. Such as virtual reality, image processing, augmented reality etc. and other hand we will be face many security issues through the mobile cloud applications. In this paper I will be point out that security issues.

III. Mobile Cloud Computing Securty Issues

When people need is increasing , likewise technology uses also increasing. Because of this , security issues also increasing in the MCC technologies. So we want to protect our data in mobile devices. This not only enough , because we are using cloud also we should protect cloud data also. “Figure 1 shows the data protection risks.”[6,2]

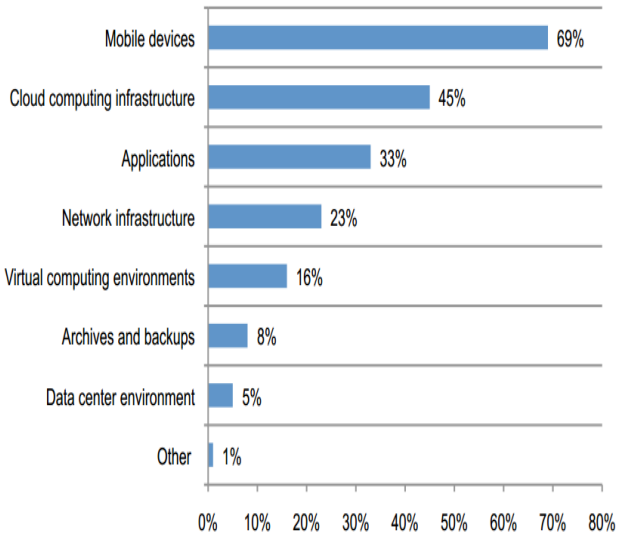

Figure 1: Data Protection Risks

Mobile Phones are becoming more modern and more attractive caution of malware designers. As a network enabled number Phone equipment continues to grow, the core threats of the internet grow the biggest problem of security, not only in the form of viruses and pipes, but also areas of destructive damage to identity strike and spam [6][4]
We can categorize main MCC security issues. Such as,

1. Mobile Terminal Security

Mobile terminal security issues are very serious issues. Because we can open OS, we can use third party software and we can access internet anytime and anywhere. We will talk about 2 security issues of mobile terminal.

- Malware
- Software Vulnerabilities

A. Malware

Malware is the harmful software in the mobile terminal. These malwares delete the personal files and data without user permission. Some antivirus companies like kespersky, Avast, Eset etc. have developed software for these malwares that is called antivirus. Malware spread many ways in the mobile terminals. For example 3G Networks, Emails, Bluetooth etc. We can divide many types of malware for example Trojan Horse, Bugs, Spyware etc.

B. Software Vulnerabilities

- Application

  Nowadays smart phones are the trending mobile terminals. Many users are using smart phones for file transfer between computer and phone. FTP is used for this process. When transferred the files through the network can illegal access the files. Because of this, personal information will be leakage and intentional delete.

- Operating Systems

  Operating Systems are very complexity software. This OS control software and also hardware. When attack the OS attackers can control hardware also. Because of this, mobile phones are used for destroy these operating systems by attackers.

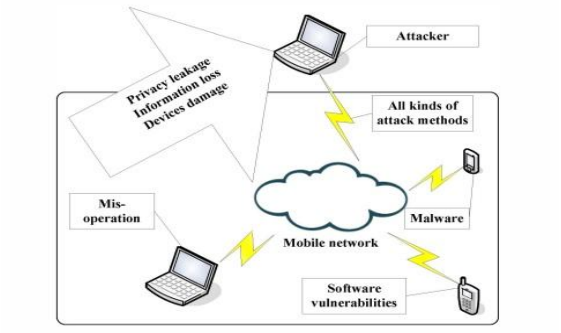

Figure 2 : Mobile Terminal Security issues

2. Mobile Network Security

Recently mobile devices have network nodes. These devices can access to network in many ways, for example SMS and 3G Networks. Nowadays all mobile devices are using network through the Wi-Fi and Bluetooth. We are using mobile devices through the many public Wi-Fi. Such as, University, Hospital and Shopping Complex etc. When people use the free public Wi-Fi people's important information will be steal by hackers and private Wi-Fi also has this security risks. Main reason is Wi-Fi's encryption mechanism is very low.

3. Mobile Cloud Security

A. Platform Reliability

Why attackers choose the cloud platform for steal the data? Because many people store the data in the cloud. So attackers decide when we attack the cloud we can get many information or data from the one place. that's way they are choose the cloud platform. This type of attacks will happen from external environment or internal environment, internal environment mean is cloud users or cloud platform members.

This type of attacks made for down the cloud service. DoS attack is the common one in this type[6]. When this attack happen that users do not have any backup firms to their data and they will face very risky loss. So cloud service providers should be increase their cloud security and users do not depend only the cloud service providers.

B. Data and Privacy Protection

This is the major issue in the cloud computing. They can't protect sensitive data in single way and need a fully security solution.

4. Cloud Threats

Users can't know all things about the cloud data and users can't control the cloud service activities. Cloud computing is the responsible for the cloud data. This cloud security divided to two groups one is cloud providers other one is cloud users. These security things maintain a legal agreement with users and cloud providers.

5. Infrastructure Issues

Infrastructure of the cloud computing has the possible burden in cloud computing. Attackers can attack many possible ways in the infrastructure of the cloud computing. for example unauthorized access, unauthorized authentication, virtual machine attack and phishing problem etc.

6. Cloud Architecture Issues

Cloud computing architecture has some issues and always data is a highly risks. Cloud computing architecture issue is the basic thing in CC. When create a cloud computing architecture that CC providers very carefully built security part in the architecture. Architecture issues have migration and internal sectors, high cost and service level. CC architecture should have resource consumption is very high and effective technology.

IV. Possible Approches For Security Issues

In section 3 we talk about the different security issues in MCC and in this section we will be describe about how to we solve that security issues. Mainly security issues deal with the cloud data, we have big challenge is secure the data. Above approaches will be help to protect the data.

- Mobile Terminal Security Issue

1. Anti-Malware

Mobile terminal attacked two ways by attackers. first one is malware detection by the anti malware then that malware will be remove. Malware detection can do the cloud. Because of this, we can increase the detection rate. cloud has any malwares anti-malware will be detect and remove from the cloud. This is the legal authenticated software. Cloud AV is a antimalware. this is perfect example for anti-malware. Cloud AV is doing detection in the mobile terminals. This is give some important benefits. For example, this is the best detection software, remove the vulnerabilities, improved deploy management and this is include many anti-virus engines. In one research said that is ten antivirus engine and two detection engines.

other way of the anti-malware protection is handling users. Because this malware spread by users. so we will discuss about this way of the anti-malware in the section User's Behaviors.

2. Software Vulnerabilities

When we update the mobile phone operating system we should be very carefully update that OS. Because many viruses are spreading this way. Every time OS companies introducing patches for that version OS. If we want to reduce the software vulnerabilities we should be check the software legitimacy before the software installation. That result is positive after we can install the software. This way we can reduce the software vulnerabilities.

3.User's Behaviors

Many malwares are spreading and attacking through the user's miss-operations. So we must do the many awareness programs to users. Mainly focus for that awareness program poor technology mind users. We should talk about spreading way of the malwares. For example, when any one send some links we don't open until what is the link has include, avoid new software, when we use the Bluetooth we must do very carefully. Many viruses are spreading Bluetooth and if we finished the sharing through the Bluetooth we must off the Bluetooth and Wi-Fi also like this.

- Network Security Issue

Network security issue are solved by two protected things. One is data encryption other one is security protocols. Encryption means when we send a message through the Messenger that message will become encrypt a unknown code. When that message receive by receiver that message will become decrypt which message sender sent. This process called encryption. Security protocols reduce many different attacks. This is the benefit of the security protocols.

- Cloud Security Approach

1. Protection of the PR (Platform Reliability)

Cloud providers should give two types of protection for their cloud users. First one is providers must integrate all security technologies. For example Virtual Private Network (VPN) technology, encryption and access control etc. When they integrate these kind of protection cloud will be protected from DOS attacks, data stealing

and other attacks. Second thing is cloud provider must give backup solution and also recovery. If any serious attacks will happen users can recover their data from backup. So these things will be increase users hope.

2. Data Encryption

Data encryption mean user's information stored cipher text form in cloud. When any attackers steal the data that data will not use them. Because all information changed cipher text. Current research said homomorphism algorithm is using on the cipher text processing[5].

3. Privacy Protection

Every government have already created their data protection plan and data protection strategy. British government introduced their data protection plan in 1998, European Union introduced their data protection strategies in 1995. Platform for Privacy preferences (P3P) is the example of protection plan. 40% of internet sites use this P3P technology for protect their details[6].

Security issues		Current approaches
Mobile terminal	Malware software	Detection and prevention CloudAV
	Software vulnerabilities (application software; operating system)	Installing the system patches Checking the software legitimacy and integrity
	Others(lack of security awareness, mis-operation)	Regulating the users' behavior
Mobile network	Information leakage or Malicious attack	Data encryption
		Security protocol
Mobile cloud	Platform reliability	Integrating the current security technologies; Key management and data encryption; Authentication and access control Privacy and data protection
	Data and privacy protection	

Figure 3 : Security Issues and Current Approaches

V. Discussion

MCC has access the network and this is implemented by three services such as Software as a Service(SaaS), Platform as a Service(PaaS) and Infrastructure as a Service(IaaS). These three services are together help to build a system in efficiency manner. When user use this system user can get many advantages through this system. But we have the big problem that is protection of the data. We was discussed about the security issues and possible approaches to protect mobile cloud computing.

VI. Acknowledgment

I would like to give my sincere gratitude to my Independent studies supervisor Mr.Firthous Mohamed, Senior Lecturer of Department of Information Technology, for his guidance and precise suggestions which inspired me on this accomplishment.

VII. Conclusion

This paper presents a review on different phases of security in MCC, Various research paper and journals are referred for this purpose. MCC is the most powerful technology in the world. We was discussed the MCC which security issues are already existing and how to provide possible approaches to solve this issues. User's data protection is the most challenging in the MCC.

References

[1] Khan, A., Othman, M., Xia, F. and Khan, A. (2015). Context-Aware Mobile Cloud Computing and Its Challenges. *IEEE Cloud Computing*, 2(3), pp.42-49.

[2] Shahzad, A. and Hussain, M. (2013). Security Issues and Challenges of Mobile Cloud Computing. *International Journal of Grid and Distributed Computing*, 6(6), pp.37-50.

[3] Z. Sanaei, S. Abolfazli, A. Gani, and R. H. Khokhar, "Tripod of requirements in horizontal heterogeneous mobile cloud computing," Proceedings of the 1st International Conference on Computing, Information Systems, and Communications, 2012.

[4] Waseem, M., Lakhan, A. and Jamali, I. (2016). Data Security of MCC on Cloud Server. OALib, 03(04), pp.1-11.

[5] Fernando, N., Loke, S. W., & Rahayu, W. (2012). MCC: A survey. *Future Generation Computer Systems, 29*, pp. 84-106.

[6] Hui Suo, Zhuohua Liu, Jiafu Wan, Keliang Zhou, "Security and Privacy in Mobile Cloud Computing"