IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 6, June 2021

DOI 10.17148/IJARCCE.2021.10657

# CLOUD SECURITY PROBLEMS AND STRATEGIES

**Suhaas Nagabhirava[1], Nagaraj G Cholli [2]**

Student, Information Science and Engineering, R V College of Engineering, Bengaluru, India [1]

Associate Professor, Information Science and Engineering, R V College of Engineering, Bengaluru, India[2]

**Abstract**: Cloud computing is a technology encompassing a set of resources and services that are offered over the internet or a network. Cloud Service Providers (CSP) provides virtual resources over the internet to its users. It is absolute necessity to have secure architecture to provide services through the cloud in safe manner. The cloud infrastructure uses virtualization extensively. Extensive usage of virtualization causes security concerns for customers of public cloud service. Virtualization alters the relationship between the OS and hardware in all the three areas namely computing, storage and networking. The data is stored in the cloud by the users for accessing whenever they need. Any compromise in the security of the data in the cloud causes loss of trust in the cloud service provider (CSP). We will discuss, in this paper, few cloud security issues in certain aspects like multi-tenancy, elasticity, availability etc. and various methods on how to overcome these security issues of the cloud. We will also discuss the techniques and approaches for security of the data in the cloud.

**Keywords**: Cloud Security Standards, Cloud Computing , Cloud Security, Cloud Security Standards, Security Techniques, Security Threats

## I. INTRODUCTION

One can call Cloud computing as another name for Internet computing. As per National Institute of Standards and Technology (NIST), the definition for cloud computing is: “Cloud computing is a model for enabling on-demand and convenient network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and deprovisioned with minimal management effort or CSP interaction.

There are various ways of utilizing the cloud services. Some users consume just computing power and storage while others access a particular application from the cloud.

Cloud computing is very useful across the user communities. Cloud computing is useful for flexibility, scalability, and easy availability of data. This is also an enabler for cost reduction as multiple organizations share the resources in an optimum manner. Gmail, Dropbox, Instagram, and Facebook are some examples of cloud computing solutions.

## II. CLOUD DEPLOYMENT MODELS

i) Private cloud – Leased or owned by an organization for their individual use. For example, a large organization that does not want to expose their data to outside their network.
ii) Public cloud – Large Data Centers hosting services for many customers across geographies over the internet.
iii) Hybrid cloud – Combination of two or more clouds such as a public cloud and a private cloud. Few organizations chose public cloud for less sensitive applications and private cloud for their internal financial related applications which are more secure in nature.
iv) Community cloud – Shared infrastructure for specific community such as a group of Cooperative Banks, NGOs etc.

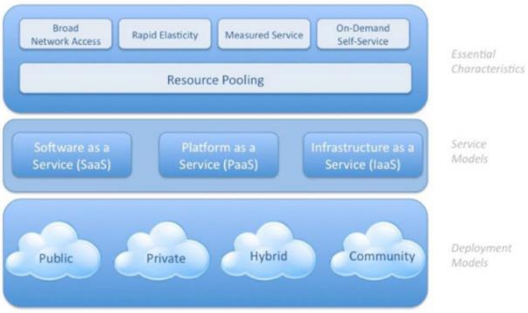

Fig. 1 **NIST model - definition of Cloud computing**

## III. TYPES OF CLOUD SERVICE

Cloud computing consists of three different types of service provision as shown in Fig 2. In each case services are hosted remotely and accessed over internet through customer web browser, rather than being installed locally on customer ‘s computer.

- **<u>SaaS</u> (software as a service)**: refers to the provision of software applications in the cloud customizable within limits, solving specific business needs, with focus on end user requirements.
- **<u>PaaS</u> (platform as a service)**: refers to the provision of services that enable the customers to deploy in the cloud, applications created using programming languages and tools provided by the supplier. No need to directly manage OS, databases,
- **<u>IaaS</u> (infrastructure as a service)**: refers to the services providing compute services, there is no need to procure and manage physical data center equipment (servers, storage, networking, etc.)

Following pictorial representation clearly shows different types of cloud service models and how they are managed.

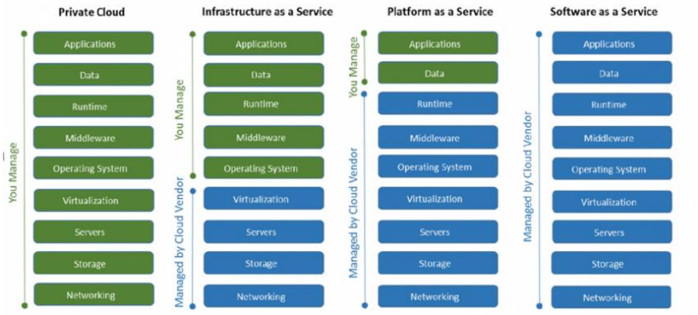

Fig. 2 **Cloud Service models**

## IV. MAIN CHARACTERISTICS OF CLOUD

A. **<u>On-demand self-service</u>** - A consumer can configure and provision services such as Compute, Storage and Network as per his/her requirements using provisioning tools automatically without requiring CSP intervention.
B. **<u>Ubiquitous network access</u>** - Network Access Capabilities are available over the network and accessed through standard techniques that promote use by thick or thin client platforms.
C. **<u>Location independent resource pooling</u>** - (Multi-Tenant) The provider ‘s computing resources are pooled to serve multiple customers using a multi-tenant model, with different physical and virtual resources assigned and reassigned dynamically according to the demand from time to time.
D. **<u>Rapid elasticity</u>** - Computing Resources can be rapidly and elastically provisioned to quickly scale-out and quickly scale-in as per the user requirements This appears to the user as if the resources are available dynamically at the touch of a button. Hence the user has access for unlimited quantity while he can provision only the required number of resources based on his actual need.

Vol. 10, Issue 6, June 2021

DOI 10.17148/IJARCCE.2021.10657

## V. CLOUD SECURITY ISSUES AND THE FACTORS AFFECTING.

The cloud is defined as – "delivery of on-demand computing resources / services over the internet". IaaS, PaaS, SaaS are various cloud services that different organizations generally use. Despite of its merits such as reduced capital costs, improved accessibility, flexibility to use on demand; there persist some security issues in using the cloud services. Security issues are of TWO types. One is from service provider point of view and the other is from customer's point of view.

### A. **Multi-tenancy**

Sharing of common cloud resources between multiple co-located customers is called multi-tenancy. CSP (Cloud Service Provider) will allocate resources depending on type of cloud services requested by the consumer such as IaaS, Paas and SaaS. At an entry level CSP implements logical controls to separate user data and operations. This sharing of resources results in violation of confidentiality of data which in turn leads to leakage of information and encryption. This increases the vulnerability and hence the possibility of attacks.

In order to deliver cloud services in secured manner in multi tenancy environment, care should be taken to isolate the tenant data and its location so that location of the data is not known to the tenants. Data must be kept at multiple locations / DCs of the cloud service provider (CSP) so that the data is still be intact in the event of an unforeseen attack at a place.

### B. **Insider attacks Or Malicious insiders**

A malicious owner is a current or a former employee or a contractor or other business partner who had access to organizations' data or system or network in the past and later misuses the access. This kind of threat arises within the organization. This is a pity that it goes with little risk of detection.

### C. **Elasticity**

Elasticity implies scalability of resources on demand wherein workloads can be provisioned and deprovisioned in an automatic manner on user's request at any time as closely as possible. This type of auto scaling implies a tenant can use resources which were used by a different tenant previously and vice versa. This also may lead to confidentiality issues.

### D. **Outsider attacks**

This is another issue of concern in an organization where the confidential information of an organization is leaked. Public Clouds have many interfaces as part of their design. Hence, attackers and hackers get an opportunity to exploit the APIs, weakness in networks and may indulge in breaking the connections.

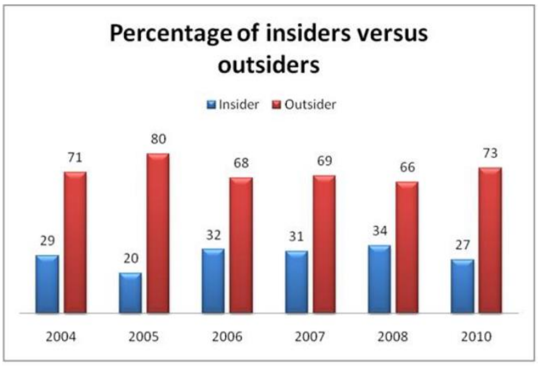

*Fig. 3 Insider/ Outsider Attack Ratio*

### E. **Information integrity and privacy**

As a matter of practice, resources are exposed over the internet to genuine users. However, malicious attackers pose a valid threat wherein they get access to tenant's resources through remote connections. There are few information security privacy issues such as, lack of authentication / authorization and absence of accounting controls with no proven protocols of encryption and decryption keys.

There should be proper authentication to overcome this problem.

### F. **Multiple Stake holders**

Cloud computing has Three main stake holders. Namely,

- Cloud Service provider (CSP) provides a cloud-based platform, infrastructure, application, or storage services
- Cloud User (Consumer) uses the services hosted by CSP on cloud environment
- Cloud Broker is an important entity in cloud ecosystem. Cloud Broker manages the cloud usage, its performance, and the delivery of cloud services. It manages relationships of CSP and consumer.

### G. **Data Loss**

DOI 10.17148/IJARCCE.2021.10657

There are multiple tenants in a cloud, hence data integrity and safety could be a genuine issue. An organization may incur financial loss if data loss occurs at any point of time. Updating and deletion of data without proper back up policy in place is an example. Data Loss / Leakage can occur due to any of the following:

- Data owner not having control over his data.
- Data is deleted or decoupled with malign intentions.
- Loss of Encryption keys.
- Access by unauthorized parties.

However, most of the public providers provide >99.999% availability of the Data.

### H. Loss of Control

Losing control of the cloud resources leads to a major problem for an organization. One of the major concerns a CIO encounters is lack of information with respect to the location transparency before a decision is taken to transfer their data to the cloud. To overcome this a solid understanding of cloud provider ‘s security & storage policies apart from the location from where the services are provided, and the SLAs committed by CSPs is required. This brings in the transparency between the CSP and the customer and helps building trust and understanding with respect to customer’s data handling in the cloud.

### I. Network security

- **Distributed Denial of Service (DDOS)** attacks – In this type of attack, lot of unwanted data is pumped so that servers and networks are brought down. This results in not getting the access to services.
- **Port scanning** – Hackers use port scanning to discover the vulnerabilities in the network and hence the weak points from where they can enter an organisation’s network. Cyber criminals use this technique to get information about security devices like firewalls usage etc.
- **Malware Injection Attack** - Transfer of data (huge quantities) takes place between cloud provider and the consumer. In this type of attack the attacker indulges in malicious activity to manipulate, steal the data or eavesdropping. This results in the user waiting for longer periods to have access to his data. Cross-site stripping as one form of malware injection attack.
- **Man**-in-the-**middle Attack** – In attacks like this, a malicious attacker intercepts, sends and receives data clandestinely without customer realizing or it is too late.

## VI. Data Security Techniques in Cloud

### A. Data encryption

Data encryption is the technique used for storing the information securely. By using a secret key, data is encrypted and stored in the cloud. People who know the secret key only can access the data. With the data getting encrypted, a secret code is generated and sent separately to the recipient. Conversion of data into secret code by itself is a technique. To get access to the encrypted data, one would need the encryption key. Data has no value without this key.

### B. Authentication and Identity

There are various ways of Authentication of users to allow access. They can be passwords that is known only to the concerned individuals. When the enterprises use multiple cloud service providers using traditional identity approaches, they are faced with security challenges.

Authenticated identity of an individual which focuses on access to digital information is called Identity-based security and is used extensively.

### C. Secure Information Management

This type of security technique comprises of agents running on systems and information is sent to “Security Console”. An administrator manages this console and takes necessary actions for the alerts raised. A Log is created for all the incidents, aberrations which is reviewed for corrective actions.

### D. Information Privacy and Integrity

Cloud computing gives access of information and resources to genuine users. These users can access the resources through web browsers. However, malicious attackers can also access these resources. Proper authentication, authorization and accounting controls solution can also be provided as a solution.

### E. Flooding Attack Solution

The cloud infrastructure consists of a fleet of servers hosted at CSP’s Data center. Each fleet of server is used for different type of services such as system requests, memory management, and some other jobs related to computation. These servers

Vol. 10, Issue 6, June 2021

DOI 10.17148/IJARCCE.2021.10657

communicate with each other in a fleet. The Over loaded server in the fleet, as and when occurs, is replaced by a new server. The record of current states of servers is maintained by Name Server. To manage such jobs a Hypervisor is used. Hypervisor also handles authorization and authentication of jobs.

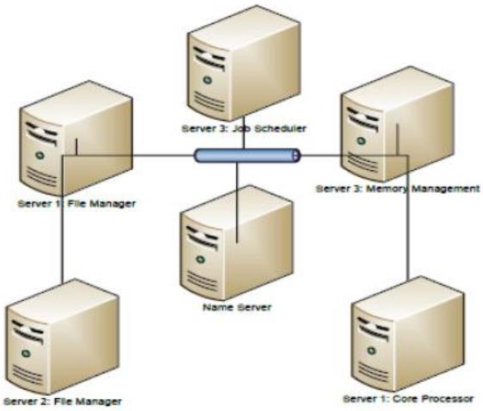

Fig. 3 **Flooding Attack solution**

## VII. CLOUD COMPUTING SECURITY STANDARDS

Security standards are the procedures for implementing a security program. To keep the environment secured and protected, few activities are executed to ensure privacy and security. If a particular system fails to provide security overlapping techniques can be used.

### A. Open Authentication (OAuth)

The method used for accessing the secured data is known as OAuth. . The users and consumers provide the access to information without giving their identity. Data access to developers is provided by this method. SSL is one of the protocols on which OAuth depends for providing security.

### B. Security Assertion Markup Language (SAML)

There are few protocols used for secure communication between online partners. SAML is one of them. It is used for authentication, authorization among the partners on an XML based standard. The three roles defined by SAML are: 1) Service Provider (SP) 2) User (Principal) and 3) an identity provider (IDP).

### C. SSL/TLS

SSL/TLS is another method which provides secure communication over TCP/IP. The three phases of TLS are 1) negotiation between clients, 2) Key exchange algorithm 3) Message encryption and cipher encryption.

### D. OpenID

User can login using the process of OpenID for the first time using a specific password and thereafter gets access to all other applications used by the user without asking for the password again. This is called SSO (Single Sign On) method.

## VIII. CONCLUSION

This paper explains a few concepts of as well as it demonstrates the properties of cloud like low-cost, platform independent, elasticity, scalability, and reliability. We have discussed few of the techniques to prevent the security challenges in cloud computing. They can secure communication by maintaining it and overcoming issues in security of the system. In this study we understood the basic issues like data loss and unauthorized attacks, and the steps to overcome these issues.

As we know the cloud computing is complex and dynamic. Some organizations like NIST and CSA are working on the cloud computing security on a continuous basis and new methodologies are continuously emerging. Some specified standards are maintained to ensure secure communications plus maintain security inside the cloud perform operations as many systems communicate with each other.

## REFERENCES

[1] Akhil Behl (2011), Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation).

[2] Akhil Behl & Kanika Behl (2012), An Analysis of Cloud Computing Security Issues.

[3] L. Ertaul, S. Singhal & G. Saldamli, Security Challenges In Cloud computing

[4] Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009

[5] Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA(European Network and Information Security Agency), Crete, 2009.

[6] Cloud computing security forum http://cloudsecurity.org/

[7] Cloud Computing – A Practical Approach by Velte, Tata McGraw- Hill Edition (ISBN-13:978-0-07-068351-8)

[8] Yashpalsinh jadeja & kirti modi (2012) cloud computing- concepts, architecture and challenges

[9] Satyendra singh rawat & Mr. Alpesh Soni (2012) ,A Survey of Various Techniques to Secure Cloud Storage

[10] R. Balasubramanian, Dr.M.Aramuthan (2012) Security Problems and Possible Security Approaches In Cloud Computing