MPRI-JNSA | INTERNATIONAL JOURNAL OF NATURE AND SCIENCE ADVANCE RES.
VOL. 1 NO. 1 JUN-2022

# CLOUD SECURITY ISSUES AND TECHNIQUES

**YAKUBU NUHU DANJUMA [1], LELE MOHAMMED[2], YAMUSA IDRIS ADAMU[3]**

*Department of Computer Science, the Federal Polytechnics Bauchi.*

## Abstract

*According to a Forbes' report published in 2015, cloud-based security spending is expected to increase by 42%. According to another research, the IT security expenditure had increased to 79.1% by 2015, showing an increase of more than 10% each year. International Data Corporation (IDC) in 2011 showed that 74.6% of enterprise customers ranked security as a major challenge. This paper summarizes a number of peer-reviewed articles on security threats in cloud computing and the preventive. This increase in cloud computing environment also increases security challenges for cloud developers. Users of cloud save their data in the cloud hence the lack of security in cloud can lose the user's trust. In this paper, I will discuss some of the cloud security issues in various aspects like multi-tenancy, elasticity, availability etc. the paper also discuss existing security techniques and approaches for a secure cloud.*

***KEYWORDS:*** *Cloud Computing, Cloud Security, Security Threats, Security Techniques, Cloud Security Standards.*

## INTRODUCTION

Cloud computing is increasingly being adapted by a wide range of users starting from commercial entities to consumers. A survey by Right Scale found that an average user runs at least four cloud-based applications and at any point in time is evaluating another four. The survey also found that 41% of commercial entities run significant workload on public clouds. With so much of our



**EDITOR-IN-CHIEF**
**Prof. E. McLenna [Austrilia]**

workload moving to cloud, security in cloud computing is under increased scrutiny. This assessment is also supported by the 2017 report by Forbes, which says that in 15 months, while 80% of all IT budgets will be committed to cloud solution, 49% of the businesses are delaying cloud deployment due to security skills gap and concerns. The problem appears to be multi-dimensional, with lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few. Adaption of cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to cloud from not just average Internet users, but also from most if not all commercial entities.

However Cloud provides various facility and benefits but still it has some issues regarding safe access and storage of data. Several issues are there related to cloud security as: vendor lock-in, multi-tenancy, loss of control, service disruption, data loss etc. In this paper I analyse the security issues related to cloud computing model. The main goal is to study different types of attacks and techniques to secure the cloud model.

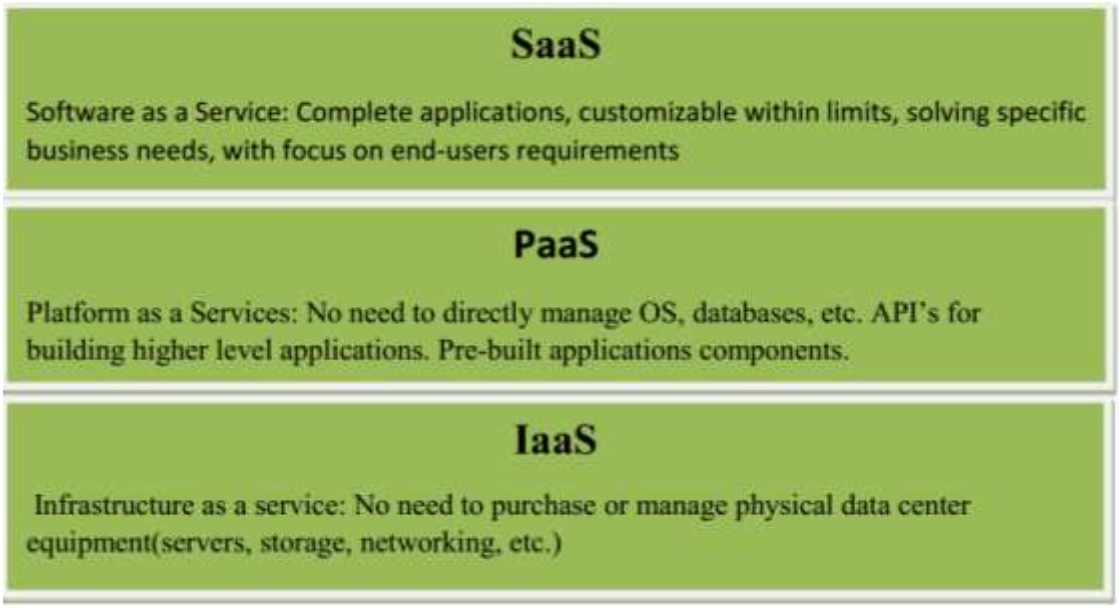



Figure 1: Cloud Computing Layers

**Cloud security issues**

Organization uses various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and services has various cloud security



**EDITOR-IN-CHIEF**
**Prof. E. McLenna [Austrilia]**

issues. Each service model is associated with some issues. Security issues are considered in two views first in the view of service provider who insures that services provided by them should be secure and also manages the customer's identity management. Other view is customer view that ensures that service that they are using is secure enough.

**Multi-tenancy**

A cloud model is built for reasons like sharing of resources, memory, storage and shared computing. Multi-tenancy provides efficient utilization of resources, keeping cost lower. It implies sharing of computational resources, services storage and application with other tenants residing on same physical or logical platform at provider's premises. Thus it violates the confidentiality of data and results in leakage of information and encryption and increase the possibility of attacks.

**Elasticity**

Elasticity is defined as the degree to which a system is able to adapt to workload changes by provisioning and deranged resources in an autonomic manner, such that the available resources match the current demand at any time as closely as possible. Elasticity implies scalability. It says that consumers are able to scale up and down as needed. This scaling enables tenants to use a resource that is assigned previously to other tenant. However this may lead to confidentiality issues.

**Insider attacks**

Cloud model is a multitenant based model that is under the provider's single management domain. This is a threat that arises within the organization. There are no hiring standards and providers for cloud employees. So a third party vendor can easily hack the data of one organization and may corrupt or sell that data to other organization.

**Outsider attacks**



**EDITOR-IN-CHIEF**
**Prof. E. McLenna [Austrilia]**

Outsider attacks is one of the major concerning issue in an organization because it releases the confidential information of an organization in open. Clouds are not like a private network, they have more interfaces than private network. So hackers and attackers have advantage of exploiting the API, weakness and may do a connection breaking. These attacks are less harmful than the insider attacks because in the later we sometimes unable to identify the attack.

**Loss of control**

Cloud uses a location transparency model by which it enable organizations to unaware about the location of their services and data. Hence provider can host their services from anywhere in the cloud. In this case organization may lose their data and possibly they are not aware about security mechanism put in place of the provider.

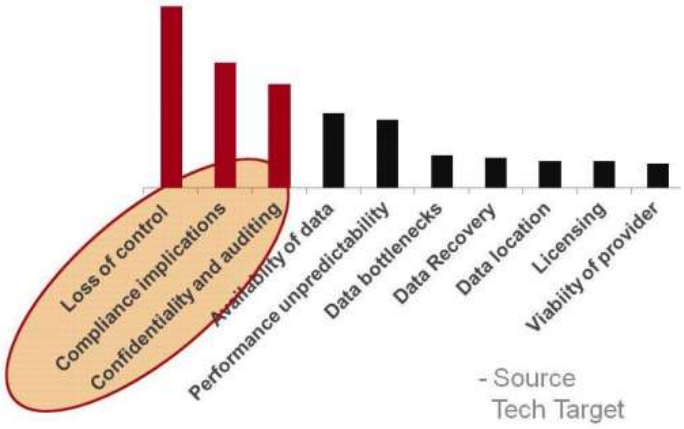



Figure 3: Loss of Control over Data

**Data Loss**

As in cloud, there are multiple tenants, data integrity and safety could not be provided. Data loss can results in financial, customer count loss for an organization. An important example of this can be updating and deletion of data without having any backup of that data.

**Network security**

**Man in middle attack**

In this attack, attacker makes an independent connection and communicates with the cloud user on its private network where all control is in the hand of attacker.



**EDITOR-IN-CHIEF**
**Prof. E. McLenna [Austrilia]**

**Distributed denial of service attacks**

In DDOS attack, servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based Service.

**Port scanning**

Port is a place from where information exchange takes place. Port scanning is taking place when subscriber configures the group. Port scanning is done automatically when you configure the internet so this violates the security concerns.

**Malware Injection Attack Problem**

In cloud computing, a lot of data is transferred between cloud provider and consumer, there is a need of user authentication and authorization. When the data is transferred between cloud provider and user, attacker can introduce malicious code into it. As a result, the original user may have to wait until the completion of the job that was maliciously introduced.

**Flooding Attack Problem**

In cloud, there is a number of servers that communicate with one another and transfer data. The requests is processed, the requested jobs are authenticated first, but this authentication requires a lot of CPU utilization, memory and finally due to these server is overloaded and it passes its offload to other server. By all this the usual processing of system is interrupted, and the system is flooded.

**Techniques to secure data in cloud**

**Authentication and Identity**

Authentication of users and even of communicating systems is performed by various methods, but the most common is cryptography. Authentication of users takes place in various ways like in the form of passwords that is known individually, in the form of a security token, or in the form a measurable quantity like fingerprint. One problem with using traditional identity approaches in a cloud



**EDITOR-IN-CHIEF**
**Prof. E. McLenna [Austrilia]**

environment is faced when the enterprise uses multiple cloud service providers (CSPs). In such a use case, synchronizing identity information with the enterprise is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution.

**Data Encryption**

If you are planning to store sensitive information on a large data store then you need to use data encryption techniques. Having passwords and firewalls is good, but people can bypass them to access your data. When data is encrypted it is in a form that cannot be read without an encryption key. The data is totally useless to the intruder. It is a technique of translation of data into secret code. If you want to read the encrypted data, you should have the secret key or password that is also called encryption key.

**Information integrity and Privacy**

Cloud computing provides information and resources to valid users. Resources can be accessed through web browsers and can also be accessed by malicious attackers. A convenient solution to the problem of information integrity is to provide mutual trust between provider and user. Another solution can be providing proper authentication, authorization and accounting controls so the process of accessing information should go through various multi levels of checking to ensure authorized use of resources. Some secured access mechanisms should be provided like RSA certificates, SSH based tunnels.

**Availability of Information (SLA)**

Non availability of information or data is a major issue regarding cloud computing services. Service Level agreement is used to provide the information about whether the network resources are available for users or not. It is a trust bond between consumer and provider. A way to provide availability of resources is to have a backup plan for local resources as well as for most crucial information. This enables the user to have the information about the resources even after their unavailability.



**EDITOR-IN-CHIEF**
**Prof. E. McLenna [Austrilia]**

**Secure Information Management**

It is a technique of information security for a collection of data into central repository. It is comprised of agents running on systems that are to be monitored and then sends information to a server that is called "Security Console". The security console is managed by admin who is a human being who reviews the information and takes actions in response to any alerts. As the cloud user base, dependency stack increase, the cloud security mechanisms to solve security issues also increase, this makes cloud security management much more complicated. It is also referred as a Log Management. Cloud providers also provide some security standards like PCI DSS, SAS 70. Information Security Management Maturity is another model of Information Security Management System.

**Malware-injection attack solution**

This solution creates a no. of client virtual machines and stores all of them in a central storage. It utilizes FAT (File Allocation Table) consisting of virtual operating systems. The application that is run by a client can be found in FAT table. All the instances are managed and scheduled by Hypervisor. IDT (Interrupt Descriptor Table) is used for integrity checking.

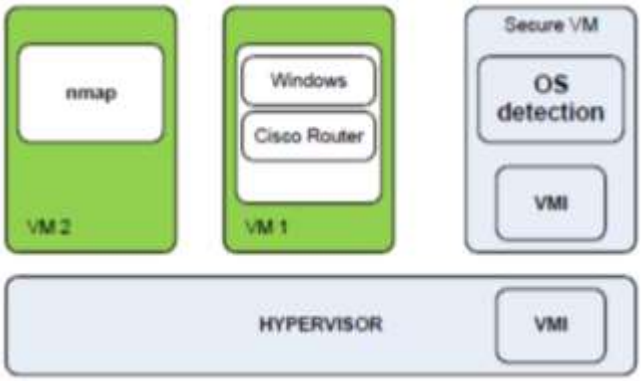



Figure 4: Malware-Injection attack solution

**Flooding Attack Solution**

All the servers in cloud are considered as a fleet of servers. One fleet of server is considered for system type requests, one for memory management and last one

for core computation related jobs. All the servers in fleet can communicate with one another. When one of the server is overloaded, a new server is brought and used in the place of that server and an another server that is called name server has all the record of current states of servers and will be used to update destinations and states. Hypervisor can be used for managing jobs. Hypervisor also do the authorization and authentication of jobs. An authorized customer's request can be identified by PID. RSA can also be used to encrypt the PID.

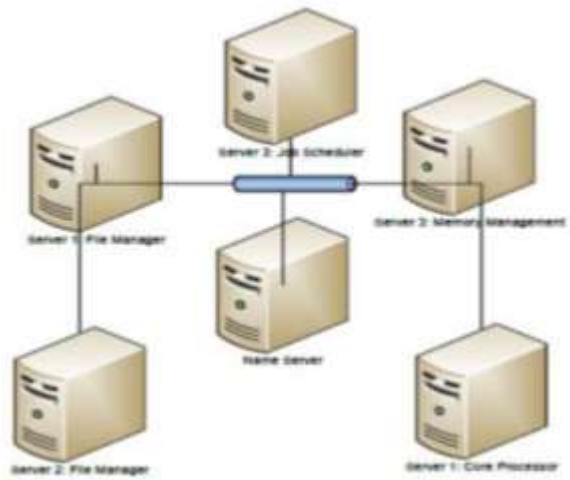


Figure 5: Flooding Attack solution

**Cloud Security Standards**

Standards for security define procedure and processes for implementing a security program. To maintain a secure environment, that provides privacy and security some specific steps are performed by applying cloud related activities by these standards. A concept called "Defence in Depth" is used in cloud to provide security. This concept has layers of defence. In this way, if one of the systems fails, overlapping technique can be used to provide security as it has no single point of failure. Traditionally, endpoints have the technique to maintain security, where access is controlled by user.

**Security Assertion Markup Language (SAML)**

SAML is basically used in business deals for secure communication between online partners. It is an XML based standard used for authentication, authorization among the partners. SAML defines three roles: the principal (a user), a service provider (SP) and an identity provider (IDP). SAML provides queries and responses to specify user attributes authorization and authentication information in XML format. The requesting party is an online site that receives security information.

**Open Authentication (OAuth)**

It is a method used for interacting with protected data. It is basically used to provide data access to developers. Users can grant access to information to developers and consumers without sharing of their identity. OAuth does not provide any security by itself in fact it depends on other protocols like SSL to provide security.

**OpenID**

OpenID is a single-sign-on (SSO) method. It is a common login process that allows user to login once and then use all the participating systems. It does not based on central authorization for authentication of users.

**SSL/TLS**

TLS is used to provide secure communication over TCP/IP. TLS works in basically three phases: In first phase, negotiation is done between clients to identify which ciphers are used. In second phase, key exchange algorithm is used for authentication. These key exchange algorithms are public key algorithm. The final and third phase involves message encryption and cipher encryption.

**Conclusion**

This paper describes some of the cloud concepts and demonstrates the cloud properties such as scalability, platform independent, low-cost, elasticity and reliability. Although there are various security challenges in cloud computing but in this paper, I have discussed some of them and also the techniques to prevent them, they can be used to maintain the secure communication and remove the security problems. This research is basically done to study some of the problems like attacks, data loss and unauthenticated access to data and also the methods to remove those problems. As the cloud computing is dynamic and complex, the traditional security solutions provided by cloud environment do not map well to its virtualized environments. Organization such as Cloud Security Alliance (CSA) and NIST are working on cloud computing security. In this paper we have discussed a few security approaches but several other approaches are also



**EDITOR-IN-CHIEF**
**Prof. E. McLenna [Austrilia]**

there that are in the process. Some standards are also specified which can be used to maintain secure communication and security in a cloud as many systems communicate in it and perform operations.

## References


Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. Procedia Technology, 12, 529-534.

Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In 2011 World Congress on Information and Communication Technologies (pp. 217-222). IEEE.

Behl, A., & Behl, K. (2012, October). An analysis of cloud computing security issues. In 2012 world congress on information and communication technologies (pp. 109-114). IEEE.

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, 465-472.

Columbus, L. (2018). State Of Cloud Adoption And Security, 2017. URL: https://www. forbes. com.

Sharma, R., & Trivedi, R. K. (2014). Literature review: cloud computing–security issues, solution and technologies. International Journal of Engineering Research, 3(4), 221-225.

Rawat, S. S., & Sharma, N. (2012). A survey of various techniques to secure cloud storage. International Journal of Computer Science and Network Security, 12(3).





**EDITOR-IN-CHIEF**

**Prof. E. McLenna [Austrilia]**