International Journal of Computer Applications Technology and Research
Volume 5–Issue 12, 725-729, 2016, ISSN:-2319–8656

Review on Security Techniques using Cloud Computing

Supreet Kaur
Guru Nanak Dev University, Amritsar, Punjab.
India

Sonia Sharma
Guru Nanak Dev University, Amritsar, Punjab.
India

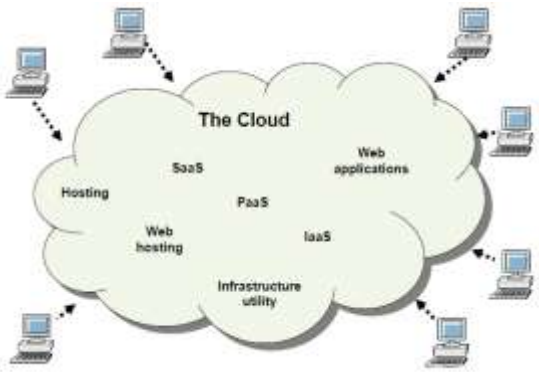
Abstract: Cloud Computing is the nascent technology which is based on Pay-Per-Use Model. Cloud computing is emerging as a model of "Everything as a Service" (XaaS). Cloud Computing is computing paradigm where applications, data bandwidth and IT services are provided over the Internet. Cloud Computing is a relatively new computing model that provides on demand business and IT services over the Internet. The main concerns in adapting Cloud Computing is its security, different security risks that affects the cloud environment in the area of confidentiality, Integrity and computing on data is thoroughly investigated.

Keywords: Cloud Computing, Security, Cloud Security Reference Model, Principal Security Dangers to Cloud Computing, Identity Management, SSL Overview

1. INTRODUCTION

The term cloud is "A network that delivers requested virtual resources as a service."**[D]** Cloud Computing refers to application and services that run distributed network using "Virtualized Resources" and accessed by common Internet Protocol and networking standard. **[K]** The need of cloud computing are as :

a) Cloud Computing is a compelling paradigm.
b) Making internet the ultimate resource of all computing needs. **[I]**



NIST Model stands for the US National Institute for Standards and Technology. It has the set of working definition that separate cloud computing into service model and the deployment model. **[F]** NIST Cloud Model does not address a intermediately services such as transaction or service brokers, provisioning and interoperability services that from the basis for many cloud computing.

1.3 CLOUD VULNERABILITIES

In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements :

1.1 CHARACTERISTICS OF CLOUD COMPUTING

a) **On-Demand Self-Service :** Computing resources can be gathered and used at anytime without the need for manual interaction with cloud service providers.
b) **Poor of Virtualized Resources :** It focuses on delivering IT services through resource pool.
c) **Broad Network Access :** The available resources can be accessed over a network using "Heterogeneous Devices" such as Laptops or Mobile Phones.
d) **Measured Service :** Resource usage is measured using appropriate metrics such monitoring storage usage, CPU Hours, bandwidth usage etc.
e) **Rapid Elasticity :** A user can quickly obtain more resources by scaling out from the cloud. **[B]**

1.2 CLOUD SUPPORT TECHNIQUES

Cloud computing has leveraged a collection of existing techniques, such as Data Center Networking (DCN), Virtualization, distributed storage, MapReduce, web applications and services, etc. There are techniques are the followings :

I. **Modern of data center :** It provides massive computation and storage capability by composing thousands of machines with DCN techniques.

II. **Virtualization :** With virtualization, multiple OSs can core side on the same physical machine without interfering each other.

III. **MapReduce :** MapReduce is a programming framework that supports distributed computing on mass data sets. **[C]**

a) A system susceptibility or flaw.
b) An attacker access to the flaw.
c) An attacker capability to exploit the flaw. **[E]**

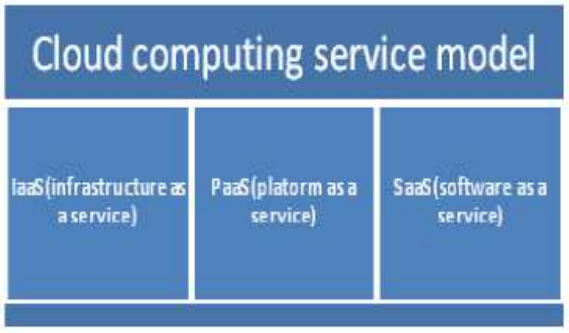
1.4 MODEL OF CLOUD COMPUTING

There are two Model of Cloud Computing are the followings :

a) Service Model
b) Deployment Model

a) Service Model :

It tells us what are services the cloud is providing. These types are as the followings :



i. **Software as a Service (SaaS) :** It manages the user data and interaction. It does not require client installation just a browser or other client device and network connectivity. **[D]**

ii. **Platform as a Service (PaaS) :** It provides virtual machines, operating system application services, deployment framework, transaction and control structure.

iii. **Infrastructure as a Service (IaaS) :** It provides virtual machines, virtual storage and virtual infrastructure and other hardware access as resources that client can provision. **[A]**

b) **Deployment Model :** It tells us where the cloud is located and The National Institute of Standards and Technology (NIST) defines four cloud deployment types :

i. Private Clouds :

The cloud infrastructure is used solely by the organization that owns it. May reside in-house or off premises. There are two types of Private Clouds are the following :

a) **Private Internal Clouds :** The organization acquires the necessary hardware and maintains it for itself.

b) **Private External Clouds :** The organization pays a cloud provider to provide this as a service. **[L]**

ii. Public Clouds :

Service Provider lets clients access the cloud via the Internet.

iii. Community Clouds :

Used and Controlled by a group of organizations with a shared interest.

iv. Hybrid Clouds :

Composed of two or more clouds (private, public or community) that remain unique entities, but that can interoperate using standard or proprietary protocols. **[A]**

1.5 ADVANTAGES OF CLOUD COMPUTING

a) Cloud Computing environment are scalable system and a customized software stack.
b) In addition to the IT industry, even small scale business can adopt this environment model.
c) **Reduced setup costs :** The cost involved in setting up a data center are not very high. **[G]**
d) **Lower Cost :** Because lower cost operate at higher efficiencies and with greater utilization significant cost reduction are often encounter. **[G]**
e) **Outsourced IT management :** Capabilities required and how outsourcing vendors are developing them.

1.6 DISADVANTAGES OF CLOUD COMPUTING

1. **Network Failure :** It can result in loss to the company by causing extensive time delays.
2. **Quality of Service :** It is a key determining factor in the efficiency of a cloud network. **[J]**
3. Cloud Computing is a "**stateless system**" in order for a communication service on distributed system.
4. All cloud computing application suffers from the "**inherent latency**" i.e. intrinsic in the WAN connectivity.
5. The lack of state allow messages to travel over different routes and data to arrive out of sequence and communication to succeed even when the system is faulty.

2. SECURITY IN CLOUD COMPUTING

Cloud Computing presents an added level of risk because essential services are often outsourced to a third party. Cloud Computing shifts much of the control over data and operations from the client organizations to it cloud provider :

a) Clients must establish a trust relationship with the providers and understand the risks.
b) A trust but verify relationship is critical. **[D]**

Security areas to focus on include :

I. Recognizing Security risks
II. Carrying out required security tasks
III. Managing user identity
IV. Using detection and forensics programs
V. Encryption data
VI. Creating a security plan **[H]**

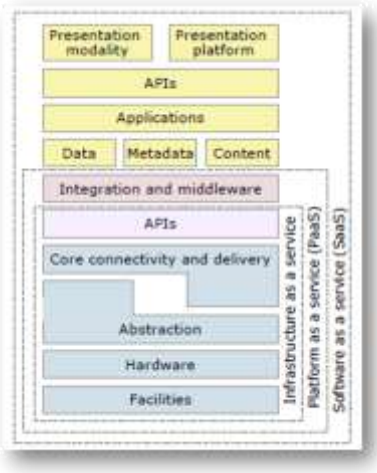
2.1 CLOUD SECURITY REFERENCE MODEL

Integration of Security into cloud reference model. The relationship and dependencies between these are important to fully grasp the security risks to cloud computing :

a) IaaS is the base of all cloud services.
b) PaaS is layered on top of IaaS.
c) SaaS is built upon PaaS. **[D]**

Layered Architectures inherit capabilities :

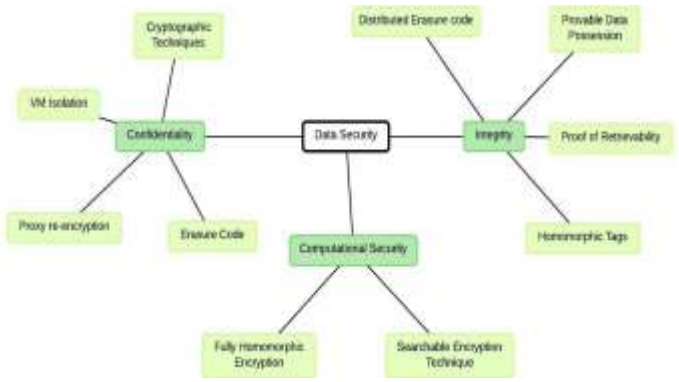
I. These capabilities includes operations and functionality.
II. Unfortunately, they also inherit risks, including security risks. **[D]**



I. **Infrastructure as a Service (IaaS) in Security :** IaaS provides few application features but tremendous flexibility. This opens up the application layer and middleware layer requiring the cloud provider to focus the security, capability on the Operating System (OS) and underlying infrastructure.
II. **Platform as a Service (PaaS) in Security :** PaaS provides a layer in which developer works providing them the freedom to create functionality. The increase flexibility, removes additional security layering that was providing in SaaS. PaaS Security comprises of two types :
    a) Security of the PaaS platform itself, normally provided by cloud service provider.
    b) Security of customer applications deployed on a PaaS platform. **[C]**
III. **Software as a Service (SaaS) in Security :** SaaS in Security is a software deployment model where applications are remotely hosted by the service provider and made available to customers on demand, over the Internet. SaaS is rapidly emerging as the dominant delivery model.

2.2 IMPORTANT TYPES OF CLOUD DATA SECURITY

There are important three types of Cloud Data Security are as follows :



a) **Confidentiality :** Confidentiality refers to any authorized parties having access to protected data. **[C]**
b) Integrity : Integrity refers that data can be modified only by authorized parties or in authorized ways. **[C]**
c) **Computational Cloud Security :** The fundamental service enabled within the cloud paradigm is computation outsourcing. Users can make use of unlimited computing resources in a pay-per-use model. **[C]**

2.3 CLOUD SECURITY RISKS

Security Risks is very complicated area of Cloud Computing for three reasons are as follows :

a) Security is a trusted to the cloud provider; therefore, if the provider has not done a good job, there may be problems.
b) Security is difficult to monitor, so problems may not be apparent until there is a problem.
c) Measuring the quality of the cloud provider's security approach may be difficult because many cloud provider's do not expose their infrastructure to customers. **[D]**

2.4 PRINCIPAL SECURITY DANGERS TO CLOUD COMPUTING

The principal security dangers to cloud computing include dangers that currently exist in pre-cloud computing. These includes are :

a) Virtualization and Multi-Tenancy
b) Non-Standard and Vulnerable APIs
c) Internal Security Breaches
d) Data Corruption or Loss
e) User Account and Service Hijacking **[D]**

a) **Virtualization and Multi-Tenancy :** Virtualization and Multi-Tenancy architects make this possible.

Virtualization and Multi-Tenancy were not designed with strong isolation in place :

I. Hypervisors have extended these risks, potentially exposing the Operating System.

II. Creating an environment where attackers can gain accept at the OS level (hypervisors) and higher level services (functionality and data).

b) **Non-Standard and Vulnerable APIs :** Application Programming Interfaces are the software interfaces that cloud provider offer, allowing customers access into their services. Cloud API's are not standardized, forcing user of multiple cloud providers to maintain multiprogramming interfaces, Increasing complexity and security risk.

c) **Internal Security Breaches :** The IT industry has well documented that over 70% of security violation are internal :

I. This threat is amplified in Cloud Computing as both IT providers and consumers are under a single management domain.

d) **Data Corruption or Loss :** Data Corruption in an amplified since the cloud provider is a source for companies data, not the company itself. These operational characteristics of cloud environment at PaaS and SaaS layers, amplify the threat of data loss or leakage increase.

e) **User Account and Service Hijacking :** User Account and Service Hijacking occurs when attackers obtains your cloud services information and uses it to take over your cloud access. If attackers gain access to cloud user's traditional make an eavesdrop on activities and transaction, manipulate or steal data, return falsified data and redirect clients to illegitimate sites.

2.5 REDUCING CLOUD SECURITY BREACHES

The following steps offer a guideline to reduce cloud security breaches :

1. Implement security best practices including human processes.
2. Implement OS security best practices such as patch management.
3. Implement application & API systems security best practices.
4. Implement strong encryption, SSL, digital signatures & certificate practices.
5. Ensure that auditing & logging is being used to monitor activities.
6. Ensure that strong disaster recovery process exist.
7. Transparency in information & internal management practice.
8. Understanding the human resources requirements.
9. Have a clear level of escalation & notification of a breach, ensuring that you are in the loop if an internal breach occurs with the cloud provider (with your data or another customer's). **[D]**

2.6 IDENTITY MANAGEMENT

Identity Management is a broad administrative area that deals with identifying individuals in a system & controlling access to the resources in that system by placing restrictions on the established identities of the individuals. **[D]** The benefits of Identity Management are as follows :

a) Improved User Productivity
b) Improved Customer and Partners Services
c) Reduced help desk costs
d) Reduced IT costs

The Aspects of Identity Management are as follows :

a) Centrally locate the data
b) Integrating
c) Strength Authentication
d) Provisioning
e) Single sign-on
f) Security Administration
g) Analyzing Data

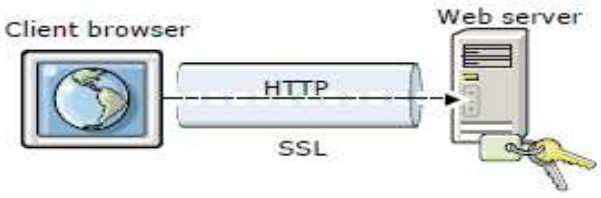
2.7 SSL OVERVIEW

SSL stands for Secure Sockets Layer. SSL provides connection security through :

a) **Communication Privacy :** The data on the connection can be encrypted.

b) **Communication Integrity :** The protocol includes a built-in integrity check.

c) **Authentication :** The client knows who the server is. **[D]**



SSL is the standard security technology for establishing an encrypted link between a web server & a browser. This link ensures that all data passed between the web server & browsers remains private and integral. SSL is an industry standard & is used by millions of websites in the protection of their online transactions with their customers.

Solve the following security problems :

I. Tampering

II. Impersonation

III. Eavesdropping

2.8 CLOUD SECURITY CHALLENGES

a) Indirect administrative accountability.
b) Proprietary cloud vendor implementations can't be examined.
c) Loss of Physical Control.
d) Possibility for massive outages.
e) Encryption needs for cloud computing :

i. Encrypting access to the cloud resource control interface.
ii. Encrypting administrative access to OS instances.
iii. Encrypting access to applications.
iv. Encrypting application data at rest. **[H]**

3. CONCLUSION

Cloud Computing is the promising paradigm for delivered IT services as computing utilities. Cloud are designed to provide services to external user; provider need to be compensated for sharing their resources and capabilities. Security Challenges and the privacy of data are the major obstacles for the success of Cloud Computing. We have performed a systematic review of security issues for cloud environment where we enumerated the main cloud threats and vulnerabilities.

4. REFERENCES

[A] Krishan Kant Lavania , Yogita Sharma , Chandresh Bakliwal, "Review on Cloud Computing Model", International Journal on Recent and Innovation Trends in Computing and Communication
[B] Navdeep Kaur, A Review Paper on various scheduling techniques in cloud computing
[C] Balasubramanian, Review of on various data security issues in cloud computing environment and it solutions
[D] IBM, Fundamentals of Cloud Computing (Student Notebook), WebSphere Education
[E] Cloud Computing Architecture & its Vulnerabilities with Presentation, Vinay Dwivedi (Visual Information Processing and Embedding Systems)
[F] https://en.wikipedia.org/wiki/Cloud_computing
[G] https://www.cse.unr.edu/~mgunes/cpe401/cpe401sp12/lect15_cloud.ppt
[H] https://en.wikipedia.org/wiki/Cloud_computing_security
[I] https://www.youtube.com/watch?v=ae_DKNwK_ms
[J] https://www.tutorialspoint.com/cloud_computing/
[K] https://www.youtube.com/watch?v=bsIZ_-8u4fE
[L] www.thbs.com/downloads/Cloud-Computing-Overview.pdf