International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 3 (May-June, 2016), PP. 279-282

MOBILE CLOUD COMPUTING: ARCHITECTURE AND SECURITY ISSUES

Shakti Shivalingam[1], Ranjana Rai[2]
Thakur Institute Of Management Studies & Research Kandivali(East)
Mumbai 400101
e.shiva.shakti@gmail.com

Abstract— **Mobile Cloud Computing (MCC) has revolutionized the way in which mobile subscribers across the globe leverage services on the go. As MCC is still at the early stage of development, it is necessary to grasp a thorough understanding of the technology in order to point out the direction of future research. . MCC integrates cloud computing into the mobile environment and overcomes obstacles related to performance (e.g. battery life, storage, and bandwidth), environment (e.g. heterogeneity, scalability, availability) and security (e.g. reliability and privacy).**

I. INTRODUCTION

The market of mobile phones has expanded rapidly. According to Cisco, the premier global market intelligence firm, the worldwide Smartphone market is expected to grow from 32% to 40% year over year from 2015 to 2020. The growth of mobility has changed our lives fundamentally in an unprecedented way is depicted in fig(1).

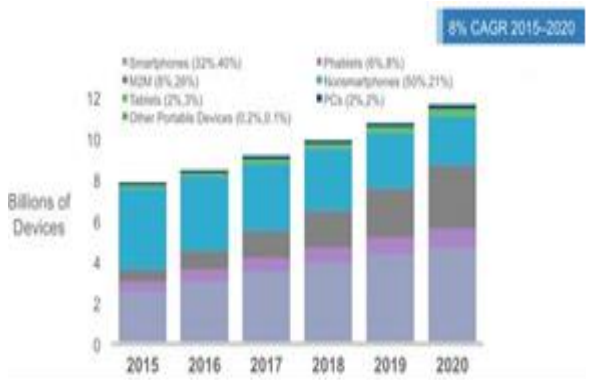

Fig 1

Seemingly the number of mobile user has increased from normal Pc users. As an inheritance and development of cloud computing, resources in mobile cloud computing networks are virtualized and assigned in a group of numerous distributed computers rather than in traditional local computers or servers, and are provided to mobile devices such as Smartphone's, portable terminal, and so on as shown in fig(2).

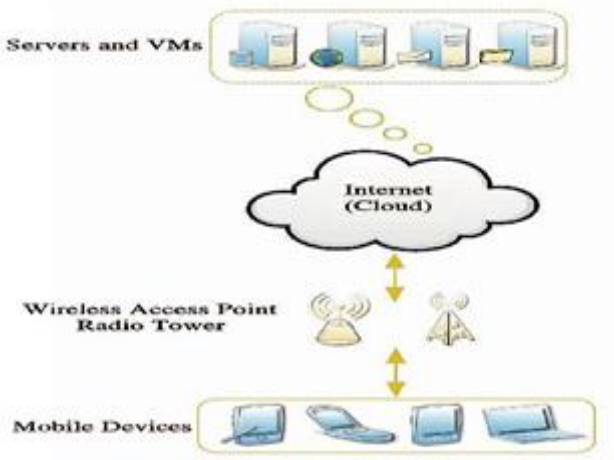

Fig 2

II. BACKGROUND

As a development of Cloud Computing and Mobile Computing, Mobile Cloud Computing, as a new phrase, has been devised since 2009.

I Essential Characteristics

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

II Service Models

A cloud computing is a large-scale distributed network system implemented based on a number of servers in data centers. The cloud services are generally classified based on a layer concept (Fig.3). In the upper layers of this paradigm, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are stacked.

Fig 3

• Data centers layer: This layer provides the hardware facility and infrastructure for clouds. In data center layer, a number of servers are linked with high-speed networks to provide services for customers. Typically, data centers are built in less populated places, with a high power supply stability and a low risk of disaster.

• Infrastructure as a Service (IaaS): IaaS is built on top of the data center layer. IaaS enables the provision of storage, hardware, servers and networking components. The client typically pays on a per-use basis. Thus, clients can save cost as the payment is only based on how much resource they really use. Infrastructure can be expanded or shrunk dynamically as needed. The examples of IaaS are Amazon EC2 (Elastic Cloud Computing) and S3 (Simple Storage Service)

. • Platform as a Service (PaaS): PaaS offers an advanced integrated environment for building, testing Accepted in Wireless Communications and Mobile Computing

• Software as a Service (SaaS): SaaS supports a software distribution with specific requirements. In this layer, the users can access an application and information remotely via the Internet and pay only for that they use. Salesforce is one of the pioneers in providing this service model. Microsoft's Live Mesh also allows sharing files and folders across multiple devices simultaneously.

III. Mobile Cloud Computing Architecture

The mobile cloud computing is a combi-nation of the two technologies, a development of distributed, grid and centralized algorithms, and have broad prospects for application

"Mobile Cloud Computing at its simplest, refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smartphone users but a much broader range of mobile subscribers"

I Concept and principle

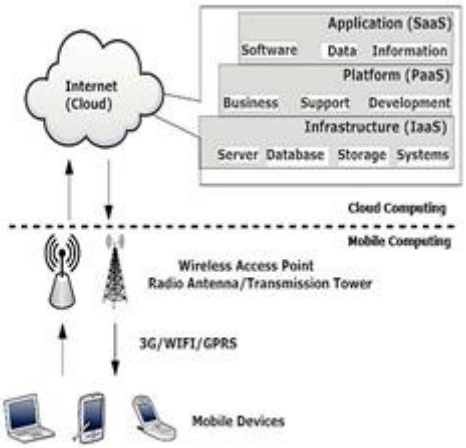

Fig 4

As shown is the Fig 4. , mobile cloud computing can be simply divided into cloud computing and mobile computing. Those mobile devices can be laptops, PDA, smartphones, and so on. which connects with a hotspot or base station by 3G, WIFI, or GPRS. As the computing and major data processing phases have been migrated to 'cloud', the capability requirement of mobile devices is limited, some low-cost mobile devices or even non-smartphones can also achieve mobile cloud computing by using a cross-platform mid-ware. Although the client in mobile cloud computing is changed from PCs or fixed machines to mobile devices, the main concept is still cloud computing. Mobile users send service requests to the cloud through a web browser or desktop application, then the management component of cloud allocates resources to the request to establish connection, while the monitoring and calculating functions of mobile cloud computing will be implemented to ensure the Quality of Service(QOS) until the connection is completed.

IV. CHALLENGES AND SOLUTIONS

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

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. 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.

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: WiFi, 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 multicustomer 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 multiuser 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.

V. OPEN RESEARCH ISSUES

A. Energy efficiency

Owing to the limited resources such as battery life, available network bandwidth, storage capacity and processor performance, on the mobile devices, researchers are always on the lookout for solutions that result in optimal utilization of available resources.

B. Better service

The original motivation behind MCC was to provide PC-like services to mobile devices. However, owing to the varied differences in features between fixed and mobile devices, transformation of services from one to the other may not be as direct.

C. Task division

Researchers are always on the lookout for strategies and algorithms to offload computation tasks from mobile devices to cloud. However, due to differences in computational requirement of numerous applications available to the users and the variety of handsets available in the market, an optimal strategy is an area to be explored.

VI. 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] https://mumscomputing.wordpress.com/2012/05/08/defining-the-essential-characteristics-of-the-cloud-mobile-cloud- computing/

[2] http://www.datacenterknowledge.com/archives/2011/05/09/the-mobile-cloud-what-it-is-why-it-matters/

[3] http://www.computerweekly.com/news/2240037496/Overcoming-mobile-cloud-computing-challenges-with-distributed-apps

[4] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6215350&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6215350

[5] http://www.slideshare.net/prasaugus/prassanna-session-i

[6] https://www.eecis.udel.edu/~cshen/859/papers/survey_MCC.pdf

[7] http://www.krishisanskriti.org/vol_image/02Jul201506075820.pdf

[8] http://www.ijeit.com/Vol%203/Issue%201/IJEIT1412201307_73.pdf

[9] https://www.eecis.udel.edu/~cshen/859/papers/survey_MCC.pdf

[10] http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085

[11] https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

[12] https://cloudsecurityalliance.org/group/top-threats/