# Data transmission security challenges in cloud computing as a SaaS Model

Ashish A. Patokar, Dr. V. M. Patil

**Abstract**— Cloud computing is one of the developing technologies in the field of IT and Computer Science which is remotely sharing all the resources and the services that can be attached to it. This is the classic idea of attaching resources and services under the name of cloud computing that provide the services to the internet and client end side do not require any type of applications software to be installed in order to provide the services related to the cloud computing. According to studies of this field, one of the major challenges of this technology is the security and safety required for providing services and built trust in consumers to transfer their data into the cloud. In this paper propose discuss and focus and challenges regarding the security of data storage and transmission in cloud environment as a SaaS model.

**Index Terms**— Cloud computing, Security, Software as a Service (SaaS) , Security challenges.

---

## 1 Introduction

Now a day's cloud computing play an important role in order to access the data and sharing the various resources with an efficient, flexible and class effective manner. However hackers, attackers and security researchers have shown that the most of the security model develop for this purpose are not hundred percent secure. In a clouded environment security issue are play between cloud services provider and cloud user. There is a scope for improving security in order to recover security threads that can be raised inside or outside of cloud provider and consumers environment that can be broadly classified as inside threads outsiders malicious attack data loss of control issue related to multi-tenancy and data destructions [1][2].

Cloud computing is the technique which is remotely sharing all resources and services by means of Services as a Software for many application through internet and in most of the cases no required any special types of software in order to access this devises and services [8].

### 1.1 Services of Cloud Computing

Broadly divide this cloud computing in three types:
a. SaaS b. PaaS c. IaaS

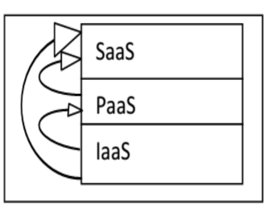



**Figure 1:-Types of cloud computing**

- *Ashish Patokar is currently working as Asstt. Professor in Deptt. Of Computer Science & IT, Shri Shivaji College of Akola.*
- *Dr. V. M. Patil is currently working as a Head & Associate Professor in Department of Computer Science & IT, Shri Shivaji College of Akola.*

a. **SaaS** –Is a delivery model used as application and manage in a services provider data center and access via a browser over internet connection. The client has to depends on the service provider for proper security measure and in case of multi user don't gate to access the data of each other in order to maintain the security and assure that the applications will be available whenever that will be need. In SaaS software vender made the applications on its private server and deployed in cloud computing infrastructure service available by third party (Amazon, Google etc.) that can reduce the investment in infrastructure services and provide the better service to the customer how ever in SaaS model enterprises data is available at SaaS provider data center as well as data center of other enterprises. The cloud provider replicates the data at multiple locations across the countries in order to maintain high availability and reduce the searching time

Cloud computing provider faces the common security challenge by traditional communication system [3] [7].

b. **PaaS** – Platform as a service is the next level of service that is used as a software/ application platform. This layer consist of application framework on the basis of SaaS layer for example Google Apps engine and Microsoft azure both offer a number of programming tools for this level [3].

c. **IaaS** – This layer provides infrastructure services such as CPU, memory, storage and networking products known as Infrastructure as a service [3][9].

## 2 CLOUD COMPUTING TYPES

Cloud computing provides the facility to access and shared resources and common utilization of infrastructure, offering services on demand over the internet to perform operations as per the need of enterprises.

The cloud computing environment can broadly split into the following types of clouds.

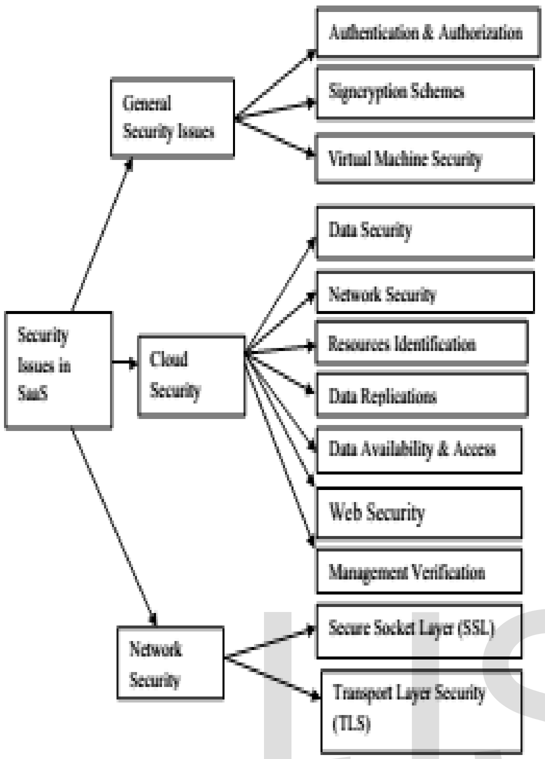
### 2. 1 Public Clouds

In Public Clouds infrastructure are made available to the general public by a service provider who hosts the cloud infrastructure. It is acceable to all in which the resources, applications and web server through internet and the public organizations help to provide and supply sub structure to own the public clouds [3].

### 2.2 Private Clouds

Private Cloud can utilize the cloud infrastructure to a

**Figure 2 :** Security Issues in SaaS




particular enterprise. These clouds computing environments utilize within the organizations and only for organizations benefits this is also called as internal clouds that can be used to optimize the infrastructure resources within the enterprise using the concept of greed and virtualization that improve the average server utilization with low cost and maximum efficiencies. The high level of atomization and reducing the operation cost [3].

### 2.3 Community Cloud

Community Clouds shares infrastructure within several organizations for a specific Community and managed internally by common facility [3].

### 2.4 Hybrid Cloud

The Hybrid cloud is a combination of two or more clouds including Public, Private and Community and that can be used for internal and external clouds [3].

## 3 DATA TRANSMISSION SECURITY CHALLENGES IN CLOUD COMPUTING

The sensitive data of the various enterprises continue the reside within inside and the boundary of the cloud which is subject to which physical ,logical and personnel security and types of access control. In SaaS model the data is stored in a server and that can be transmit or can be communicate within the cloud. For these purpose security checks are essential to ensure the data security vulnerabilities in applications or through malicious employees. These force to develop security of the cloud data during transmission and face to challenges. The data transmission security challenges over the cloud computing can be broadly categorized into following types:

**3.1 General Security Issues**
**3.2 Cloud security Issues**
**3.3 Network Security Issues**

3.1 General Security Issues:
- 3.1.1 Authentication and Authorization
- 3.1.2 Signcryption Schemes
- 3.1.3 Virtual Machine Security

3.2 Cloud Security Issues
- 3.2.1 Data security
- 3.2.2 Network Security
- 3.2.3 Resources Identifications
- 3.2.4 Data Replications
- 3.2.5 Data Availability and access
- 3.2.6 Web Security
- 3.2.7 Management Verifications

3.3 Network Security Issues
- 3.3.1 Secure Socket layer (SSL)
- 3.3.2 Transport layer Security (TLS)

### 3.1 General Security Issues:

#### 3.1.1 Authentication and Authorization

Authentication and Authorization provides a way of identifying a user by having the user enter a valid user name and valid password before access is granted. The authorization process determines whether the user has the authority to issue such type of commands. This scheme also provides mutual authentication, identify management, user privacy and security for the cloud environment.

#### 3.1.2 Signcryption Schemes

Signcrption is combination of encryption and digital signature security schemes. Signcrption is used to minimize the cost overhead which is more in case of encryption and digital signature. Time and cost are the required factors for any process and we are incorporating security levels to the data and this will results improving time and cost factors.

#### 3.1.3 Virtual Machine Security

Virtualization is a recent phenomenon in virtualized infrastructure. The virtual machines used in cloud providers may have vulnerabilities such type of vulnerabilities represent more serious problem in multi-tenant environment.

### 3.2 Cloud Security Issues

#### 3.2.1 Data security

The data security issue is mainly related to the polices provided to the user during accessing a data. In typical cases a small enterprise can use a cloud provided by some enterprises to carry out a business process. This organization will have its own security strategies based on employ access to a particular data on a cloud. These security policies must be bound to the cloud to avoid intrusion of data by unauthorized access . The SaaS model must be flexiable to deploy a specific policy suggested by organization and also boundary within the cloud in case of multiple organization within a single cloud environment.

### 3.2.2 Network Security

In SaaS model precise data is obtained from the enterprises, refined by the SaaS application stored at the end of SaaS vendor. All the data flow over these networks needs to be secured in order to prevent leakage of sensitive information.

The network layer provides significant protection across traditional network security issue, such as MITM (man-in –the-middle) attacks, IP Spoofing, port scanning, packet sniffing etc. Amazon S3 is accessible via SSL encrypted endpoints in case of maximum security [4].

### 3.2.3 Resources Identifications

In SaaS model of cloud computing environment the end user utilize the services attach by cloud without knowing exactly where the resource are located and identified possibly in other legislative domains these cause of potential problem disputes arrives during the identification of resources available in service providers .Due to the compliances and data private locks in different countries., the identifications of data is the most important in such enterprises architecture. In a SaaS secure model give the service that is reliable to the costumer after identification of data for that costumers.

### 3.2.4 Data Replication

Data replication is the process of copying or moving enterprise data from one storage system to another. The SaaS vendor needs to ensure that all sensitive enterprise data is regularly backed up and in cloud vendors such Amazon, the data at rest in S3 is not encrypted by default. DR is sometimes confused with ETL (extract, transform, and load) tools [4].

### 3.2.5 Data availability and access

Data availability and access is mainly associated to security polices supplied to the users while accessing the data. Small business organization can use a cloud supplied by some other provider for carrying out its business process. The SaaS model must be flexible enough to incorporate the reserved polices put forward by the organization [4].

### 3.2.6 Web Security

SaaS software deployed over the internet and is setup to run behind a firewall in local area network or personal computer.

The key features include network-based access and commercially available software and managing activities from central locations rather than at customer's site, permissive customers to access applications remotely via the web. SaaS model may use various types of software components and frameworks. For example components for subscription management grid computing software, web application frameworks etc [4].

### 3.2.7 Management Verifications

Management verifications are part of the internal control system of managed organisation. They are the normal day to day controls made by management within an organisation. A simple example of one such verification in a typical organisation would be to compare goods actually delivered to the related purchase order in terms of quantity of goods, price and condition. This verification ensures that the actual quantity of goods ordered have been received at the agreed price and are of the desired quality[4][10].

### 3.3 Network Security Issues

Network Security Issues broadly consider in following ways:

### 3.3.1 Secure Socket layer (SSL)

In cloud computing all data flow over the internet need to be secure in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) [4].

### 3.3.2 Transport layer Security (TLS)

Transport Layer Security (TLS) are frequently referred to as 'TLS', are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols are in widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP(VoIP)[4]

## CONCLUSION

In this paper focus on cloud computing service providing SaaS model for which the data transmission security faces so many challenges in data storage cloud environment particularly for identification resources and data when it is located in public cloud.

## REFERENCES

[1] Sajjid Hashemi, "Data storage Security Challenges in Cloud Computing", International Journal of Security , Privacy and trust Management(IJSPTM), Vol. 2, No 4 August 2013,pp 1-9.

[2] Kevin Hamlen, Murat Kantarcioglu, Latifur khan and Bhavani Thuraisingham, "Security issues for cloud computing", International journal of Information security and privacy, 4(2), April-June 2010, pp 39-51.

[3] Seema B. Bhalekar, "Cloud Computing structure, services and challenges: A Review", National conference on Recent Advances in Electronics and computer science-NCRAECS-2014, 2014, pp 199-203.

[4] Rashmi, Dr. G. Sahoo, and Dr. S. Mehfuz, "Securing software as a service Model of cloud computing: Issues and solutions", International Journal on cloud computing: Services and Architecture, vol. 3, No. 4, August 2013, pp 1-11.

[5] Sunil Maggu, Dr. V. K. Gupta, Meenu Dhingra, " Data Security using Signcryption and Relocation Techniques in cloud computing," International Journal of Advances in Engineering Sciences, ISSN:2231-0347, vol. 3, Issue 2,April 2013, pp 8-11.

[6] Boyang Wang, Sherman S.M. Chow, Ming LI and Hui Li, "Storing shared data on cloud vi Security-Mediator" IEEE 33rd International Conference on Distributed computing systems, 1063-6927/13, 2013, pp 124-133.

[7] Srinivasa Rao, Nageswara Rao and E Kusuma Kumari, "Cloud computing: An Overview", Journal of Theoretical and Applied Information Technology, 2005-2009 JATIT, pp 71-76.

[8] Deepanchandravarthi Purushothaman and Dr. Sunita Abburu, "An approach for data storage security in cloud computing", ISSN: 1694-0814, vol. 9, Issue 2, No 1, March 2012, pp 100-105.

[9] Rampal singh, Sawan kumar, Shani kumar Agrahari, "Ensuring data

storage security in cloud computing", and IOSR Journal of Engineering e-ISSN: 2250-3021, p-ISSN: 2278-8719, vol.2, Issue 12, Dec. 2012, pp 77-21.
[10] Valid Ashktorab and Seyed Reza Taghizadeh, "Security Threats and Countermeasures in Cloud Computing", ISSN 2319-4847, vol. 1, Issue2,October 2012,pp 234-245.