Security and Threats in Cloud Computing: A Comprehensive Literature Review

Dr Kavipriya T[1], Sayush Ramesh[2], Arshaad Basel I[3]
Department of Computer Science with Cyber Security, Sri Ramakrishna College of Arts & Science, Coimbatore
tkavipriya@srcas.ac.in , 23130042@srcas.ac.in, 2313005@srcas.ac.in

Abstract

Cloud computing has revolutionized modern information technology by enabling organizations to store, process, and manage data through remote computing infrastructure accessible over the internet. The model offers scalability, flexibility, and cost efficiency, making it a preferred solution for businesses, educational institutions, and government agencies worldwide. Despite these advantages, cloud computing environments face numerous security challenges that threaten data confidentiality, system integrity, and service availability.

This paper provides a comprehensive review of security threats associated with cloud computing systems by examining existing academic and industry literature. The study explores critical threats such as data breaches, insider attacks, account hijacking, insecure application programming interfaces, distributed denial-of-service attacks, virtualization vulnerabilities, and advanced persistent threats targeting cloud infrastructure. In addition, the research analyzes the effectiveness of current security mechanisms including encryption techniques, identity and access management systems, intrusion detection mechanisms, and compliance frameworks designed to enhance cloud security.

The study highlights key research gaps in areas such as multi-cloud security governance, automated threat detection, and cross-jurisdictional regulatory compliance. The paper aims to support researchers, cybersecurity professionals, and cloud architects by providing an integrated overview of the current cloud security landscape and identifying directions for future research.

Keywords: Cloud computing, cloud security, data breaches, insider threats, denial-of-service attacks, API security, encryption, identity and access management, virtualization security.

I. INTRODUCTION

Cloud computing has become a fundamental component of modern digital infrastructure. Organizations increasingly rely on cloud services to manage their information systems due to the flexibility and scalability offered by cloud platforms. Instead of maintaining expensive on-premise infrastructure, companies can access computing resources such as storage, networking, and processing power through remote data centers operated by cloud service providers.

Major cloud providers including Amazon Web Services, Microsoft Azure, and Google Cloud Platform deliver services that support millions of users worldwide. These platforms operate under different service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model provides different levels of control and responsibility for users, which also influences the type of security measures required.

Although cloud computing offers significant advantages, security concerns remain one of the primary obstacles to widespread adoption. Sensitive organizational data stored in cloud environments can become targets for cybercriminals seeking financial gain, corporate espionage, or political advantage. Security incidents involving cloud systems can lead to severe financial losses, operational disruption, and reputational damage.

The shared responsibility model used in cloud computing further complicates security management. Under this model, cloud service providers are responsible for protecting the underlying infrastructure, while customers are responsible for securing applications, data, and access permissions within the cloud environment. Misunderstanding this division of responsibilities often leads to security vulnerabilities.

This paper presents a literature review of security threats affecting cloud computing environments. The objective is to analyze the most significant threats documented in existing research and examine the strategies proposed to mitigate these risks.

II.CLOUD COMPUTING ARCHITECTURE AND SECURITY CONSIDERATIONS

Cloud computing architecture consists of multiple interconnected components that work together to deliver computing services to users. These components include data centers, virtualization platforms, networking infrastructure, management interfaces, and application programming interfaces. Each of these elements can potentially become an entry point for cyberattacks if not properly secured. Virtualization technology is a key component of cloud infrastructure. It allows multiple virtual machines to operate on a single physical server, improving resource efficiency and scalability. However, virtualization also introduces security risks. Attackers may exploit vulnerabilities in the hypervisor to gain access to other virtual machines hosted on the same physical server.

Another major concern in cloud environments is the multi-tenant architecture, where multiple customers share the same infrastructure. Although logical isolation mechanisms are implemented, attackers may attempt to exploit vulnerabilities that allow them to access resources belonging to other tenants.

Cloud systems are also distributed across multiple geographic locations. While this improves availability and redundancy, it introduces challenges related to data privacy, regulatory compliance, and incident investigation.

III. MAJOR SECURITY THREATS IN CLOUD COMPUTING

Research literature identifies several major threats affecting cloud computing systems. These threats vary in their technical mechanisms and impact on system security.

1) Data Breaches

Data breaches occur when unauthorized individuals gain access to sensitive information stored in cloud systems. These breaches may result from misconfigured storage services, weak access control mechanisms, or compromised user credentials. Data breaches can expose confidential information such as financial records, personal data, and intellectual property.

2) Insider Threats

Insider threats originate from individuals who have legitimate access to cloud systems. These individuals may intentionally misuse their access privileges or unintentionally expose sensitive information through negligent behavior. Detecting insider threats is difficult because attackers already possess authorized credentials.

3) Account Hijacking

Account hijacking occurs when attackers obtain user credentials through phishing attacks, malware, or credential reuse. Once attackers gain access to an account, they can manipulate data, deploy malicious workloads, or launch further attacks within the cloud environment.

4) Insecure APIs

Application Programming Interfaces play a critical role in cloud computing because they allow applications to interact with cloud services. If APIs are not properly secured, attackers may exploit vulnerabilities to gain unauthorized access to data or system resources.

5) Denial of Service Attacks

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks aim to disrupt the availability of cloud services by overwhelming servers with excessive traffic. These attacks can make applications inaccessible to legitimate users and cause significant financial losses.

6) Virtualization Vulnerabilities

Hypervisor vulnerabilities and virtual machine escape attacks allow attackers to bypass isolation mechanisms and access other virtual machines running on the same host system. Such vulnerabilities represent a major security risk in cloud infrastructure.

7) Advanced Persistent Threats

Advanced Persistent Threats involve highly sophisticated attackers who maintain long-term access to targeted systems. These attackers often use stealth techniques to remain undetected while gradually extracting valuable information from cloud environments.

IV. CLOUD SECURITY FRAMEWORKS AND PROTECTION MECHANISMS

Researchers and industry organizations have proposed various security frameworks to protect cloud environments from cyber threats.

8) Identity and Access Management

Identity and Access Management systems regulate user access to cloud resources. These systems ensure that only authorized individuals can access sensitive information. Techniques such as role-based access control and multi-factor authentication are widely used to strengthen authentication mechanisms.

9) Encryption Techniques

Encryption is essential for protecting sensitive data stored in cloud environments. Encryption can be applied to data stored on servers (data at rest) and data transmitted across networks (data in transit). Strong cryptographic algorithms help prevent unauthorized access to sensitive information.

10) Intrusion Detection Systems

Intrusion Detection Systems monitor network activity and system behavior to identify suspicious activities. Modern IDS solutions often use machine learning techniques to detect abnormal patterns that may indicate cyberattacks.

11) Zero Trust Security Model

The Zero Trust model assumes that no user or system should be automatically trusted. Every access request must be verified regardless of the user's location or network environment. This approach reduces the risk of unauthorized access in distributed cloud environments.

12) Compliance and Security Standards

Several international standards provide guidelines for cloud security management. Frameworks such as ISO 27017 and the NIST Cybersecurity Framework help organizations implement best practices for protecting cloud infrastructure.

V. EMERGING CLOUD SECURITY THREATS

Cloud computing technologies continue to evolve rapidly, introducing new attack surfaces that require further research.

Supply chain attacks have become a growing concern in cloud environments. These attacks target software dependencies and development pipelines used by organizations.

Containerization technologies such as Docker and Kubernetes also introduce security challenges related to container isolation and configuration management.

Another emerging threat is cryptojacking, where attackers exploit cloud computing resources to mine cryptocurrencies without the owner's permission. This activity can significantly increase operational costs for cloud users.

VI. RESEARCH GAPS AND FUTURE DIRECTIONS

Although extensive research has been conducted on cloud security, several challenges remain unresolved. Many studies rely on simulated environments rather than real-world data, limiting the practical applicability of research findings.

Multi-cloud environments present additional challenges because organizations often use services from multiple cloud providers simultaneously. Managing security policies across different platforms requires improved tools and frameworks.

Another important research area involves developing automated systems capable of detecting cloud misconfigurations before they lead to security incidents.

Advances in artificial intelligence also present opportunities for improving threat detection and response in cloud environments.

VII. CONCLUSION

Cloud computing has become an essential technology for modern organizations, providing flexible and scalable computing resources. However, the widespread adoption of cloud platforms has also introduced numerous security threats that require continuous monitoring and management.

This literature review examined the major security threats affecting cloud computing systems and analyzed the defensive mechanisms proposed by researchers and industry experts. While technologies such as encryption, identity management, and intrusion detection systems have significantly improved cloud security, vulnerabilities still exist due to complex system architectures and evolving attack techniques.

Future research should focus on developing advanced security frameworks capable of addressing emerging threats in multi-cloud and cloud-native environments. Strengthening collaboration between researchers, industry practitioners, and regulatory organizations will be essential for ensuring secure and reliable cloud computing systems.

VIII. REFERENCES

1. Cloud Security Alliance. (2022). *Top Threats to Cloud Computing Report*.
2. IBM Security. (2023). *Cost of a Data Breach Report*.
3. NIST. (2023). *Cloud Computing Security Guidelines*.
4. *challenges in cloud computing environments*. Journal of Cloud Computing.
5. Zhang, Q., Chen, M., & Li, L. (2021). *Security and privacy in cloud computing: Challenges and future directions*. IEEE Access.
6. Singh, A., & Chatterjee, K. (2022). *Cloud security risks and mitigation strategies*. Future Internet Journal.
7. Kumar, R., & Sharma, P. (2023). *Multi-cloud security architecture and management*. International Journal of Information Security.
8. Ometov, A., et al. (2022). *Authentication and identity management in cloud computing*. Computer Networks Journal.
9. Wang, S., & Liu, Z. (2021). *Intrusion detection in cloud environments using machine learning*. IEEE Transactions on Cloud Computing.
10. Chen, Y., & Zhao, G. (2024). *Emerging threats in cloud-native computing environments*. Journal of Cybersecurity Research.