A study on vulnerable risks in security of cloud computing and proposal of its remedies

Rashi Saxena1, E. Gayathri2

1Research Scholar, 2Associate Professor
Department of Computer Science & Engineering, K L Deemed to be University, Hyderabad, Telangana, India.
E-mail: rashisaxena.cse@klh.edu.in

Abstract. Data innovation worldview empowers pervasive access to shared pools of configurable framework assets and more significant level administrations that can be quickly provisioned with minimal administration exertion, regularly over the Internet. Cloud computing provides dynamic asset administrations for the client on request, and it is becoming increasingly popular. Cloud administrations are conveyed from server farms all through the world (as it is otherwise called Networks of systems). Outsider associations are additionally present there, because of which some significant security dangers came and make organize helplessly so the security of cloud information is imperative to keep over Cloud architecture to offer better support, ease administrations, and so forth. Despite that there are a few undermined hazards in cloud computing security. We will be concentrating majorly on cloud computing fraught with threats and how to overcome those threats. This paper is intended to introduce information about the most current attacks on cloud computing, just as safety efforts. The seriousness and impact of these attacks are talked about alongside genuine instances of these attacks. The paper likewise proposes alleviation strategies that can be utilized to decrease or dispose of the risks of the threats talked about. Moreover, the general cloud security proposals are given.

Key words: Cloud security, Cloud threats, Cyber-attacks, Security Tools.

1. Introduction
Cloud computing simplifies and adapts everything, but cloud architecture is complicated, and resolving any security or network-related issue is difficult. In brief, there are three sorts of clouds: public, private, and hybrid. In addition to Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS), cloud providers provided three categories of services [1] as seen in figure 1. A commercial name for "Cloud Computing" is Cloud [2].
Nonetheless, because cloud computing is not completely secure against specific attacks, it can cause difficulties for both end-users and cloud service providers. It is our primary goal to describe the vast majority of the threats while also attempting to outline some strategies for overcoming them.

2. Literature Survey

Author of [3] discussed about cloud security concerns. They sparked interest in security concerns that were centered on specialized security in cloud administrations, among other things. They discuss the hazards associated with cloud administration that have been overlooked, such as there are four types of assaults: VM-level attacks, compliance issues, isolation failure, and management interface compromise. They also used cloud security engineering in order to shield themselves from attacks and assaults on their infrastructure. Also covered are the critical components of this architecture: single sign-on, increased accessibility, a single administration dashboard, virtual machine protection, and a defense-in-depth cybersecurity strategy.

In [4], the author discussed several important risks that must be avoided to provide a secure cloud environment. Security elements such as those found inside threats, framework communication capabilities, and access control were built into the design (e.g., virtualization, data encryption, host Operating System, and visitor framework, backup, firewall, server location, etc.). The author shows how a major issue will shape cloud security in the future. Additionally, an in-depth exploration of such problems as vendor lock-in and contradictions is conducted. Security ideas might also be applied in cloud computing settings as cloud computing itself does not have any special security standards.

The author of the study article [5] investigated several risks and characteristics associated with cloud computing, as well as developing a strategy for its remediation. The researcher focused on the seven most major threats, as well as a few others, such as session riding and hijacking, weak cryptography, data protection, and portability. Also, customers will have better security because of the absence of uniformity. Struggled to demonstrate creativity while simultaneously implementing a very effective security system, which should be established in order to generate inventive innovation without going into detail.

3. Vulnerable threats/attacks on cloud computing with suggested moderations

Because a third party is engaged in cloud computing, security is the most important consideration. Consequently, certain tools and methods that are required to resolve this issue are presented. Several risks and assaults against the cloud computing environment are discussed, as well as some effective mitigations that may be implemented. Using the cloud computing platform as an example, [6] Figure 2 depicts the danger landscape –
3.1 Nefarious usage of cloud computing

It has been designated as the most danger by the Cloud Security Alliance (CSA) [7]. Botnets are used to distribute viruses and spam over the internet. IaaS companies give their clients with a variety of benefits, including unlimited compute space, network bandwidth, and storage capacity. Then the attackers seize the opportunity to launch an assault against the seller.

**Suggested moderation:** Initial registration, credit card monitoring, and network traffic monitoring are just a few of the processes that can help to mitigate this issue.

3.2 Insecure Internet connections

Another hazard to cloud computing is the use of insecure interfaces. When developing APIs, it is critical to consider security factors such as authentication, access control, and a monitoring system.

**Suggested moderation:** Monitoring access control and authentication is permitted under tight conditions as specified.

3.3 Invading Saboteurs

When dealing with a hostile insider, it is critical to consider the sort of standard or employee who will be employed since there is no monitoring or reporting mechanism that would reveal their access data.

**Suggested moderation:** Through chain management, a security breach notification system and a reporting system are implemented.

3.4 Loss of data

Unreliable media, a weak password, no encrypted data, a lack of a secure backup system, hard drive failure, and other factors can all result in data loss and leaking, which is a serious concern.

**Suggested moderation:** It is necessary to implement an encryption and decryption mechanism, as well as monitoring, file backup, and a strong password.
3.5 Account, Service & Traffic Hijacking

Another concern that cloud clients should be aware of is account, service, and traffic hijacking, with the objective of preventing this from happening again. From a man-in-the-middle attack, phishing, and spam to denial-of-service assaults, re-used secret keys, extortion, and programming flaws, these dangers have evolved throughout the years. The hijacking of traffic is a recurring topic in cloud computing.

**Suggested moderation:** Understand a security strategy, put a few ideas into practice among clients and suppliers, implement a confirmation mechanism, and provide a means for ensuring the system's integrity.

3.6 DoSA (Denial of Service Attacks)

DoS attacks provide the impression that an authorized user is inaccessible; for example, when anybody visits a website, they may see an error page or a page that is not available for DoS attacks.

**Suggested moderation:** When dealing with this issue, an Intrusion Detection System (IDS) might be employed [8]. The defensive federation [9] is yet another type of detecting system.

3.7 Multi-tenancy natures

Since this threat targets service providers online that provide services to numerous customers on demand, the attack can occur regularly through VM (virtual machine), and the danger has an impact on IaaS (Internet of Things) services. A comparable program is used by several different customers who connect to the virtual machine over the internet.

**Suggested moderation:** This danger may be identified using strong authentication and access control.

3.8 Risk assessment

Programming variations, code upgrades, and disruption Endeavor security rehearsals are all things that clients or customers should be aware of. The user must be aware of the location in which the data or logs are stored. However, risk assessment never accomplishes this [7].

**Suggested moderation:** Clear information regarding logs and data, as well as monitoring and an alarm system, can help to avoid risk assessment from taking place.

3.9 SQL injection attacks

It is possible that malicious code has been embedded inside a carefully written SQL code, and this has resulted in a touchy assault and some unexpected results [10]. Access to a database without authorization is a type of assault that occurs from time to time.

**Suggested moderation:** SQL infusion can be stopped by filtering techniques; however, an intermediary engineering should be developed that gradually differentiates and eliminates contributions from clients that are suspected of overseeing SQL injection.
3.10 XSS (Cross-Site Scripting) attacks

In this sort of attack, a variety of malicious scripts are uploaded to the web and executed. It can occur in two ways: because of a stored XSS or because of a reflected XSS. One is utilized on a permanent basis, whereas the other is not [11].

**Suggested moderation:** Provide or implement some type of error-prone data disinfection mechanism, which protects components on both the consumer and server sides.

3.11 MIMA (Man in the Middle attacks)

It is an alluring danger in which an entity constantly seeks to remain between a sender and a receiver, implying that they constantly offer information between the sender and clients, resulting in the clients receiving erroneous information.

**Suggested moderation:** This challenge may be solved by implementing service security procedures that are distinct from endpoint and server security processes [12], the topology of the network can affect the setup of the network.

3.12 Theft of Identity

It is another danger to cloud computing. Sometimes identity alterations occur when a fraudster steals another person's identity and use it for all their advantages, and the victims suffer as a result in the long term.

**Suggested moderation:** Strong password is solution.

4. Tools for cloud computing security

These applications are designed to keep malware out of the system, as well as protect against unwanted system logins and external cloud applications like Salesforce and Google Docs. This is just the beginning. These concepts are discussed at the beginning of this article (shown in figure 3), we discussed hazard and remediation apparatus.

![Figure 3: Cloud Computing Security Tools](image-url)
4.1 Qualys

It secures devices, web applications, and web applications, but does not require any hardware or software. Malicious software is detectable, repair issues if found, scan apps, and save web apps in the cloud.

4.2 Okta

One of the most essential pieces of technology, it keeps a log of all the employees who use information. The first job is identity management. the overall objective of Okta is to make SSO (Single-Sign-on) available for all cloud-based applications.

4.3 Cipher Cloud

Cipher Cloud secures further, such as Salesforce, Chatterbox, Office 365, Gmail, Amazon Web Services, and various other products and services. It ensures that the administration model is encrypted, including for sending and receiving data, as well as to check traffic, which acts as a hostile to antivirus.

4.4 Bitglass

The ability to offer information and threat protection in any context, on any device, at any time, is what Bitglass delivers with aim to detect and reduce the risk of loss of data, while maintaining visibility of data even in the cloud.

4.5 Sky-high

It has the capability of discovering, analyzing, and securing applications that we use in the cloud. It has the capability of discovering or detecting which cloud applications are being used by the employees.

4.6 Antivirus

Security tools such as antivirus are not new to cloud computing. The virtual computer is protected by a Kaspersky Lab formula. E-mail security is provided by McAfee.

4.7 Netskope

Cloud apps are discovered and monitored by Netskope, which is a service that is utilized on your network to identify and monitor them. Based on the information collected by Netskope, it gives extensive statistics on users, sessions, shared and downloaded content as well as the contents of the shared content.

5. Conclusion

As far as we can tell, cloud computing is going to be with us for a long time to come. Cloud computing will be used in many ways soon. Even though it offers several features, the cloud is not reliable when it comes to security. A robust security model is required to manage all the layers of the cloud and it should be able to do so in a secure manner. This subject is covered in-depth in this article, and many strategies to counter these security concerns in cloud computing are laid forth. Threatened risk could not exist without all these protective and mitigative measures. Following this study, we can predict that a significant number of vulnerabilities would be solved in the upcoming years if these tools are employed. In this paper, a fundamental understanding of threatened risks is laid out, as well as various methods.
for dealing with them in cloud computing. All of these and similar resources are crucial for dealing with elevated risk. In this case, the tools can solve a lot of future security problems.

References

[1] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satyapathy. “Cloud Computing: Security Issues and Research Challenges”. IJCSITS Vol. 1, No. 2, December 2011.
[2] Qi Zhang, Lu Cheng, Raouf Boutaba. “Cloud Computing: State-of-the-art and research challenges”. J Internet ServAppl (2010).
[3] Tripathi and A. Mishra, “Cloud computing security considerations” IEEE Int. conference on signal processing, communication, and computing (ICSPCC), 14-16 Sept., Xi'an, Shaanxi, China, 2011
[4] Amutha devi, Gayathri MonickaJ, “Emerging bio-medical applications and open research challenges in cognitive internet of things (CIOT)” International Journal of Pharmacy and Technology” Dec-2016 Vol. 8 Issue No.4 5049- 5054
[5] Mervat Adib Bamiah* et al. / (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 26, Issue No. 1, 012 – 015
[6] https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/
[7] CSA, “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1” Cloud Security Alliance, 2009, [Online], Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[8] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, “Intrusion detection techniques for Grid and Cloud Computing Environment”, IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.
[9] Gayathri Monicka, J & Jamuna, V 2015, ‘Hybrid Cascaded MLI topology using Ternary Voltage Progression Technique with Multicarrier Strategy’, Journal of Electrical Engineering &Technology (JEET) vol.10,pp.1610- 1620,2015
[10] Liu, Y. Yuan, A Stavrou, “SQLProb: A Proxy-based Architecture towards Preventing SQL Injection Attacks”, SAC March 8-12, 2009
[11] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, “Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis”, Proceedings of the Network and Distributed System
[12] Eric Ogren, “Whitelists SaaS modify traditional security, tackle flaws”, Sep. 17, 2009. [Eric Ogren is the founder and principal security analyst at Ogren Group]
[13] http://www.hongkiat.com/blog/cloud-security-tools/