Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 7; October, 2014 pp. 83-86
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Analysis of Security Issues for Mobile Cloud Computing

Shuchi Srivastava

Northern India Engineering College, Shastri Park, Delhi

Abstract: **Today the capabilities of mobile devices have improved in terms of speed, computing power, real world user friendly applications, storage and feature support. Nowdays, the storage capacity can tremendously be increased with the use of cloud computing. Cloud computing is a flexible, cost effective and proven delivery platform for providing business or consumer IT services over internet.**

Mobile cloud computing means the availability of cloud computing services in a mobile environment . It is a combination between mobile network and cloud computing, thereby providing optimal services for mobile users. However, a lot of risk is associated if the storage and data processing are migrated from the mobiles to clouds. User's privacy and integrity of data and applications is one of the key issues most of the cloud provider give attention. This paper discusses the various security issues for mobile cloud computing .It also identifies the main vulnerabilities in these types of systems and the preventive measures that could be taken to deal with such problems . To attain more security in mobile cloud environment, threats need to be addressed and studied.

Keywords: **Mobile cloud computing, cloud computing, architecture of mobile cloud computing, security issues**

1. INTRODUCTION

Mobile cloud computing technology is growing rapidly among the users due to anywhere anytime data access. At present there is a wide range of mobile cloud applications available. These applications fall into different areas such as image processing, natural language processing, shared GPS, shared Internet access, sensor data applications, querying, crowd computing and multimedia search. Even though there are a large number of benefits of mobile computing, yet there are a number of security issues that not be addressed.

2. CLOUD COMPUTING

Cloud computing is a flexible and cost effective method for providing business or consumer IT services over the internet. With this technology, the essential sources of a business is often outsourced to a third party, which causes a threat to the security and privacy of data.

Cloud computing can also be defined as Common Location Independent Online Utility on Demand. The main objective of cloud computing is to increase the capacity and capability of client devices by accessing leased infrastructure and software applications instead of owing them.

3. CLOUD SERVICES

Generally cloud services can be divided into three categories:

Software-as-a-Service (SaaS): SaaS can be described as a different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; ontinuing operation, safeguarding and support .

Platform as a Service (PaaS): PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications.

The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com.

Infrastructure as a Service (IaaS): Infrastructure as a service(IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using

Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud.

4. MOBILE CLOUD COMPUTING

Mobile computing means using portable devices to run stand-alone applications **and/or accessing remote applications via** wireless networks.

In mobile cloud computing mobile network and cloud computing are combined, thereby providing an optimal services for mobileusers.Data are kept on the internet rather than on Individual devices, providing on-demand access. Applications are run on a remote server and then sent to the user . Figure below shows an overview of the mobile cloud computing architecture.

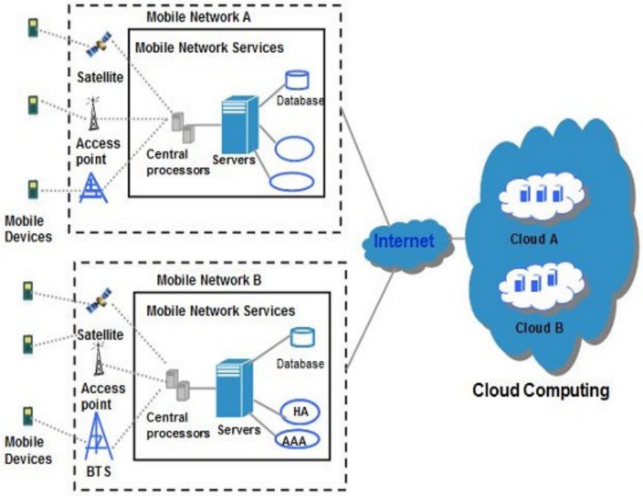

Fig1. Mobile Cloud Computing Architecture

The architecture of mobile cloud computing is shown in the Figure 1. Here the Mobile devices connect to the mobile wireless network base stations. Some base stations are Satellite and Base Transceiver Station (BTE). They act as the interface which establishes the network connection between the mobile devices and the internet. User requests are sent through the wireless network to access the cloud server by Authentication, Authorization and Accounting (AAA) mechanism. After the delivery of user requests to the cloud, the cloud controllers process those requests to provide users with the corresponding cloud services.

3.1 Characteristics of Mobile Cloud Computing

The characteristics of MCC can be described as agility, scalability, reliability, security, reduced cost and reduced maintenance.

3.2 Mobile Security Service Layers

The security services in mobile ecosystem are divided into three different layers.

1. *Backbone layer* - The backbone layer constitutes the security surveillance on cloud physical systems. This helps in monitoring the servers and machines in the cloud infrastructure.

2. *Infrastructure layer* - The infrastructure layer monitors the virtual machines in the cloud. Various activities such as Storage verification, VM migration, Cloud Service Monitoring, VM Isolation, Risk Evaluation and Audits are carried out in this layer to secure cloud host services.

3. *Application and Platform layer* - Application layer performs activities such as user management, key management, authentication, authorization; encryption and data integration. According to a recent survey, 73% of IT Executives and Chief Executive Officers are unwilling to adopt cloud services due to the associated risks with privacy and security. To attract consumers, the cloud service provider (CSP) has to target all the security issues to provide a highly secure environment.

5. MOBILE CLOUD COMPUTING SECURITY

Since mobile cloud computing is a combination of mobile networks and cloud computing, the security issues can be divided into

A. Mobile network user's security

Numerous security vulnerabilties and threats such as malicious codes are known to the different mobile devices such as Smartphones, PDAs, cellular phones, laptops, and the like. Some applications to these devices can cause privacy issues for mobile users . There are two main issues concerning the subscriber's security.

1. *Security for mobile applications:* The simplest ways to detect security threats will be installing and running security software and antivirus programs on mobile devices. But since mobile devices are constrained with processing and power limitations, protecting them from these threats could be more difficult compared to regular computers. Several approaches have been developed transferring threat detection and security mechanisms to the cloud. Before mobile users could use a certain application, it should go through some level of threat evaluation. All file activities to be sent to mobile devices will be verified if it is malicious or not. Instead of running anti-virus software or threat detection programs locally, mobile devices only performs lightweight activities such as execution traces transmitted to cloud security servers.

2. *Privacy*: Providing private information such as indicating your current location and user's important

information creates scenarios for privacy issues. For example, the use of location based services (LBS) provided by global positioning system (GPS) devices. Threats for exposing private information could be minimized through selecting and analyzing the enterprise needs and require only specified services to be acquired and moved to the cloud.

B. Security Issues in Cloud

There are nine major threats to security in clouds known as the notorious nine.

1. Data Breaches
2. Data Loss
3. Account or Service traffic hijacking
4. Insecure interfaces and APIs
5. Denial of Service Ranks
6. Malicious insiders
7. Cloud Abuse
8. Insufficient Due delligence
9. Shared technology vulnerabilities

6. SECURITY MEASURES IN MOBILE CLOUD COMPUTING

Since the security issues fall in two categories, the security measure is also described as:

A. Mobile network user's security:

1. Don't leave your mobile device unattended;
2. Protect Your Device with Passwords: Enable your device's power-on login, system login authentication, and password-protected screen saver.
3. Disable Wireless Connection When It Is Not In Use: Wi-Fi, infrared, and Bluetooth devices are constantly announcing their presence if they are enabled.
4. Protect your device with anti-virus software using the latest virus definitions.
5. Remove Your Preferred Network List When Using Public Wireless Service.
6. Encrypt Your Wireless Traffic Using a Virtual Private Network (VPN).
7. Turn off Ad-Hoc Mode Networking.
8. Turn off Resource Sharing Protocols for Your Wireless Interface Card

B. Measures for cloud Security:

The data can be encrypted to reduce the impact of a breach, but if the encryption key is lost, the data is also lost. However, if offline backups of the data are kept to reduce data loss, the exposure to data breaches increases.

A malicious hacker might delete a target's data out of spite -- but then, the data could be lost to a careless cloud service provider or a disaster, such as a fire, flood, or earthquake. Compounding the challenge, encrypting the data to ward off theft can backfire if the encryption key is lost.

The key to defending against this threat is to protect credentials from being stolen. Organizations should look to prohibit the sharing of account credentials between users and services, and they should leverage strong two-factor authentication techniques where possible.

IT admins rely on interfaces for cloud provisioning, management, orchestration, and monitoring. APIs are integral to security and availability of general cloud services. From there, organizations and third parties are known to build on these interfaces, injecting add-on services. "This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency".

DoS outages can cost service providers customers and prove pricey to customers who are billed based on compute cycles and disk space consumed. While an attacker may not succeed in knocking out a service entirely, he or she "may still cause it to consume so much processing time that it becomes too expensive for you to run and you'll be forced to take it down yourself".

From **IaaS** to **PaaS** to SaaS, the malicious insider has increasing levels of access to more critical systems and eventually to data. In situations where a cloud service provider is solely responsible for security, the risk is great. "Even if encryption is implement, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack, " according to CSA.

Organizations embrace the cloud without fully understanding the cloud environment and associated risks. For example, entering the cloud can generate contractual issues with providers over liability and transparency. What's more, operational and architectural issues can arise if a company's development team isn't sufficiently familiar with cloud technologies as it pushes an app to the cloud. CSA's basic advice is for organizations to make sure they have sufficient resources and to perform extensive due diligence before jumping into the cloud.

"Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models, " according to the report.

The information on cloud can thus be secured by-

- *Authentication* - The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
- *Authorization* - Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth)
- *Encryption* - The translation of data into a secret code. Encryption is the most effective way to achieve data security
- *Integrity*- Every mobile cloud user must ensure the integrity of their information stored on the cloud. Every access they make must me authenticated and verified. Different approaches in preserving integrity for one's information that is stored on the cloud is being proposed. For example, every information stored by each individual or enterprise in the cloud is tagged or initialized to them wherein they are the only one to have access (move, update or delete) such information. Every access they make must be authenticated assuring that itis their own information and thus verifying its integrity.
- *Legal Provision*- Distribution and piracy of digital contents such as video, image, audio, and e-book, programs should becriticized. The solutions to protect these contents from illegal access are applied such as encryption anddecryption keys to access these contents.

7. CONCLUSION

Mobile cloud computing is a technology that combines the advantages of mobile networks and cloud computing. Cloud computing offers on-demand network access to a shared pool of computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This paper discusses mobile cloud computing, its architecture, characteristics and the various security issues associated with it. It also deals with the measures to be taken for the prevention of the security problems.

REFERENCES

[1] D. Huang, Z. Zhou, L. Xu, T. Xing and Y. Zhong, "Secure Data Procesing Framework for Mobile Cloud Computing", IEE EINFOCOM 2011 Workshop on Cloud Computing, 978-1-424-920-5/1/$26.0 ©2011 IEEE, (2011) p. 620-624.

[2] S. Morrow, "Data Security in the Cloud", Cloud Computing: Principles and Paradigms, Edited by Rajkumar Buyya, James Broberg and Andrzej Goscinski Copyright 2011 John Wiley & Sons, Inc., (2011) pp. 573-592.

[3] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing, " Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[4] B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues, " 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[5] Mahadev Satyanarayanan, "Mobile computing: The next decade, " Proc. 11th Intl. Conf. on Mobile Data Management (MDM'10), Kansas, MO, 2010.

[6] http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428

[7] Marcus, A. and Maletic, J. I., "Recovering Documentation-to-Source-Code Traceability Links using Latent Semantic Indexing", in Proceedings 25th IEEE/ACM International Conference on Software Engineering (ICSE'03), Portland, OR, May 3-10 2003, pp. 125-137.

[8] Salton, G., Automatic Text Processing: The Transformation, Analysis and Retrieval of Information by Computer, Addison-Wesley, 1989.

[9] Anand Surendra Shimpi and R. Chander, "Secure Framework in Data Processing for Mobile Cloud Computing" International Journal of Computer & Communication Technology, ISSN (Print) 0975- 7449, vol. 3, Iss. 3, 2012.

[10] Soeung-Kon(Victor) Ko1), Jung-Hoon Lee2), Sung Woo Kim3), "Mobile Cloud Computing Security Considerations", Journal of Security Engineering,

[11] V.Gayathri, , G.Nithya., , K.S.Saravanan, M.Jothilakshmi, "Protection Issues in Mobile Cloud Computing", INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS, Vol.2 Issue.1, Pg.: 93-98, January 2014