ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

REVIEW PAPER ON MOBILE CLOUD COMPUTING SECURITY

PRIYANKA D. RAUT , DINESH S. DATAR
(M.E.) Computer Science and Engineering
G.H.Raisoni College Of Engineering & Management, Amravati
Amravati, Maharashtra 444701, India

Abstract: Nowadays smart-phones are being capable of supporting a broad range of applications, many of which demand an increasing computational power. This leads to a challenge because smart-phones are resource-constrained devices with finite computation power, memory, storage, and energy. With the development of mobility and cloud computing, mobile cloud computing (MCC) has introduced and become a point of research. With the need of extendibility and on-demand self-service, it can provide the good infrastructure, platform and software services in a cloud to mobile clients through the mobile network. Therefore, Cloud computing is anticipated to bring an innovation in mobile computing, where the mobile devices can make use of clouds for data processing, storage and other intensive operations. Despite the surprising advancement achieved by MCC, the clients of MCC are still below expectations due to the related risks in terms of security and confidentiality. The more and more information is placed onto the cloud by individuals and enterprises, the more the security issue begins to grow. This paper presents the various security issues that arise about how secure the mobile cloud computing environment is.

Keywords - Mobile Cloud Computing; Mobile Computing; Cloud Computing; Mobile Cloud Computing security; Data security.

1. Introduction

These days, the IT computing paradigm is rapidly moving into cloud-based services and applications. In addition, with the advent of smart devices, the cloud environments are including mobile-based convergent services. Mobile devices (e.g., smartphone, tablet pcs, fablet etc) are increasingly becoming a crucial part of human life as the most effective and convenient communication tools not bounded by time and place. However, the mobile devices are facing many challenges in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., mobility and security) [3]. Mobile Cloud Computing (MCC) aims to overcome these limitations by integrating cloud computing into the mobile environment to enable mobile users and mobile application providers to elastically utilize resources in an *on-demand fashion*.

MCC can be a composition of mobile technology and cloud computing infrastructure where data and the related processing will happen in the cloud only with an exception that they can be accessed through a mobile device and hence termed as mobile cloud computing [4]. It's becoming a trend now-a-days and many organizations are keen to provide accessibility to their employees to access office network through a mobile device from anywhere.

In Wikipedia, it is mentioned as a form of human-computer interaction by which a computer is expected to be transported during normal usage [8]. Mobile cloud computing depends on a collection of three major concepts: hardware, software and communication. The concepts of hardware can be considered as mobile devices, such as smartphone and laptop, or their mobile components. Software of mobile computing is the numerous mobile applications in the devices, such as the mobile browser, anti-virus software and games. The communication issue includes the infrastructure of mobile networks, protocols and data delivery in their use. They must be transparent to end users.

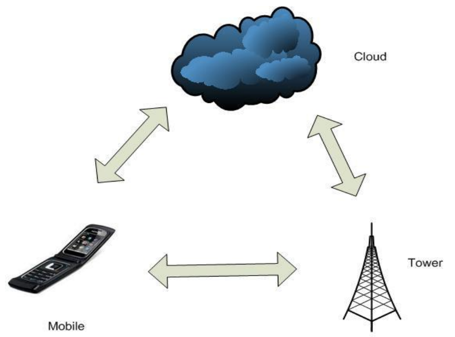

Fig. A Mobile Cloud Computing Scenario

We consider the cloud computing is a large scale economic as well as business computing paradigm with virtualization as its core technology. The cloud computing system is the development of parallel processing, distributed and grid computing on the Internet, which provides various QoS guaranteed services such as hardware, infrastructure, platform, software and storage to different Internet applications and users.

Cloud computing systems can be thought as a collection of different services, thus the framework of cloud computing is divided into three different layers, which are infrastructure layer, platform layer, and application layer.

a) Infrastructure layer: It is denoted as Infrastructure as a Service(IaaS). IaaS or Infrastructure as a Service (IaaS) is the lowest layer that provides basic infrastructure support service. IaaS refers to the sharing of hardware resources for executing services, typically using Virtualization technology. It provides the consumer with the capability to offer with large processing, storage, networks, and other fundamental computational resources, and allow the consumer to deploy and run arbitrary software, which could include operating systems and applications.

b) Platform Layer: This approach is termed as Platform as a Service approach (PaaS), the offering also includes a software execution environment. PaaS layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications. The consumer does not control the underlying cloud infrastructure including network services, servers, operating systems, storage or memory, but has control over the problem of deployed applications and possibly application hosting environment configurations.

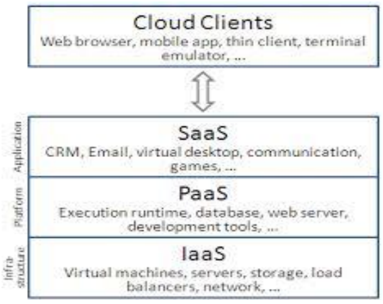
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

Fig. A Simple Cloud Computing Service Model

c) Application or Software Layer: Software as a Service (SaaS) is the topmost layer which features a complete application offered as service on demand [6]. SaaS ensures that the complete applications are hosted on the internet and users use them. The applications are accessible from various client side devices, with the help of a thin client interface, such as a web browser (e.g. web-based e-mail).

Depending upon the customers' requirements, cloud services can be deployed in four ways:

a) *Public Cloud:* The cloud infrastructure is become available to the general public or a large industry group and is owned by an organization that sells cloud services. Users can dynamically provision resources through the internet from an off-site service provider.
b) *Private Cloud:* Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider [2].
c) *Community cloud*: The cloud infrastructure is shared by various organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations).
d) *Hybrid Cloud:* A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other.

2. Literature Survey

For the last few years Mobile Cloud Computing(MCC) has been an active research field, as mobile cloud computing is in initial stage, limited surveys have been made in different domain of MCC. In this paper we focus on securing the data in mobile cloud computing. Itani et Al. [5] presented an Energy efficient framework for verifying integrity of storage services using incremental cryptography and trusted computing.

Incremental cryptography has a characteristic that when this algorithm is applied to a document, it is possible to quickly update the outcome of the algorithm for an updated document, rather than to re-compute it from scratch. In this system three main entities are involved which are responsible for performing all the computations in the system: Mobile Client/User (MC): Mobile client/user is a person who utilizes the storage services provided by Cloud service provider (CSP).Cloud Service Provider (CSP): CSP provides storage services to mobile client. CSP is also responsible for managing, operating and allocating cloud resources efficiently. Trusted Third Party (TTP): TTP installs coprocessors on remote cloud; who is associated with a number of registered mobile clients. Coprocessor provides secret key (SEK) to mobile client and is also responsible for generating message authentication code (MAC) for mobile client. There are number of operations involved in this scheme shown by

(1) MC generates MACfile and saves MACfile in local memory
(2) MC uploads the file on server
(3) CSP saves file on cloud
(4) MC sends request to CSP to perform insertion/deletion in the file
(5a) CSP forwards requested file to MC
(5b) CSP sends requested file to TCO
(6) TCO forwards MACtco to MC directly
(7) MC compares MACfile and MACtco to verify Integrity.
(8) MC insert/delete a block in a file and calculates MAC for that block
(9) MC uploads modified block on cloud
(10) CSP stores updated file.

3. Data Security in Mobile Cloud Computing

With an rapid rise towards the deployment of Cloud Computing, the ever consistent security and privacy issues have become more sophisticated.[1]. With the increase of on-demand application usage, the potential of cyber attacks also increases. following schemes should be deployed at least to ensure data security [7] to some extent like:

- An authentication techniques such as, incremental cryptography should be applied to prevent unauthorized access to the cloud data.
- Inflexible access controls to prevent unauthorized and illegal access to the servers controlling the network.
- The Service Providers should be given limited access to the data, just to manage it without being able to see what exactly the data is.
- An encryption scheme to ensure data security in a highly interfering environment maintaining security standards against popular threats and data storage security.

We can also implement a technique to make the cloud data more secure. In this implementation we can think of biometrics such as, fingerprints, ear shape, voice tone, retinal recognition, iris recognition etc. Among all these physiological biometrics we have a focus on iris recognition. In this method scan is done by camera of the user's mobile phone. The acquired picture is analyzed by the device, and it contains 266 different spots. Moreover iris is stable through the whole life. The 266 spots are based on characteristics of the iris, such as furrows and rings. The iris recognition seems difficult to be fooled. Hence we have been focusing on this technique to provide authentication to the more sensitive cloud data.

3. Conclusion

Since Mobile cloud computing combines the virtue of cloud computing and mobile computing, it is one of the mobile technology trends in the future thereby providing optimal services for mobile users. It seems that after few years a number of mobile users will be using cloud computing on their mobile devices. According to a recent study by ABI Research, a New York-based firm, more than 240 million business will use cloud services through mobile devices by 2015. Although it has revolutionized the computing world, it is liable to manifold security threats varying from network level threats to application level threats. These security threats need to be controlled to keep the Cloud secure. This paper has explored a mechanism for providing security to threats and the solutions to safeguard them have been discussed, so that Mobile Cloud Computing can be widely accepted by a number of users in future.

References

[1] Gellman R., "Privacy in clouds: Risks to security and confidentiality with cloud computing," The World Privacy Forum, 2009. http://www.worldprivacyforum.org/WPF_Cloud_Privacy_Report.pdf.

[2] Grossman R. L., "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, Mar-April, 2009, ISSN: 1520-9202, INSPEC Accession Number: 10518970, DOI: 10.1109/MITP.2009.40.

[3] Dinh H. T., Chonho Lee, Dusit Niyato and Ping Wang, "A survey of mobile cloud

computing: infrastructure, applications, and approaches," Wirel. Commun. Mob. Comput. ,2011.

[4] Ingthorsson Olafur; "Improving the Mobile Cloud", July 18, 2011 in Cloud Computing and Mobile Cloud Computing. http://cloudcomputingtopics.com/2011/07/improvingthe- mobile-cloud/.

[5] Itani W., A. Kayssi, A. Chehab, "Energy-efficient incremental cryptography for securing storage in mobile cloud computing," in: Proc. Int. Conference on Energy Aware Computing, ICEAC '10, Cairo, Egypt, Dec. 2010.

[6] Jensen Meiko, 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.

[7] Kaufman Lori M., "Data security in the world of cloud computing," IEEE Security and Privacy Journal, vol. 7, issue. 4, pp. 61-64, July- Aug 2009, ISSN: 1540-7993, INSPEC Accession Number: 10805344, DOI: 10.1109/MSP.2009.87.

[8] (2009, Sept) Mobile cloud computing subscribers to total nearly one billion by 2014. [Online]. Available: http://www.abiresearch.com/press/1484