International Journal of Recent Research and Review, Special Issues- 2025
ISSN 2277 – 8322

SECURITY ISSUES ON CLOUD COMPUTING

Ankit Kumar Taneja 1, Poornima Kumawat [2], Bhawana Asthana [3]
[1]Assistant professor, [2,3]Research scholar
[1,2,3]Department of computer science
Arya College of Engineering, Jaipur, Rajasthan

Abstract- Cloud computing has revolutionized the way businesses and individuals store, manage, and process data, offering unparalleled scalability, cost-effectiveness, and accessibility. However, as reliance on cloud services grows, so do concerns about data security and privacy. In an era where AI-driven technologies are advancing rapidly, securing cloud environments has become more critical than ever. This paper explores the various security challenges associated with cloud computing, including data breaches, unauthorized access, service disruptions, and compliance risks. While cloud platforms offer robust solutions for data management, they also introduce vulnerabilities that can compromise sensitive information. Through this study, we analyze the key risks, examine existing security measures, and propose strategies to enhance cloud security. By understanding these challenges and solutions, organizations and individuals can make informed decisions to safeguard their data in the cloud.

Keywords- Cloud Computing, Services of Cloud Computing, Deployment Model, Security Issues, Data Protection.

1. Introduction

Cloud computing is a novel concept that has gained widespread adoption over the past few years, becoming a fundamental aspect of modern computing. As digital transformation accelerates and the number of web- connected devices continues to rise exponentially, the demand for efficient data storage, processing, and management has grown significantly. Cloud computing provides a scalable and cost-effective solution to these challenges by enabling businesses and individuals to store, manage, share, and analyze vast amounts of data seamlessly over the internet.

One of the core strengths of cloud computing is its ability to facilitate resource sharing. A massive network of interconnected commodity hardware forms the backbone of cloud infrastructure, allowing users to access computing resources dynamically based on demand. This architecture enhances high availability, flexibility, security, and ease of maintenance. Additionally, cloud services offer accessibility beyond geographical limitations, allowing users to leverage computing power, storage, and applications from anywhere, at any time, with just an internet connection.

However, alongside its vast benefits, cloud computing also introduces significant security challenges. As organizations migrate sensitive data to cloud platforms, concerns about data privacy, unauthorized access, cyberattacks, and service disruptions have become more prevalent. Issues such as data breaches, insecure APIs, insider threats, and compliance risks pose substantial

challenges to cloud security. The shared responsibility model of cloud security requires both service providers and users to implement robust security measures to mitigate risks effectively.

This paper explores the security challenges associated with cloud computing, analyzing common threats and vulnerabilities while discussing existing security frameworks and best practices. By understanding these challenges and implementing proactive security strategies, organizations and individuals can enhance the safety and reliability of cloud-based systems.

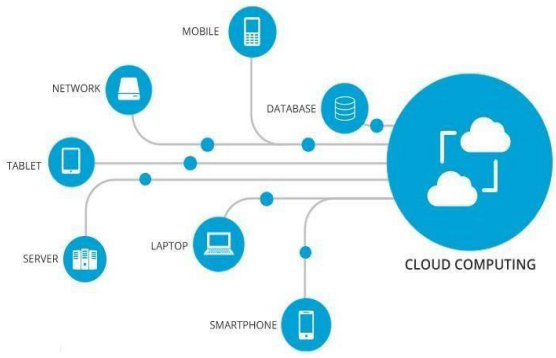

Fig 1: Cloud Computing

2. Services of Cloud Computing

A selection of the various services that cloud computing offers are discussed below:

A. **Software as a Service(SaaS)-** SaaS is sometimes referred to as "on-demand software." A cloud service provider hosts the apps in this software. Users only need a web browser and an internet connection to access these programs.

B. **IaaS-** Servers or make labor-intensive hardware investments, IaaS gives customers access to processing power or virtual machines. The networks, servers, and data centers where the hardware resources are physically supplied are all maintained and managed by the cloud service provider.

C. **Platform as a Service(PaaS)-**This cloud-based IaaS version is more sophisticated. PaaS offers the IT infrastructure as well as the computing platform and solution stack as a service. Programmers may create unique apps with the help of PaaS, a cloud computing service. Platform as a service allows software developers to design and construct custom online apps without worrying about hosting, manufacturing, or storing data.

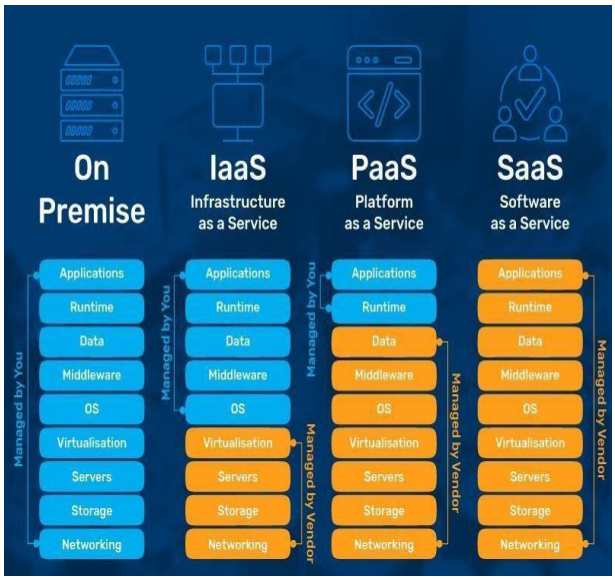

Fig 2: Cloud Computing Services

3. Deployment Models

A Cloud deployment model details who owns the server and where they are located. It describes the layout of your cloud infrastructure, what you may change, and if you will get services or have to start from scratch. The connections between your customers and the infrastructure are also determined by the types of cloud deployment.

A. Public Cloud

The public cloud provides systems and services that are open to everybody. Since everyone may access the public cloud, it can be less secure. Public clouds are those that make their cloud infrastructure services accessible to the general public or to significant trade groups over the Internet.

B. Private Cloud

The deployment strategy used by a private cloud differs greatly from that of a public cloud. This environment has only one user, and that is the consumer. You don't have to lend out your equipment. There are differences between private and public clouds in terms of how all the hardware is managed. The ability to access systems and services inside a certain organization or set of boundaries is referred to as the "internal cloud".

C. Hybrid Cloud

Hybrid cloud computing combines the best features of both worlds by using a layer of proprietary software to provide a barrier between the public and private realms. You may host the app in a

secure location and benefit from the public cloud's financial advantages by using a hybrid approach.

D. Community Cloud

It makes systems and services accessible to a large number of organizations. In order to meet the specific requirements of a community, business, or company, the elements of many clouds were combined to form this decentralized system. The group that deals with shared problems or obligations may share the infrastructure of the community.

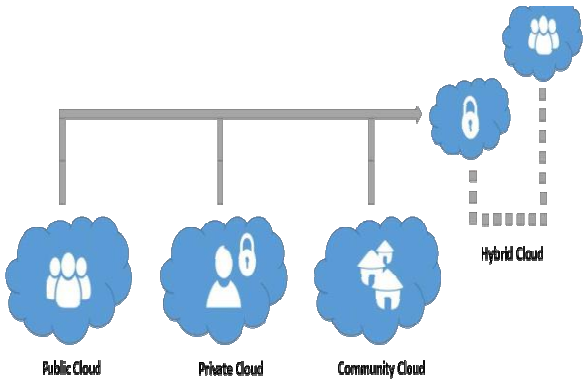

Fig 3: Cloud Deployment Models

4. Security Issues in Cloud Computing-

Undoubtedly, cloud computing offers several advantages; yet, there are also noteworthy security issues. The list of these cloud computing security issues is provided below.

4.1 Unauthorized Access

Unlike an organization's on-premises infrastructure, cloud-based installations are immediately accessible from the public Internet and are located outside the network perimeter. On the other hand, this improves user and customer accessibility to the infrastructure. Additionally, it makes it easier for unauthorized users to access a business's cloud based services. If credentials are hacked or security is configured incorrectly, an attacker could be able to get direct access without the organization's awareness.

Mitigation

1. Enrolling people should be carried out through appropriate authentication.

2. Reporting suspected security breaches should happen right away.

4.2 Insecure API

Using application programming interfaces (API), users may customize their cloud computing experience. As API infrastructure grows to provide greater services, security risks rise. An API's communication between apps is where vulnerabilities exist. Organizations and programmers can gain from this, but it also exposes them to security risks.

Mitigation

1. For cloud provider APIs, the strong authenticated security paradigm is applicable.

2. Authentication, access control, encryption, and activity monitoring should all be considered while designing APIs.

3. APIs have to be kept private and not shared.

4. Depend on industry-standard API frameworks that have been security-engineered like Open Cloud Computing Interface (OCCI) and Cloud Infrastructure Management Interface (CIMI).

4.3 Interior hazard

Workers who have been given permission to use a company's cloud-based services might abuse them or have access to private information including customer accounts, financial records, and other data.

Mitigation

1. Limiting the influence and potential of an insider assault requires the use of the Principle of Least Privilege.

2. Beware of third-party vendors.

3. DSPM (Data Security Posture Management) is intended to assist in preventing insider threats by identifying and obstructing efforts to transfer confidential information across the network.

4.4 Account and Traffic Hijacking

Since the cloud has become more widely used in businesses, account hijacking has given birth to a whole new set of issues. With the login credentials you (or your employees) provide, attackers can now access confidential data stored on the cloud from a distance. They can even use stolen credentials to alter and fabricate data.

When a user reuses their credentials and passwords, attacks become more significant. An attacker with access to the credential can use it to fabricate information, misuse our data, lead clients to illegal websites, and snoop on our commercial dealings. Additionally, in the upcoming days, an attacker may conduct more attacks.

Mitigation

1. Implement two-factor authentication.
2. Next-generation firewalls, cloud access security brokers (CASBs), and other security measures are needed for the majority of cloud services.
3. Before sending critical information to the cloud, encrypt it.
4. In the unlikely event that your data is lost on the cloud, be sure it is all properly backed up.
5. Verify with your service provider that background checks have been performed on staff members who have direct access to the servers in their data centers.

4.5 Data Loss

Numerous problems can result in data loss, such as corrupted or lost data, hardware malfunctions, natural disaster- related access loss, and malware assaults for which the cloud service provider (CSP) is unprepared.

Mitigation

1. Backups can shield you against ransomware and related threats as well as unintentional or purposeful data loss.

2. Make use of strong encryption for connections and stored data. security and provide a transparent environment.

4.6 Lack of Compliance and Legal Issues

Cloud service providers often operate in multiple jurisdictions, each with its own data protection laws and regulations. Organizations using cloud services must comply with various security, privacy, and industry- specific regulations, such as GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), or PCI DSS (Payment Card Industry Data Security Standard). There may be financial penalties, legal repercussions, and harm to one's reputation if these rules are broken.

Additionally, organizations may have limited visibility and control over how their data is stored, processed, or shared, leading to potential compliance violations.

Mitigation

1. Understand Regulatory Requirements: Organizations should assess and ensure that their cloud provider meets industry-specific compliance requirements before migrating sensitive data to the cloud.
2. Data Sovereignty Awareness: Businesses should confirm where their data is being stored and whether it complies with local regulations.

3. Regular Compliance Audits: Conduct frequent security and compliance audits to ensure that cloud services adhere to legal standards.
4. Cloud Security Agreements: Establish Service Level Agreements (SLAs) that clearly define security responsibilities between the cloud provider and the organization.
5. Encryption and Access Control: Protect sensitive data with encryption and ensure strict access control policies to avoid unauthorized data exposure.

5. Conclusion

Cloud computing has emerged as a transformative technology, revolutionizing the way data is stored, managed, and accessed. Its advantages, such as scalability, cost-effectiveness, and flexibility, have made it an integral part of modern digital infrastructure. However, despite these benefits, cloud computing also presents significant security challenges, including data breaches, unauthorized access, service disruptions, and compliance risks. As more organizations migrate sensitive information to the cloud, addressing these security concerns has become crucial to ensuring data integrity and user trust.

To mitigate these risks, cloud security measures must continuously evolve to counter emerging threats. Implementing strong encryption techniques, multi-factor authentication, access controls, and real-time threat monitoring can enhance cloud security. Additionally, organizations must adopt best practices such as regular security audits, employee training, and compliance with global security standards to minimize vulnerabilities. Cloud service providers also play a critical role in securing infrastructure by offering robust security frameworks, automated threat detection, and secure APIs.

As cloud computing continues to expand, the future of cloud security lies in advanced technologies such as zero-trust architecture, AI-driven cybersecurity, and blockchain-based security models. These innovations can further strengthen data protection and reduce the risks associated with cloud environments. By adopting proactive security strategies and fostering a shared responsibility model between providers and users, cloud computing can remain a reliable, secure, and efficient solution for managing vast amounts of data in the digital age.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.
2. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.
3. Hashizume, K., Rosado, D. G., Fernández- Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1-13.
4. Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. International Journal of Information Security, 13(2), 113-170.
5. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of

Standards and Technology (NIST) Special Publication, 800(145), 1-7.
6. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.
7. Rittinghouse, J. W., & Ransome, J. F. (2017). Cloud computing: Implementation, management, and security. CRC Press..
8. Wang, C., Wang, Q., Ren, K., Lou, W., & Li, J. (2010). Privacy-preserving public auditing for data storage security in cloud computing. Proceedings of IEEE INFOCOM 2010, 1-9.
9. Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 9(2), 50-57.
10. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.