Cloud Computing Challenges in Security Applications – A Review

P. P. Joby

Professor and Head, Department of Computer Science and Engineering, St. Joseph's College of Engineering and Technology, Kerala.

Email: jobypcse@gmail.com

Abstract

Cloud computing platforms provide an advanced computer system that allows organizations and individuals to operate a wide range of tasks such as using online storage capacity, implementing business applications, developing customised computer software, and creating a "realistic" communication network. Because of numerous security and privacy concerns, cloud technology has struggled to gain popularity among many large and established organizations. This research discusses the security challenges of cloud computing networks, beginning with a description of cloud computing and its various types. Furthermore, it provides a brief explanation of the most common cloud computing service challenges.

Keywords: Cloud Computing; Security; Attackers; DoS

1. Introduction

1.1 Cloud Computing

The term cloud means a Network or Internet. WAN, LAN, or VPN are examples of public or private networks through which cloud services can be delivered.

Cloud computing is the new generation technology with a sustainable IT infrastructure. It provides user the ability to use and utilize an application through the internet. It also means a type of internet-based computing. The cloud computing has different services such as servers, storage, and software applications, that are delivered to an organization's computers and devices through the internet. With this technology, accessing cloud vendors does not require

DOI: https://doi.org/10.36548/rrrj.2022.1.010

significant capital investments. Instead, the cloud supports “pay-per-use”, which means that the users of the organizations can only pay that fixed amount to access the cloud infrastructure. In other words, cloud computing describes applications and services that leverage virtualized resources to run over a distributed network and use conventional internet protocols to connect. Cloud computing refers to operating, configuring and retrieving the hardware and software assets remotely. It provides internet data storage, infrastructure and application as shown as figure 1.

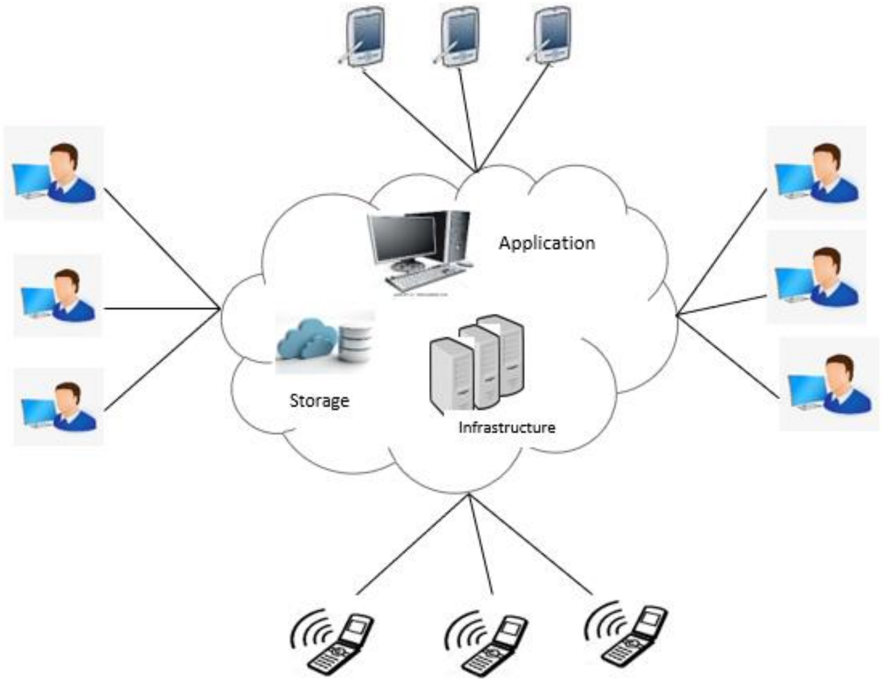

Figure 1. Cloud Computing

1.2 Concepts of cloud computing

The cloud computing is feasible and available to end users due to the number of services and models operating in the background [11]. The working models for cloud computing are as follows:

- Deployment Models
- Service Models

1.2.1 Deployment Models

The cloud deployment models define the particular type of cloud domain based on ownership, scalability, access, and the nature and function of the cloud. There are four types of deployment models: public, private, community and hybrid.

Public cloud:

The public can easily access the system and service in the public cloud. Since public clouds are more accessible, they could be less secure.

Private cloud:

The private cloud is only managed by the organization and serve within an organization. Since private clouds are less accessible, they cloud be more secured.

Community cloud:

The community cloud is managed by group of organizations and supports a specific community that has the same interest.

Hybrid Cloud:

The hybrid cloud is the combination of public cloud and private cloud, wherein the non-essential tasks are completed using the public cloud and the critical tasks are completed utilizing the private cloud.

1.2.2 Service Models

There are three important cloud service models, which are:

- Infrastructure-as–a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Infrastructure-as–a-Service: IaaS is a basic service where the providers can offer computing power and storage space on demand. It gives load balancers, software packages, IP address, etc. The benefits of IaaS are dynamic, renting, full control and easy access. It also includes some drawbacks, like limited flexibility and user privacy, dependence on virtual services, and requirement for an internet connection.

Platform-as-a-Service: PaaS is a full-featured cloud development and deployment environment that has the facilities needed to produce everything from basic cloud-based apps to complex corporate applications. It provides scalability, and is low in cost, simple and easy to use. PaaS offers some demerits, like vendor migration, mix-up complexity, and data privacy.

Software-as-a-Service: A method of distributing applications over the internet as a service is known as SaaS. Complicated software and hardware maintenance can be avoided by just accessing software over the internet rather than installing and maintaining it. SaaS provides some benefits like easy to buy, specialised software, and low maintenance. It has some disadvantages such as latency factor, switching, and internet connection.

Technology of the next generation benefits from the cloud. However, if sufficient security protection is not provided, cloud services may eventually lead to increased costs & potential corporate losses, negating any potential advantages of cloud technology. Consequently, the goal of cloud security and its researchers is to assist organisational information technology and decision makers in analysing the security implications of cloud computing in their business. When a consumer decides to use cloud computing, they are fully aware of the security and risk issues that could arise.

2. Related Works

Nowadays, cloud computing is an emerging technology that is a more successful implementation of cloud technology for an enterprise. However, there are still certain challenges with cloud computing security. Some research focused on these challenges, as shown in table 1.

Kulkarni et al., [1] proposed a method of end-to-end encryption for more security. It gives some possible solution to avoid untrusted components, also ensure secure operations. It solves the security risks, threats, vulnerabilities, and server breakdowns. Zaman et al., [2] described a Cloud forensics for security enhancement. This method detected the legal activity and improved the network infrastructure, cloud provided features and cloud consumers. Such research issues are elasticity, multitenancy, and layers dependency stack. Srivastava et al., [3] claimed that data security can be enhanced using Bio computing algorithm. Users, sharing and processing the data is very difficult in the security of cloud system. It provided storage, processing, and multimedia security, to protect the network from interference. Parast et al., [4] investigated the security issues using the types of service models such as IaaS, PaaS, and SaaS, that improved the cloud security. Sasubilli et al., [5] analysed the performance of DevSecOps processes. It reduced the threats over its security, availability, reliability, and confidentiality.

Kanwal et al., [6] proposed a data protection using cloud, which provides low cost and flexible and secure internet connection. Shirgaonkar et al., [7] studied to improve the cloud security using cryptography algorithm. It provided data storage and remote access, also resolved the data breaching issues.

Table 1: Comparison of Different Techniques

S.No	Reference	Proposed Technique	Application	Research Issues	Possible Solutions	Merits
1.	Kulkarni et al. [1]	End to end encryption	Security enhancement	1. Security risks 2. Threats 3. Vulnerabilities 4. Server breakdown	▪ To avoid untrusted components ▪ To ensure secure operations	➢ Malware injection attack ➢ Flooding attack ➢ Accountability check
2.	Zaman et al. [2]	Cloud forensics	Security solution	1.Data center 2.Multitenancy 3.Elasticity 4.Layers Dependency Stack	To detect legal activity	➢ Network infrastructure ➢ Cloud-provided features ➢ Cloud consumers ➢ Cloud service delivery methods
3.	Srivastava et al. [3]	Bio computing algorithm	Enhancement of data security	Sharing and processing the data is very	Providing storage, processing,	➢ Enhance multimedia security

				difficult in the security of cloud system.	and multimedia security	➢ Protect the network from interference ➢ Data security
4.	Parast et al. [4]	IaaS, PaaS, and SaaS	Security enhancement	1.Virtualization 2.Multitenancy	Using three-layer model to increase the security	Improve the cloud security
5.	Sasubilli et al. [5]	DevSecOps processes	Security enhancement	1.Availability 2.Reliability 3.Integrity 4.Confidentiality	Integrated security with centralized administration	Reduce the threats over its security
6.	Kanwal et al. [6]	Cloud computing	Data protection	Cost-effectiveness	Secure internet connection for remote access	➢ Flexible ➢ Low cost
7.	Shirgaonkar et al. [7]	Cryptographic Algorithms	Improve cloud security	Resolving data breaching issues	Hybrid Encryption for more security	➢ Data storage ➢ Remote access
8.	Kaufman et al. [8]	Security Content Automation Protocol	Data security	1.Dynamic 2.Reliable 3.Customizable	SCAP used to offer security during data transmission	➢ Confidential ➢ Integrity ➢ Availability
9.	Behl et al. [9]	Cloud-aware security solutions	Security Enhancement	1. Openness 2. Trust	Pre-emptive protection	➢ Inside threats

				3. Security Threats		➢ Outsider malicious attacks ➢ Multitenancy
10.	Shabbir et al. [10]	Modular Encryption Standard	Mobile Cloud Computing	1. Security breaches 2.Vulnerabilities	Blockchain security model	➢ Health record monitoring ➢ Low system efficiency

In [8], the author evaluated the performance of cloud security using security content automation protocol. It improved the security during data transmission and produced confidentiality, integrity and availability. Behl et al., [9] analysed the performance of cloud aware security solutions that provides pre-emptive protection for complex network. Due to the openness of accessible information and data relying on trust between cloud provider and customer, heightened security threats must be overcome in order to fully benefit from this new computing exemplar.

Shabbir et al., [10] investigated the Modular Encryption Standard (MES) in mobile cloud computing for security enhancement. Using layered modelling to describe the security mechanisms, the MES was developed. The performance analysis demonstrated that, in terms of improved performance and supplementary qualitative security assuring measures, the work outperformed other frequently employed algorithms against the security of health information at the MCC environment.

3. Cloud Computing Challenges

3.1 Cloud security

In cloud technology, all shared data are stored in cloud infrastructure. Sometimes anyone can access the data, because of its nature of transmitting resources. As a result, the data stored in the cloud should be maintained in encrypted form. As the number of companies using cloud technology for data operation has increased, effective security and other potentially unsafe areas are considered more important for companies that work with cloud providers.

Security for cloud computing manages cloud protection controls and offers client data security, privacy, and compliance with applicable standards.

Users need to analyse the several characteristics before using cloud technology.

- Users must analyse the vulnerability to risk of resources.
- At various levels of service, the models of cloud services mandate that the client is accountable for security.
- Understand the methods the providers of cloud service use to store and transfer data.
- Consider proper cloud type to be used, such as public, private, community or hybrid.

3.2 Cloud Security Challenges

Some of the most common security attacks in cloud computing have been discussed.

3.2.1 Cloud Malware injection attacks

Cloud malware relates to a cyberattack using malicious software and services on a system based on cloud computing. Cyberattacks are a perfect method for different cloud-based malware. The systems that are most vulnerable to cloud-based technologies are listed below.

- Open cloud-based system on the internet.
- Standard and easy to learn cloud-based system.

Cloud-based systems are composed of a variety of components, including virtual machines, storage devices, and containers. A cloud malware injection attack is used to attack the cloud computing platforms. A hacker attempts to introduce a harmful service or virtual machine onto the cloud-based system in this case. This causes it to produce malicious SaaS, PaaS, or IaaS implementation modules or virtual machine instances.

Types of cloud malware attacks

- ➢ DDoS Attacks
- ➢ Hypercall Attacks
- ➢ Hypervisor DoS
- ➢ Hyperjacking

3.2.2 Abuse of cloud services

Criminals may target their victims via cloud computing and exploit the cloud service against them. Misuse of cloud resources can take many forms, including DDoS attacks, phishing attempts, email spam, and mining for digital currencies. A user's cloud infrastructure could be compromised, with serious repercussions for the company. Enterprises need to keep an eye on who has access to the cloud and set up countermeasures for any dangers or threats. If misuse of cloud services should occur, data loss prevention and disaster recovery plans can help with the recovery process.

3.2.3 Denial-of-Service attack

A Denial-of-Service (DoS) attack is a kind of cyberattack, where an unreliable hacker attempts to prevent a computer or other device from being used for the purpose for which it was intended by disrupting its regular operation. DoS attacks frequently target the web servers of well-known corporations, including media, financial, and commercial companies, as well as governmental and commercial organisations. DoS attacks can cost the victim a lot of time and money to deal with, even while they normally do not lead to the theft or loss of important information or other assets.

DoS attacks can be performed in one of the two ways: flooding service or crashing services. Flood assaults occur when there is too much traffic for the server to handle, which makes the system slow and finally unresponsive. Popular flood attacks involve:

- Buffer overflow attacks – This type of attacks can send more traffic to a network resource that was designed to handle. It includes the following attacks in addition to others that attempt to take advantage of vulnerabilities, unique to particular networks or applications.
- ICMP flood - An Internet Control Message Protocol (ICMP) flood DoS attack, pings every device on the network connect instead of just one particular machine by using faked packets that are sent through improperly configured connected devices. The traffic is subsequently amplified by the network. The smurf attack and the ping of death are some names for this attack.
- SYN flood - The TCP handshake protocol, which a client uses to connect to a server using TCP, is being abused in this attack. In a SYN flood attack, the attacker sends a large number of requests to the victim server's TCP port, with no

thought to closing the circuits. A successful attack may prevent authorised users from accessing the server.

3.2.4 Insider attacks

A security risk known as an insider threat occurs from inside the targeted company. It usually involves a current or previous employee or business acquaintance who gains unauthorised access to private data or privileged accounts on an organization's network. Traditional security procedures often concentrate on external threats rather than internal threats that may come from within the company.

Types of insider threats include:

- Malicious insider – It is often referred to as a "Turncloak," when someone purposefully and maliciously abuses authorized credentials, usually to steal data for financial or personal gain. For instance, a person with a grudge against a previous company or a shrewd employee who sells confidential knowledge to a rival. Turncloaks have an advantage over the other attackers since they are acquainted with an organization's security rules, procedures, and weaknesses.
- Careless insider – It is an unsuspecting pawn who unintentionally exposes the system to threats from outside. This is the most prevalent kind of insider threat and is brought on by errors like leaving a gadget accessible or falling for a trap. For instance, a worker who has no malice in mind might click on an unsafe link and introduce malware into the system.
- A mole – A pretend who, while technically an outsider, has succeeded in obtaining insider access to a restricted network. This is a person from outside the company who poses as a shareholder or employee.

3.2.5 Account or Service Hijacking

The process of a cloud account being stolen or taken over by an attacker is known as cloud account hijacking. Identity theft tactics frequently use cloud account hijacking, in which the attacker uses the account information they have obtained to engage in illegal or unlawful behaviour. When a cloud account is hijacked, the attacker frequently poses as the account owner using a hacked email address or other credentials.

While cloud computing has several advantages for businesses, such as lower capital expenses and access to resources whenever needed, it also gives cybercriminals a target-rich environment because large amount of data are stored in one location. The hazards posed by cloud account hijacking are numerous as a result of the fact that the data are reserved and accessible on equipment and resources that are frequently shared by numerous users.

4. Conclusion

Cloud computing is constantly evolving in order to provide customers with various levels including services. While people can benefit from cloud computing, security in clouds is a major challenge. Clouds are still vulnerable, and hackers are exploiting these security bugs. Security flaws must be described in order to deliver better platform to cloud users. Furthermore, security challenges seem to be countless, providing many opportunities for attackers to breach the authorization level and obtain the data. Due to the immediate need for cloud technology and the requirement for it among many businesses, their trust in technology and data storage is required. Computing constantly calls for the improvement of security, a raising of the level of security, and a try to prevent all types of cyber-attacks on it.

References:

[1] Kulkarni, G., Chavan, N., Chandorkar, R., Waghmare, R., & Palwe, R. (2012, October). Cloud security challenges. In 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA) (pp. 88-91). IEEE.

[2] Zaman, M. T., & Rani, M. (2022). Cloud computing security challenges, analysis of security problems and cloud computing forensics issues. In Security and Privacy Trends in Cloud Computing and Big Data (pp. 147-164). CRC Press.

[3] Srivastava, A., & Ahmad, S. (2022, June). Bio-Computing Based Algorithms for Cloud Security: A Critical Review. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) (pp. 894-900). IEEE.

[4] Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. Computers & Security, 114, 102580.

[5] Sasubilli, M. K., & Venkateswarlu, R. (2021, January). Cloud computing security challenges, threats and vulnerabilities. In 2021 6th International Conference on Inventive Computation Technologies (ICICT) (pp. 476-480). IEEE.

[6] Kanwal, I., Shafi, H., Memon, S., & Shah, M. H. (2021). Cloud computing security challenges: A review. Cybersecurity, Privacy and Freedom Protection in the Connected World, 459-469.

[7] Shirgaonkar, M., Shinde, A., Sankpal, P., & Gutte, V. (2022, March). Cloud Computing Security using Cryptographic Algorithms. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 31-37). IEEE.

[8] Kaufman, L. M. (2009). Data security in the world of cloud computing. IEEE Security & Privacy, 7(4), 61-64.

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

[10]Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N., & Lin, J. C. W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. IEEE Access, 9, 8820-8834.

Author’s Biography

P P. Joby is Professor and Head of Computer Science Engineering Department at St. Joseph's College of Engineering and Technology, Palai, Kerala, India. He completed his Doctorate in Information and Communication Engineering expertise in the field of wireless sensor networks. He completed M.Tech in advanced computing from Sastra University and B.E. in Computer Science and Engineering. He has many international and national publications. He is Active Member in professional bodies such as ISTE, IAENG, UACEE, and IACSIT.