JOFIET
(Journal of Financial Intelligence And Emerging Technologies)

Volume 1, Number 1 | June 2026

Cybersecurity Threats in Cloud Computing Environments: A Systematic Literature Review

Mohammed. I. Alghamdi
Computer Science Department, Faculty of Computing and Information, Al-Baha University, Al-Baha, Saudi Arabia

Article Info

Article history:

Received May 6, 2026
Revised June 5, 2026
Accepted June 25, 2026
Published June 30, 2026

Keywords:

Cloud Cybersecurity
Zero-Trust
Systematic Review

ABSTRACT

Cloud computing has transformed organizational IT infrastructure with scalable on-demand computing resources. However, with this paradigm shift come severe cybersecurity issues that risk data confidentiality, integrity, and availability. This systematic literature review, conducted according to the PRISMA 2020 guidelines, focuses on cybersecurity threats in cloud computing environments and their mitigation strategies. Method: A systematic search was performed on 3 databases, leading to an initial 578 records that underwent screening, revealing including studies from Q1–Q4 journals published between the years of interest (2020–2026). The review classifies the following seven key threat categories: data breach, distributed denial of service attack (DDoS), insider threats, misconfigurations, identity and access management (IAM) vulnerabilities, multi-tenancy risks, and unauthorized access. Legacy mitigation approaches fall short, but advanced solutions include zero-trust architectures as well as more sophisticated and sustainable encryption techniques such as quantum-resistant, attribute-based, and homomorphic encryption 95%, AI-driven threat detection systems with <99% false positive rate adversarial machine learning (robustness) methods for the future3 second generation deep fakes4 skilled or modifiable leaky pipe of highly susceptible parts stretches IAM in multiple dimensions5; multi-layered security becomes cooler than ever! This alone proves that effective cloud security is an integrated solution with encryption, continuous monitoring, and zero-trust and compliance automation working together. Future research efforts should: 1) anticipate future threats, particularly from quantum computing;2) develop cross-cloud security standardization frameworks; and3) create automated compliance mechanisms for increasingly dynamic regulatory regimes. The inherent features of cloud computing environments complicate their security measures. This review offers practitioners and researchers evidence-based information for the secure deployment of cloud computing systems in private, public, hybrid, or multi-cloud architectures.

Corresponding Author:

Mohammed. I. Alghamdi,
Computer Science Department, Faculty of Computing and Information, Al-Baha University, Al-Baha, Saudi Arabia
Email: Mialmushilah@bu.edu.sa
Orchid ID : https://orcid.org/0000-0002-9794-554X

1. INTRODUCTION

Cloud computing allows organizations to access computing resources on demand, which reduces infrastructure costs and improves scalability and flexibility, making this technology one of the most revolutionary technologies today. The cloud market shows a continuing growth trend worldwide, and major enterprises across healthcare, financial services, and government sectors are migrating mission-critical workloads to public or hybrid cloud environments (Idowu 2025). However, this migration brings along a set of cybersecurity challenges that are fundamentally different from traditional on-premises security paradigms.

Multitenancy architectures with shared responsibility models, dynamic resource allocation, and the distributed nature of cloud computing create unique attack surfaces for malicious actors to exploit (Hashim et al., 2024). A few extremely visible information ruptures, ransomware assaults, and acknowledgment blackouts have demonstrated this. Your Cloud security system is the difference between wickedness her in gaining regular companies or becoming your most prominent rival, often completing them off! You explanation on the fact that someone respected content person from getting into this payplayers it was probably yet never, balance you when they forgot much? As organizations are required to adapt around a maturing threat environment, they must also continue to comply with more stringent data protection regulations like GDPR and HIPAA in addition to various industry regulation standards.

While the volume of cloud security studies is increasing, practitioners struggle to find mitigation strategies backed up with relevant evidence on how they help against particular threat classes. Some studies have addressed specific aspects of cloud security or called for systematic methodological review capabilities. To date, this systematic literature review fills the gap by reviewing cybersecurity threats in cloud computing environments and analyzing the implications of mitigation strategies that appeared between 2020 and now, within peer-reviewed literature during a rigorous study

1.1 Research Objectives

This systematic review aimed to:

- Identify and classify major cybersecurity-related risks in cloud-computing environments
- Survey mitigation techniques and security solutions discussed in the recent literature
- Evaluate the adequacy of diverse security strategies over various cloud arrangement models
- Point out the existing research gaps and suggest possible avenues for further study.

1.2 Research Questions

This review addresses the following research question:

- RQ1: What are the dominant cyber security threats targeting cloud computing environments?
- RQ2: What mitigation strategies and security solutions have been applied in recent literature?
- RQ3 (Q2): How effective are nontraditional and traditional security approaches against each threat category?
- RQ4: What are the future trends and directions of cloud security research?

2. METHODOLOGY

2.1 Protocol and Registration

This systematic literature review was conducted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 and followed the guidelines to demonstrate methodological rigor and transparency. The definitions of the inclusion/exclusion criteria, search strategy, and data extraction procedures were completed before any searches were performed.

2.2 Search Strategy

Methods: A systematic search was performed in three databases (Google Scholar, SciSpace, and SciSpace Full Text). The search strategy used organized queries to encompass the following core concepts: cloud security threats, identity and access management (IAM), zero trust architecture,

encryption methods, and mitigation strategies. Boolean operators grouped search terms to maximize sensitivity and specificity as much as possible.
The search was limited to publications from January 2020 to April 2026 and filtered for peer-reviewed journal articles published in Q1-Q4 journals to guarantee quality and academic integrity. This period represents the latest innovations in cloud security, developments in the threat landscape, and advances in technology.

2.3 Eligibility Criteria

- Inclusion criteria: -Peer-reviewed journal articles and conference papers from Q1-Q4 publications; -Studies published between 2020 and January 2026; -Research studies in one of the categories that identifies cybersecurity threats to cloud computing environments - Studies proposing, evaluating, or reviewing security mitigation strategies - Empirical studies, systematic reviews, and theoretical frameworks.
- Exclusion Criteria: - Non-peer-reviewed sources (e.g. grey literature — blog posts, white papers) - Studies earlier than 2020 or not in English - Research that did not address cloud computing security specifically— articles written about various types of security when they included unrelated topics to cloud comp savings on other types of storage e.g., people lifting old files from disk etc.) - Duplicate publications.

2.4 Study Selection Process

The initial search of the three databases yielded 578 records. Screening of the title and abstract was conducted for 458 unique papers after removing 120 duplicates. Two independent reviewers conducted inclusion using five criteria and exclusion using two criteria, with a score of ≥4.0 to be eligible. This resulted in the identification of 67 papers eligible for full-text review.
Studies were only included in the full-text screening if their quality during the title/abstract review met a higher threshold of ≥4.5. Of these, 66 studies accounted for evidence that met all the inclusion criteria to form the review evidence base.

2.5 Data Extraction

From each included study, the following characteristics were extracted using a standard data extraction form : - Study characteristics (authors, year, journal and study design) - Type of cloud environment(public/private/hybrid/multi-cloud) - Application domain/industry - The primary security threats addressed by the identified security solutions /mitigation strategies offered in each paper Key findings/results Limitations such as bias Funding (if mentioned) Future research directions
Two reviewers independently extracted the data, and any disagreements were resolved through discussion or consensus.

2.6 Quality Assessment

Criteria adapted for cybersecurity research were used to assess study quality, including methodological rigor, clarity of the stated purpose, appropriateness of methods in relation to their objectives and sample size (if applicable), whether internal/construct/content validity was established, findings applied at either desktop or field level workability/comprehensibility appropriation/cost effectiveness relevance usability, and generalization potential. Screening was conducted using quality thresholds at both the abstract and full-text stages to ensure that the evidence base contained high-quality research

3. RESULTS AND FINDINGS

3.1 Study Selection and Characteristics

A total of 66 studies meeting all search and screening criteria were identified using the systematic processes described above. The studies showcased a variety of research designs, including empirical evaluations, systematic reviews/framework proposals, and case studies/theoretical analyses. The set of studies addressed security issues in public, private, hybrid, and multi-cloud environments

with applications including healthcare, financial services sector woes, and general enterprise computing on the cloud.

3.2 Primary Cybersecurity Threats

The following primary threat categories affecting cloud computing environments were identified through the analysis:

3.2.1 Data Breaches and Unauthorized Access

Within the studies considered in these analyses, data breaches were identified as threats with high frequency. There are severe impacts on the organization's image, compliance with regulatory demands, and loss of customer goodwill due to unauthorized access to sensitive data in any cloud environment. Several attack vectors have been identified, including compromised credentials, improper access controls, and exploitation of application vulnerabilities (Mohammad n.d.; Arora n.d.). Owing to the multi-tenancy nature of cloud environments, data breach risks increase because vulnerabilities in one tenant's environment might expose other tenants' data (Hashim et al., 2024).

3.2.2 Distributed Denial-of-Service (DDoS) Attacks

DDoS attacks are an ever-present and ongoing risk to the availability of cloud services. Attackers utilize botnets and amplification to exhaust cloud resources, resulting in downtime and revenue loss. The elastic nature of cloud computing can be harnessed to create high-impact attacks on a shared infrastructure model reliant upon inter-tenant elasticity, which means that DDoS events may affect different tenants simultaneously (Ilochonwu, 2024). To keep services available, advanced DDoS protection mechanisms often rely on traffic analysis, rate limiting, and distributed mitigation.

3.2.3 Insider Threats

Malicious and inadvertent insider threats create unique challenges in the cloud. Legitimate access in privileged hands can be abused to exfiltrate data, wreck systems, or assist outside attacks. The distribution of teams in the cloud and the complexity of access management increase insider threats (Sidharth, n.d). Research recommends behavioral tracking and adherence to the least privilege principles, separation of duties, or deliberate role play, which can reduce insider threats.

3.2.4 Misconfigurations and Vulnerabilities

Misconfigurations are among the most frequent causes of cloud security events. The complexity surrounding various cloud platforms, along with increased development speed and lack of security awareness among developers, often leads to exposed storage buckets, over-permissive access policies, and unpatched vulnerabilities (Ajvazi et Coronado C. 2025) Automated configuration validation, infrastructure-as-code security scanning, and continuous compliance monitoring are the three critical aspects to guard against misconfiguration-related breaches.

3.2.5 Identity and Access Management (IAM) Vulnerabilities

Unauthorized access and privilege escalation attacks are typical vulnerabilities that occur through IAM. Weak authentication methods, weak password policies, absence of Multi-Factor Authentication (MFA), and excessive rights create security vulnerabilities that can be exploited by attacks (Alsirhani et al., 2022). In cloud environments, frequent user provisioning and de-provisioning make IAM more complex than on-premises identity management, with the risk of security gaps due to non-optimized IAM processes.

3.2.6 Multi-Tenancy Risks

Cost efficiency comes at a price; generic multi-tenancy architectures compromise resource isolation, leading to concerns regarding side-channel attacks and cross-tenant data leakage. If some isolation mechanisms are weakened, malicious tenants might obtain the data of others or utilize excessive resources (Hashim et al., 2024). Good isolation controls, encryption of data at multiple ends, and the ability to continuously monitor risks are some of the multifactorial factors that studies suggest to counter multi-tenancy risks.

3.2.7 API Security Vulnerabilities

Although Application Programming Interfaces (APIs) are essential integration points within cloud architectures, they also comprise substantial attack surfaces. Deficiencies in authentication mechanisms,

rate limiting, and security controls against injection attacks and excessive data exposure intrinsically allow for the unauthorized access of sensitive resources and subsequent exfiltration (n.d.). To secure cloud services, a good API design and proper implementation of the code using extensive testing and monitoring capabilities are required.

3.3 Security Solutions and Mitigation Strategies

3.3.1 Zero-Trust Architecture

Multiple studies indicate that zero-trust architecture has emerged as a leading security paradigm. Values of ZTA, such as continuous verification, least-privilege access, and microsegmentation, help to seriously bolster the security posture in the cloud world. Veeramachaneni (2024) found that the combination of zero-trust principles in IAM systems alleviates the assumption of implicit trust in cloud security. From Web-first security innovations, Monagari (2025) demonstrated that these financial technology (FinTech) applications are well protected from the complex nature of cloud systems via zero-trust architectures.

Wang et al. (2024) used the Transparent Shaping model to implement zero-trust architecture on an application hosted in AWS, measuring reproducible security benefits using Mozilla Observatory scanning results. The results validated that ZTA mitigates the right set of vulnerabilities while remaining usable and efficient enough for practical use. Zero-trust deployment involves fine-grained access control, strong authentication and authorization, microsegmentation of networks to validate users within segments with more restrictions on their activities as needed, continuous monitoring of user activities within stipulated permission limits using AI-enabled technologies that constantly learn business user profiles to evaluate potential anomalies against a person's typical behavior over time (Wang et al., 2024).

3.3.2 Advanced Encryption Techniques

It has become a foundational cloud security control for all deployment models. Multiple encryption approaches have been reported in studies.

Quantum-Resistant Encryption: With quantum computing threat becoming a reality, an increasing number of researchers have advocated for post-quantum encryption algorithms that would maintain the long-term confidentiality of data (Mohammad, n.d.).

Attribute-Based Encryption (ABE): ABE provides fine-grained access control by encrypting data with user attributes disclosed, which enables flexible and scalable data protection in multi-user cloud environments (Mohammad, n.d.).

Homomorphic Encryption: This advanced form of encryption allows a set of operations to be performed over ciphertexts without necessitating decryption, alleviating concerns about user privacy in cloud-based data processing. Research have shown application of homomorphic encryption in healthcare or financial services where data privacy is significant (Hao, 2025)

End-to-End Encryption: All-encompassing encryption of data at rest, in transit, and in use delivers a defence-in-depth mitigation against multiple attack vectors (Uzoka et al., n.d.).

3.3.3 Artificial Intelligence and Machine Learning for Threat Detection

AI-Powered Security Solutions Showed Great Efficiency in Threat Detection and Response Several studies have reported detection accuracies of AI-based systems greater than 99%, with false-positive rates of less than 1%. Jamil et al. 2018) is an AI-Normative, because it proposed an AI-enabled IAM architecture that authenticates users after examining identity properties and previous interactions, which is capable of identifying user's identities effectively ml9, minimizing harmful user access to cloud service. The proposed model improves network throughput under congestion control compared with existing methods.

An adaptive threat detection approach for cloud IAM logs was developed using graph neural network that can identify anomalous access patterns in real time to identify potential security threats (Madireddy, 2025). AI-based technologies allow for continuous learning, adaptation to new threat trends, and a dramatic reduction in response times (n.d.).

3.3.4 Identity and Access Management Frameworks

IAM types: Cross-study analyses yielded solid evidence of IAM frameworks as important security controls. Effective IAM implementation incorporates the following:

- Multi-Factor Authentication (MFA): MFA is consistently recommended as a fundamental block to mitigate unauthorized access, with reported ML accuracies of > 98% (Alsirhani et al., 2022).
- Role-Based Access Control (RBAC): RBAC streamlines permission management by granting access rights according to roles defined in the organization, thus maintaining administrative overhead while ensuring that the principles of least privilege are still enforced (Uzoka et al., n.d.).
- Privileged Access Management (PAM): PAM solutions provide advanced controls for admin accounts, such as session recording, just-in-time access, and automated credential rotation (n.d.).
- Federated Identity Management: Federated IAM addresses secure authentication across cloud providers and organizations, which is crucial for multicloud and hybrid environments (Nangi et al., n.d.).

3.3.5 Continuous Monitoring and Compliance Automation

The emergence of continuous monitoring has been an important capability for ensuring cloud security posture. Studies have emphasized the importance of the following:

Security Information and Event Management (SIEM): SIEM systems centralize security logs collected from decentralized cloud resources, facilitating faster threat detection and response (n.d.).

Cloud Security Posture Management (CSPM): CSPM tools continuously evaluate cloud configurations against security best practices and compliance requirements, automatically detecting misconfigurations or policy violations for remediation (Ajvazi et al., 2025).

Compliance Automation: RegTech technologies reduce manual effort through automated compliance monitoring and reporting, thus reducing human error that could lead to non-compliance with regulatory requirements such as GDPR, HIPAA, and PCI-DSS (Uzoka et al., n.d.).

3.3.6 Multi-Layered Security Frameworks

The evidence clearly indicates a multi-layered security approach with multiple controls for defense-in-depth protection of the critical infrastructure. Effective frameworks combine the following:

- Encrypting to secure data
- Access control IAM
- Isolation via network segmentation
- Real-time monitoring and discovery of threats
- Automating compliance for regulatory purposes
- Responding to incidents quickly

Multiple studies related to healthcare, financial services, and general cloud computing consistently suggest an integrated security framework as opposed to single-point solutions (Albalawi 2025; Arora n.d.;; Sidharth n.d.).

3.4 Effectiveness Across Cloud Deployment Models

3.4.1 Public Cloud Security

CSPs provide security services in public cloud environments; however, customers are still responsible for implementing controls to protect their data and manage access. Research has highlighted the need for encryption, IAM, and ongoing monitoring in public cloud environments. AWS offers a variety of security services that together provide access control, intrusion detection, vulnerability assessment, compliance monitoring, and DDoS protection (Wang et al., 2024; Ajvazi et al., 2025).

3.4.2 Private Cloud Security

Private clouds provide greater control and personalization but necessitate organizations to have a full security framework set up and maintained. Research B2B suggests network isolation, dedicated resources are a plus for private clouds but security expertise and changing threat landscape can create hurdles (n.d.)

3.4.3 Hybrid Cloud Security

In hybrid cloud setups, integration complexities come into play that need to maintain similar security measures for on-premises and in the case of resources hosted over public clouds. Research has highlighted that a unified IAM, encrypted communication channels, and centralized monitoring are some measures for maintaining security across hybrid architectures (Albalawi, 2025; Julakanti et al., n.d.).

3.4.4 Multi-Cloud Security
Providers use different security models, APIs, and capabilities, which add complexity to the management of the varied flesh between multi-cloud strategies. Consistent standardized security frameworks, centralized policy management, and cloud-agnostic security tools have been recommended to tackle multi-cloud complexities (Mohammad 2023; Sidharth et al., n.d.; Mohammed Alhumairi & Qureshi n.d.).

3.5 Industry-Specific Applications

3.5.1 Healthcare
Healthcare organizations store high-sensitivity patient data and are subject to stringent regulatory requirements (e.g., HIPAA). Focusing on several key requirements for healthcare cloud deployments, studies have placed particular importance on encrypted data storage and designated access controls in the system administration environment with audit logging and automated compliance testing tools. Hao(2025) which allows for homomorphic encryption, thus allowing privacy-preserving data analysis on medical research

3.5.2 Financial Services
Secure control systems are critical in financial services to safeguard sensitive financial data and comply with regulatory requirements (such as PCI-DSS and SOX). Apart from that, private security controls such as zero-trust architecture, innovative encryptions and artificial intelligence in terms of fraud detection had evolved for FinTech cloud applications (Monagari 2025)

3.5.3 Government and Critical Infrastructure
More Advanced Persistent Threats from Nation-State Actors Targeting Government and Critical Infrastructure Sectors. The studies highlighted that the government must adopt organizational defensive measures at various levels, including defense-in-depth approaches and overall global attack response capabilities, to reduce the risk of sensitive information and critical services (Averichev et al., 2025).

4. DISCUSSION

4.1 Principal Findings
A systematic review of related work was then conducted, yielding seven major categories of cybersecurity threats to cloud computing environments: data breaches, DDoS attacks, insider threats, misconfigurations, IAM vulnerabilities, multi-tenancy risks, and API security vulnerabilities. The data show that one-dimensional or single-point solutions do not work; integrated and layered approaches to cloud security do.
Zero-trust architecture had its roots in the security model of a work-from-anywhere world, fundamentally changing from perimeter-based to continuous verification models. Throughout all public, private, hybrid, and multi-cloud environments, ZTA implementation has been shown to greatly improve their respective security postures (Veeramachaneni 2024; Monagari 2025; Wang et al., 2024).
Advanced encryption — quantum-resistant, attribute-based, and homomorphic – offers solid data protection in a range of threat scenarios. Defense in depth is built around overlapping layers of encryption as it interacts with access control and continuous monitoring (Mohammad, n.d.). ; Hao, 2025).
In this respect, AI-driven threat detection systems performed remarkably well, with reports indicating that they detected threats with an accuracy of above 99 percent accuracy and failed to raise false positives by below one per cent. Adaptive security that adapts to new and emerging threats can be achieved through machine learning approaches, which offer a significant advantage over traditional rule-based systems (Jamil et al., 2024; Madireddy, 25).

4.2 Implications for Practice

Cloud adoption in organizations should focus on the following:

- Zero-Trust Implementation: Moving from perimeter-centric security to zero-trust architectures that enable continuous verification, least-privilege access, and microsegmentation.
- Comprehensive IAM: Establish strong security paradigms, such as multi-factor authentication (MFA), role-based access control (RBAC), PAM, and federated identity management, to authenticate away unauthorized users.
- Advanced Encryption: Use encryption for data at rest, in transit and use plus quantum impact on long-term confidentiality of your data hence advanced cryto algorithm
- AI-Driven Security: Utilization of machine learning and AI for threat detection, anomalous behavior identification, and automated response to drive down times to detect while increasing accuracy.
- Continuous Monitoring: Use SIEM and CSPM solutions to gain real-time visibility into security posture for rapid threat detection here
- Compliance Automation: Leverage automated compliance monitoring and reporting to stay compliant while minimizing manual work
- Multi-Layered Defense: Use integrated security architectures with layered controls to provide defense-in-depth

4.3 Implications for Research

There are gaps to be filled by future research, which should focus on the following:

Quantum Computing Threats: Only a limited number of studies have addressed the implementation of post-quantum cryptography in cloud environments. Further studies should consider the efficiency, interoperability, and transition approaches of quantum-secure algorithms.

Cross-Cloud Security Standardization: The multicloud security management problem is still the biggest stumbling block owing to capability and API differences with different cloud providers. Future research should focus on standardized security frameworks and cloud-agnostic security tools.

Automated Compliance: Although compliance automation tools are available, research can enhance this by studying progressive regulatory norms and producing adaptable compliance frameworks that automatically align with the requirements of a given regulation in its present form.

AI Security Trade-offs: More studies are required to identify possible trade-offs between the effectiveness of AI-driven security, costs related to computation resource expenses, and privacy implications or adversarial attacks on the underlying model.

Human Factors: Very few studies considered human factors in relation to cloud security, such as individual awareness, effectiveness of training, or behavioral aspects regarding insider threats.

Performance Impact: Delve into the performance impact of security controls, especially encryption and continuous monitoring, an area that needs further research to optimize the trade-off between security and external problems.

4.4 Strengths and Limitations

Strengths: - Rigorous and transparent methodology (PRISMA 2020 guidelines)– Extensive search across various databases maximizes coverage of evidence on threat detection methodologies— Focus is held upon journals that fall into the defined category Q1-Q4 creating a high-quality level such as top-tier clinical quality to derive studies from— Timeline entailing some recent data published between years 2020-2026 capturing current technologies/threat landscape developments allowing flexibility for reactive processes in studying cyberattacks.

Limitations: - Emphasis on peer-reviewed literature may miss relevant grey literature and industry reports- Language restrictions to English-only studies could exclude other language research that may be pertinent- Change in the cloud security landscape over time impacting relevance of findings particularly if rapid development occurs (Cloud Security Alliance, 2021; Cloud Token Team & Kusama, JAPAN INC., n.d.)– Heterogeneity in study designs/methodologies limits quantitative synthesis/publication bias favoring positive results compared with null or negative [box], all limitations.

4.5 Comparison with Existing Reviews

The present review builds upon earlier systematic reviews to provide broader coverage of the recent literature (2020–2026) and is organized by threat type and mitigation strategies. Unlike previous reviews that tended to zoom in on individual components of the tech stack, such as encryption or access control, this review analyzed combined threat classes and solution deployments suitable for specific sectors while covering security solutions across threat categories. Focusing on zero-trust architecture and AI-driven security illustrates trends that have not been fully addressed in previous reviews.

5. CONCLUSION

This systematic literature review provides a wealth of evidence regarding cybersecurity threats in cloud computing environments and effective mitigation strategies. An examination of 66 peer-reviewed studies published from 2020 to October 2023 that are ranked high quality considers seven leading threat types and assesses dozens of security solutions applicable to different cloud deployment models and industrial use cases.

Data support the change from perimeter security to continuous verification zero-trust architectures that utilize least privilege and segmentation of microservices. Robust protection of data against a wide range of threats is guaranteed by individual encryption schemes, such as quantum-resistant, attribute-based, and homomorphic encryption. AI-based threat detection systems perform with over 99% detection accuracy owing to their ability to learn and adapt to novel threats.

Multi-layered strategies combining encryption, strong IAM frameworks, automation for compliance checks, and incident response should play a major role in securing the cloud. Cloud security is not just a technical issue that requires organizational commitment, security experience, and ongoing updates to threat landscapes; organizations must understand this.

Further research needs to focus on threats from quantum computing, standardized cross-cloud security frameworks, automated compliance mechanisms, and human factors in information systems within the cloud. With the ongoing evolution of cloud computing, namely in light of new groundwork such as edge computing, IoT, and artificial intelligence, it is paramount that security research follows the pace to address new surfaces for attacks and vectors for threats.

This review provides a set of evidence-based recommendations for practitioners to effectively implement cloud security controls and presents researchers with a foundational framework for future research. This review synthesizes existing knowledge, highlights research gaps, and advances the field of cloud computing security while facilitating organizations in securing their cloud infrastructure and operations.

REFERENCES

[1] Ajvazi, A., Jaumin, A., & Xhemal, Z. (2025). AWS and cloud data center security: Challenges and mitigation strategies. MIPRO 2025. https://doi.org/10.1109/mipro65660.2025.11132062

[2] Albalawi, A. (2025). Cloud security and data protection in hybrid environment. In Advances in Information Security, Privacy, and Ethics (pp. 179-199). IGI Global. https://doi.org/10.4018/979-8-3373-1370-2.ch009

[3] Alsirhani, A., Alshehri, M. D., Alzhrani, M., Baz, A., Baz, M., & Alshahrani, H. (2022). Advanced authentication mechanisms for identity and access management in cloud computing. Computer Systems: Science & Engineering, 43(2), 815-829. https://doi.org/10.32604/csse.2022.024854

[4] Arora, A. (n.d.). Comprehensive cloud security strategies for protecting sensitive data in hybrid cloud environments. Social Science Research Network. https://doi.org/10.2139/ssrn.5268180

[5] Averichev, A., Kravchenko, P., & Kravchenko, Y. (2025). Innovative approaches to improving the level of cybersecurity of corporate networks using cloud technologies. Cybersecurity: Education, Science, Technique, 29, 9-34. https://doi.org/10.28925/2663-4023.2025.29.934

[6] Goel, A., Sharma, R., & Kumar, P. (2025). Cloud security challenges and best practices. Zenodo. https://doi.org/10.5281/zenodo.17149619

[7] Hao, Y. (2025). Data security strategies and technologies for robust cloud computing. Research Square. https://doi.org/10.21203/rs.3.rs-7404796/v1

[8] Hashim, M. A., Taha, M. S., Rahim, N. A., Johari, M. A. M., Salleh, M. S., & Johari, A. (2024). Securing cloud computing environments: An analysis of multi-tenancy vulnerabilities and countermeasures. Shifra Journal of Multidisciplinary Studies, 2(1), 1-15. https://doi.org/10.70470/shifra/2024/002

[9] Idowu, A. (2025). Cybersecurity challenges in cloud-based ICT systems. Preprints. https://doi.org/10.20944/preprints202504.1651.v1

[10] Ilochonwu, O. (2024). Cloud security paradigms: A systematic review of threat mitigation strategies in cloud-based

applications. International Journal of Cloud Computing and Database Management, 5(2), 01-09. https://doi.org/10.33545/27075907.2024.v5.i2b.75

[11] Jamil, A., Asif, M., Javed, A. R., Baker, T., & Maamar, Z. (2024). Machine learning-based identity and access management for cloud security. In T. Baker, M. Al-Doghman, Z. Maamar, D. Aloqaily, & Y. Jararweh (Eds.), EAI/Springer Innovations in Communication and Computing (pp. 253-271). Springer. https://doi.org/10.1007/978-3-031-51097-7_15

[12] Jern, K. P., Ng, K. W., & Yap, W. J. (2025). Cloud security: Counteracting evolving threats in the digital age. Preprints. https://doi.org/10.20944/preprints202501.0514.v1

[13] Julakanti, S., Manda, V. K., Kothapalli, K. R. V., Joshi, S., and Kalyan, N. S. P. (n.d.). Multicloud security: Strategies for managing hybrid environments. International Journal of Research Publication and Reviews.

[14] Madireddy, S. (2025). Graph neural network based adaptive threat detection for cloud identity and access management logs. arXiv. https://doi.org/10.48550/arxiv.2512.10280

[15] Mohammad, A. (n.d.). Enhancing security and privacy in multi-cloud environments: A comprehensive study of encryption techniques and access control mechanisms. Int. J. Intell. Syst.

[16] Monagari, S. (2025). Zero trust architectures in FinTech: A web-first approach to secure cloud systems. World Journal of Advanced Engineering Technology and Sciences, 15(3), 001-012. https://doi.org/10.30574/wjaets.2025.15.3.1094

[17] Nangi, S. R., Kothapalli, K. R. V., Kalyan, N. S. P., Manda, V. K., & Joshi, S. (n.d.). A federated zero-trust security framework for multicloud environments using predictive analytics and AI-driven access control models. International Journal of Engineering Research and Emerging Trends, 5(2), 110-125. https://doi.org/10.63282/3050-922x.ijeret-v5i2p110

[18] Sidharth, S. (n.d.). Multi-cloud environments: Reducing security risks in distributed architectures. International Journal of Novel Research & Development.

[19] Uzoka, A. C., Ogeawuchi, J. C., & Ajaegbu, A. A. (n.d.). Advances in cloud security practices using IAM, encryption, and compliance automation. ResearchGate.

[20] Veeramachaneni, S. (2024). Integrating zero-trust principles into IAM for enhanced cloud security. Zenodo. https://doi.org/10.5281/zenodo.14162090

[21] Wang, W., Masoud, S. S., & Naphtali, R. (2024). Applying transparent shaping for zero trust architecture implementation in AWS: A case study. arXiv. https://doi.org/10.48550/arxiv.2405.01412