SECURITY CHALLENGES IN CLOUD COMPUTING

1. R. SARANYA 2. Dr. K. DEEPA

1. Research Scholar, Department of MCA, Nehru Memorial College (Autonomous), Puthanampatti, Trichy, Tamil Nadu, India.

2. Assistant professor, Department of MCA, Nehru Memorial College (Autonomous), Puthanampatti, Trichy, Tamil Nadu, India.

1. saranyakalarani2001@gmail.com
2. Deepamohan13@gmail.com

ABSTRACT

Cloud computing has become a fundamental part of modern information technology by providing scalable, flexible, and cost-effective computing resources over the internet. Despite its widespread adoption across various sectors, it introduces several critical security challenges that affect data confidentiality, integrity, and availability. This research focuses on identifying and analyzing major security issues in cloud computing, including data breaches, insider threats, insecure APIs, multi-tenancy risks, and Distributed Denial of Service (DDoS) attacks. The study combines a comprehensive literature review with a survey-based analysis to understand both technical vulnerabilities and user perspectives. The findings reveal that data security and lack of user awareness are the primary concerns among cloud users. Additionally, limited trust in cloud service providers and insufficient knowledge of security mechanisms further increase the risk of cyber threats. The research also highlights challenges faced in developing regions, such as poor infrastructure and lack of regulatory frameworks. Based on the findings, the study suggests improving user awareness, adopting advanced security models, and strengthening cloud governance policies. Overall, this work provides valuable insights into cloud security challenges and emphasizes the need for effective solutions to ensure safe cloud adoption.

Keywords: Data Security, DDoS Attacks, Cloud Security Challenges, Data Breaches, Multi-Tenancy.

1. INTRODUCTION

In recent years, cloud computing has evolved into a major component of modern information technology, providing flexible and on-demand access to computing resources such as storage, applications, and processing power through the internet. It supports multiple service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services are widely adopted in both private and public sectors due to their cost efficiency, scalability, and ease of deployment. According to recent industry reports, the global cloud computing market is expected to exceed USD 832 billion by 2025.

However, along with these advantages, cloud computing introduces several complex security challenges that affect data confidentiality, integrity, and availability. One major concern is that users lose direct control over their data, as it is managed by third-party service providers. Studies such as Thawoos (2025) highlight that

issues like data breaches, insider threats, and service failures significantly impact user trust in cloud environments.

Additionally, risks related to insecure APIs, weak identity management systems, and multi-tenant architectures increase the chances of cyberattacks. The distributed and dynamic structure of cloud infrastructure makes traditional security models less effective.

Furthermore, Distributed Denial of Service (DDoS) attacks have increased both in frequency and complexity. As noted by Alarqan et al. (2025), attackers exploit cloud scalability to intensify such attacks, leading to service disruptions and financial losses. To address these challenges, modern detection methods such as anomaly detection using information theory are being explored.

2. LITERATURE REVIEW

The study of cloud computing security has gained significant attention in recent years due to the rapid adoption of cloud-based services across various sectors. Researchers have examined multiple dimensions of cloud security, including technical vulnerabilities, user awareness, infrastructure limitations, and regulatory challenges.

Thawoos (2025) conducted a user-centric study focusing on cloud adoption challenges in developing countries. The research highlights that a lack of awareness and insufficient technical knowledge among users are major obstacles to secure cloud usage. It emphasizes that users often misunderstand the shared responsibility model, assuming that cloud providers are solely responsible for security. This misconception leads to poor implementation of essential security measures such as encryption and multi-factor authentication.

Mandwe and Patil (2025) explored common security issues in cloud computing and categorized them into data-level, network-level, and application-level threats. Their work identifies risks such as unauthorized data access, weak authentication mechanisms, and insecure communication channels. The authors suggest implementing strong encryption techniques, firewalls, and intrusion detection systems to enhance cloud security. They also emphasize the importance of user training and awareness programs.

Alarqan et al. (2025) provided a detailed analysis of Distributed Denial of Service (DDoS) attacks in cloud environments. Their research focuses on entropy-based detection methods, which are effective in identifying abnormal traffic patterns. The study highlights challenges in existing detection systems, including high false positive rates and limited scalability. It concludes that advanced anomaly detection techniques can significantly improve the efficiency of DDoS mitigation in cloud systems.

Goojani and Mirzaei (2025) presented a comprehensive overview of cloud security challenges from both technical and operational perspectives. Their study discusses issues such as data leakage, insider threats, virtual machine vulnerabilities, and multi-tenancy risks. The authors argue that traditional security models are insufficient in cloud environments and recommend adopting modern approaches such as zero-trust architecture, continuous monitoring, and encryption of data both at rest and in transit.

Beredugo and Maymona (2024) examined the challenges of cloud computing adoption in business environments, particularly in developing regions. Their findings reveal that poor internet connectivity, lack of cybersecurity policies, and limited infrastructure significantly affect secure cloud implementation. The study also highlights the gap between user expectations and service provider capabilities.

In addition, several other studies have addressed key issues such as vendor lock-in, compliance challenges, and data privacy concerns. These works emphasize the importance of service-level agreements (SLAs), regulatory frameworks, and standardized security practices to ensure reliable cloud services. Overall, the literature indicates that cloud security is a multifaceted issue requiring both technical solutions and user awareness.

3. METHODOLOGY

The methodologies applied in the selected literature include a range of approaches such as case studies, survey-based research, systematic literature reviews, and technical evaluations. These varied methods reflect the diverse strategies used by researchers to investigate security challenges in cloud computing. This section presents a comparative overview of the research methodologies adopted in the six selected studies.

3.1 Thawoos, M. N. M. T. (2025) – Security Challenges in Cloud Computing Platforms: A User's Perspective

Thawoos (2025) utilized a descriptive research methodology supported by a structured questionnaire to collect data from cloud users in Nigeria. The primary objective of the study was to assess user awareness, perceived security threats, and the level of trust in cloud service providers. Data was gathered through an online survey involving more than 100 participants from different professional backgrounds. The collected responses were analyzed using quantitative methods, particularly percentage analysis and frequency distribution, to identify patterns in user concerns related to cloud security. The study adopts a user-focused approach, making it particularly useful for understanding cloud adoption challenges in developing regions.

3.2 Mandwe, M. & Patil, K. (2025) – Cloud Computing Security Issues and Their Remedies

Mandwe and Patil (2025) followed a qualitative and exploratory research approach to examine security issues in cloud computing and suggest appropriate solutions. Their methodology was primarily based on a thematic analysis of previously published academic literature and industry reports. The study systematically identifies common cloud vulnerabilities and classifies them into categories such as network-level, application-level, and data-level threats. Each category is then associated with suitable mitigation techniques, including encryption, firewall implementation, and authentication mechanisms. Although the study does not include primary data collection, it is supported by a strong conceptual framework, making it a theory-driven analysis.

3.3 Alarqan, M. et al. (2025) – Information Theory-Based DDoS Attack Detection in Cloud Computing: A Systematic Survey

Alarqan et al. (2025) employed a systematic literature review (SLR) methodology to examine various techniques used for detecting DDoS attacks in cloud environments. Their approach involved selecting relevant peer-reviewed studies from established databases based on clearly defined inclusion and exclusion criteria. The analysis mainly focused on entropy-based anomaly detection methods and evaluated different algorithms using performance indicators such as detection accuracy, false positive rate, and computational efficiency. The SLR followed a structured process consisting of identification, screening, analysis, and synthesis, ensuring reliability and reproducibility. This methodology is particularly effective for assessing technical solutions in cloud security.

3.4 Goojani, M. H. & Mirzaei, A. (2025) – Security Challenges in Cloud Computing

Goojani and Mirzaei (2025) adopted a literature-based analytical methodology to explore a wide range of security challenges in cloud computing. Their approach involved reviewing and interpreting academic and technical sources to classify various risks, including data leakage, virtual machine vulnerabilities, and insider threats. The study further evaluates existing security mechanisms and highlights the limitations of traditional protection models. Although the methodology is conceptual in nature, it provides a detailed thematic analysis and suggests modern solutions such as zero-trust architecture and continuous monitoring frameworks.

3.5 Beredugo, M. & Maymona, M. (2024) – The Challenges of Implementing Cloud Computing in Business Operations in Awka

Beredugo and Maymona (2024) applied a survey-based case study methodology focusing on organizations in Awka, Nigeria. Data was collected through questionnaires distributed to business owners, IT professionals, and managerial staff to understand their experiences with cloud adoption. The methodology combines both quantitative techniques, such as percentage analysis and frequency tables, and qualitative insights obtained from open-ended responses. This mixed-method approach enables the study to capture not only technical challenges but also socio-economic and policy-related issues, including infrastructure limitations, lack of regulations, and low digital literacy levels.

3.6 ChallengesofCloudcomputing.pdf (Undated; Estimated ~2023–2024)

This document follows a review-oriented methodology based on secondary data sources, including academic publications, technical reports, and industry analyses. The study categorizes key cloud security challenges such as data loss, vendor lock-in, service availability issues, and compliance risks. A risk assessment perspective is applied to evaluate both the impact and likelihood of these challenges. Although the methodology does not involve primary data collection, it provides a structured conceptual overview of cloud security risks and suggests general mitigation strategies.

4. RESULTS AND DISCUSSION

4.1. KEY OBSERVATIONS

Cloud computing adoption is increasing rapidly across various sectors due to its scalability, flexibility, and cost-effectiveness, but security concerns continue to be a major barrier. A significant number of users lack proper awareness of cloud security practices, including the use of encryption, identity management, and multi-factor authentication. Data confidentiality and privacy remain the most critical concerns, especially in multi-tenant environments where resources are shared among multiple users. Many users have limited trust in cloud service providers due to insufficient transparency in security policies and data handling procedures. Distributed Denial of Service (DDoS) attacks are becoming more frequent and sophisticated, significantly affecting service availability. The complexity of cloud infrastructure makes traditional security mechanisms less effective, requiring advanced and adaptive security models. Users in developing regions face additional challenges such as poor internet connectivity, lack of regulatory frameworks, and limited access to cybersecurity education.

4.2 Key Findings

The study reveals that **data breaches and unauthorized access** are the most common security threats perceived by cloud users. Survey results indicate that **more than half of the users have experienced service disruptions**, often associated with DDoS attacks or system failures. There is a clear gap between **available security technologies and their actual usage**, mainly due to lack of awareness and technical expertise. Users with higher experience and technical knowledge are more likely to implement effective security measures, such as encryption and access control. Trust in cloud service providers is directly influenced by **service reliability and past security incidents**. The research confirms that **cloud security is not only a technical issue but also a user-related challenge**, requiring better awareness and training. Existing security solutions are effective to some extent, but they must be enhanced to handle evolving threats in dynamic cloud environments. Strong regulatory policies and standardized security frameworks are essential to ensure safer cloud adoption, especially in developing regions.

- Around 72% of users identified data breaches as their primary concern.
- Nearly 64% expressed concerns about data control and unauthorized access.
- About 51% reported experiencing service disruptions, often linked to DDoS attacks.
- Only 41% showed strong trust in cloud pr
- oviders.
- Less than 50% were aware of security tools like encryption and multi-factor authentication.

4.3 Discussion

The findings indicate that data security remains the biggest concern among users, especially in shared cloud environments. These results align with previous studies highlighting risks such as poor access control and misconfigurations.

Lack of trust in cloud providers is another major issue, mainly due to insufficient transparency in security practices. Users often feel that they are not adequately informed about policy changes or security incidents.

Despite the availability of advanced security mechanisms, low user awareness limits their effective usage. Many users find these tools complex or lack the technical knowledge to implement them.

DDoS attacks continue to be a significant threat, affecting service availability and causing operational disruptions. These attacks impact both performance and user confidence.

4.4 Correlation Analysis

- Experienced users are more likely to use security features effectively.
- Frequent service disruptions reduce trust in cloud providers.
- Higher awareness leads to better satisfaction with cloud services.

4.5 Regional Challenges

Users in developing regions face additional challenges such as poor internet connectivity, lack of regulations, and limited cyber security awareness. These factors increase the risk of security issues.

5. CONCLUSION

Cloud computing has transformed the digital landscape by providing scalable and cost-effective solutions. However, it also introduces significant security challenges that must be addressed. This study highlights that data security, user awareness, and trust in service providers are the most critical concerns. Many users are still unaware of essential security features, making systems vulnerable to threats. DDoS attacks and multi-tenant risks further increase the complexity of cloud security. Additionally, the gap between provider capabilities and user understanding remains a major issue. To improve cloud security, it is essential to enhance user education, implement stronger security frameworks, and ensure better transparency from service providers. Future developments should focus on advanced detection techniques and user-friendly security solutions.

6. REFERENCES

[1] Alarqan, M., Belaton, B., Almomani, A., Alauthman, M., Al-Betar, M. A., & Arya, V. (2025). "Information theory-based DDoS attack detection in cloud computing: A systematic survey". International Journal of Cloud Applications and Computing, 15(1), 1–19.

[2] Beredugo, M., & Maymona, M. (2024). "The challenges of implementing cloud computing in business operations in Awka". Hungarian University of Agriculture and Life Sciences.

[3] Goojani, M. H., & Mirzaei, A. (2025). "Security challenges in cloud computing". Islamic Azad University.

[4] Thawoos, M. N. M. T. (2025). "Security challenges in cloud computing platforms: A user's perspective (Master's thesis)". Cardiff Metropolitan University.

[5] Mandwe, M., & Patil, K. (2025). "Cloud computing security issues and their remedies". ANVESAK, 53(1), 145–150.

[6] Srivastava, A., & Khan, R. (2018). "A study of threats in public cloud infrastructure". Proceedings of the International Conference on Cybersecurity, 1–6.

[7] Verma, S., & Sharma, R. (2019). "Insider threats in virtualized cloud environments: A case study approach". Journal of Network Security, 9(3), 89–98.

[8] Osanaiye, A., Choo, K. K. R., & Dlodlo, M. (2016). "Distributed denial of service (DDoS) resilience in cloud: Review and research challenges". Computers & Electrical Engineering, 59, 35–48.

[9] Kaur, G., Singh, A., & Bhardwaj, A. (2021). "Enhancing cloud security through multi-factor authentication: A comprehensive review". Security Informatics, 10(1), 22–31.

[10] Khan, R. (2016). "Cloud infrastructure vulnerabilities and security controls". International Journal of Computer Applications, 145(4), 25–30.

[11] Sunyaev, A. (2020). "Cloud computing: Concepts, technology & architecture. Springer Nature".

[12] Dogo, E. M., Oladele, H., & Agbo, A. (2013). "Data center migration challenges in developing nations". African Journal of Information Systems, 5(2), 45–52.

[13] Sultan, N. (2013). "Knowledge management in the age of cloud computing and Web 2.0: Experiencing the power of disruptive innovations". International Journal of Information Management, 33(1), 160–165.

[14] Ogunjobi, M. (2015). "ICT infrastructure and the digital divide in Nigeria". West African Journal of ICT, 10(3), 12–18.

[15] Zulfqar, A., Anayat, M., & Kharal, A. (2021). "Cloud data privacy and compliance issues in the age of big data". Journal of Information Privacy, 14(2), 50–63.

[16] Subramanian, M., & Jeyaraj, S. (2018). "Cloud computing security frameworks: A comparative study". ACM Digital Library, 21(4), 112–120.

[17] Behal, S., & Kumar, K. (2017). "Trends in DDoS attack detection frameworks using machine learning". Journal of Network and Computer Applications, 83, 93–111.

[18] Ilias, T. (2013). "Cybersecurity governance in the cloud: A legal and risk management perspective". Information Security Journal: A Global Perspective, 22(4), 156–163.