THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Mobile Cloud Computing and Security Challenges

SAID, Kabir Sulaiman
Computer Analyst, Department of MIS, Kano University of Science & Technology, Nigeria
Usman Saadu
Education Officer, Department of Sciences, Federal Government College, Nigeria

Abstract:
Cloud computing is gaining a tremendous momentum and transmogrifying many interconnected systems by providing social organization with computing resources that features easy computerization, connectivity, scalability, construction and stationing. Altogether it creates extensive variety of privacy and security concerns which need to be addressed.

Keywords: *Mobile cloud computing, security, privacy, virtualization*

1. Introduction

There is a lot of confusion in the IT communities regarding how cloud technology differs from the existing model and how the difference affects its adoption. Some consider cloud as new technical revolution while some sees it as a natural evolution of technology, culture and economy.

However, cloud computing is an indispensable model with the possibility of reducing cost through optimization and increased operating and economic efficiencies. More so, cloud computing could enhance collaboration and agility significantly. However, security, privacy and trust remain the major concern posing various challenges to its adoption. Thus, this potential model would be a failure without an appropriate design of security and privacy apparatus that can secure cloud arena thereby, giving the potential users the confidence to embrace cloud computing.

This paper, however, explains issues of cloud computing that pose various challenges to it security and privacy. It also illustrates various approaches to address these challenges.

2. Literature Review

In case of the cloud computing domain, users mainly use cloud Services through a Web-based user interface (WBI), either a web browser or a mobile application, or a Web service application programming interface (API). Authentication is a way to provide secure access to users who are known as authorized users only. Simple text password is the widely used authentication system. Many researches have been carried out on the matter of improvement about the level of mobile cloud security. This has been treated as one of the major challenges. Handwriting recognition system has been proposed by Omri et al. [1] to uniquely identify password and unique handwriting style. Two implementation ways (web base and mobile application) have been used to set-up the connection between the mobile phone as a biometric-capture device. This method also uses Hadoop to set up the connection. Rassan et al. [10] has proposed another popular method based on finger print scan. Quick response code (QR code) based user authentication system for mobile based cloud has been proposed by [2] where conversion of the user ID, password, and the user's image to QR Code is made. Multiple level of password authentication is being done here.

Access to the cloud is allowed if authentication is successful in all levels.

- First level also known organization level. The organization password is being read at this level. Without authentication the connection tends to be terminated. After authentication it goes to the second level.
- Second level also known as the team level. As this level, team password is being read. After this it goes to user-level authentication.
- Third level provides the user privileges and permission.

An extension of Yang and Chang [4] proposed by Chen, et al. [3] in the year of 2011 by incorporating password protection-based mechanism with dynamic ID

3. Background And Related Work

Cloud and mobile cloud computing are discussed under this section. The related research work in MCC are also highlighted.

3.1. Definition and Features

According to the defines it as follows: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable 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 cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models (US National Institute of Standards and Technology) [5].

A cloud is a virtual pool of computing resources that comprises computers, servers, and the systems that provide resources to clients. Also, defined cloud computing as a parallel and distributed computing system employing virtualization with internal links and a Service Level Agreement (SLA), followed by scheduled allocation of resources [12] [13][14]. The primary five characteristics are being provided below [5];

- Measured service or billing: an automated billing system based on a 'pay as you use basis', with.
- Resource pooling: on demand allocation of cloud resources. This result cost effective and convenient to the customers.
- On-demand self- service: Complications can be avoided by the human interference in services delivered, as customers can get whatever they need, once the request for service is made.
- Broad network access: Cloud Computing services and its features must be constantly available over the internet or other networks based on standard protocols.
- Rapid elasticity: There is ability to scale up or down requested services as demanded by customers. This should be accomplished without any noticeable reduction in the quality of service delivery.

3.2. Mobile Cloud Computing (MCC)

Mobile cloud computing removes many drawbacks of mobile computing by associating the potency of cloud computing and mobile internet and hence offering an integration of mobile and cloud computing technology. Through this wireless network can access internet via the power of cloud computing on device [8]. Mobile network often faces challenges due to failure in network signal, difference in uplink and downlink, atmospheric condition, topography and building, security breaches. From 2.4 billion users in 2013 to approximately 3.6 billion internet users in 2018 have started using cloud computing services (statista.com [6]). A report presented by statista.com [7], among all mobile data traffic, 81% is being contributed by mobile cloud traffic.
This share is projected to grow to 90% in 2019 at a CAGR of 60%.

3.3. Key Concepts and Technologies

Easily available clouds services have been provided by the major IT vendors like Microsoft, Google and Amazon. Hardware resources and support live migration of VMs have been used in addition to dynamic load-balancing and on-demand provisioning. Although it is cost effective but it has issues with security. Virtualization mechanisms, varieties of cloud services are some of the widely used key concepts and technologies in cloud computing.

3.4. Virtualization Mechanisms

A hypervisor or virtual machine monitor (VMM) controls the virtualized resource residing between VMs and hardware. It aims to control many independent virtual machines on the same physical host. It can be divided into two major groups:

- Type I: Here the hypervisor runs directly on the real system hardware, and there is no Operating System (OS) under it. This proposition is proficient as it abolishes any Intermediary layers. Security improvement is another benefit of this type of hypervisor.
- Type II: This operates on a hosted OS that gives virtualization services, such as input/output (IO) device support and memory management.

4. Issues in Mobile Cloud Computing Arena

Major challenges of cloud computing are listed below [9][11]:

4.1. Cloud API Security Management

This is the major challenge of MCC. Poor management of this causes severe damages via viruses, Trojan horses, worms, malware. Installing and updating strong security software on mobile devices can help to detect threats and protect subscribers. However, cloudAV remain the effective uniform protection.

4.2. Battery Life Conservation

Another major constraint of mobile devices is battery conservation. Mobile and cloud computing usage get disconnected through flat battery. Many studies had focused on many solutions that can administer and improve the screen and the disk space and to progress the central processing unit (CPU) recital assiduously.
All these are effort proposed to optimize and subsequently reduce power consumption effectively. One of the goals of MCC is to allow it subscribers to a constant service irrespective of their location. Once the battery goes off, users cannot access service, leading to denial of service, poor connectivity, or total downtime. In other to pre-empt these, resources such as battery must be optimized.

4.3. Network Congestion

Because of heavy traffic of mobile cloud computing, network congestion is creating lot of challenge. Example of offloading in MCC which includes; cuckoo, spectra, hyrax, Chroma. However, these offloading are vulnerable to network congestion. Virtualization is another alternative to this offloading.

4.4. Platform Heterogeneity and Resource Constraints

Mobile devices are limited in screen size, storage capacity, battery life and network availability due to the mobility factor. Any kind of small problem in network often causes serious problem. An effective, reliable and secure mobile cloud computing (MCC) is required for this.

The system architecture has four layers.

- Access layer: Provides cooperation between client and cloud end, obeying MCC rules for effectual access.
- Basic managing layer: Takes standard operations to services like noticing, acknowledgement, directory and security, provides standard procedure interface and protocol to application service.
- Virtual layer: Virtual environment, system, platform for computing, storage and network pools.
- Physical layer: Hardware equipment and the technology that supports mobile cloud service.

4.5. Mobility Management

To ensure availability, intelligent mobility management techniques are required in mobile cloud computing. The method to accomplish QoS irrespective of location change in MCC could be infrastructure based orpeer-based techniques. The infrastructure-based mobility management use WI-FI, GSM, GPS, although this technique is not very good for mobile and cloud computing due to its energy consumption.

4.6. Security and Trust

Security and privacy are an important concern in the mobile cloud computing MCC domain, although majority users not paying any attention to this.

5. Conclusion

Mobile Cloud Computing is one of the best mobile technology in the future for providing prime services for mobile. According to recent study by ABI research, a New York based firm, more than 240 million business will use cloud services through mobile device by 2015. $5.2 billion revenue can be earned by the traction. This review paper presents the overview, advantages, disadvantages of mobile cloud computing. Challenges and their solutions are described MCC supported different type of application mention it clearly for wide range of mobile services. Finally, several open issues were described as future use.

6. References

i. F. Omri, R. Hamila, S. Foufou, and M. Jarraya, "Cloud-Ready Biometric System for Mobile Security Access," Networked Digital Technologies, pp. 192-200, 2012.
ii. D. S. Oh, B. H. Kim, and J. K. Lee, "A Study on Authentication System Using QR Code for Mobile loud Computing Environment," Future Information Technology, pp. 500-507, 2011.
iii. T. H. Chen, H. Yeh, and W. K. Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing," in Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on, 2011, pp. 155-159.
iv. J. H. Yang and C. C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," Computers & Security, vol. 28, pp. 138-143, 2009.
v. US National Institute of Standard and Technology (NIST): https://csrc.nist.gov/publications/detail/sp/800-145/final#pubs-abstract-hearder. (September 2011).
vi. Statista.com https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/
vii. Statista.comhttps://www.statista.com/statistics/292840/distribution-global-and-non-cloud-traffic/
viii. Eweoya, I. and Daramola, O., 2015. A Systematic Literature Review of Mobile Cloud Computing. *International Journal of Multimedia and Ubiquitous Engineering*.
ix. Tayade, D., 2014. Mobile cloud computing: Issues, security, advantages, trends. *International Journal of Computer Science and Information Technologies*, *5*(5), pp.66356639.
x. Rassan, I.A. and Al Shaher, H., 2013. Securing mobile cloud using finger print authentication. *International Journal of Network Security & Its Applications*, *5*(6), p.41.
xi. Sarrab, M. and Bourdoucen, H., 2015. Mobile Cloud Computing: Security Issues and Considerations. *Journal of Advances in Information Technology Vol*, *6*(4).
xii. Dinh, H.T., Lee, C., Niyato, D. and Wang, P., 2013. A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing*, *13*(18), pp.1587-1611.
xiii. Sarddar, D. and Bose, R., 2014. A mobile cloud computing architecture with easy resource sharing. *Int J CurrEngTechnol*, *4*(3), pp.1249-1254.
xiv. Bahar, A.N., Habib, M.A. and Islam, M.M., 2013. Security architecture for mobile cloud computing. *International Journal of Scientific Knowledge Computing and*
xv. *Information Technology*, *3*(3), pp.11-17.