A SURVEY ON CLOUD SECURITY ISSUES AND TECHNIQUES USING CLOUD COMPUTING

Abstract

Nowadays, we know that cloud computing is one of the most needed ways of computing in the sector of information technology. It is the services and resources which are provided to the user on the internet and network. Grid computing and distributed computing are some of the computing techniques used in current trends and are also used in industrial, academic, and research fields. Day by day new techniques are coming into the market which is subsequently spreading the use of cloud computing. As there is an increase in the use of cloud computing mechanisms, there is a high increase in security issues and challenges faced in cloud computing. The data is saved in the cloud which is a virtual location and lack of security will lead to a loss of user's trust in the service providers.

Discussing this in our paper, we have surveyed the security issues in the cloud and the countermeasures which need to be taken to reduce them. Some common aspects are taken into consideration such as multi-tenancy, elasticity, availability, etc. The paper will give insight to academicians, researchers, and professionals to learn about the security issues in the cloud and the models proposed to solve them.

Keywords:
Cloud Security, Data Encryption, Network Security, Attacks, Authorization.

Authors

Sayan Mandal
Student (BCA)
Jharkhand Rai University
Ranchi

Avinash Kumar
Student (BCA)
Jharkhand Rai University
Ranchi

Kumar Amrendra
Assistant Professor
Jharkhand Rai University
Ranchi

Anuradha Sharma
Assistant Professor
Jharkhand Rai University
Ranchi

I. INTRODUCTION

Cloud computing is a technology that allows users to get the features of virtual storage by accessing and using the resources. The resource can be any applications, storage, and processing power provided on the internet. These resources are hosted on remote servers, typically owned and operated by third-party companies known as cloud providers.

Layers of Cloud Computing:

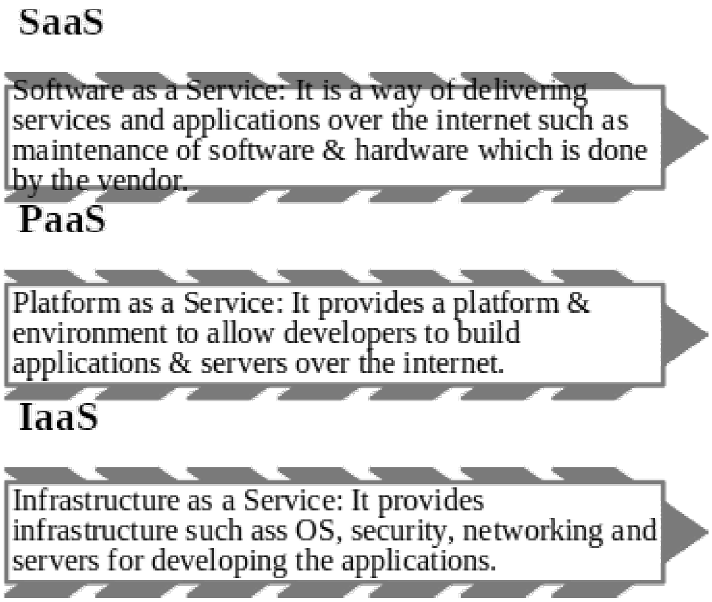
SaaS
Software as a Service: It is a way of delivering services and applications over the internet such as maintenance of software & hardware which is done by the vendor.
PaaS
Platform as a Service: It provides a platform & environment to allow developers to build applications & servers over the internet.
IaaS
Infrastructure as a Service: It provides infrastructure such ass OS, security, networking and servers for developing the applications.

Figure 1 . Layers of Cloud Computing

Benefits of cloud computing include:

- **On-demand access to resources:** customers can access and use resources as needed, without the need to invest in and maintain their IT infrastructure.
- **Scalability:** customers can easily scale the requirement of resources as and when needed.
- **Cost savings:** customers need to pay only for the resources they will be using instead of investing and maintaining one’s own IT infrastructure.
- **Flexibility:** customers can access and use resources from anywhere with an internet connection. Cloud computing services are offered by some companies, including Amazon Web Services (AWS), IBM Cloud, Microsoft Azure, Oracle Cloud, and Google Cloud Platform.

II. CLOUD SECURITY ISSUES

1. **Different types of cloud services:** IaaS, PaaS, and SaaS accompanied by different deployment models: public cloud, private cloud, and hybrid cloud, can each have their unique security issues.

In the IaaS (Infrastructure as a Service) model, the responsibility for securing data and applications is on the user and customers; the infrastructure facility is provided and maintained by the service provider. Security issues in this model can include:

- Lack of control over network security
- Difficulty in protecting data at rest and in transit
- Difficulty in implementing compliance requirements

In the PaaS (Platform as a Service) model, the responsibility for securing data and applications is on the user and customers; the establishment and maintenance of the platform and infrastructure is done by the service provider. Security issues in this model can include

- Lack of control over the underlying infrastructure
- Difficulty in implementing custom security control

In the SaaS (Software as a Service) model, the responsibility of securing data and applications is on the cloud service provider. Security issues in this model can include:

- Lack of control over the underlying infrastructure
- Difficulty in implementing custom security controls
- Difficulty in meeting compliance requirements

In the public cloud model, customers share the same infrastructure with other customers, which can lead to security risks such as a lack of control over who has access to the data, or difficulty in implementing custom security controls.

In the private cloud model, customers have a dedicated infrastructure, which can provide more control over security, but it also can be more expensive and less scalable.

In the hybrid cloud model, customers use a combination of public and private cloud services, which can provide more flexibility and scalability, but it also can lead to complexity in security management, especially when it comes to data sharing and integration between the two environments.

Security risks have to be evaluated by the organizations. Here, security risks are associated with various cloud services, and deployment models, and implement appropriate security measures to mitigate those risks.

2. **Multi-Tenancy:** Multi-tenancy in cloud computing refers to the concept of multiple customers or tenants sharing the same infrastructure, applications, and other resources in a cloud environment. This is a common feature of many cloud computing services, particularly those that are offered on a public or community cloud basis.

Efficient utilization of resources can be availed through multi-tenancy which leads to lower cost. Thus, sharing of computational resources, service storage, and related applications is shared with another user who belongs to the same platform at the service provider's end. It results in the violation of confidentiality of data, leakage of information, and encryption and enhances the attack's possibility.

- **Elasticity:** In cloud computing, the ability to automatically scale up and down a cloud system by the change in demand is known as elasticity. It allows the cloud system to dynamically adjust both the capacity and resources to fulfill meet the current needs of the tenants and applications while minimizing the costs associated with underutilized or overutilized resources.

There are two types of elasticity in cloud computing:

- Vertical elasticity
- Horizontal elasticity.

Vertical elasticity refers to the ability to scale up or down the capacity of a single server by adding or removing resources such as CPU, memory, and storage.

Horizontal elasticity refers to the ability to scale out or in the number of servers in a system. This can be done by adding or removing virtual machines, or by deploying containers or functions.

- **Insider Attacks:** Insider attacks in cloud computing refer to security breaches or malicious activities that are carried out by someone within an organization or an authorized user with access to the organization's cloud environment. These attacks can be intentional or unintentional and thus leaves a significant impact on the security and integrity of the organization's useful data and resources. Examples of insider attacks include theft of sensitive data, unauthorized access to resources, and sabotage of systems. To prevent insider attacks, organizations should implement strict access controls, monitoring, and security policies and conduct regular security audits and employee training programs.

- **Outsider Attacks:** Outsider attacks in cloud computing refer to security breaches or malicious activities that are carried out by someone outside of an organization, such as a hacker or cybercriminal. These attacks can target the organization's cloud environment, infrastructure, or applications. Examples of outsider attacks include phishing, malware, and Distributed Denial of Service (DDoS) attacks. There is a significant impact on the security and integrity of an organization's data and resources due to outsider attacks. Implementation of different security-solving techniques e.g. intrusion detection and prevention, firewalls, encryption of data, and very strong authentication methods are used to prevent outsider attacks in the organization. Regularly, there should be security audits & checks, and assessments regarding vulnerability should be organized to identify and resolve potential vulnerabilities.

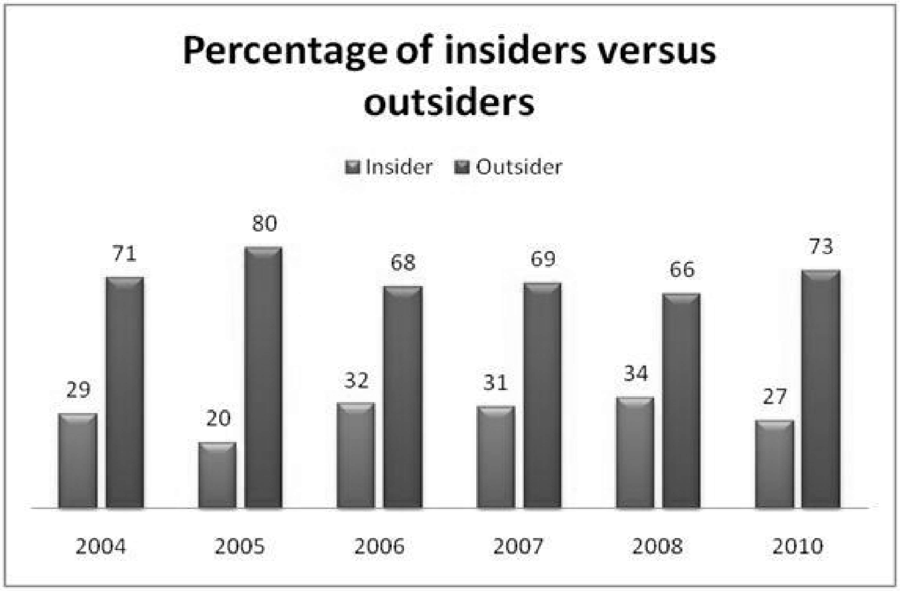

Figure 2: Insiders versus Outsiders (percentage) [1]

- **Loss of Control:** In the cloud, the location transparency model is used thus authorizing organizations to hide the location of their services and data. Thus, the services can be hosted anywhere in the cloud by the service provider. There is a chance of data loss and the organization is not aware of the security mechanism used by the provider.

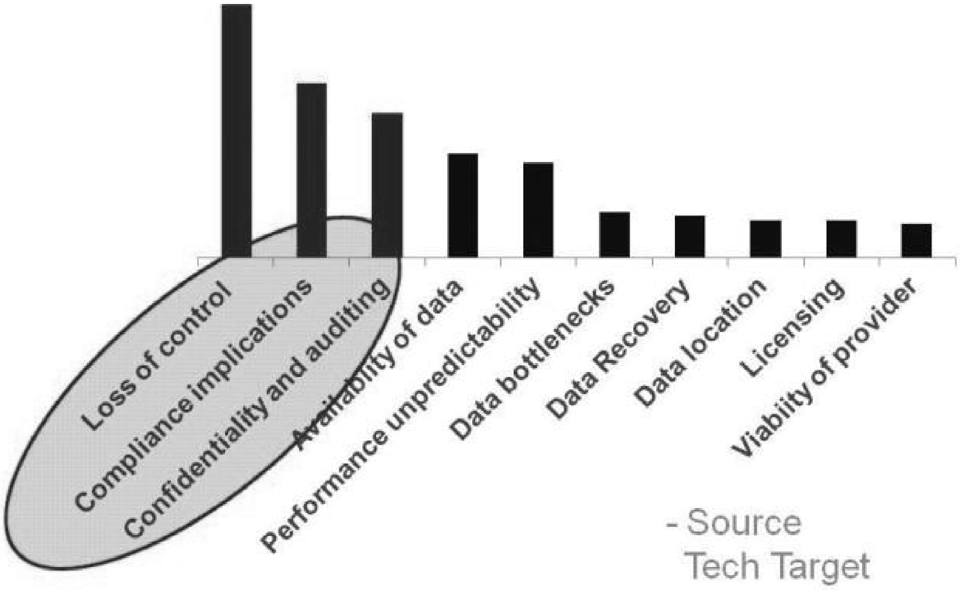

Figure 3: Loss of Control.

- **Data Loss:** Data loss in cloud computing refers to the unintentional or intentional loss of data that is available in the cloud storage. There are various reasons like human error, system failure, malware, or cyber-attacks that result in data loss. Data loss in the cloud can have a significant impact on an organization's operations, reputation, and compliance.

Some examples of data loss in cloud computing include

- ➢ Accidental deletion of files or data by an employee
- ➢ Corruption of data due to hardware or software failure
- ➢ Data breaches resulting in the theft or unauthorized access to sensitive data
- ➢ Ransomware attacks that encrypt and hold data hostage

- **Network Security**

  - ➢ **Man in the Middle attack:** A man-in-the-middle (MITM) attack in cloud computing is a sub-category of cyber-attack in which the attacker interrupts and changes or updates the communication between the user and server, without either party being aware of the interception. The intruder usually steals sensitive information and injects malware, or disrupts communications.

  - ➢ **Distributed Denial of Service attacks:** A Distributed Denial of Service (DDoS) attack in cloud computing is a sub-category of cyber-attack in which a network or website is flooded with a large amount of traffic by an attacker thus creating huge traffic resulting in overwhelming the system. This results in the unavailability of resources to the legitimate users. DDoS attacks are usually launched by a network of compromised devices such as a botnet, which amplifies the attack's power and makes it difficult to trace the origin of the attack. [3]

  - ➢ **Port Scanning:** Port scanning is a type of technique that is used to detect open ports and various services on a networked device, such as a computer or a server. A port scan is typically performed by a hacker or security professional to identify potential vulnerabilities in a system.

    During a port scan, an attacker sends message packets to different ports on the receiver’s end to identify which ports are active and which services are running. By identifying open ports and services, an attacker can then target specific vulnerabilities in the system. [3].

There are different types of port scans, such as:

- ➢ **TCP Connect Scan:** A full three-way handshake is attempted to open a connection on a specific port.
- ➢ **SYN Scan:** To check the status of the SYN packet it is sent to the specified ports.
- ➢ **UDP Scan**: To check the status of the UDP packet it is sent to the specified ports.

- **Malware Injection Attack Problem:** A malware injection attack in cloud computing refers to a security breach where an attacker injects malware into a cloud environment, infrastructure, or applications. The malware can then spread within the cloud environment, compromising data and systems, and potentially leading to data breaches, service disruptions, and financial losses.

Examples of malware injection attacks in cloud computing include

- ➢ An attacker injects malware into a cloud-based application, which then propagates to other systems and steals sensitive data
- ➢ An attacker injects malware into a cloud infrastructure, which then spreads to other systems and causes service disruptions
- ➢ An attacker injects malware into a virtual machine, which then ex-filtrates data or disrupts services

- **Flooding Attack Problem:** A flooding attack in cloud computing refers to a category of cyber-attack where the attacker usually floods the given network with huge traffic, which results in a delay in the system and makes it unavailable to users in need. Flooding attacks can be of two types: either network-based or application-based.

Examples of flooding attacks in cloud computing include

- ➢ Network-based flooding attacks: In this, the network becomes unavailable due to heavy traffic as the attacker floods the cloud-based network.
- ➢ Application-based flooding attack: In this, the application becomes unavailable due to the large number of requests as the attacker floods the cloud-based network.

3. Techniques to Secure Data in the Cloud

- **Authentication and Identity:** Authentication and identity management are critical components of cloud computing security. Authentication refers to the process of verifying a user's identity, while identity management involves the process of managing and controlling access to resources.

  In cloud computing, authentication, and identity management are typically handled by the service provider. This means that users need to provide credentials, such as a username and password, to access cloud services. Multi-factor authentication is also available in the case of some of the cloud providers. In this users need to provide some additional authentication forms like fingerprint or some security tokens to get the service accessed successfully.

  Identity management in cloud computing involves creating, managing, and controlling access to user accounts and resources. This typically involves the use of identity and access management (IAM) systems, which allow organizations to control who has access to what resources. IAM systems also include features such as role-based access control and user provisioning, which allow organizations to fine-tune access controls based on an individual's role or job responsibilities.

To ensure secure authentication and identity management in cloud computing, organizations should use strong, unique passwords and multi-factor authentication, use IAM systems to control access to resources, and regularly review and update access controls. It is also important to ensure that the cloud provider's security measures align with the organization's security policies and compliance requirements.

- **Data Encryption:** A data protection technique that is used to protect sensitive data by encrypting or converting it to some format that is not readable to unauthorized users is known as data encryption. In cloud computing, data encryption is used to save the data which is stored, transmitted, and processed in the cloud.

There are several types of data encryption which is used in cloud computing:

- **Storage Encryption:** In this, encryption is used to protect the data which is stored in the cloud. This can include data stored on virtual machines, databases, and storage services.
- **Transit Encryption:** In this, encryption is used to protect the data which is transmitted over a network. This can be data sent between a client and a server.
- **End-to-End Encryption:** In this, encryption is used to protect the data which is stored on a client device like a laptop or a mobile phone, and then transmitted to the cloud.

Data encryption in cloud computing is typically managed by the cloud provider, but organizations can also use their encryption tools and technologies to get the data encrypted before it is sent to the cloud. This is just like client-side encryption, in which the data is encoded on the client side before sending to the cloud whereas, in server-side encryption, the data is encrypted on the server side before sending to the cloud.

- **Information Integrity and Privacy:** Information integrity and privacy are two important concepts in cloud computing.

Information integrity refers to maintaining the accuracy, completeness, and consistency of data over its entire lifecycle, including when it is stored, processed, and transmitted in the cloud. To ensure information integrity, organizations should implement data validation, backup, and disaster recovery procedures, as well as access controls that restrict who can modify and delete data.

Privacy, on the other hand, refers to the protection of personal and sensitive information from unauthorized access and use. Looking into the cloud computing mechanism, this includes protecting the privacy of the data that is stored, processed, and transmitted in the cloud. It could be achieved by implementing data encryption, and access controls, and by ensuring compliance with relevant privacy regulations. [2]

- **Availability of Information (SLA):** Service level agreements (SLAs) are contracts made between the cloud service provider and the user that outline the availability of information and the level of service that the provider will guarantee. SLAs typically specify the uptime percentage, which is the amount of time that a service will be available, and the recovery time objective (RTO), which is the total time it will take for the service to be restored after an outage.

  SLAs are important in cloud computing because they help ensure that customers can access the information and services they need when they need them. They also provide customers with a measure of accountability, as they can hold the provider accountable if the service level is not met.

- **Secure Information Management:** Secure information management is the practice of protecting sensitive and confidential data in cloud computing environments. It involves implementing security measures to achieve the confidentiality, integrity, and availability of data, as well as compliance with relevant laws, regulations, and industry standards.

To ensure secure information management in cloud computing, organizations should:

- ➢ Implement data encryption, access controls, and incident response plan to protect the confidentiality of data
- ➢ Implement data validation, backup, and disaster recovery procedures to protect the integrity of data
- ➢ Monitor and ensure compliance with relevant laws and regulations, such as HIPAA and PCI-DSS, that pertain to the handling of sensitive data
- ➢ Regularly conduct security audits and assessments, including vulnerability scans and penetration testing, to identify and address security risks
- ➢ Have agreements in place with their cloud providers that address data privacy and security risks and ensure that their cloud provider's security measures align with their own security policies and compliance requirements.

- **Malware-injection attack solution:** Malware injection attacks are a type of cyber-attack in which malware is inserted into a system or network without the knowledge or consent of the user. In cloud computing, malware injection attacks can be a major threat to the security of data and systems, as the cloud environment is shared by multiple tenants and can be accessed remotely.

To protect against malware injection attacks in cloud computing, organizations can implement several solutions:

- ➢ **Use Anti-Malware Software:** Antivirus and anti-spyware programs which are classified as anti-malware software can be used to find and resolve malware from cloud systems and networks.
- ➢ **Use Firewalls:** Firewalls are used to block any unauthorized access to cloud systems and networks and to block traffic from known malicious IP addresses.

- **Use of Intrusion Detection and Prevention Systems (IDPS):** IDPS is used to find and resolve malware injection attacks by looking for any malicious activity in the network traffic.
- **Monitor and Analyze System Logs:** Regularly monitoring and analyzing system logs can help identify and respond to malware injection attacks, by detecting unusual activity and identifying the source of the attack.
- **Use Endpoint Security Solution**: Endpoint security solutions can detect and prevent malware-injection attacks by monitoring and controlling access to the cloud system and network.
- **Keep the Software, Systems, and Network Updated:** Regularly updating software, systems, and networks will help to patch vulnerabilities that could be exploited by malware injection attacks.
- **Educate and Train Employees:** Educating and training employees on how to recognize and avoid malware injection attacks can help prevent successful attacks by providing employees with the knowledge and skills to avoid clicking on suspicious links or attachments. [10]

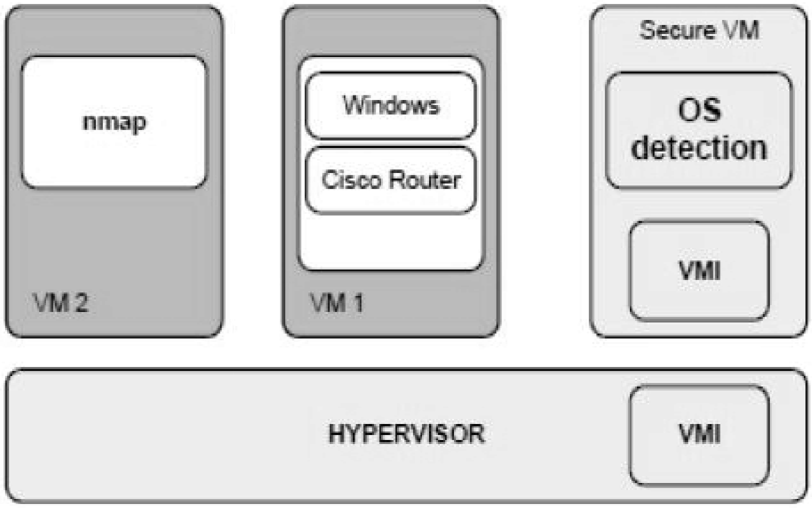

Figure 4 : Malware-Injection attack solution [10]

- **Flooding Attack Solution:** The fleet of servers is the servers that are present in the cloud. There are three types of fleet of servers classified according to their uses such as for system-type requests, memory management, and computation-related jobs. The servers present in a fleet can communicate among themselves. A new server is used when some of the server becomes overloaded. This new server is called the name server and it has all types of data and records of the state of servers. Further, it is also used to store and update the destination and states. The authorization and authentication of jobs are done by managing the jobs using hypervisors. PID identifies the authorized customer’s request. RSA is also used to encrypt the PID.

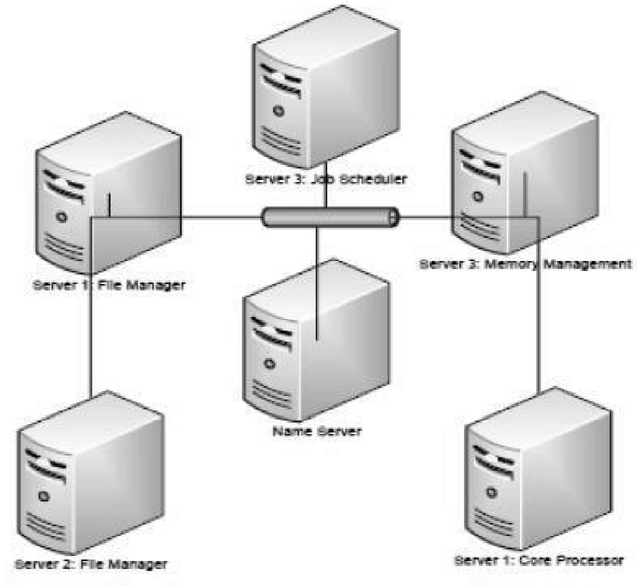

Figure 5: Flooding Attack solution [10]

4. **Cloud Computing Security Standards:** Cloud computing security standards are some set of rules and regulations which needs to be followed by organizations to keep check and ensure the security of their data and systems which are hosted on the cloud. Security standards are also known as the process and procedures which need to set up a security program. Some given steps need to be performed to maintain the security of the environment which provides privacy and security. This is done by applying cloud-related activities by these specified security standards.

   "Defense in Depth" is the concept of having multiple layers of defense used to provide security in the cloud. In case, anyone of the system fails, a different overlapping technique is used to provide security as it has no single point of failure.

   - **Security Assertion Markup Language (SAML):** Security Assertion Markup Language (SAML) is used for business deals for secure communication between online partners.

     SAML is an open standard used for exchanging authentication and authorization data between parties. It is done between an identity provider (IdP) and a service provider (SP). It is used to provide secure single sign-on (SSO) and federated identity management across different systems, applications, and domains.

     SAML works by allowing the IdP to authenticate a user and then issue a SAML assertion, which stores the details and information about the user's identity and authentication status. The SP can then use this assertion to grant the user access to its resources, without having to perform its authentication [3].

- **Open Authentication (OAuth):** Open Authentication (OAuth) is also an open standard that allows users to access third-party applications and resources without sharing their credentials. OAuth enables a user to give an application permission to access their data or resources on another website, without sharing their login credentials. [3]. OAuth is not responsible for providing any security by itself. It depends on other protocols like SSL to provide security.

- **OpenID:** Open Authentication (OAuth) is an open standard for authorizing third-party access to a user's resources, such as their data stored in a cloud-based service, without sharing their passwords. It is often used for allowing users to grant access to their data to third-party applications, such as mobile apps or web-based services, without having to share their login credentials [3].

OAuth provides several benefits for cloud computing environments:

- **Increased Security:** OAuth allows users to get access to their resources without having to share their passwords, reducing the risk of phishing and other attacks.
- **Improved user Experience:** OAuth enables users to get access to their resources from within the application, rather than having to go to a separate login page.
- **Increased Flexibility:** OAuth allows organizations to use different identity providers and authentication methods, and to add new systems and applications to the environment without having to re-architect the entire system.
- **Allow for Easy Integration with Third-Party Services:** OAuth allows for easy integration of third-party services with a user's account, enabling the use of additional services without the need to create a separate account.

- **SSL/TLS:** Secure Sockets Layer (SSL) and its successors like Transport Layer Security (TLS) is a type of cryptographic protocol which provides secure communication over the network. It is used to secure web traffic and protect sensitive information e.g. login credentials and financial data.

  In cloud computing, SSL/TLS is commonly used in securing communication between users and cloud-based services, such as web-based applications and APIs.

III. CONCLUSION

This paper comprises the concept of cloud computing and security. It also demonstrates some of the properties of the cloud like scalability, platform independence, low cost, elasticity, and reliability. As we know that there are various security issues and challenges which are there in cloud computing techniques, and we have discussed a few of them in this paper. We have also discussed some of the prevention techniques which are used to secure the cloud. This is a survey study which is done to look after different security issues and how to resolve those. As we know that cloud computing is a dynamic and complex mechanism and the traditional security resolution methods are not good enough to solve these problems in the virtualized environment. Some of the security approaches are discussed in this paper but there are others in the process. In this paper, some standards are also discussed which are used for maintaining communication secure and error-free.

REFERENCES

[1] Akhil Behl (2011), Emerging Security Challenges in Cloud Computing (An insight into 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.