A CRITICAL AND COMPARATIVE STUDY OF SECURITY AND PRIVACY ON CHALLENGES IN MOBILE CLOUD COMPUTING

[1]Vijayakumar S, [2]Amutha R

[1]Associate Professor, [2]II MCA Student,
[1 2]Department of Computer Applications,
[1 2]Priyadarshini Engineering College, Vaniyambadi, Vellore, Tamilnadu, India

ABSTRACT: Cloud computing technology has brought great opportunity to the development of mobile cloud computing. However it is also facing unprecedented challenges. The mcc combination of three main part mobile device, mobile computing and mobile internet There are number of loopholes and challenges exist in the security policies of mobile cloud computing. Numerous reaches indicates various security and privacy issues that are related to mcc .This paper analysis and compare various possible approaches of security and privacy issues in mcc The importance of cloud computing is increasing and it is receiving a growing attention in the scientific and industrial communities. This paper also discuss about the security and privacy issues and vulnerability affecting cloud computing system.

IndexTerms: Cloud computing, mobile cloud computing information, mobile cloud security, vulnerability, privacy, mobile device, mobile remote, challenges.

1. INTRODUCTION

Mobile cloud computing is the mobile computing and cloud computing .This provides full access to all technology resource through the cloud “Anytime” , ”Anywhere ”, “Any how”. A mobile cloud computing is a model device capabilities via ubiquities wireless access to cloud storage and computing resource with change in operating condition. The mcc is becoming a new hot technology. With the development of the mobile cloud computing new security issues are there which need more security approaches. The information technology will not only change the way of the world. The cloud computing has been used and promoted in the field of HealthCare, manufacturing, financial service, energy communication and other key areas which will play an important role for improving the efficient use of resource information and integration. The service model in cloud

1. Software or Application as a service (SaaS),
2. Platform as a Service (PaaS),
3. Infrastructure as a Service (Iaas)

Mobile cloud computing: Cloud computing is a general term for the delivery of hosted services over the internet. Mobile cloud application more the computing power and data storage and mobile computing not only to smart phone user. Which run an the devices and or remote server via wireless networks a powerful trend in develop of it technology. Could computing application cloud based server e.g: Mobile Email, Google Maps, Google cloud print, other Apps.,

2. SECURITY ARCHITECTURE OF MOBILE CLOUD COMPUTING (MCC)

Protecting user privacy and data/application secrecy from adversary is a key to establish and maintain consumers’ trust in the mobile platform, especially in MCC. A general architecture in a broader sense depicted in end to end mcc security architecture.

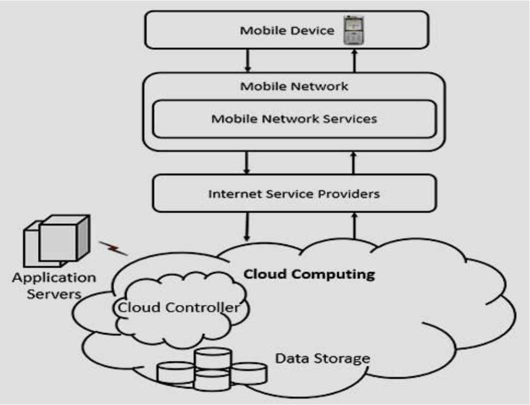

Fig 2.1 End to End Mobile Cloud Computing Security

Architecture The security related issues in MCC are introduced in two categories: the security for mobile users and the security

The security related issues in mcc are introduced two categories: the security for mobile users and the security for data.

2.1. Security for mobile users

Mobile devices such as cellular phone, PDA, and Smartphone are exposed to numerous security threats like malicious codes (e.g. Virus, Worm, and Trojan horse) and their vulnerability.

Security data on Clouds: Although both mobile users and application developers benefit from storing a large amount of data/applications on a cloud, they should be careful of dealing with the

data/ applications in terms of their integrity, authentication, and digital rights .

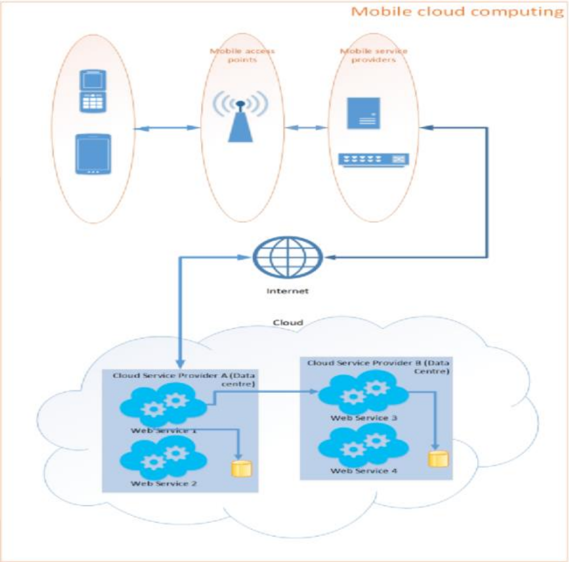

fig:2.2 Architecture of Mobile Cloud Computing

3. TYPES OF SECURITY ISSUES

3.1. Data Ownership

Cloud computing provides the facility to store the personal data and purchased digital media such as e-books, video and audio files remotely. For a user, there is a chance of risk to lose the access to the purchased media data. To avoid these types of risks, the user should be aware of the different rights regarding the purchased media.

3.2. Privacy

Privacy is one of the biggest challenges in the mobile cloud computing environment. Third party companies may sell this important information to some government agencies without the permission of the user. For example: Mobile devices use location based services which help their friends and other persons to get the updates about the location of the user.

3.3. Security Issues

Mobile devices are famous for malicious code. There are many chances to lose or steal the data because Mobile devices are mostly unprotected. An unauthorized person can easily access the information stored on the mobile devices. The top mobile threats that affect security are mentioned as under

.

4. SECURITY AND PRIVACY CHALLENGES IN MCC:

The MCC utilizes many traditional as well as recent technologies such as partitioning, offloading, virtualization, outsourced storage, and mobile-cloud based application etc., and it adopts several new security challenges along with traditional challenges. In this section, we present the list of potential security and privacy challenges within MCC. The challenges are discussed as following categories.

Data security challenges: The major data security challenge is introduced as the consequence of mobile users ‘data is stored and processed at clouds that are located at service providers ‘ends. The data related challenges include data loss, data breach, data recovery, data locality and data privacy. The data loss and data breach break two security requirements such as integrity and confidentiality. Here, the data loss means the users ‘data is in error condition that damaged or skipped by any physical means during processing, transmitting or storage. In data breach situation, users ‘data is stolen, copied or used by any other unauthorized users. These two can be occurred by malicious insider or from outside through malicious applications. The data recovery problem is another concern. This is a process of recovering the data from damaged, failed, corrupted or lost mobile user data or from physical storage device. Extend the storage capacity, mobile users lose the physical control of their data simultaneously. Thus, the correctness of the data becomes one of the concerns for mobile users in cloud storage scenario.

Partitioning and offloading security challenges: During offloading process, there requires to access to cloud through wireless networks. Since the mobile users do not have any access and control over their offloading processes, hence, there is a risk of unauthorized access to offloaded content. And due to the offloading content executions are done within the cloud or edge servers instead of mobile device, there is also possibility to violate the integrity and confidentiality of offloaded contents. The integrity challenge arises due to after execution of offloaded content, if the result is not correct or altered, the mobile devices can not verify easily the correctness of the results. However, other challenges include availability attack and malicious content threats. Virtualization security challenge: MCC, the cloud service providers offer cloud services using virtualization techniques to the mobile users. In cloud end, an image of virtual machine (VM) of the mobile device is pre-installed and the tasks of the mobile device are offloaded to the VM for processing. This VM is also called thin VM or phone clone. The main function of virtualization is to provide several VMs running in a same physical machine or mobile devices and the VMs are isolated from each other. An additional layer called hypervisor or VM Monitor or Manager (VMM) is software that allows creating, running and controlling VMs and its other virtual subsystems.

Mobile cloud applications security challenges: The cloud based mobile application level attacks can affect the integrity and confidentiality of both the data and applications by different strategies, for example, integrating malware. The malwares such as virus, worm, Trojan, rootkit, botnet (Arab and Praga no, 2013) are unfavorable, contrary, intrusive, bothering applications or programmed codes. The targets of these malwares are to run with intentions at mobile devices or attach with applications without users ‘compliances.

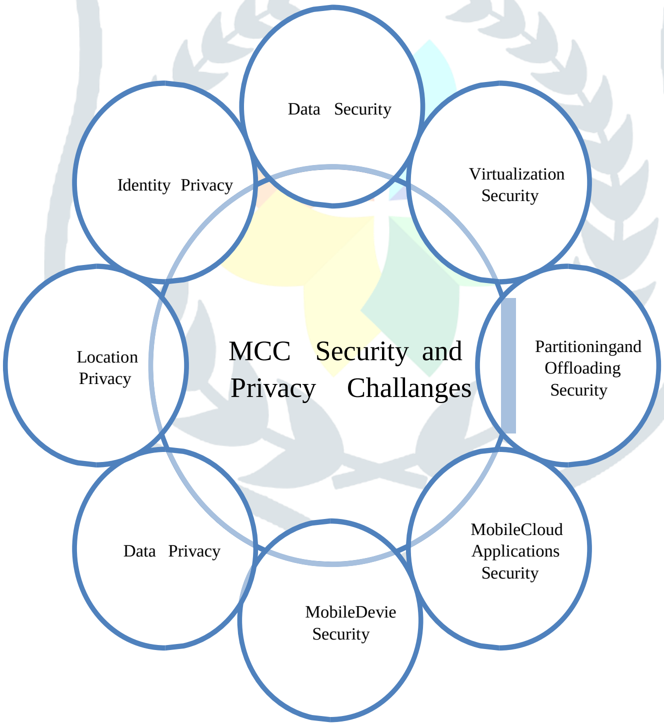
Data Security
Identity Privacy
Virtualization Security
Location Privacy
MCC Security and Privacy Challanges
Partitioningand Offloading Security
Data Privacy
MobileCloud Applications Security
MobileDevie Security

Fig 4.1 The Main security and privacy in mcc :

Mobile devices security challenges: There are some physical threats to mobile devices. It is possible to loss, leakage, access or unintentionally disclose of the data or applications to unauthorized users, if the mobile devices are misplaced, lost or theft. Although there are password or pattern based locked features; many mobile users do not use these features. And the identity module card inside the mobile device also can be taken aside from device and accessed by unauthorized persons. Moreover, most of mobile devices are lack of security mechanism against threats. The attackers can attack by utilizing different avail-ability attack techniques such as by sending high malicious traffic stream, huge messages to targeting mobile devices to make unused or reducing the capability. Attentions here Consequently, the malwares are serious security concerns for mobile users ‘privacy, application.

Privacy challenges: Privacy is one of the major challenges as the mobile users ’confidential data or applications are processed and shifted from mobile devices to the heterogeneous distributed cloud servers while availing different cloud services.

These servers are located at different places that are owned and maintained by the service providers only. Here, the users can not physically be worth the storage of their data and thus, data privacy and protection related challenges are in the hands of service providers, and the users are not accountable for privacy lost. Cloud storage and processing in multiple locations raise privacy problems. The cloud servers of service providers are located at different regions and countries. For example, Google's cloud servers are located almost around the world such as seven locations in Americas, two locations in Asia and three locations in Europe (Online, 2016), (Online,2016).

5. SERVICE MODEL IN CLOUD

According to NITS, cloud computing services can be readily broken down into three layered services models.

1. Software application as a service (SaaS).
2. Platform as a services (paaS).
3. Infrastructure as a services (IaaS).

5.1. Software as a service

The capabilities provided to the end users is to use the providers application running on the cloud infrastructure .The application are accessible from various line devices through a thin client interface such as a web browser (e.g., web enabled e-mail. The end user does not manage or control the underline cloud infrastructure including network, servers, operating system, storage, or even individual application capabilities, with the possible exception of limited use specific application configuration settings .Today SaaS is offered by companies such as Google, sales force, Microsoft, Zoho, etc.

5.2. Platform as a service

It is the delivery of computing platform and solution stack as a service. The end user does not manage or control the underlying cloud infrastructure including network, server, operating system, or storage. PaaS provider of a refined combination of OS and application servers, such as WAMP platform (window, Apache, MySQL, and PHP),LAMP platform (Linux, Apache, MySQL and PHP),and XAMP(cross platform) etc are some of the popular PaaS examples

5. 3.Infrastructure as a service

This model provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data center space etc. are pooled and made available to handle workloads. The capability provided to the customer is to rent processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has the control over operating systems, storage, deployed applications, and possibly select networking components

We can briefly summarize the various security issues in the mobile cloud computing paradigm as follows:

Privacy and confidentiality: Given the amount of personal data stored in mobile phones, data privacy becomes a key issue in mobile cloud scenarios. Privacy of cloud-stored data can be possibly breached by multiple entities including cloud vendors, other users and malicious attackers. In many cases Service Level Agreements are required to provide clauses which prevent cloud vendors from surreptitiously accessing private user data and selling it to third parties without authorization.

5.4. Data Migration

Data, often sensitive in nature, is offloaded to the cloud. The exact physical location of data may not be transparent which could lead to complications in jurisdiction scope and privacy commitments. The loss of physical control over the storage of data, combined with multi- tenancy of shared storage devices, potentially with domain competitors can be unnerving for the customers.

5.5. Integrity

Data integrity makes sure that the data remains consistent and accurate; it is guarded from illegitimate updates. This is of prime importance in a mobile cloud computing environment where the data could be distributed across multiple data centers, possibly in different geographic locations.

5.6. Data Ownership

Specifically in the case of purchased digital media, data ownership is an often- debated issue in mobile cloud computing. Today, users can purchase access to media content using a service; even after purchase, the content may be stored remotely rather than locally. This could give rise to contentions on copyright and ownership issues later, if not carefully handled.

5.7. Security and access

Data access and availability becomes key issues in mobile cloud environments as vast majority of data is stored in remote locations. With ever-increasing mobile user requests to access cloud resources, efficient network connectivity and seamless data availability are critical.

5.8. Authentication

A related problem is establishing the right data security mechanisms to ensure that only entities with the verified credentials are allowed to access and modify the data. It is the process of confirming the identity of the user who attempts to access a resource or service. It is of prime importance in the mobile cloud computing scenario and in the following sections, we attempt to examine a few traditional and novel mechanisms for authentication in MCC.

6. ARCHITECTUR AND CLOUD ISSUCES MODEL

Apart from data and information security, the mobile cloud computing have some general issues in terms of their architecture are highlighted below.

1. Computing off-loading
2. Security for Mobile Users/Applications/Data
3. Improvement in Efficiency Rate of Data Access
4. The Context Aware Mobile Cloud Services
5. Migration and Interoperability
6. Service Level Agreement (SLA)
7. Cost and Pricing

The cloud computing service delivery model has its own issues which are highlighted below. IaaS model security issues:

1. Virtual Machine Security
2.Virtual Machines images repository
3. Virtual network security

PaaS model security issues:

1. Structured Query Language related
2. Application Programming Interface Security

SaaS model security issues:

1. Data Security Management
2. Web Application Vulnerability and Scanning

7. CONCULSION

This paper investigates the concepts of mobile cloud computing (mcc),challenging security issues and privacy breaches, assorted subsisting security framework and conclusively some solution that increase the security in Mobile Cloud Environment. Data privacy and application that utilities cloud are the most challenges factor. To procure more security in mobile cloud environment, thread need to be addressed and accordingly. Cloud computing is clearly one of the most enticing technology areas of the current times due at least in part to its cost_ efficiently and flexibility. Security and privacy are in of the most challenges issues in mcc. The limited processing power and memory of a mobile device dependent on inherently unreliable wireless channel for communication and battery for power leaves little scope for a reliable security layer.There is a need for a secure communication channel between cloud and the mobile device. The secure routing protocols can be used to protect the communication channel between the mobile device and cloud. We also need to address issues pertaining to data security, network security, data integrity, authentication, authorization and access control. In the future, our research work focus on to propose a security model framework to enhance security and privacy in MCC. Deposit its advantage, many organization are still not adopting it because of security reasons associated with it. This paper analyzed the problem of security associated with cloud. Encryption is the foremost option for security the data and this paper highlights comparative analysis of symmetric as well as asymmetric encryption algorithm for providing security in cloud computing system.

8. REFERENCES

[1] R. Buyya, “Introduction to the IEEE Transactions on Cloud Computing,” IEEE Transactions on Cloud Computing, vol. 1, no. 1, 2014, pp. 3-9. 19. H. Hu, Y. Wen, T.S. Chua and X. Li, “Toward Scalable Systems for Big Data Analytics: A Technology Tutorial,” IEEE Access, vol. 2, 2014, pp. 652-687.

[2] Oberheide, J., Veeraraghavan, K., Cooke, E. and Jahanian, F.2008, Virtualized in-cloud security services for mobile devices. In Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt), 31- 35. Zhang, X., Schiffman, J.,. Gibbs S, Kunjithapatham, A., and Jeong S.2009, Securing elastic applications on mobile devices for cloud computing. In Proceeding ACM workshop on Cloud computing security, CCSW ’09, Chicago, IL, USA.

[3] Xiao, S. and Gong , W.,2010. Mobility can help: protect user identity with dynamic credential. In Proceeding 11th International Conference on Mobile Data Management, MDM ’10, Missouri, USA, May 2010.

[4] IBM 2013 Annual Report, “The IBM Strategy: We are remaking enterprise IT for the era of cloud,” Available at https://www.ibm.com/annualreport/2013/strategy- cloud.html

[5] International Data Corporation (IDC) Worldwide Quarterly Cloud IT Infrastructure Tracker,

[6] “Worldwide Cloud IT Infrastructure Market Growth Expected to Accelerate to 21% in 2015, Driven by Public Cloud Datacenter Expansion, According to IDC,” Press Release, 21 April 2015.

[7] S. O. Kuyoro, F. Ibikunle and O. Awodele, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), vol. 3, Issue 5, (2011).

[8] K. opovi and Z. Hocenski, "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of the 33rd International Convention, (2010) May 24-28.

[9] Rajashri Khanai, G. H. Kulkarni, "Crypto-Coding as DES-Convolution for Land Mobile Satellite Channel", International Journal of Computer Applications © 2014 by IlCA Journal Volume 86 - Number 18 Year of Publication: 2014.

[10] Honggang Wang, Shaoen Wu, Min Chen, Huazhong ,Wei Wang, Secunty Protection between Users and the Mobile Media Cloud" IEEE Communications Magazine ,Volume 52,issue 3, March 2014

[11] Dr. Vineet Shanna, Preeti Garg “An Efficient and Secure Data Storage in Mobile Cloud Computing through RSA and Hash Function” 978-1- 4799-2900-9 ©2014 IEEE