IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Security Attacks and Reduction of Risk Using Mitigation Techniques in Cloud Computing

Surendra Kumar Patel*
Assistant Professor
Dept. of Information Technology
Govt.Nagarjuna P.G. College of Science,
Raipur, Chhattisgarh, India

Abstract*— Cloud computing is a hurriedly on the increase internet modern technology for facilitating with an assortment of services to its users. However, Along with rapid development and interesting proposals, there are many problems associated with this technology, which must be addressed with confidence, which represents the strongest barrier to its adoption. Computers play an important role in network attacks. Today, cloud services are also defunct. Attacks reduce the quality of services on computer networks and cloud platforms. Effective use of cloud computing in attacks that create services for needy users requires us to reduce vulnerability to attacks and improve security. This study addresses a variety of attacks that target cloud environments and potential mitigation techniques to mitigate attacks and relief from problems.

Keywords*— Cloud Computing, Security Attacks, Threats Attacks, Mitigation Techniques.

I. INTRODUCTION

Today, cloud computing technology is widely used by many organizations. They facilitate consumers and users with different platforms and IT infrastructure. With the assistance of cloud computing services, customers and users can steer clear of upfront costs and complexity by owning and maintaining their own IT infrastructure. You are gaining increasing interest in areas such as science, industry, and web services. According to Gartner, cloud computing is one of the 10 most important technologies and is one of the best trends in the coming years. Go businesses and organizations Cloud computing enables cost-effective, ubiquitous, on-demand network access permissions for networks, servers, storage, applications, and services such as networks, servers, storage, applications, and services with configurable groups of computers.Designed quickly and easily with operator interaction or supervision [1]. State-of-the-art and advanced cloud computing provides a host of services for your needs. This includes services like Gmail for buyers or cloud backups on users' computers. Although it is a service that allows large companies to meet face to face. Data and run all your applications in the cloud.

Using cloud computing technology has many benefits in a computing environment. However, organizations will use this technology in many ways. But it also means managing data in the cloud and making it easy to access services anytime, anywhere. With better geographic coverage and faster times. Less investment in infrastructure, etc., but that is a reasonable point. One of them is security. And this article examines the security challenges of cloud computing and provides ways to address the security challenges of cloud computing technologies.

II. DEFINITION, HISTORY AND ARCHITECTURE OF CLOUD COMPUTING

A. Cloud Computing and its types

Cloud Computing technology performs over the Internet, because of that user of this technology is also have to be use Internet. Basically clouds can be classified in two ways depending on their services, accessibility restrictions and the deployment model [9] (Figure 1):

1. Based on deployment model,
2. Based on service model.

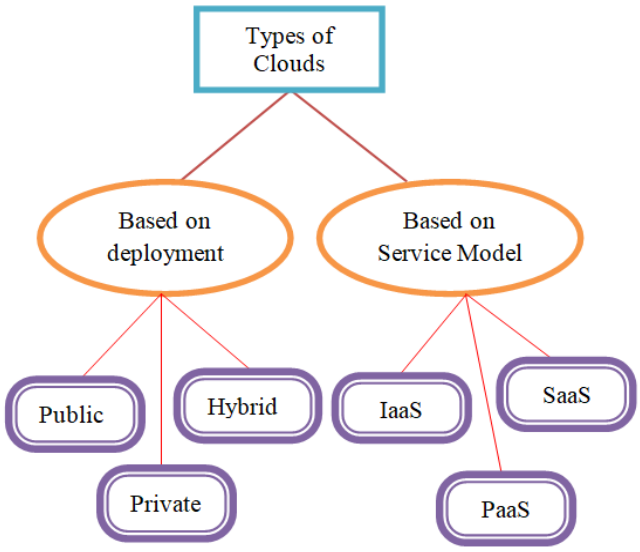

Figure 1: Types of Cloud Computing based on deployment model

1. Pubic Cloud:-A public cloud is the most financial option for users in which the cloud vendor spread the express of bandwidth and infrastructure. It has bounded configuration and

the cost is determined by usage capacity, so it is made available in a 'pay-as-you-go' model manner. Because of lack of high reliability, lower costs, zero maintenance and on-demand scalability, the public cloud is not suitable for organizations operating with fragile information as they have to fulfill with stringent security procedures.

2. Private Cloud:-Private cloud facilitates more control over customizability, scalability and flexibility to its users. It is costly to manage and cloud vendors deciding for providing services to users and hardly strict for security. This cloud can be used by organization, where sensitive information are executing between them.

3. Hybrid Cloud:-Hybrid cloud is the union of two or more public or private clouds and it facilitates on-demand and cost efficiency of public cloud and customizability, scalability and flexibility of private cloud. This cloud is generally used by organizations, where public cloud for running high-volume applications like user interface and using private cloud for sensitive assets like financial, data recovery and during scheduled maintenance and rise in demand.

Based on service model:

1. IaaS:-Stands for Infrastructure-as-a-Service and virtual equivalent of a traditional data centers. Cloud vendors are responsible for whole infrastructure; they provide scalable compute resources such as servers, networks and storage of user's data, but cloud users have entire control over it.

2. PaaS:-The Platform-as-a-Service environment provides services of software and hardware infrastructure components. The PaaS environment enables cloud users to install and host data sets, development tools and business analytics applications separately from building and maintaining necessary hardware.

3. SaaS:-Software-as-a-Service cloud vendors provides the entire software package as a pay-per-use model. Vendors offer cloud-based software to users to get access in it.

B. History of Cloud Computing

The concept of Cloud Computing is originated in 1960s, when the time-sharing concept became popularized via RJE (Remote Job Entry), this term was mostly corresponded with large vendors such as IBM (International Business Machine) and DEC (Digital Equipment Corporation). At 1970s the around the clock allocation environments were accessible on such platforms as Multics (on GE hardware), Cambridge CTSS and the earliest UNIX ports (on DEC hardware). Yet the "data centers" model where users submitted job to operators to run on IBM mainframes was overwhelmingly predominant [11, 12].

C. Architecture of Cloud Computing

The architecture of Cloud Computing comprises of many computing technology, which are loosely coupled. The Cloud architecture can by divide in two parts:

a) Front end,
b) Back end.

Each and every ends is associated from side to side a network, usually Internet.

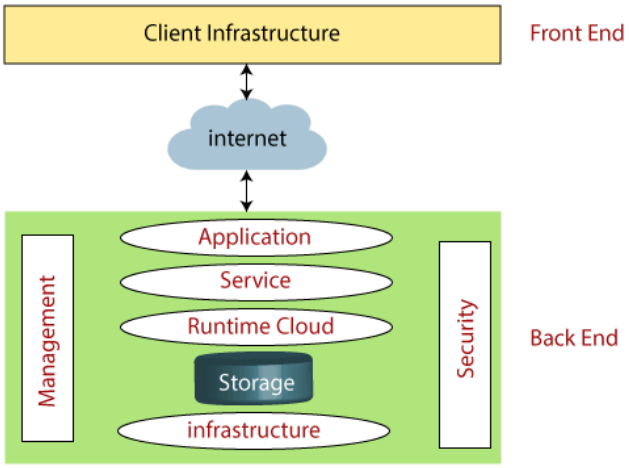

Figure 2: Architecture of Cloud Computing [10].

a) Front end: The frontend consists of the client infrastructure responsible for the graphical user interface (GUI) and used by the cloud users.
b) Back end: The backend is managed by the cloud provider and includes data storage, security mechanisms, virtual machines, model implementations, servers, traffic control mechanisms, etc.

Components of cloud computing architecture:

Cloud service manages services on demand. There are general services services provided by technology: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Runtime Cloud provides runtime and runtime environment for virtual machines. Storage in the cloud is one of the most important storage capabilities for data collection and management. Infrastructure provides services at the host, application and network levels. Cloud infrastructure environment includes hardware and software components such as servers, storage, network devices, virtualization software, and other storage resources needed to support the cloud computing model. organization is worn to manage and harmonize components such as applications, services, cloud runtime environments, storage, infrastructure, and other security issues in the backend. Security is an integrated back-end component of cloud computing, it implements a security mechanism at the back-end.

III. SECURITY AND SECURITY ATTACKS IN CLOUD COMPUTING

As for as consider about security in Cloud Computing technology then Data in Cloud should be stored in encrypted form. To control client from accessing the shared data honestly, proxy and brokerage services should be employed.

A. Security Planning

Sooner than deploying a fastidious resource to cloud, user should require look into and analyze some mandatory characteristics of the resource such as [13]:

- Selection of computing resources that needs to move to the Cloud environment and analyze its understanding.
- Think about Cloud Computing overhaul models such as IaaS, PaaS and SaaS. These models necessitate customer to accountable for security at different levels of service.

- Consideration of various type of Cloud services to be used such as public, private or hybrid.

As for as risk is consider in cloud deployment mainly depends in the lead the service models.

B. Understanding Security of Cloud

1) Security Boundaries

A specific service model defines the boundary between the service provider and the consumer's responsibilities. The Cloud Security Alliance (CSA) package framework defines the boundaries between each type of service and shows how different the functional components are. The following diagram shows the contents of the CSA package [13]:

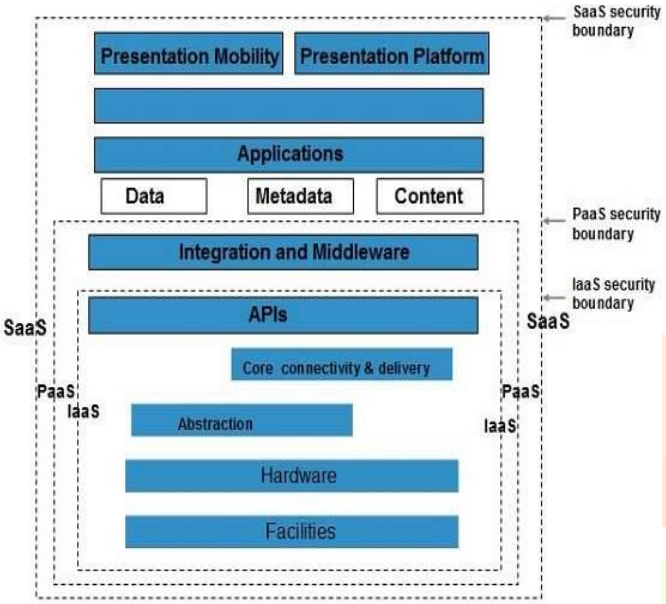

Figure 3: Cloud Security Alliance (CSA) Model [13]

2) Important aspects of CSA model

• IaaS is the lowest level of service with PaaS and SaaS in addition to the above services.
• In the future, individual projects will inherit security strengths and weaknesses in the next example.
• IaaS provides infrastructure, PaaS provides an altar development environment, and SaaS provides an operational environment.
• IaaS has the lowest level of integration and security services, while SaaS has the most.
• This policy defines the security boundaries within which the responsibilities of the cloud provider end up with the responsibilities of the customer.
• Any security policy that falls below the threshold of customer safety.

While each type of service is a security device, security requirements also depend on where those services are available - private, public, or in general the cloud.

3) Special Requirements for Cloud Security

As all data is transferred over the Internet, data security is a major concern in the Clouds. [13][14] The International Organization for Standardization (ISO) identifies security vulnerabilities that may present us in terms of important requirements for IT security in a transparent and secure technology solution. Here are some important data security techniques:

Privacy means that user data is stored and only important authorities have access to that data.
Stability is the determination to ensure that no data change or modification occurs during storage or transfer and that only authorized users have the ability to modify, modify, copy or delete your data.

Authentication is the process of verifying a user's identity before accessing data and this can be done by using special protections to their identity.
Consent means ensuring that users requesting private information are entitled to it.
Figure 4 shows the primary security requirements for Cloud Deployment along with Cloud Deployment delivery templates and Cloud Deployment service templates and can be seen in position as guidelines for security isolation. In Figure 4, essential supplies are represented by "✓" and optional or non-compulsory requirements are represented by the "✗" symbol.

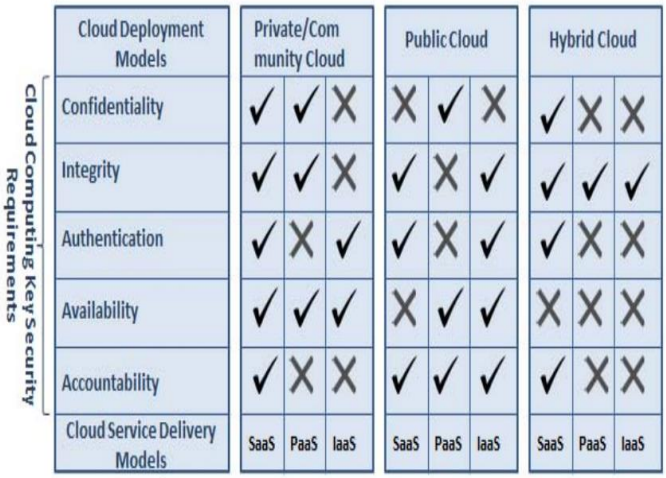

Figure 4: Key security requirements coupled with cloud computing deployment models and cloud computing service delivery models [14]

All work models must include safety methods that work in all of the above areas.

4) Access to isolated data

Because data stored in the cloud is everywhere, we need technology to organize the data and prevent the customer from accessing it directly.
Discovering a cloud store is one way to isolate the cloud store. In this way, two functions are created:
• Broker with full access to storage, but without access to the client,
• An agent who does not have access to storage, but who has access to both the customer and the retailer.

5) Work on boring cloud access

When a client submits a data request:
• request customer data for the interaction of the agent's external service,
• the agent sends a request to the broker,
• Cloud storage system back to the secretary,
The broker returns the information to the agent,
• Finally, the agent sends the data to the customer.
All the above steps are shown in the table:

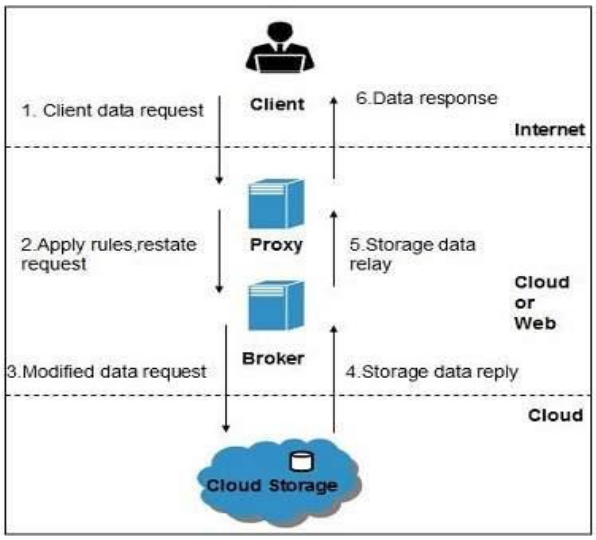

Figure 5: Broker Cloud Storage access system [13]

C. Security attacks against cloud computing

It has many advantages when using cloud computing technology. Information; Operating System; Think about the resources of resources; transport management; This has many problems because it involves simultaneous memory management and control. [4]. This is very important to secure a cloud attack. Cloud service providers should ensure that users do not face serious security issues. Malicious users become legitimate users and spread the cloud.

Cloud computing faces various security attacks; Some are shown in Figure 6; Appropriate mitigation measures should be taken to prevent or reduce these attacks.

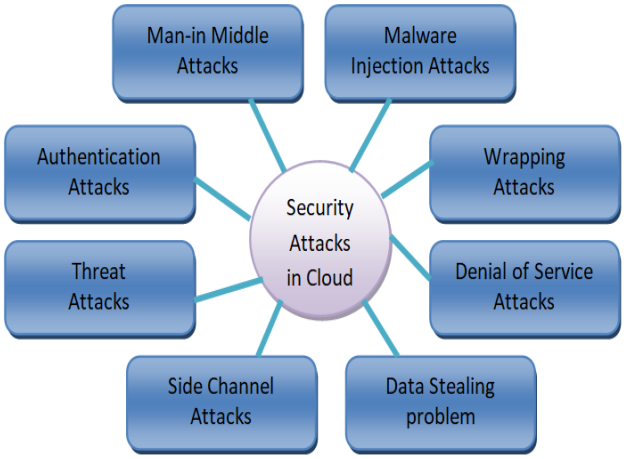

Figure 6: Security attacks in Cloud [5]

1) Malware infection attacks

With cloud computing technology, we rely on the identification of user applications and command commands. During this attack, focus on placing a partition or virtual machine in the cloud environment. The main purpose of this attack is to take control of the user's data in the cloud, allowing the attacker to upload the created image and make it part of the user's cloud environment. After a faulty system/service is installed in a cloud environment, user requests are no longer encrypted.

(a) prevention of malware infection

When a cloud user adapts an open environment to the cloud environment, the service provider creates a user image of the virtual device in the cloud image storage system. The applications used by the user are measured for their high performance and stability. As infrastructure such as tier of service (IaaS) becomes more difficult to attack, the cloud plans to consider stability at the demand level. The most obvious method is to freeze the system's file system (FAT) (5) [6], which awaits almost all existing systems. Parts of a shared table can identify the code or application that the cloud user will use. To verify the robustness and stability of the following examples, you can confirm that the event was successfully downloaded by the user: To avoid this process, we need to send a hypervisor to the provider. Cloud computing is considered to be the most secure and advanced component and its security is never compromised. The hypervisor is responsible for all planning and activities; Therefore, it can be configured to monitor file delivery schedules to validate and integrate user profiles.

(i) The hypervisor

Hypervisor is responsible for preparing all events; However, before planning, you should ensure consistency on the virtual machine tools [5,7] such as the customer allocation table.

Another solution is to save the operating type of the customer in the cloud in the first step while creating the account in the cloud system in the cloud customer. [5] Since the cloud is an independent operating system, web analysis can be performed by an operating system that maintains the math, for example, before the cloud is emulated.

Alternatively, we may protect user-type platform data as a first step to ensure that the user opens an account and ensure the effectiveness of the new customer model.

(ii) stick to the fabric

Outbreak logging is avoided by sending messages to web servers using Simple Access Protocol (SOAP) [6]; This attack exploits vulnerabilities through the use of XML signatures. An attacker intercepts SOAP messages between a user and a web server. By resetting the user account and password during logon, the attacker inserts an error message into the communication system, replaces the original message with the wrong one, and sends it to the mailbox's mail server. Therefore, the basic body is useful. Service to verify corrupted information may be fraudulent. [14] At the end of the attack, the attacker would have copied the SOAP message during translation and sent it to the server as an authorized user, using malicious code to create cloud services.

(b) prevention of serious diseases

Participants can use Transport Layer services. When data is sent from a web server to a web browser using SOAP messages, encryption avoids waiting. Redundancy An extension called STAMP [5] is added to the value of the certificate and to the SOAP address. This additional key protects against attacks by modifying the value of the ticket [6]; During an attack, this attack can only reach this location and securely transmit effective messages between the sender and the recipient.

(c) Denial of Service (DOS attack)

Today, cloud computing is an important part of the IT world. Many users are involved in cloud applications. Cloud systems

provide value-added services to consumers. DoS can easily fall into cloud applications. The cloud enhances computing power through the use of virtual machines. Denial of service can be stressful. Participants can bypass HTTP, which can lead to HTTP DDOS attacks. They cannot handle XML DDoS attacks.

(d) protection against DoS attacks

The eye filter method shown in Figure 7; certificate root method; DoS attacks can be eliminated, such as fire extinguishers, using the following parameters:

Filtering method: Stream filtering is used to detect low-level DoS attacks. The low level of DoS speeds up traffic and overtake by hosts on the network. Power level filter protects against DoS attacks.

Signature-Based System: Manages the signature traffic on a computer network through a signature process. The attack models were compared using the database. The record contains the number or more of those signatures that were previously signed. Route signers shall take necessary measures to prevent attacks on traffic.

Fire-Based Approach: Firewall is one of the network security systems that makes it difficult to access the cloud. The main purpose of using a firewall inside the system is to simplify the process and protect the actual data of the user group internally and externally, rather than preventing DoS/DDoS attacks.

2) Data theft problem

Data theft is a method of hacking user accounts using cloud computing technology. This attack can steal passwords and passwords of user accounts. Competitive performance loses current user information. Cloud service providers and users are prone to these problems.

(i) Protection against data theft

Data theft prevents the user from constantly presenting a unique number while logged in. At the end of the meeting, the proportional-integral-derivative PID engine performs the main function and the PID engine remains in the hypervisor [5] [7].

(ii) Side channel connection

This type of attack happens in infrastructures like IAAS. Infrastructures such as cloud computing (IaaS) provide storage resources to store information, such as multi-computer storage, virtual machines (VMs), and storage resources. In cloud-based server systems, one machine attacks the group channel [5] [6] [15]. Channel attacks aimed at implementing covert tactics have become a major security threat. Calculating systems that can resist hidden side attack attacks is critical to the secure design of systems. Side channel attacks follow two stages of transmission and recovery. The site runs virtual machines and installs them in compartments in the cloud. The second problem is that of withdrawal. After transferring painful stars, receive confidential information from other servers in cloud computing sites. It's very easy to get sensitive information out of a device, so you should be able to avoid parallel cloud computing attacks.

(iii) protection against side channel attacks

In this attack, the attacker collects information about the capabilities of the secret machine while performing covert operations and uses that information to modify the operating system. The integration of firewall applications in parallel can be used to prevent attacks on the cloud. According to research on the Amazon EC2 service, a hacker can create a new virtual machine to identify cloud-facing virtual machines and delete sensitive data. During an attack on the group's channel, private firefighters trying to break into a car accidentally stopped it. Another option is to use an indistinguishable encryption system (with a method that spreads confusion or noise) to avoid the secondary production of side channel attacks.

(iv)Verification attack

As described above, "authentication" means verifying a user's identity before providing data and this can be done using special brand security, but authentication is a weak point in cloud computing services, which is always vulnerable to attacks. targets. These attacks can easily occur in critical areas [18]. The attacks target the user's device. The method used for authentication was discovered and the attackers attempted to obtain confidential information. They use various secrets and processing to make the data as reliable as possible. The service provider delivers significant value to the consumer and must consent before leaving the service.

Some authentication attacks include:

1) Powerful attack: This type of attack uses all possible key combinations to crack the password. The most robust attack performed using practical methods requires a great deal of computational power and time to be successful [5] [8].

2) Critical Attack: This type of attack is faster than violent attack [5]. Here, the attacker tries to guess the secret key in a predefined keyword dictionary. To counter this type of attack, the password must be random, not a dictionary [8]. Native language passwords are also not as common as most local language dictionaries.

3) Shoulder search: The user gains knowledge of the type of privacy of the site through visual access to suspicious data via keyboard [8]. Shoulder browsing is another name for "espionage", where the browser follows the user's movements to obtain the password [5]. the user detects such an attack; how to enter password

For example, password length information obtained from an arm scan can be used to launch a password detection attack. The result of this attack is information leakage and, in the context of cloud computing, it can be mitigated by two safe spot alerts and peer review methods.

4) Recurrent seizures: Recurrent seizures are also called cerebral seizures [5]. This is one way to overcome the challenge of completing consumer certification programs.

The key to absorbing a caption address attack that involves identification is to ensure that the content of the message changes from time to time. According to this section, many processes use timestamps or infinite values that are randomly generated to prevent recurring attacks, allowing the investigator to check for a new or correct message.

5) Violation attacks: A web attack in which the marketer redirects a fake user to a website to recover the user's password/sharing rules [5]. In November 2007, SalesForce, a SaaS member, was implicated in a personal attack that resulted in the disclosure of SalesForce account information to some customers [16].

6) Unlock Keys: Key readers are software programs that track user activity by recording each key pressed by the user [5]. Major sponsors collect information and pass it on to third parties, whether it is the Department of Criminal Justice, law enforcement, or IT. Tom Bain, vice president of security at Morphisec (Allied Threat Infrastructure, Abuse, Unnecessary Fraud and Target Transfer, among other threats), said, "Key developers are software programs that provide algorithms that model computer failures using detection and other techniques. track down.") [17].

D. Techniques to prevent authenticated attacks

This problem occurs when a simple authentication tool, such as a username and password, is used. Each system must have more than one recognized machine. The second method of recognition and advanced recognition should be used. disposable password; Button highly recognized attack [5, 7]

1) Human injuries

Personal intrusion (MIM) is monitored and manipulated by a group of unauthorized communications between two users. In other words, this can happen if the forum is configured on two nodes or on one computer. Therefore, the interruption of the communication system alters the order of the actual data or information. Human-based attacks can be used to communicate with malicious users; Allows you to send and use some MIME attacks like [5].

Communication Address Address Process (ARP): In standard ARP communication, the server sends a packet containing the source and end IP addresses and distributes it to all devices connected to the network. A client with an IP address will only send ARP responses including the MAC address. Then the call will be made. The ARP method is not a secure process; ARP storage is not a stupid feature that causes big problems.

2) ARP Storage Poisoning: Monitors network traffic for ARP storage poisoning attacks and decrypts ARP packets between the host and the server. An attack can damage a network.

3) Domain Name Server (DNS) Violation - In this case, the target will provide false information which can lead to loss of credentials. As I mentioned earlier, this is a type of direct MIM attack where the seller created a fake website for his bank. When you visit your bank's website, you will be redirected to the website that is under attack. Accept all your credentials.

4) Delay - Once established between the host computer and the host web server, it may be part of a time setting that violates the cookies used to set the time.

E. Prevention of infectious diseases in humans

Avoid such attacks to a reasonable degree. You can use the advanced degree method. The method is used for the sender group and the exception is for the recipient group. Therefore, the attacker cannot modify the analyzed data. Many encryption algorithms include Advanced Encryption (AES); Data Encryption (DES) and Triple DES must be used.

To avoid these attachments, you can use a temporary password, as the temporary password is not protected from MIM attacks.

Another way is to get accreditation from multiple services and providers. The first dependence is on one-way communication between the customer and the service provider. In a collaboration agreement, the server runs the server to verify the client and ensure a valid exchange. Verification can be done with public and private keys.

F. Threat Attacks in Cloud Technology

There are many security issues with cloud computing which is widely used today. According to www.synopsys.com [19], there are some serious threats to cloud computing in 2018. The above threats are displayed in the following format.

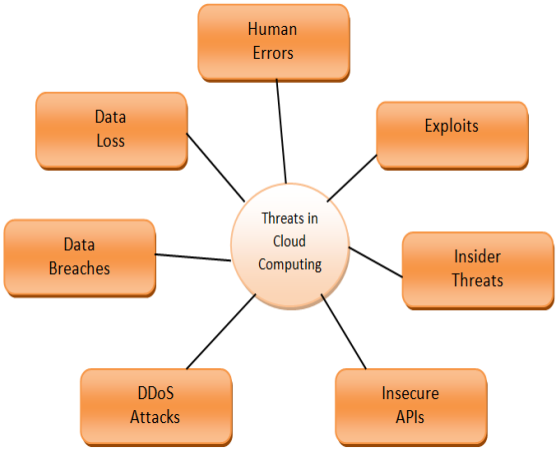

Figure 7: Threats in Cloud Computing [19][22]

7.1 Human Error

Human slogans are like dolls, and controlling your mistakes is good for this type of bullying. According to Gartner, by 2023, at least 99% of security breaches in the cloud will be customer failures [20]. Many of these successful cyber attacks will be the result of hackers using human vulnerabilities to successfully access destructive networks and infrastructure. One of the most common forms of human error that can easily expose any organization to security threats is the stability of the resulting cloud. Fuga found that 64% of the groups said that human error is the main cause of inequality.

Measures to remove human error

You can't completely eliminate these types of problems, but using checklists to document and correct activities is a great way to turn the world of human error into a real problem.

Cloud security providers can also combat these issues by using appropriate technologies.

7.2 data leak

Data breach threats are rare in cloud computing systems, but they always rank as the best customer support in the cloud. Because of this threat, all cloud services only offer IaaS, PaaS, and SaaS [14].

Data stored by users in the cloud can be important and fascinating. Data storage in the cloud can be stolen by unauthorized users and can be dangerous for users who have been attacked. This is one of the biggest threats in cloud computing because hackers can easily access user data stored in the cloud. The cloud has stored a lot of confidential information for many users. Cloud users are also required to verify the quality, reliability and performance of cloud service providers through Service Level Agreements (SLAs) agreed upon by providers and users [4], so data breaches are a serious problem. Cloud Computing data interruption technology to prevent data breaches, cloud service providers (CSPs) must protect data transfers. Proper encryption techniques must be used when transferring information back and forth.

Critical and powerful generation, storage and control Legislature refers to a legislator clearing the media before throwing it into the lake.

The law prescribes the methods of arrest and detention.

With the implementation of powerful Application Programming Interface (API).

7.3 Iinternal threats

According to Wikipedia [21], "Inside threats are harmful threats against an organization by members of the organization, such as employees, former employees, employees or business partners, who have internal information about security practices, organization, data and programs. A According to a recent report, 53% of investigative teams have confirmed attacks within their organization."

Many organizations are aware of these dangers. Malicious threats or threats are too high for the driver's influence in the organization. At your income level, they can infiltrate companies and properties and cause damage to brand identity, financial losses and productivity losses. Therefore, it is important for cloud customers to understand the monitoring capabilities that cloud providers provide to identify and protect them from malicious threats [22].

There can be many instances of insider threats, such as shipwrecks or stupid leaders. In situations where the cloud provider is responsible for security, the potential risk from insider threats is usually higher [24]. Internal threats can be addressed through trade cooperation, access control and advance efforts.

G. Director Hazard Removal Process

Harmful threats can be reduced by reviewing staffing requirements as part of legalization measures such as legal agreements, overall vendor evaluation, public information disclosure, and compliance reporting and identification of security breaches [22].

Another strategy is:

To prevent such groups in this case, we first identify and protect these institutions with the necessary resources and develop an internal threat that has been released. It then proposes solutions to monitor employee actions and complaints.

7.1 API not certified

Customers can tailor their cloud computing experience to their needs using Application Programming Interfaces (APIs). [24] The API facilitates communication between applications when they are vulnerable. Businesses should focus on designing approved APIs, other access control systems, and encryption technology.

Using weak combinations and APIs can expose your computer to a number of security risks, such as the use of widgets, updates or passwords, text verification or content transfer, malicious traffic management, or incorrect commands. recording capability [22].

As for the Reference API, these are the standards and procedures that clients use to connect to cloud services. Since the security of cloud services is based on these APIs, they must have secure certification levels, good authentication controls and performance monitoring methods to avoid threats such as widget authentication, script authentication, hacking keys. or reboot, inappropriate command, restricted monitoring [22].

The latest example of an unreliable API is Salesforce, where an API flaw in a cloud marketing service exposed customer data. It allows data to be transferred from one customer's account to another customer's account. API reduction technology is not guaranteed to mitigate this, consider the connector security model offered by the cloud. There should be strict certification and access control. Secrets should be used for information transfer and the API chain of trust should be clearly understood.

8.2. Violation

The multi-cloud nature (where clients share computing resources) means that shared memory and resources can create new attack areas for malicious gamers. This is nothing more than the benefit of any weakness in the cloud. A hacker or hackers have access to all legal information of the user, which is harmful to the user. This generally affects public clouds including IaaS, PaaS, and SaaS [25].

Ways to end abuse

Your cloud provider should have advanced patch management. They should regularly monitor their cloud service vulnerabilities and regularly update and secure the clouds to limit potential access and reduce the risk of hacker attacks on the cloud. A cloud service provider may also use an Integrated Discovery System (IDS) to ensure that the cloud service it provides is secure [22].

8.3. Distributed Denial of Service (DDoS)

Job creation attacks share major threats to customers and cloud service providers, including protracted service outages, reputational corruption, and disclosure of customer data.

DDoS is a combination of DOS attacks where multiple malicious programs are infected with Trojan horses that take a system location and result in a DoS attack. Some victims of DDoS attacks appear to be attacking a target system and the programs are malicious and controlled by a hacker in range. In a DDoS attack, the incoming traffic is hacked from multiple sources. A DDoS attack cannot be prevented by blocking a single IP address, and it is also very difficult to differentiate between legitimate user traffic and malicious traffic [26].

The DDoS attack is led by three operational units: Master, Slave and Victim. After all these attacks by the network's slave DDoS, the mater became an attacker, which acted as the starting point of the master. Jehovah offered an altar to attack the victim. That's why it is also called organized attack. Basically, a DDoS attack works in two phases: the first is the ingress segment where the master attempts to release non-essential resources to support the mainstream. Then install the DDoS tool and click on the victim's server or device. So, a DDoS attack is happening and there can be no user DoS attack mode, but it depends on how it was launched. A case similar to the experience of the Postal Service attack on CNN news websites left many users unable to access the site for three hours [22].

H. Mitigation techniques for Distributed Denial of Service Attack (DDoS)

Proxies are mainly used for core network changes to deal with multiple DDoS attacks. These changes may cause concern for consumers. [50] A comprehensive strategy is proposed to prevent DDoS attacks. This knowledge ensures an open transfer that can easily bypass simple processes like HTTP, SMTP, etc. The use of IDS in virtual machines has been suggested to prevent DDoS attacks in the cloud [4]. SNORT as a virtual search engine is ready to record all dispatches whether received or not. Another common way to prevent DDoS is to program intrusion intelligence on all

physical devices, including user virtual machines. This system has been shown to work well in the eucalyptus cloud.

7.1 data loss

Loss or loss of data may adversely affect your business. The trademark or trademark disappears completely and damages the behavior and trust of the buyer. evidence that such loss or damage is incomplete; command and control oversight; Misuse of keys and encryption software; loss of challenges; Perhaps because of the reliability of the data center and disaster recovery.

Data can be lost in ways other than malicious attacks. dismantling the reorganization; Loss of encryption key and loss of data due to natural calamities. To prevent such threats, organizations must keep their data complete. data loss removal process Protect data consistency from threats of data loss or loss; analysis of data security over time with design; implementation; Reduce critical visibility in storage and management. The supplier undertakes to clear the product through customs prior to delivery within the supplier group and the manufacturer's definition and storage methods.

IV. CONCLUSION AND FUTURE WORK

However Cloud Computing can be described as a new attraction that changes the way we use the internet. Since the computing cloud is still in its infancy and due to the high demand for organized criminals, we can expect more security incidents and similar vulnerabilities in the next decade. Security risks affect cloud computing systems. This leads to data loss and financial loss for cloud owners, cloud providers, and cloud users, as explained in this article about the new types of threats that are continually being introduced with this updated technology. This study focuses on cloud computing attacks and mitigates these issues through the use of mitigation techniques. Attacks must be avoided before they occur. With these solutions, we can prevent attacks on cloud computing systems.

REFERENCES

[1] Keiko Hashizume, David G Rosado, Eduardo Fernandez-Medina, Eduardo B Fernandez, “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications, 2013.

[2] P. Ravi Kumar. P. Herbert Raj, P. Jelciana, “Exploring Data Security Issues and Solutions in Cloud Computing”, 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India.

[3] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu, “Data Security and Privacy in Cloud Computing”, 16 July, 2014.

[4] Y Z An et al 2016 IoP Conf. Ser., Master. Sci. Eng. 160 012106, “Reviews on Security Issues and Challenges in Cloud Computing”.

[5] Subramaniam T.K. Deepa. B, “Security Attacks Issues and Mitigation Techniques in Cloud Computing Environment”, International Journal of UbiComp (IJU), Vol. 7, No. 1, January 2016

[6] Dr. V. Venkatesa Kumar, M. Nithya, “Improving Security issues and Security Attacks in Cloud Computing”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10 October 2014.

[7] Priyanka Chauhan, Rajendra Singh, “Security Attacks on Cloud Computing with Possible Solution”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, Issue 1, January 2016.

[8] B. Sumitra, C.R. Pethuru, M. Misbahuddin, “A survey of Cloud Authentication Attacks and Innovation Research in Computer and Communication Engineering”, Vol 2, Issue 10, October 2016

[9] Saakshi Narula, Arushi Jain, Ms. Prachi, “Cloud Computing Security: Amazon Web Service”, 2015 Fifth International Conference on Advanced Computing and Communication Technologies.

[10] https://www.javatpoint.com/history-of-cloud-computing, Access : July 2020

[11] https://en.wikipedia.org/wiki/Cloud_computing, Access : July 2020

[12] https://en.wikipedia.org/wiki/John_McCarthy_(computer_scientist), Access : July 2020

[13] https://www.tutorialspoint.com/cloud_computing/cloud_computing_security.htm , Access : August 2020

[14] Naseer Amara, Huang Zhiqui, Awais Ali, “Cloud Computing Security Threats and Attacks with their Mitigation Techniques”, 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery.

[15] https://resources.infosecinstitute.com/cloud-computing-attacks-vectors-and-counter-measures/#gref, Access : August 2020

[16] M.Misbahuddin, “Secure Image Based Multi-Factor Authentication (SIMFA): A Novel approach for Web Based Services, Ph.D Thesis, Jawaharlal Nehru Technological University, [Online], http://shodhganga.inflibnet.ac.in/handle/10603/3473, 2010

[17] https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html, Access : August 2020

[18] https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm, Access : September 2020

[19] https://www.synopsys.com/blogs/software-security/10-cloud-security-threats-2018/

[20] https://www.fugue.co/blog/the-human-factor-in-cloud-misconfiguration, Access : September 2020

[21] https://en.wikipedia.org/wiki/Insider_threat, Access : September 2020

[22] Mohsin Nazir, Mirza Shuja Rashid, “Security Threats with Associated Mitigation Techniques in Cloud Computing”, International Journal of Applied Information Systems (IJAIS), Foundation of CS FCS, New York, Vol. 5, No. 7, May 2013

[23] https://insights.sei.cmu.edu/sei_blog/2017/11/5-best-practices-to-prevent-insider-threat.html, Access : September 2020

[24] https://hashedin.com/blog/5-security-concerns-in-cloud-computing/, Access : September 2020

[25] https://www.cloudflare.com/learning/cloud/what-is-multitenancy/, Access : September 2020

[26] Usman Amir, Khalid Hussain,”DDoS Attacks Detection and Prevention Techniques in Cloud Computing: A Systematic Review”, IJCSIS, Vol.14, No. 10, October 2016