Security Considerations for Public Mobile Cloud Computing

Ronnie D. Caytiles[1] and Sunguk Lee[2*]

[1]Society of Science and Engineering Research Support,
Korea
rdcaytiles@gmail.com

[2]Research Institute of Industrial Science and Technology
Pohang, Korea
sunguk@rist.re.kr
**Correspondent Author: Sunguk Lee* (sunguk@rist.re.kr)*

Abstract

Mobile cloud computing refers to the incorporation of the elements of mobile networks and cloud computing that offers optimal services for mobile users. It offers 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. The more and more information is placed into the cloud by individuals and enterprises, security issues begins to grow and raised. This paper discusses the different security issues that arise about how safe the mobile cloud computing environment is. The list of considerations for cloud computing security are identified and discussed which needs to be understood and assess the risks associated.

Keywords: *cloud computing, security issues, mobile cloud computing*

1. Introduction

Potential benefits that includes cost savings and improved business outcomes can be offered by Cloud computing. It entails the availability of software, processing power and storage on demand. It is already a permanent fixture of consumer oriented services such as email, storage and social media [4]. The opportunities provided by cloud computing becomes available to enterprises of all sizes that enables them to deliver more scalable and resilient services to employees, partners and customers at lower cost and with higher business agility [1]. Mobile cloud computing refers to the availability of cloud computing services in a mobile environment. It incorporates the elements of mobile networks and cloud computing, thereby providing optimal services for mobile users. In mobile cloud computing, mobile devices do not need a powerful configuration (e.g., CPU speed and memory capacity) since all the data and complicated computing modules can be processed in the clouds [2, 5].

The more and more information that is placed in the cloud by individuals and enterprises, the more and more they become vulnerable to attacks and threats the Internet has to offer. The promise of cloud computing to gain fast access to business applications and boosting their infrastructure resources with reduced capital expenses put the business world into a more risky environment. A variety of information security risks for cloud computing need to be carefully considered. Risks vary depending on the sensitivity of the data to be stored or processed, and how the chosen cloud provider has implemented their specific cloud services.

In this paper, we discuss the overview of cloud computing technology together with the challenges and promises cloud computing and associated benefits. The different issues that arises with the emergence of mobile cloud computing have been identified and discussed, thus drawing and realizing the security risks the cloud environment has to offer. This paper provides a list of considerations for cloud computing security that are needed to understand and assess the risks associated.

The rest of this paper is organized as follows: Section 2 explains the cloud computing overview; Section 3 outlines the security issues concerning cloud computing; and the concluding remarks in Section 4.

2. Overview of Cloud Computing

Cloud computing as a delivery model for IT services is defined by the National Institute of Standards and Technology (NIST) as “a model for enabling convenient, ondemand 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”[11].

NIST specify five characteristics of cloud computing that describe and differentiate Cloud services from conventional computing approaches:

a. On-demand self-service involves customers using a web site or similar control panel interface to provision computing resources such as additional computers, network bandwidth or user email accounts, without requiring human interaction between customers and the vendor.

b. Broad network access enables customers to access computing resources over networks such as the Internet from a broad range of computing devices such as laptops and smartphones.

c. Resource pooling involves vendors using shared computing resources to provide cloud services to multiple customers. Virtualization and multi-tenancy mechanisms are typically used to both segregate and protect each customer and their data from other customers, and to make it appear to customers that they are the only user of a shared computer or software application.

d. Rapid elasticity enables the fast and automatic increase and decrease to the amount of available computer processing, storage and network bandwidth as required by customer demand.

e. Pay-per-use measured service involves customers only paying for the computing resources that they actually use, and being able to monitor their usage. This is analogous to household use of utilities such as electricity.

Cloud services are often but not always utilized in conjunction with, and enabled by, virtualization technologies [6, 7].

2.1 Cloud Service Offerings

Cloud computing service offerings are broadly classified into three delivery models: the Infrastructure as a Service (IaaS); the Platform as a Service (PaaS); and the Software as a Service (SaaS) [1, 3, 4, 6].

The Cloud computing services provisioning is shown in Figure 1. For SaaS, the service levels, security, governance, compliance, and liability expectations of the service are contractually stipulated, managed to, and enforced to the provider. For PaaS or IaaS, the consumer’s system administrators has the responsibility to effectively manage this issues, with some offset expected by the provider for securing the underlying platform and infrastructure components to ensure basic service availability and security. It should be clear in either case that one can assign/transfer responsibility but not necessarily accountability for both consumers and providers.

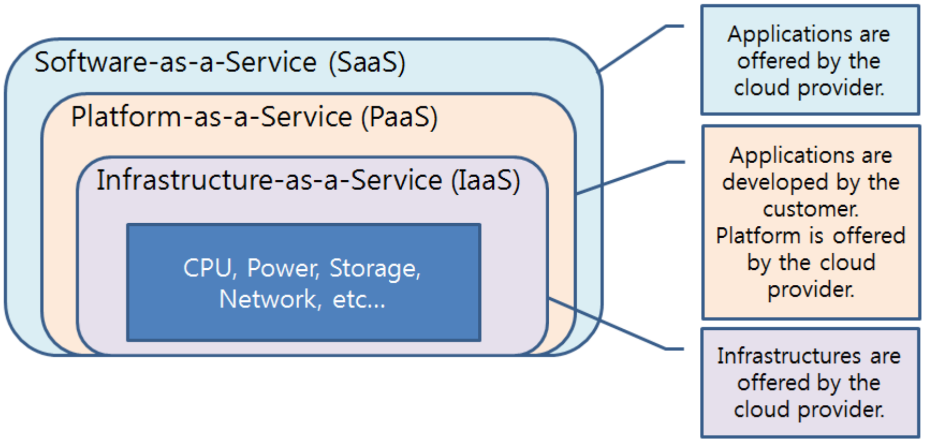
Software-as-a-Service (SaaS)
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service (IaaS)
CPU, Power, Storage, Network, etc...
Applications are offered by the cloud provider.
Applications are developed by the customer. Platform is offered by the cloud provider.
Infrastructures are offered by the cloud provider.

Figure 1. Cloud Computing Service Offerings

2.1.1 Software as a Service (SaaS) offers complete and finished software applications on demand. A single instance of the software runs on the cloud and services multiple end users or client organizations. It is a model of software deployment where an application is hosted as a service provided to customers across the Internet. By eliminating the need to install and run the application on the customer’s own computer, SaaS alleviates the customer’s burden of software maintenance, ongoing operation, and support. Example applications include email and an environment for users to collaboratively develop and share files such as documents and spreadsheets. These end user applications are typically accessed by users via web browser, eliminating the need for the user to install or maintain additional software. The provider controls and maintains the physical computer hardware, operating systems and software applications. The provider allows the customer only to use its applications

Most widely used examples of SaaS include Gmail, Google Docs, and Salesforce.com.

2.1.2 Platform as a Service (PaaS) offers an operating system and can provide for every phase of software development and testing as well as suites of programming languages that users can use to develop their own applications. It provides a set of software and development tools hosted on the provider’s servers. PaaS enables customers to use the provider’s cloud infrastructure to deploy web applications and other software developed by the customer using programming languages supported by the provider. Typically the vendor controls and maintains the physical computer hardware, operating systems and server applications. Typically the customer only controls and maintains the software applications developed by the customer.

Commercial examples include Microsoft Windows Azure and Google App Engine, Force.com, and the Amazon Web Services Elastic Beanstalk.

2.1.3 Infrastructure as a Service (IaaS) offers end users direct access to physical computer hardware including CPU processing, memory, storage, network connectivity and other computing resources over the network. It provides virtual servers with unique IP addresses and blocks of storage on demand. The provider may share their hardware among multiple customers referred to as “multiple tenants” using virtualization software. IaaS enables customers to run operating systems and software applications of their choice. Typically the vendor controls and maintains the physical computer hardware. Typically the customer controls and maintains the operating systems and software applications.

Examples of IaaS include Amazon Elastic Compute Cloud (EC2), Joyent, GoGrid, Rackspace Cloud, and IBM Computing on Demand.

2.2 Deployment Models for Cloud Applications

There are four basic cloud application deployment and consumption models that the Cloud computing architects must take into consideration: public, private, hybrid, or community clouds. Each offers complementary benefits, and has its own trade-offs [1, 3, 4, 6, 11].

2.2.1 Public Clouds: Public clouds are owned and managed by Providers, and applications from different customers are likely to be mixed together on the cloud’s servers, storage systems, and networks. However, this model has a variety of inherent security risks that need to be considered. . A well architected private cloud properly managed by a provider provides many of the benefits of a public cloud, but with increased control over security. Public clouds are most often hosted away from customer premises, and they provide a way to reduce customer risk and cost by providing a flexible, even temporary extension to enterprise infrastructure.

2.2.2 Private Clouds: Private clouds are client dedicated and are built for the exclusive use of one client, providing the utmost control over data, security, and quality of service. The enterprise owns the infrastructure and has control over how applications are deployed on it. If the private cloud is properly implemented and operated, it has reduced potential security concerns A managed private cloud may enable enterprise customers to more easily negotiate suitable contracts with the provider, instead of being forced to accept the generic contracts designed for the consumer mass market that are offered by some public cloud providers. Private clouds may be deployed in an enterprise datacenter, and they also may be deployed at a co-location facility.

2.2.3 Hybrid Clouds: A Hybrid cloud involves a combination of both public and private cloud models. They can help to provide on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload fluctuations. Enterprise Computing and private cloud extend outward to consume public compute resource for peak need or deliver on Industry cloud. An example is using commodity resources from a public cloud such as web servers to display non-sensitive data, which interacts with sensitive data stored or processed in a private cloud. Focus primarily on proprietary data centers, but rely on public cloud resources to provide the computing and storage needed to protect against unexpected or infrequent increases in demand for computing resources.

2.2.4 Community Clouds: Community clouds are tailored to a specific vertical industry, such as government, healthcare or finance, offering a range of services, including infrastructure, software or platform as a service. It involves a private cloud that is shared by several organizations with similar security requirements and a need to store or process data of similar sensitivity. This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud. An example community cloud is the sharing of a private cloud by several agencies of the same government.

3. Mobile Cloud Computing

The usage of cloud computing in combination with mobile devices is known as mobile cloud computing. It is a combination between mobile network and cloud computing, thereby providing optimal services for mobile users. Cloud computing exists when tasks and 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 [2, 5]. Figure 2 shows an overview of the mobile cloud computing architecture.

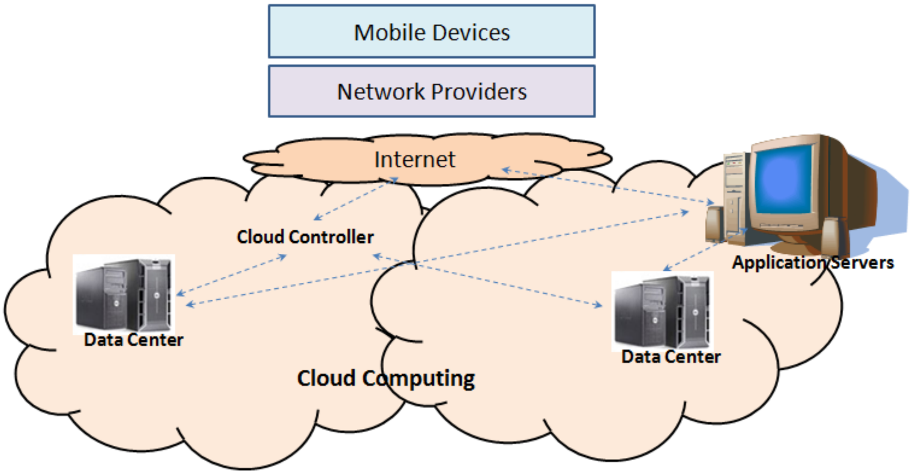

Figure 2. Mobile Cloud Computing Architecture Overview

3.1 Mobile Cloud Computing Security

Securing mobile cloud computing user's privacy and integrity of data or applications is one of the key issues most cloud providers are given attention. Since mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: Mobile network user's security; and cloud security [8, 9, 10].

3.1.1 Mobile Network User's Security

Numerous security vulnerabilities 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 [10]. There are two main issues concerning the subscriber's security.

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.

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. This leads to concerns that companies will use or sell this information as well as concerns that the information could be given to government agencies without the user's permission or knowledge.

Data Ownership: Another issue that arises from mobile cloud computing relates to the ownership of purchased digital media. With cloud computing it becomes possible to store purchased media files, such as audio, video or e-books remotely rather than locally. This can lead concerns regarding the true ownership of the data. If a user purchases media using a given service and the media itself is stored remotely there is a risk of losing access to the purchased media.

Data Access and Security: Related issues of access and security are significant to applications that rely on remote data storage and internet access in order to function. For example a user stores all of their calendar and contact information online, power outages can affect their ability to function from day to day. Mobile cloud computing is vulnerable due to multiple points at which access can be interrupted. Reception and high speed availability can vary greatly for mobile devices utilized by the users.

3.1.2 Securing Information on the Cloud

Individuals and enterprises take advantage of the benefits for storing large amount of data or applications on a cloud. However, issues in terms of their integrity, authentication, and digital rights must be taken care of [10].

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 it is their own information and thus verifying its integrity.

Authentication: Different authentication mechanisms have been presented and proposed using cloud computing to secure the data access suitable for mobile environments. Some uses the open standards and even supports the integration of various authentication methods. For example, the use of access or log-in IDs, passwords or PINS, authentication requests, etc.

Digital rights management: Illegal distribution and piracy of digital contents such as video, image, audio, and e-book, programs becomes more and more popular. Some solutions to protect these contents from illegal access are implemented such as provision of encryption and decryption keys to access these contents. A coding or decoding platform must be done before any mobile user can have access to such digital contents.

3.2 Cloud Computing Key Security Considerations

To realize the full benefits of cloud computing, the security benefits and risks must be properly addressed. The following consideration in evaluating, implementing, managing, and maintaining cloud computing solutions must be explored.

Compliance and Risk Management: Enterprises that shift to the cloud are responsible for compliance, risk, and security management. It is important for them to understand the compliance and risk management even if the responsibility for execution may be transferred to the cloud provider.

Service Integrity: Cloud-based services should be engineered and operated with security in mind; operational processes should be integrated into the organization's security management.

Endpoint Integrity: The security, compliance, and integrity of the endpoint must be part of any security consideration.

Information Protection: Cloud services require reliable processes for protecting information before, during, and after the transaction.

3.3 Guidelines on Security and Privacy in Public Cloud Computing [11]

Guidelines on Security and Privacy in Public Cloud Computing (NIST Special Publication 800-144) provides an overview of the security and privacy challenges facing public cloud computing and presents recommendations that organizations should consider when outsourcing data, applications and infrastructure to a public cloud environment. The document provides insights on threats, technology risks and safeguards related to public cloud environments to help organizations make informed decisions about this use of this technology.

The key guidelines include:

- Carefully plan the security and privacy aspects of cloud computing solutions before implementing them.
- Understand the public cloud computing environment offered by the cloud provider.
- Ensure that a cloud computing solution—both cloud resources and cloud-based applications—satisfy organizational security and privacy requirements.
- Maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments.

4. Conclusions

Cloud computing as a transformative technology holds a considerable promise that can change the very nature of computing specifically to business enterprises. Building applications on on-demand infrastructures instead of building applications on fixed and rigid infrastructures was provided by cloud computing providers. By simply tapping into the cloud, enterprises can gain fast access to business applications or infrastructure resources with reduced Capital Expenditure (CAPEX).

Mobile cloud computing provides an optimal services for mobile users as one of the mobile technology trends in the future since it combines the advantages of both mobile computing and cloud computing.

This paper have discussed security considerations concerning mobile cloud computing. Securing mobile cloud computing user's privacy and integrity of data or applications are the key issues that most cloud providers must have given considerations. The mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: mobile network user's security; and mobile cloud security.

References

[1] NEC Company, Ltd. and Information and Privacy Commissioner, Ontario, Canada. "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach, **(2010)**, http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf.

[2] http://www.smartdevelopments.org/?p=84.

[3] https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_Framework.

[4] http://andromida.hubpages.com/hub/cloud-computing-architecture.

[5] http://www.readwriteweb.com/archives/why_cloud_computing_is_the_future_of_mobile.php.

[6] Sun Microsystems, Inc., "Introduction to Cloud Computing Architecture", White Paper, 1st Edition, **(2009)** June.

[7] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, Information Technology Laboratory, Version 15, 10-7-09 **(2009)**.

[8] D. Huang, Z. Zhou, L. Xu, T. Xing and Y. Zhong, "Secure Data Processing Framework for Mobile Cloud Computing", IEEE INFOCOM 2011 Workshop on Cloud Computing, 978-1-4244-9920-5/11/$26.00 ©2011 IEEE, **(2011)** pp. 620-624.

[9] 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.

[10] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches", Wireless Communications and Mobile Computing – Wiley, Available at http://www.eecis.udel.edu/~cshen/859/papers/survey_MCC.pdf.

[11] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication 800-144, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494, **(2011)** December.