International Journal of Multidisciplinary Research and Development

IJMRD 2015; 2(3): 17-19
www.allsubjectjournal.com
Impact factor: 3.672
Received: 08-02-2015
Accepted: 22-02-2015
E-ISSN: 2349-4182
P-ISSN: 2349-5979

N.Karthika
M.Phil full time Research Scholar, Vivekananda College of Arts and Science for Women, Namakkal, TamilNadu, India.

S.Mahima
Assistant professor, Vivekananda College of Arts and Science for Women, Namakkal, TamilNadu, India.

Correspondence:
N.Karthika
M.Phil full time Research Scholar, Vivekananda College of Arts and Science for Women, Namakkal, TamilNadu, India.

Security considerations in public mobile cloud computing

N.Karthika, S.Mahima

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.

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. 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.

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

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

2. 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)

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.

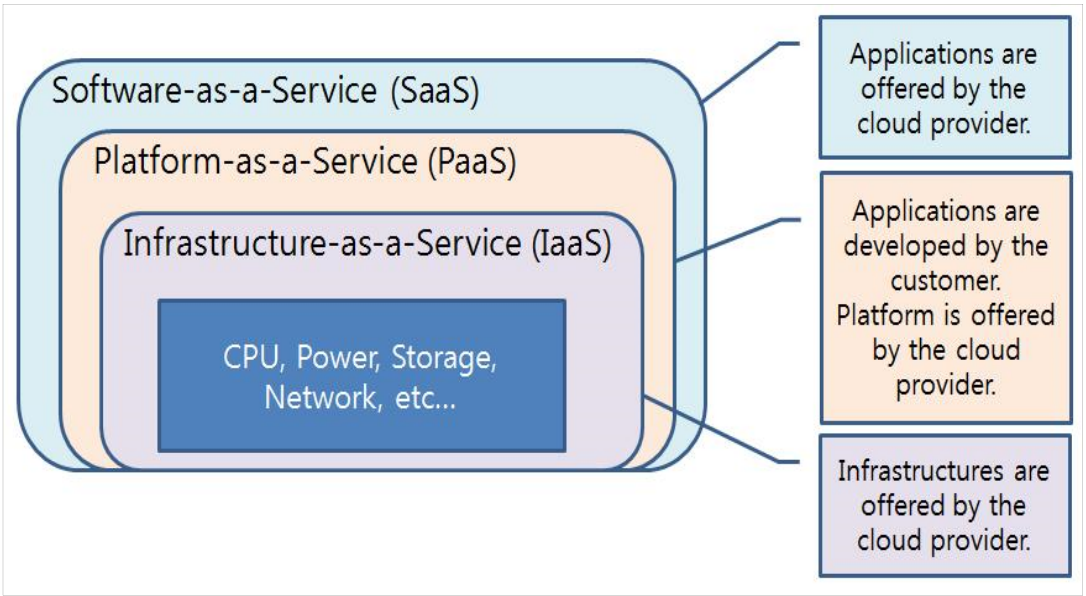

Fig 1. Cloud Computing Service

3. Software as a Service (SAAS)

It 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

2.1.1 Platform As A Service (PAAS)

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)

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.

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].

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.

2.2.1 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.

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.

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.

Conclusion
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).
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. "Modeling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach, **(2010**
2. https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_Framework.
3. http://andromida.hubpages.com/hub/cloud-computing-architecture.
4. http://www.readwriteweb.com/archives/why_cloud_computing_is_the_future_of_mobile.php.
5. Sun Microsystems, Inc. "Introduction to Cloud Computing Architecture", White Paper, 1st Edition, **(2009)** June.
6. 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)**. 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.
7. 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.
8. 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.