IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-17, May 2019 E-ISSN: 2347-2693

# Security Issues in the Cloud Computing Environment : An Overview

**S. Rajalakshmi[1*], P. Madhubala[2]**

[1]Department of Computer, Science,Government Arts College for Women-Krishnagiri,
[2]Department of Computer, Don Bosco College -Dharmapuri

*Corresponding Author: rajaylakshmiravi7@gmail.com*

**Available online at: www.ijcseonline.org**

***Abstract*—** In Cloud Computing environment, Security issues is the hottest topic. Many tools and techniques are applied to secure the data in the cloud server. Although, the security providers focus on data storage of third party at risk to be maintain sensitive information. As the information grows day by day, Security control over the data should be more effective and adaptive to changing risk services. Protection of data manages how data is stored, how it is accessed and how it is handled. Taking lease of many servers and provisioning the resources for usage cost turns to a revolution. This paper reveals the outline of cloud computing, cloud security concepts, challenges and solutions for dynamically securing sensitive data of unlimited resources and services.

***Keywords*—**Cloud Computing, Security Issues, Sensitive Data, Service Providers, Services

## I. INTRODUCTION

According to NIST (National Institute of Standard Technology), "Cloud Computing is a model of enabling 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 [1] [2].

Section II discusses about Cloud Service model, Section III delivers the Cloud Deployment model, Section IV highlights the Cloud Characteristics, Section V describes Security Architecture, Section VI reveals the Security Issues, Section VII tells Security Threats, Section VIII explains the Security Challenges and solutions, Section IX tabulates the Summary and Section X concludes the paper

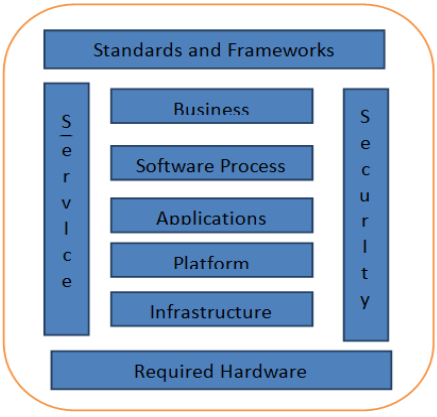


Figure 1: Basic Cloud Computing Model

## II. CLOUD SERVICE MODEL

Cloud usage decreases the cost and increases the scalable storage, computing power and service. Cloud services may be classified in to SaaS (Software as a Service), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). These services have the ability to access computing such as utility computing, grid computing and autonomic computing

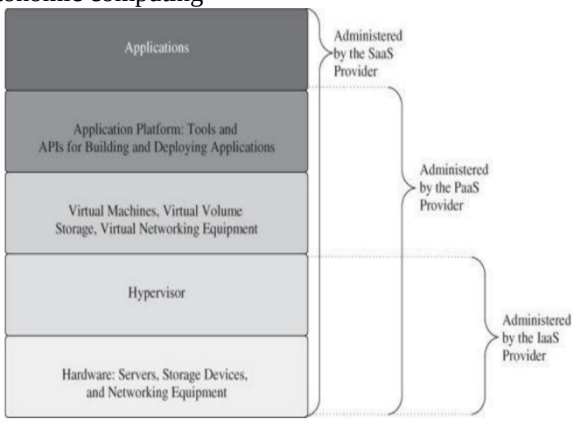


Fig. 2

## III. CLOUD DEPLOYMENT MODEL

The Cloud deployment model is a 'configuration' which includes parameters such as storage size, accessibility and it is broadly classified in to *four* models [4].

1. *Public cloud* – It is a common cloud owned by organization that sells cloud services.

 

2. *Private cloud* – It is operated exclusively which is contracted by third party.
3. *Community cloud* – It is shared by several organizations to a shared goal.
4. *Hybrid cloud* – It is composed of two or more clouds, connected to a technology enabling data and applications moving to the infrastructure among the clouds [1].

Table 1: Comparative Analysis of deployment models.

| | Public | Private | Community | Hybrid |
|---|---|---|---|---|
| **Ease of setup and use** | Easy | Requires IT proficiency | Requires IT proficiency | Requires IT proficiency |
| **Data security and privacy** | Low | High | Comparatively high | High |
| **Data control** | Little to none | High | Comparatively high | Comparatively high |
| **Reliability** | Vulnerable | High | Comparatively high | High |
| **Scalability and flexibility** | High | High | Fixed capacity | High |
| **Cost-effectiveness** | The cheapest one | Cost-intensive, the most expensive one | Cost is shared among community members | Cheaper than a private model but more costly than a public one |
| **Demand for in-house hardware** | No | Depends | Depends | Depends |

## IV. Cloud Characteristics

The cloud characteristics will help the development and adoption of the rapidly evolving technology. The cloud characteristics are as follows [6].

a) On-demand self-service: Cloud consumer are given freedom to self-provision the IT resources. Once it is configured, IT resources are automated, requiring no human interaction by cloud Providers called "On-demand Usage".
b) Broad network access: To enable the access over the network, devices such as laptop, mobile phones and PDA use standard methods to access clients of all types.

c) Resource Pooling: Resource Pooling is achieved through Multitenancy technology. It allows providers to pool large-scale IT resources to serve multi cloud consumers. Physical and virtual systems are dynamically assigned and reassigned as needed by cloud consumer.

d) Rapid Elasticity: Resource capabilities can be provisioned rapidly and elastically. Services are considered to be so elastic, such that resources can be added (scaling up) whenever needed and removed (scaling out) after completion either automatically or manually.

e) Measured Service: Based on level of services, a metered system – metric is charged. The metrics are charged by amount of storage used, number of transactions, network I/O, amount of processing power by the clients. The resource usage are monitored, measured, controlled, audited and reported to customers transparently.

## IV. Cloud Security Architecture

Cloud Security falls on responsible of both provider and consumer. To Secure the Cloud, CSP (Cloud Service Provider) should carefully review the SLA (Service Level Agreement) of the enterprise using security measures.

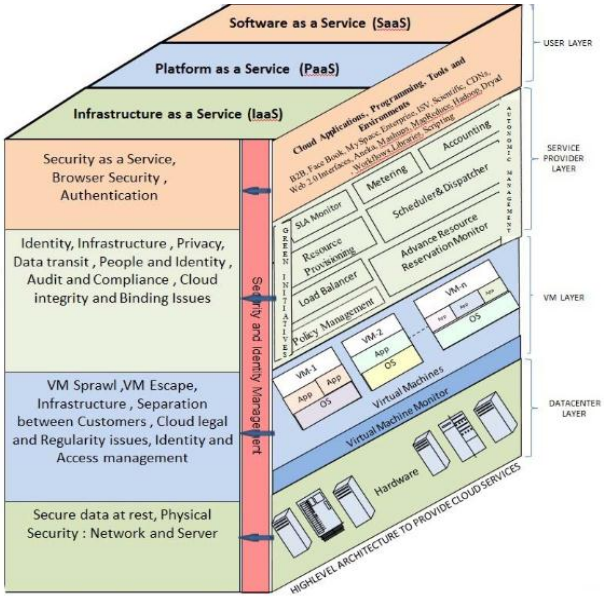


Fig. 3

## V. Cloud Security Issues

According to Security concern, security issues are categorized under security issues faced by cloud provider and security issues faced by their customers[11]. From the security Perspective, the important aspects to design a secure system includes *Confidentiality*, *Integrity* and *Availability*.

***Confidentiality and Privacy***
It refers only the authorized parties to access the protected data. The issues related are multitenancy, data remanence, application security and privacy.
*Privacy*- refers the disclosure of personal information.

***Integrity***
It describes as assets can be modified only by authorized person in authorized way of data, software and hardware.
*Data Integrity* includes protecting data from unauthorized deletion, modification (or) fabrication.
*Software Integrity* includes protecting software from unauthorized deletion, modification (or) fabrication.

 

*Authorization* is the mechanism which determines the secured resource authenticated by user. Cloud computing provider is trusted to maintain data integrity and accuracy.

***Availability***

It refers the property of a system being accessed and used by authorized user based on demand. The system should continue operations even in the situation of security breach.

Cloud Security issues which are discovered by CSA's (Cloud Security Alliance) are as follows [9].

a). Misuse and reprehensible use of cloud Computing
b). Insecure API
c). Wicked Insiders
d). Shared Technology issues / multi-tenancy nature.
f). Account, Service and Traffic Hijacking
g). Unidentified Risk Report.
e). Data Crash

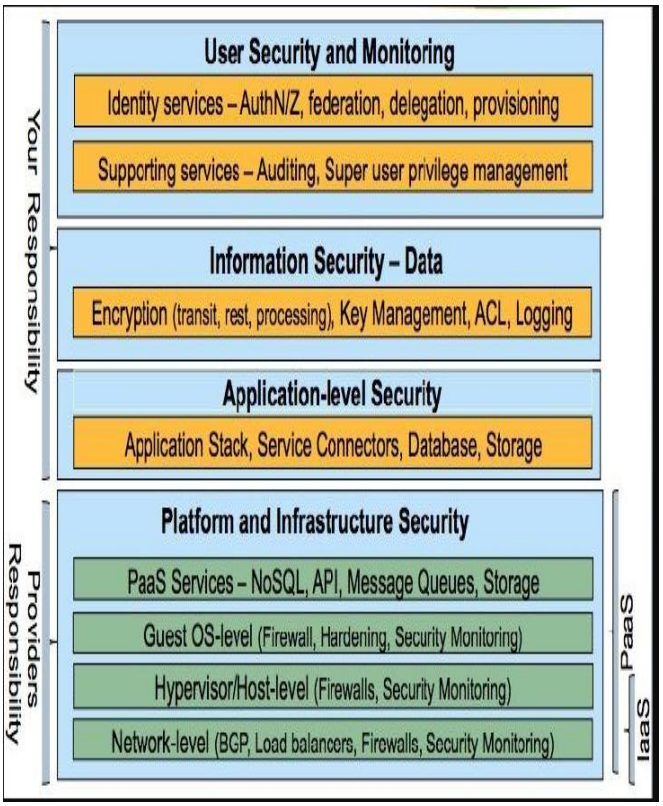


Figure 4: Cloud Security Responsibility services.

## VI. CLOUD SECURITY THREATS

From the view point of security, Cloud providers have no assurance over data security. There is a big question mark, *"Is the cloud secure or not ?".*Security mechanisms which are used to counter the security threats are listed below [12].

**Traffic Eavesdropping:** It occurs when data are copied and transferred from cloud consumer to cloud provider. The *malicious service agent* – passively attack to gather information and break the confidentiality of data.

**Malicious Intermediary:** It arises when messages are intercept and altered by *malicious service agent* of harmful data before forwarding to destination.

**Denial of Service:** This attack arises when overloading IT resources and cannot function properly. As a result, attacker gets direct access to IT resources.

**Virtualization Attack:** It exploits Vulnerabilities in the virtualization platform of its Confidentiality, Integrity and Availability.

**Overlapping Trust Boundaries:** Malicious cloud service consumers overlap trust boundary to compromise cloud consumer and other IT resources. Multiple cloud consumers share same physical server and respective trust boundary.

The additional considerations include Flawed implementations, Security policy Disparity, Contracts, Risk management.

## VII. CLOUD SECURITY CHALLENGES AND SOLUTIONS

Cloud users wish to store their data in encrypted format. Before data is stored, it must be secured for integrity of data ENCRYPTION.

Encryption mechanism helps to counter the traffic eavesdropping, malicious intermediary, insufficient authorization and overlapping trust boundaries security threats[12].

There are two forms of encryption:

- ✓ symmetric
- ✓ asymmetric

**symmetric encryption:** This method uses same key for encryption and decryption. Authentication is performed by authorized users to maintain confidentiality.

**asymmetric encryption:** This method uses different key for encryption and decryption. The private key is known to the owner where public key is commonly available.

To handle sensitive data in the cloud environment, cloud providers must face the challenge of security risks such as recovery, backup, data transition, encryption, access control, log monitoring, intrusion detection, customer service, auditing and etc.,

Key Management system (KMS) is used to secure the software updation from machine to machine communication. It generates the key, exchanges the key, handles the key, stores and finally maintains in an efficient manner for clients usage [14]. It answers to many questions like,

- ✓ How to handle keys?
- ✓ Where should keys to be stored?
- ✓ Who has the rights to access the keys?

 

- ✓ How to recover data if key is lost?

Some of the security benefits are centralizing the data, logging, forensics, auditing, developing to new concern.

## VIII. SUMMARY OF THE PAPER

Table 2: Key points of Security Cloud

| Characteristics of Security | Description |
|---|---|
| Confidentiality, Integrity,Availability | To measure security |
| Threats,Vulnerabilities, Risks | To measure and access insecurity (lack of security) |
| Security controls, Security mechanism, Security policies | To countermeasure and safeguard – for improving security. |

## IX. CONCLUSION

The cloud providers have to ensure the sensitive information of customers to overcome security issues. Integrated cloud security framework accelerate the critical services to optimize and improve security gap of dynamic resources with scalability. Thus concluding this paper, by carefully reviewing the service provider's backup procedures to avoid security threats. To get better cloud security solutions one should review and backup the file from time to time regularly. To make sense of security, improve the availability and quality of service at all levels using essential protocols, specifications and tools.

## REFERENCES

[1]Dr.P.Madhubala and Dr.P.Thangaraj – "Comprehensive and Comparative Analysis of Cryptographic Solutions in Cloud", ISSN ONLINE(2320-9801) PRINT(2320-9798).

[2] P. Madhubala, P. Thangaraj, - "Key Generation Policy for Durable Storage in Cloud" - ISSN: 232 7782 1 (Online) Computer Science and Management Studies International Journal of Advance Research in Volume 3, Issue 2, February 2015.

[3] Charles P. Pfleegar, Shari Lawrence Pfleegar, Jonathan Margulies – " Security in Computing ", Fifth edition.

[4] 4 Best cloud Deployment Models – Types and Examples, SAM solutions. Aug 15, 2017.

[5].Subra Kumarasamy, "Introduction to Cloud Security Architecture from a Cloud Consumer's Perspective", 2011.

[6] Mohammad Haris, Rafiqul Zaman Khan – A Systematic Review on cloud Computing, International Journal of Computer Sciences and Engineering Open Access, Vol-6, Issue-11, Nov 2018, E-ISSN:2347-2693.

[7] Cloud Computing Security Architecture for IaaS, PaaS, SaaS.

[8]. V. Krishna Reddy, Dr. L.S.S. Reddy – "Security Architecture of Cloud Computing", International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462, Vol 3 No. 9, September 2011

[9]. Varsha, Amit Wadhwa, Swati Gupta, "Study of Security Issues in Cloud computing", Inernational Journal of Computer Science and Mobile Computing, ISSN 2320-088X, IJCSMC, Vol. 4, Issue 6, June 2015, pg.230-234, Research Article.

[10]. Barrie Sosinsky – "Cloud Computing – Bible", Book, Wiley India Pvt Ltd.

[11]. Dimitrios Zissis, Dimitrios Lekkas – "Addressing Cloud Computing Security Issues", Future Generation Computer Systems-ELSEVIER, Vol.28, Issue 8, March-2012, Pages 583-592.

[12]. Thomas Erl, Zaigham Mahmood, Richardo Puttini – "Cloud Computing – Concepts, Technology & Architecture", Book, Pearson.

[13]. Dr. Kumar Saurabh – "Cloud Computing", Book, Wiley.

## Authors Profile

TITLE : SECURITY ISSUES IN THE CLOUD COMPUTING ENVIRONMENT : AN OVERVIEW

NAME : RAJALAKSHMI. S

DESIGNATION : GUEST LECTURER CUM RESEARCH SCHOLAR
DEPARTMENT OF COMPUTER SCIENCE
GOVERNMENT ARTS COLLEGE FOR WOMEN,
KRISHNAGIRI – 635002.

E-MAIL ID : rajaylakshmiravi7@gmail.com

CONTACT NO. :

GUIDE NAME : Dr.P.MADHUBALA, M.Sc., M.Phil., M.C.A., B.Ed., P.hd.,

DESIGNATION : HOD CUM RESEARCH SUPERVISOR,
DEPARTMENT OF COMPUTER SCIENCE,
DON BOSCO COLLEGE, DHARMAPURI.

 