IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# An Analysis Of Cloud Security Issues And Techniques

Shashi Raj Aman
School of Computer Science and Engineering
Galgotias University
Greater Noida ,India

Rajeev Kumar Yadav
School of Computer Science and Engineering
Galgotias University
Greater Noida,India

Utkarsh Lal
School of Computing Science and Engineering
Galgotias University
Greater Noida ,India

Sugan Patel
School of Computer Science and Engineering
Galgotias University
Greater Noida,India

**Abstract:** Cloud computing is a paradigm shift in the way we access, collect, and manage data and applications. With the rise of the Internet, cloud computing has become a ubiquitous computing model. which allows users to access computing resources such as servers, storage and applications over the Internet. In this architecture, users can access these resources on-demand, pay only for what they use, and scale their usage up or down based on their needs. The internet computing provides such numerous benefits like as Flexibility, Scalability, Cost-effectiveness, and Increased efficiency. This abstract provides an overview of cloud computing and its benefits, discusses its various deployment models, and highlights some of the key challenges in the adoption of cloud computing. It concludes with a discussion on the future of cloud computing and its potential to transform the way we do business and access technology.

In this article, we will investigate some of the safety issues that are associated with using cloud computing. across various domains such as multi-tenancy, scalability, and uptime. Additionally, we will explore established security methodologies and strategies for ensuring a protected cloud environment. This document aims to provide Professionals and experts with insights into the different security risks, models, and tools available.

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

## 1.Introduction

Cloud computing, often known as Internet computing, is a type of cloud computing that allows users to access a shared pool of programmable computer resources on-demand across a network. Involvement-minimal servers, networks, storage, applications, and services the service provider and little administrative effort to supply and release are examples of such resources. Cloud computing is a concept that offers storage and computing resources to some, while others view it as a means of accessing data and software from the cloud. This computing model is gaining popularity in academia and organizations because it offers scalability, flexibility and easy access to data. In addition, cloud computing Companies can move their data to the cloud, allowing stakeholders to access it. We can take Google maps, Aws, as a example of cloud computing.

In spite of the numerous preferences and comforts of cloud computing, there are still concerns around the security and security of information. A number of issues related to cloud security exist, such as merchant lock-in, multi-tenancy, misfortune of control, benefit disturbance, and information misfortune, which have been recognized as investigate issues in cloud computing . The purpose of this research is to examine the Problem associated with the model of cloud computing ,with primary objective being to investigate attacks that is many types and methodologies to ensure security of the cloud models.

**SaaS:** Software as a Service (SaaS) is an acronym that stands for "Complete Application," "Customization with constraints, "addressing concrete business challenges," and "putting the needs of the end user front and centre."

**PaaS :** Platform as a Service (PaaS) eliminates it need to directly maintain operating systems, databases, and other infrastructure components. interfaces for application programming used to create higher-level programs. components of apps that have already been pre-built.

**IaaS:** Infrastructure as a Service," and it means Owning and maintaining physical data storage devices is unnecessary. (such as a server, storage device, or networking device).

## 2. Issues on cloud Security:

Company uses different type of cloud service like SaaS, PaaS, IaaS and their various type of module like public, Private, Hybrid. In this Module and their service has different type of security issues. All of them model has some type of security issues. These security issues are considered as two types of views first one is Service provider so that the provider ensure that the service provided through them that are secure or not and able to manage costumer identity. And the second side views is costumer side look at to determine if the service they're utilising is safe enough to use.

### .2.1 Elasticity:

The elasticity of a system is its ability to automatically provide and reallocate its resources in response to fluctuations in workload, ensuring that the resources available at any one time optimally meet those demands. Scalability is a key aspect of elasticity. It states that customers can modify their service levels as required. This scalability allows tenants to make use of a resource that was being used by someone else. However, this might cause privacy concerns.

### 2.2 Multiple – tenancy :

The resources, storage, memory, and shared processing that make up a cloud are all designed to serve a specific function. Multi-tenancy allows for more efficient use of infrastructure by allowing several customers to share the same hardware, software, and network connections provided by a single service provider. Because of this , it violates encryption and information leakage as a result of data secrecy raise the risk of assaults.

**2.3 Insider attacks:**

Insider assaults are caused by insiders with information. Employees, business partners, contractors, and security admins who had access to private information may be insiders. Insider attacks are carried out by approved computer network users. This cyber assault is very risky since system workers lead it, making the entire process exposed. Computer companies usually guard against external cyberattacks but seldom internal ones.

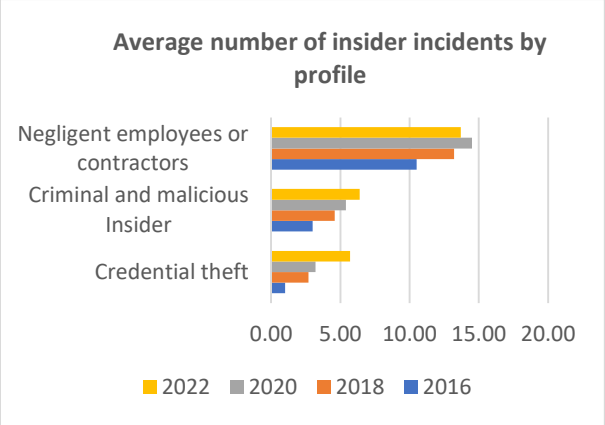


**Figure 1 . Average of insider attacks**

**2.3.1 Types of insider attacks:**

**Malicious Insider:**

Someone who steals information using valid credentials for financial or personal gain. For instance, a former employee with a grudge or an opportunistic employee who sells critical information to competitors.

**Careless Insider:**

A careless insider is a tool that allows others to compromise your system without your knowledge. This is the most typical form of bug-based internal danger. If the gadget doesn't get secured or is hacked, bad things might happen. An innocent worker, for instance, may accidentally infect the system by clicking on a malicious link.

**Mole:**

A fraudster who is not a member of the protected group but has gotten access to its sensitive information through illicit means. This is an uninvited guest posing as an insider, either an employee or a business partner.

**2.4 Outsider attacks:**

An outsider attack is a cybersecurity effort to disrupt a company's IT system or compromise its data resources. Individuals or groups can steal data or hold it for ransom in outsider assaults. A multi-layered security policy keeps outsiders out of a company's network and away from sensitive data. Data transmission encryption prohibits outsiders from viewing or utilizing stolen data.

**2.4.1 Some types of Outsides attacks:**

**Phishing attacks:**

Phishing emails are sent by attackers that look to be from reputable sources, such as banks or government organizations. When consumers click on links in these emails, they are sent to dangerous websites where malware can be installed on their systems.

**Ransomware attacks:** In order to unlock users' data, attackers encrypt it and demand a ransom payment.

**Data breaches:** Attackers might steal sensitive data by exploiting flaws in cloud services.

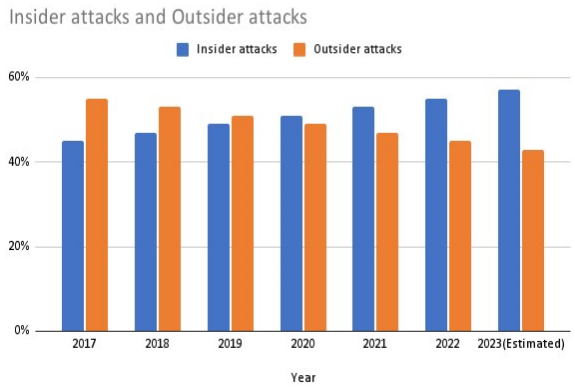


**Figure 2. Insider attacks vs Outsider attacks**

### 2.5 Loss of Control:

The loss of control over cloud security is a significant concern for organizations contemplating a cloud migration. When businesses transfer data and applications to the cloud, they cede some control over how the data is stored and managed. This poses a significant security risk, as organizations no longer have complete control over who has access to their data and how it is utilized. Several factors can contribute to the loss of authority over safety in the cloud. Cloud computing's inherent complication is among the largest factors. Frequently, cloud environments are extremely complex, containing a vast array of distinct components and systems. This complexity can make it difficult for organizations to comprehend how their data is being stored and managed, as well as to identify and mitigate security threats.

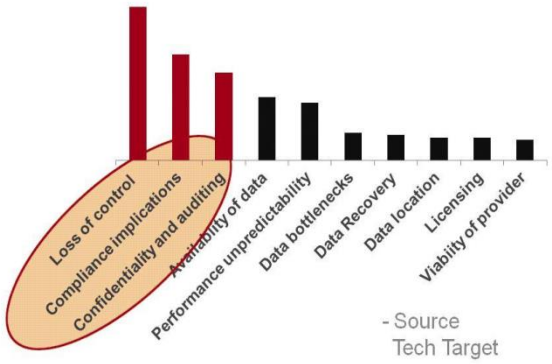


**Fig 3. Control of loss on Data**

### 2.6 Loss of Data:

Multiple tenants in cloud computing make it impossible to ensure the privacy and security of user information. The loss of data might cost an organization financially and could reduce the number of customers they have. One significant illustration of this would be making changes to data or deleting it without first creating a backup copy of that data.

### 2.7 Protection of computer networks

#### 2.7.1 Attack with a Man in Middle:

In this kind of assault, the attacker creates a new channel of communication with the cloud user, but from within the attacker's private network.

**2.7.2 Attacks that involve the (DDOS):**
An overwhelming flood of network traffic can knock servers and networks down during a distributed denial of service attack, and users are prevented from accessing a particular Internet-based service.

**2.7.3 Scanning Port:**
port is location which data may be sent to and from a computer. Whenever a subscriber configures the group, port scanning takes place in the background. When you setup the internet, port scanning is performed automatically; as a result, this raises worries about the network's security.

**2.8 The Challenge of Malware Injection Attacks:**
Because cloud computing involves the movement of a significant amount of data in transit between a cloud service provider and a user, user authentication and authorisation is necessary. While information is being transmitted from the cloud service provider to the end user, it is vulnerable to being tampered with by an attacker. This means the original user may be forced to wait for the maliciously injected task to complete before they can resume their work.

**2.9 The Threat of Flooding Problem:**
The cloud computing model utilizes a network of distributed computers that are constantly exchanging information and communicating with one another. After receiving the requests, the server authenticates the jobs that have been requested. This takes up a lot of memory and processing power, thus the server eventually sends its offload to another server. All of this causes a disruption in the normal processing of the system, and eventually it becomes overwhelmed.

**3.Methods to secure data in cloud:**

**3.1 Identifying or Verifying Authenticity:**
Cryptography is currently the most widely used approach for authenticating people and even communicating systems. Individually-known passwords, security tokens, and quantifiable characteristics like fingerprints are all examples of user authentication methods. When an organization makes use of a number of different CSPs, it might complicate efforts to apply conventional techniques to identity management in the cloud. The enterprise-wide synchronization of identities in this scenario is impractical. When transitioning from on-premises to cloud-based infrastructure, traditional methods to identity might cause additional complications.

**3.2 The Encryption of Data:**
Using data encryption methods is essential before entrusting a huge data store with sensitive information. Although passwords and firewalls help, hackers can still get unauthorized access to your information. Encrypted information is unreadable without the corresponding decryption key. For an invader, this information is completely meaningless. It's a method for encoding information in a hidden language. The encryption key, often known as the secret key or password, is required in order to decrypt the data.

**3.3 Privacy and Data Integrity:**
To authorized users, cloud computing makes available a wealth of data and tools. Resources are accessible via web browsers, making them vulnerable to both benign and criminal users. The issue of information integrity may be effectively addressed if there is trust between the information provider and the user. In addition, you may ensure that only authorised individuals have access to sensitive data by putting in place suitable authentication, authorization, and accounting controls. Secure access options, Certificate Authority Revocation Scheme (RSA) Key Exchange Secure Shell (SSH) Tunnels

**3.4 Information Availability (SLA) :**
One important drawback of cloud computing is the frequent occurrence of data and information being unavailable. The availability of network resources is communicated to end users via a Service Level Agreement. It's the connection reliability between a purchaser and a vendor. Having a backup plan for critical data and local

resources is one way to guarantee accessibility. The user can continue to have access to data about the resources even after they have been unavailable**.**

**3.5 Safeguarding Information Storage:**
It's a method of protecting information that involves storing everything together in one safe place. It consists of software agents deployed across target computers, each of which communicates with a central "Security Console" server. Admin, a real person, oversees the security console, checking it often and acting on alarms as necessary. Increases in both the size of the cloud's user base and the complexity of its dependency stack mean that managing cloud security is becoming increasingly difficult. It's also called "Log Management" sometimes. Some cloud services also include security guidelines.

**3.6 Method for Preventing Malware Injection Attacks**
In this setup, a number of client virtual machines are generated and kept in a centralized repository. FAT (File Allocation Table) is used, which is a collection of different OSes in a virtual format. The FAT table stores information about the client's running programs. Hypervisor controls and schedules all instances. Integrity testing makes use of the Interrupt Descriptor Table (IDT).

**Input validation:**
Checking input data for validity and harmful code. Regular expressions or other pattern-matching methods allow this.

**Output encoding:**
This encodes all output data to prevent malicious code. HTML entities or other encoding techniques allow this.

**Uses of security Framework:**
Security frameworks enable developers design secure code. These frameworks offer recommended practises to mitigate common security vulnerabilities.

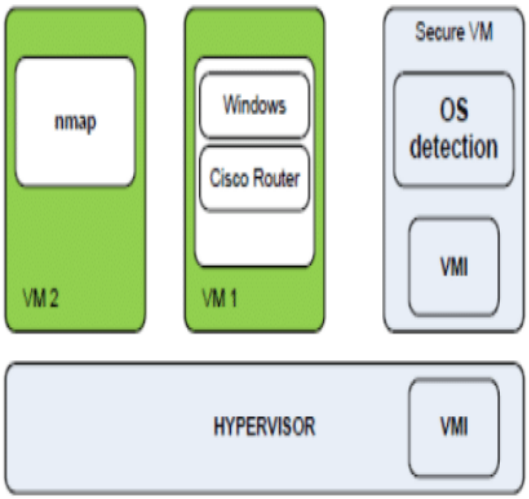


**Figure4. Malware Injection Attack.**

**Flooding Attack Solution:**
The collective group of servers that make up a cloud service is called a fleet. System-related requests are evaluated by one server fleet, memory-management requests are evaluated by another, and computation-related tasks are evaluated by a third. Each fleet server has the ability to talk to every other fleet server. When one of the servers becomes overloaded, a new one is brought in to take its place, and a third server, called the name server, is used to change the locations and the status of the servers. Task management is one application for the hypervisor. The hypervisor also provides authorization and authentication for jobs. A PID can be used to track the origin of a request from a verified buyer.

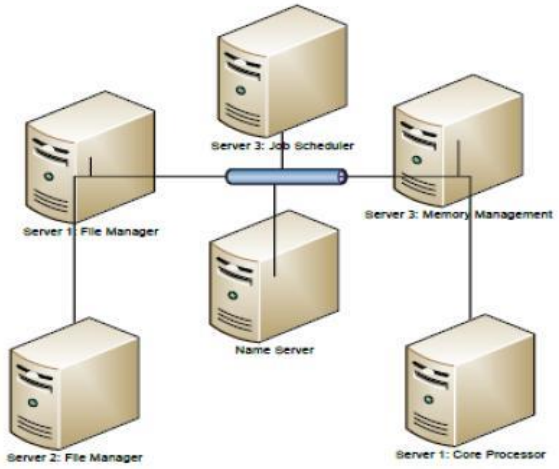


**Figure 5. Solution of flooding attack.**

**4. Measures Cloud technology Security:**

The steps and methods needed to conduct a security programme are spelt out in detail in security standards. When it comes to the cloud, special precautions are required to apply these criteria in order to keep a private and safe environment. The principle of "Defence in Depth" is applied to cloud security. This idea has several safeguards.. As there is no singular point of failure, the overlapping technique provides security even if one of the systems fails. Traditionally, endpoints maintain security using a method in which user access is controlled.

**4.1 SAML:**

To ensure confidential interactions between internet parties, businesses frequently use SAML. It is an XML-based protocol for identifying and authorising business associates. The SML defined the three roles that is Identity provider, Principal, and Service Provider. To describe authentication and authorisation data for user characteristics, SAML offers queries and replies in XML format. A website is the one making the request for the security information.

**4.2 Open Auth:**

It's a technique for accessing confidential data. Its primary use is to facilitate data access for programmers. Users can share data with developers and consumers without disclosing their identify. To ensure safety, OAuth uses additional protocols like SSL in addition to is own.

**4.3 Open ID:**

When used properly, OpenID can facilitate SSO. Users just need to sign up once to have access to all supported platforms with this unified authentication method. User authentication is handled independently of any central authority.

**4.4 SSL / TLS:**

The uses of TLS to encrypt data sent through the TCP/IP protocol stack. TLS consists of three main stages: In the first stage, clients discuss and agree on a set of cyphers to employ. The key exchange algorithm is utilised in the second stage of authentication. These are examples of key exchange algorithms that use public keys. Encrypting the message and cypher is the third and last step.

**5. Conclusion:**

In this article analysis the fundamentals of cloud computing and demonstrates its scalability, lack of platform dependencies, low cost, adaptability, and dependability.. Although there are a number of different security risks associated with cloud computing, in this article, we have examined some of those risks as well as the ways that can be employed to mitigate them. These approaches can be utilized to keep the communication safe and eliminate any security issues that may arise. This survey's primary objective is to investigate and analyses all of the potential issues, includes but is not limited to attacks, data loss, and unauthorised access, and possible

solutions to these problems. Because of the fluid and complex nature of cloud computing, traditional security measures may not easily translate to its associated virtualized systems.While we have looked at a few distinct security techniques in this work, there are many other options available and more being created all the time. It's also possible to use the standards that have been established to maintain safe channels of communication and data storage. a cloud even if there are numerous systems communicating in it and operating within it.

## REFERENCES


1. NIST Special Publication 800-145: The NIST Definition of Cloud Computing
2. Cloud Security Alliance Cloud Security Controls Matrix (CSCM)
3. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27017:2015 Information Security Management Systems for Cloud Services
4. https://www.digitalguardian.com/blog/insider-outsider-data-security-threats
5. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures/
6. https://www.geeksforgeeks.org/what-is-insider-attack/
7. Security Forum for Cloud Computing http://cloudsecurity.org/
8. Velte's Cloud Computing: A Practical Approach, Tata McGraw-Hill Edition (ISBN-13:978-0-07-068351-8)
9. Yashpalsinh jadeja and Kirti Modi (2012) Cloud Computing: Concepts, Architecture, and Challenges
10. Satyendra singh rawat and Alpesh Soni wrote a paper in 2012 called "A Survey of Different Ways to Secure Cloud Storage."
11. Akhil Behl wrote an article in 2011 called "Emerging Security Challenges in Cloud Computing." It was called "An Insight into Cloud Security Challenges and How to Handle Them."
12. An Analysis of Cloud Computing Security Issues, written by Akhil Behl and Kanika Behl in 2012.
13. Security Challenges in Cloud Computing by L. Ertaul, S. Singhal, and G. Saldamli
14. Peter Mell and Tim Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009
15. Cloud Computing: Benefits, Dangers, and Security Recommendations. In 2009, ENISA (the European Network and Information Security Agency) met in Crete.
16. Security Forum for Cloud Computing http://cloudsecurity.org/