International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307
Technical Note

Various Security Issues and Challenges in Cloud Computing

Rajat Jain
School of Computer Science & IT, DAVV University, Indore, Madhya Pradesh, India

ABSTRACT

Cloud computing is latest technology that is being widely used all over the world. Cloud is the collection of network, storage, server, services and application, interface that helps in delivering the computing as a service. Cloud Computing is the technology which uses the cloud to provide services to user whenever and wherever it require. Their main work is to perform manipulation, configuration and provide services to user. This paper outlines that what is cloud computing, the technologies which are working behind cloud computing, different models, Security issues, research challenges and security algorithm which are currently present in Cloud Computing.

Keywords: Cloud Computing, CSP, Grid Computing, Virtualization, PAAS, SAAS, IAAS.

I. INTRODUCTION

According to U.S. NIST(national institute of standards and technology) " Cloud Computing is a model for enabling convenient , on demand network access to shared pool of configurable computing resources (e.g.: network, storage, server, services and application) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction . "It is a distributed architecture that centralize the server resources on a scalable platform so that they can easily provide the demand computing services to the user. In such environment user don't have any need to install any types of software to run their business or to complete the task. It is one of the advantage of cloud computing by which the user can easily save our time and money. The goal of cloud computing is to make the use of increasing computing power to execute millions of instruction per second. Cloud computing uses the network of large group specialized connection to distribute the data processing among the server. Without installing a software suit into each computer, it provide to install a single software in each computer that allow the user to log into their web based services. It is being used to minimize the usage cost of computing resources. Cloud Computing consist of front end and back end. Front end includes user computer, software required to access the cloud network. Back end includes various computer, database system, servers that create the cloud. The user can access the cloud network from anywhere in the world by connecting to the cloud via internet. Some of the real time example which uses the cloud computing are Gmail, Dropbox, Google calendars etc. Cloud Service Provider (CSP) offers the platform to their customer or user to use and create their web services. It is like a ISP (Internet Service Provider) because ISP also offers internet services to their user. Some technologies are their which are working just behind the cloud computing platform to make the cloud more flexible, reliable, and usable.

1. **Virtualization**: It is a technique to share the physical resources among multiple organization or customer. It assigns logical name the physical resources and providing pointer to those physical resources when demanded.
2. **Service oriented architecture**: It helps to use the application as a service to other resources regardless the type of product, vendor, or technology. That's why it is possible to exchange the data between the applications of different vendor without any changes to service.
3. **Grid Computing**: It refers to the distributed computing in which multiple computer form different location are connected with each other to achieve common objective. Grid Computing breaks the complex problem into small piece of set. These set are

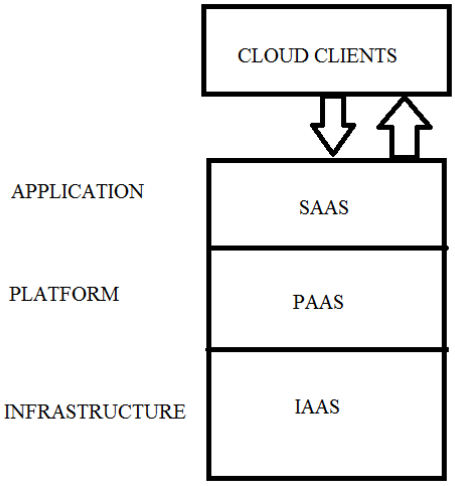
distributed to several pc which are present in Grid environment.

4. **Utility Computing:** It is based on pay per use model. It offer computational resources on demand. Cloud Computing, Grid Computing, managed IT service are based on utility computing concept.

II. Basic Building Block

In General, Cloud Computing model are divided into two categories: Service model and Deployment model. The Cloud Service Provider provide three types of services: IAAS (Infrastructure as a service), PAAS (Platform as a service) and SAAS (Software as a service).

IAAS (Infrastructure as a service): It refers to the sharing of hardware resources for executing services by using virtualization technology .Its main objective is to make the resources more readily by application and operating system .For this it provide access to user to use the resources like :physical machine , virtual machine etc. Example of Infrastructure as a service includes Amazon EC2, Go Grid etc.



PAAS (Platform as a service): It provides computing platform and software services to the end user without downloading software or installing them. It provides the infrastructure to implement the cloud application. It provide runtime environment to the application, deployment tools etc. Example of Platform as a service includes Microsoft azure etc.

SAAS (Software as a service): It allows to use software on demand pay per use to the end user. By use of this service ASP (Application Service Provider) provide software application to end user. This makes the customer to get rid of installing and operating application on own computer and it reduce load of maintenance of heavy software application. Example of Software as a service includes Google app.

Deployment Model: Mainly four types of cloud deployment model are there: Public, Private, Hybrid, and Community.

Public Cloud: It allows the system and services to be easily accessible to the general public. It is managed by third party and it exists beyond the company firewall. It is less secure because of its openness nature.

Private Cloud: It allows the system and services to be accessible within an organization. It can be owned or leased by some organization and it exists on-premises. It is more secure compare to public cloud because of it private nature.

Hybrid Cloud: It is the combination of public and private cloud. Critical activity is performed by private cloud and non-critical activity is performed by public cloud. It linked in such a way that data transfer between both of them will not affect each other.

Community Cloud: It allows the system and services to be accessible by the group of organization. These cloud are normally based on agreement between related business organizations like banking etc.

Cloud Computing Entities: Mainly Four types of entities are there in cloud computing and they are: provider, consumer, reseller, and broker.

Cloud Provider: It provides Internet Connection or infrastructure and it enable consumer to access the services.

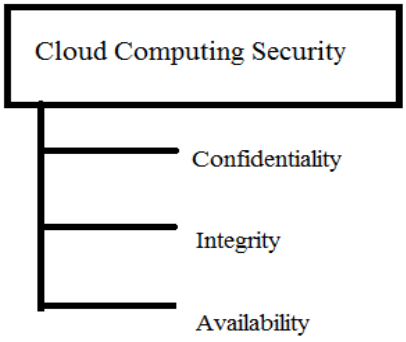
Cloud Consumer: End-user belongs to this category.

Cloud Service Broker: It is like an influencer which guide the consumer to select best cloud computing solution.

Cloud Resellers: It play vital role when cloud provider want to expand their business across the continent.

III. Cloud Computing Security

Security plays the vital role in the success of any technology. Security means to secure something from unauthorized entity. It mainly focuses on the three aspects: confidentiality, Integrity, Availability. Confidentiality means to protect data from unauthorized person. Integrity means completeness of information. Availability means authorized user should be reliable and timely access to the information. So similarly security is also requiring in Cloud Computing.



There are numerous issues are there but majorly they fall into two category: Security faced by service provider. Security faced by customer. In the case of provider, it must ensure that their infrastructure is secure and their client's data are protected. But customer must ensure that provider has taken adequate security measure to protect their data. Cloud Computing encompasses many technology include network, operating system, load balancing, concurrency control, memory management. Just because of that all security issues and concerns of these technology are also applicable to cloud computing too. In cloud computing, limited control of user over data may incur various security issues and threat in which include: data leakage, insecure interface, sharing of resources etc. The user have neither control of, nor any knowledge of, what could be happen with their data .If user want to store some personal information in the cloud so user will have to compromise with their privacy. So it's the responsibility of cloud service provider to provide the adequate security to their customer or user. Some sensitive states are there in cloud computing:

1. Transmission of sensitive data to the cloud server
2. Transmission of data from cloud server to client computer.
3. Storage of client data in cloud server which are remote server not owned by the client.

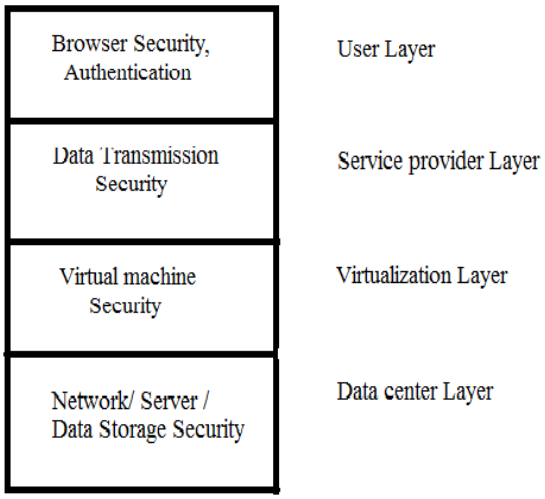


Fig.2 Cloud computing security architecture

Cloud Client are facing two type of security threat: internal and external threat .In External threat , malicious user outside the cloud often perform Dos attack to affect the availability of cloud services and resources. But internal threat are also called authorized person, it can easily get access of other user without being detected.

Various security issues concern in cloud computing environment and which are given below:

- **Data Transmission**: Encryption is a technique that we use to transfer the message from one place to another place securely. We always want that during data transmission it does not change which means whatever data that sender is sending to receiver it received correct .For maintaining authentication and integrity we use SSL protocol. But in cloud Computing, most of the data is not encrypted in processing time .Just because of this the chances of Man-In-The-Middle attack during processing time increase. So it may possible that this attack can interrupt or change the data.

- **Data Security**: To achieve the services of cloud computing the most common utilizing protocol is HTTP (Hyper Text Transfer Protocol) and to maintain the security we use HTTPS (Hyper Text Transfer Protocol Secure and Secure Shell). In traditional time, sensitive data used to present within the enterprise boundary so it's the subject to its physical security, logical security. But now in cloud computing all the sensitive information are stored at third party which means outside the

enterprise. So service provider must adopt the additional security check to protect this information.

- **Access to its server and application**: Access of data is mainly related to the security policy provided to user by the third party or CSP. Small organization uses the cloud which is provided by some other provider to run its business. But some organizations have its own security policy and which is based on that which employee access which type of data set.

- **Data Integrity**: Integrity means the uniqness of data or completeness of information .but data can be alter or corrupt at any level of storage with any type of media. So monitoring the integrity of data is very essential .But it can be easily achieved by using standalone system and with single database.

- **Data Availability**: Availability of data is one of the major issues in cloud environment .Because client always store data in cloud environment and it access remotely but data is stored at cloud service provider. And If suddenly system failure occur so client have to suffer a lot.

- **Data Location**: Location of data is also a major issues because user do not aware of the exact location of their data and they do not have a control over physical access to their data .Most of Cloud service provider have datacenter around the globe .So this may be an issue because every country has different rules and regulation.

- **Privacy**: Cloud computing use the virtual computing environment for their manipulation and data of client is stored in a scattered manner rather in a one place. User information may be leak when they are using cloud computing services. Attacker can also analyze the movement of client by performing their task activity.

- **Trust**: Trust is the most important issue in cloud computing. Because trust can be in between human to machine, machine to human, human to human, machine to machine. Trust is revolving around assurance and confidence. User stores their information on cloud because they have trust. For example: People use Gmail, yahoo because they have trust on provider.

Various Research Challenges:

- **Cloud Data Management**: The data stored in cloud, they are always in unstructured form. Cloud data management is one of the major research topic in cloud computing. Since Service provider do not have right to access data physically in the data center so for that they have to depend on infrastructure provider. So infrastructure provider must ensure the objective like confidentiality, audibility.

- **Access Contro**l: Authentication and Identity management is the important factor to control the access and protect the cloud environment form unauthorized entity. What level of password strength that service provider is providing? And what methodology is that they are using to recover username and password? If you use strong password and provide the facility to easily change them. So it helps to protect the element.

- **Reliability and availability of service**: The software needs to have reliable quality of factor so that client uses the service under any network condition. To avoid this problem, Service provider turned into the technology like: Google Gear, Adobe AIR etc. It allows the cloud based application to run locally or under any network condition.

Technologies for Security in Cloud Computing:

In Cloud Computing environment, we need secure technologies for privacy and protecting data. And some technologies are:

- **Firewall**: To decrease the attack surface of virtualized server in cloud environment, firewall is deployed on individual virtual machine for controlling incoming and outgoing traffic based on applied rule to prevent from unauthorized access.
- **Intrusion Detection System**: Intrusion is the activity to violate the security policy of system but Intrusion detection system is the process to identify those intrusion in the system.

- **Third Party Auditor**: Check the integrity of data which are present at the cloud server and ensure the user also that their data is secure.
- **Cryptography**: These is we use to hide the message so that other cannot get the message by performing encryption and decryption operation by using public and private key. Mainly two kind of cryptography algorithm are there which are given in fig 3 :

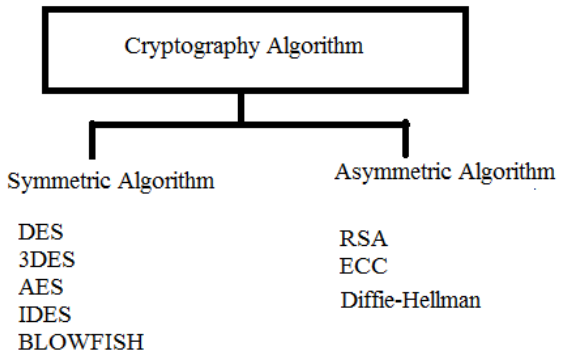


Fig 3

In Symmetric Algorithm, we perform encryption and decryption operation by using same algorithm and same key. But in Asymmetric Algorithm we use different key and different algorithm.

DES: It stands for data encryption standard. It is an improvement of algorithm Lucifer. It is the most widely used symmetric key algorithm. In which we use 64 bit plain text and try to produce 64 bit cipher text by performing 19 distinct stages.

Algorithm:
Function DES_Encrypt (M, K) where M = (L, R)
M IP(M)
For round 1 to 16 do
Ki SK (K, round)
L L xor F(R, Ki)
swap(L, R)
end
swap(L, R)
M IP-1(M)
return M
End

AES: It stands for advanced encryption standard. It is the non fiestal cipher which perform encryption and decryption operation with the key size of 128, 192,256 bit with number of rounds respectively 10, 12, 14.

Algorithm

Key Expansion
Initial Round
Add Round Key
Rounds
Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column
Add Round Key—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
Final Round (no Mix Columns)
Sub Bytes
Shift Rows
Add Round Key

RSA: It is the most widely used general public key encryption algorithm published in 1978, which involve public and private key both for encryption and decryption.

Algorithm
Key Generation: KeyGen(p, q)
Input:
Two large primes – p, q
Compute n = p . q
$\varphi(n) = (p - 1)(q - 1)$
Choose e such that $\gcd(e, \varphi(n)) = 1$
Determine d such that $e \cdot d \equiv 1 \bmod \varphi(n)$
Key:
public key = (e, n)
secret key= (d, n)
Encryption:
c = m E mod n

Diffie-Hellman key exchange: First public key type scheme in 1976 along with the exposition of public key concept. It is practical method for public key exchange of a secret Key.

IV. CONCLUSION

Cloud computing is the cost, time and performance effective technology. Of course the usage of cloud computing will surely will increase more in next few years. In this paper we have discussed what is cloud computing, their different model, various security issues in cloud computing like: privacy, availability, locality, integrity and research challenges. We also have explained various security algorithm used in cloud computing. Security of cloud computing is an non-compromised issue. Data security and data location are the two major issues in the context of cloud computing. Establishing trust is one of the way to overcome these security issues as it establishes the entity relationship quickly and safely. Security and privacy issues can be overcome by employing encryption, security hardware and security application.. DES and AES are mostly used symmetric algorithm. RSA and Diffie-Hellman key exchange are used for asymmetric algorithm. These issues will be the key research area of cloud computing. There is no doubt that cloud computing has bright future.

V. REFERENCES

[1]. Manpreet kaur , Hardeep Sinha " A review of cloud computing security issues " International Journal of Advances in Engineering & Technology, June, 2015.

[2]. Rajani Sharma , Rajendra Kumar Trivedi " Literature Review : Cloud Computing- Security issues, solution and technology " International Journal of Engineering Research Volume No.3 April 2014.

[3]. Gururaj Ramchandra, Mohsin Iftikhar "A Comprehensive Survey on Security in Cloud Computing" 3rd international workshop on cyber security and digital investigation (CSDI 2017).

[4]. Santosh Kumar and R.H. Goudar " Cloud Computing – Research Issues , Challenges, architecture , platform and application-Survey" International Journal of Future Computer and Communication Vol 1 No. 4 Dec 2012

[5]. Cloud Computing Tutorial Points

[6]. Mohsin Nazir "Cloud Computing: Overview and Current Research Challenges "IOSR Journal of Computer Enginnering Vol.8 Dec 2012.

[7]. Sonia Sindhu " A Survey of Security Algorithm in Cloud Computing " International Journal of Advanced Research in Computer Engineering and Technology Vol.4 May 2015