International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(16s) 2026 pp. 286-298
https://doi.org/10.70917/ijcisim-2026-4575
Article

Cloud Security Challenges and Risk Management in Modern Cloud Computing Environment

Veeramani Sampathkumar[1], Dinesh Kumar Ramaraj[2], Rajesh Kotha[3], Anand Edward[4]

[1] Software Engineering Advisor, Fiserv, Frisco, Texas, USA.
Email: veeras@ieee.org
[2] Cloud Architect, Ericsson, Pflugerville, Texas, USA.
Email: Dinesh.kumar.ramaraj@ericsson.com
[3] Software Development Engineering Advisor, Fiserv, Alpharetta, Georgia, USA.
Email: Rajesh.kotha28@gmail.com
[4] DevOps Architect, Cognizant Technology, Georgetown, Texas, USA.
Email: anandedward82@gmail.com

Abstract: Cloud Computing has completely transformed the way businesses operate today with its scalability, flexibility, and cost efficiency. Cloud platforms have become a key component for organizations in various sectors to store data, deploy software, manage infrastructure, and implement digital transformation efforts. But the adoption of cloud computing has made it extremely challenging to deal with several security concerns like data breach, cyberattacks, unauthorized access, insider threats, and compliance concerns. The research paper employs secondary data collection and thematic analysis to critically discuss challenges of cloud security and risk management approaches in contemporary cloud computing environment. A thorough literature review of the scholarly papers from 2015 to 2023 is conducted to assess cybersecurity threats, cloud vulnerabilities, identity management systems, encryption technologies, compliance frameworks, and artificial intelligence-based threat detection systems.

Peer reviewed journal articles, conference papers and industry reports were analysed using the method of themed analysis, which identified themes that appeared repeatedly throughout. The results show that cloud environments are still very susceptible to advanced cyberattacks, ranging from weak authentication and insecure APIs to misconfigured cloud services and inadequate governance. The study also points out the effectiveness of modern technologies like multi-factor authentication, zero-trust security models, artificial intelligence, and encryption enhance cloud security performance. But there are still issues in the way of the organizations' operations regarding regulatory compliance, data governance and shared security responsibilities.

The study demonstrates that the key factors to achieving effective cloud security are continuous monitoring, robust governance policies, employee awareness training, and high-level cybersecurity frameworks. The study adds to the body of knowledge about the security of cloud computing, and offers practical suggestions for any organization working in the cloud.

Keywords: NA

1. Introduction

1.1 Background of the Study

Cloud computing is among the biggest technologies of the digital age. Cloud computing platforms are becoming a mainstay for businesses, whether it is for data storage, software deployment, networking, or enterprise application management. Cloud services offer organizations scalability, flexibility, operational efficiency and lower infrastructure costs. Cloud service providers like Amazon Web Services, Microsoft Azure, and Google Cloud have revolutionized the way organizations use technology resources.

Cloud computing is the practice of using computer resources via the Internet. Cloud platforms can enhance business continuity, flexibility in working from a distance and scalability for organizations. The cloud environment offers a disruptive business model to organisations, as it decreases initial investment in IT systems and increases flexibility in work processes (Almorsy, et al., 2016).

Copyright: © 2026 by the authors

However, cloud computing environments are very susceptible to cyber threats. Cloud systems hold big amounts of delicate organizational and customer information that makes them appealing targets for cybercrime. Ransomware attacks, phishing attacks, insecure APIs, insider threats and data breaches are increasing risks for organizations. Cloud security is the set of technologies, policies, procedures and operational controls used to protect cloud-based systems, applications and information assets. Cloud security encompasses identity management, threat monitoring, access control, encryption, compliance management and disaster recovery planning.

In recent years, cyber-attacks on cloud systems have become more sophisticated, as shown by these incidents. Insufficient cloud security structures can result in financial damages, reputational harm, operations disruption and legal liability. Thus, robust cybersecurity measures have emerged as a must for contemporary businesses.

The research paper critically analyses the problems in cloud security and risk management strategies by secondary data collection and thematic analysis. This study identifies significant cybersecurity threats, assesses current security frameworks and offers recommendations for enhancing CSEM.

This study contributes by integrating emerging cloud security technologies, including Zero Trust, CNAPP, CSPM, CWPP, Kubernetes security, confidential computing, and AI-driven protection into a unified cloud security framework. Unlike previous reviews, it compares leading cloud providers, proposes practical implementation models, and identifies future research priorities for resilient cloud environments.

1.2 Research Aim

The aim of this study is on evaluating the cloud security challenges and risk management strategies in the modern cloud computing environment.

1.3 Research Objectives

The research will address objectives as:

1. To analyse the concept and importance of cloud security in modern organizations.
2. To identify the major cybersecurity threats and vulnerability in cloud computing environment.
3. To access the risk management strategies used for improving cloud security.
4. To understand the role of modern technologies in cloud threat detection and its prevention.

2. Literature Review

2.1 Understanding Cloud Security

Cloud security is the term that describes the safeguarding of the cloud infrastructure, applications, networks and data against cyber threats and unauthorized access. Consists of policy, technology, governance and monitoring mechanisms to safeguard confidentiality, integrity and availability of cloud resources. Cloud Computing Security Challenges are more complex than traditional cyber security challenges as Cloud systems are multi-tenanted, virtualized, elastic, and distributed systems (Almorsy, et al., 2016). Cybersecurity threats abound in cloud environments because everything is shared and operated on the internet. Thus, robust access control, encryption, and monitoring systems are crucial for organizations.

2.2 Threats of Cloud Security

Ransomware attacks, Phishing attacks, Insider threats, Data breaches, and Insecure APIs are among the cyber security threats that are common in cloud computing systems. Unauthorized access to sensitive information within an organization is one of the most severe security threats, as data breaches can occur. Hashizume et al. (2021) found insecure interfaces, malicious insiders and weak authentication systems as prime risks in cloud computing environments. Accordingly, Bellamkonda (2022) highlighted that multi-tenancy and inadequate governance structures are likely to heighten the security threat to cloud infrastructures. Another threat to cloud infrastructure availability is Distributed Denial-of-Service (DDoS) attacks which exhaust systems with malicious traffic.

2.3 Risk Management

Identity and Access Management (IAM) systems are an integral part of cloud security. IAM frameworks manage access privileges, authentication and authorization of users. Indu et al., (2018) pointed out that a robust identity

management system can greatly minimize the risks of unauthorized access in cloud environments. To improve cybersecurity, multi-factor authentication (MFA), biometric verification and role-based access control are commonly used. In today's cloud-driven landscape, zero-trust security architecture has gained traction as it is constantly reauthenticating users before allowing them to access the system.

2.4 Encryption and Data Protection

One of the best technologies for safeguarding sensitive cloud data is encryption. Encryption transforms readable information into coded information that can be accessed only with the proper decryption keys. Recent research revealed that homomorphic encryption and advanced encryption standards (AES) are effective to enhance cloud data protection and mitigate the threats caused by unauthorized access. Encryption is used for data at rest, data in transit, and backup storage systems.

2.5 Artificial Intelligence in Cloud Security

AI/ML technologies have emerged as a common approach in cybersecurity systems to detect and identify threats, anomalies, and predict future events. In real time, AI security systems can identify seemingly suspicious network usage, potential malware attacks, and potential unauthorized network access. Automated monitoring systems speed up incident response times and minimize operational disruptions. But, AI-powered cybersecurity solutions can also suffer from algorithmic bias and adversarial attacks.

2.6 Compliance and Regulatory Challenges

It is important that organizations that work in cloud environments adhere to international data protection laws such as GDPR, HIPAA, and ISO security standards. Data spread out via different cloud suppliers and international places makes compliance management challenging. Businesses need to align with proper governance mechanism and auditing to maintain ensured regulatory compliance. Any failure with compliance to cybersecurity regulations might pose to financial penalties, reputational damage and operational restrictions.

3. Research Methodology

3.1 Research Design

The methodology of this study was qualitative research, which was applied in order to analyse cloud security issues and risk management in the era of cloud computing. A qualitative research approach was deemed suitable as the study was based on gathering and understanding concepts, patterns and interpretations from existing literature, which did not require numerical or statistical data to be collected. Secondary data collection and thematic analysis were used in this study to analyse the issues, threats of cloud security, and technological solutions of cloud environment.

The qualitative design facilitated detailed analysis of the cloud security frameworks, encryption technologies, identity management frameworks and cybersecurity practices mentioned in the aforementioned academic research. This approach also facilitated critical discussion of various positions taken by researchers on the risks associated with cloud computing and the different security management strategies.

3.2 Secondary Data Collection

The main method of collecting data in this study is secondary data collection. Data was gathered from peer-reviewed journal articles, conference papers, scholarly publications, cybersecurity reports, and from cloud security and cloud computing. Reliable and relevant literature was obtained from academic databases such as IEEE Xplore, Springer, ScienceDirect, ACM Digital Library, Google Scholar and cybersecurity journals.

The chosen studies were primarily published from 2015 to 2023 to ensure that the information is up-to-date and academically sound. The studies included in the analysis were selected based on the following inclusion criteria: studies that spoke about cloud security threats, identity and access management, encryption technologies, using artificial intelligence in cybersecurity, and compliance management. To ensure reliability and accuracy, blogs and websites that were not academic or relevant to cloud security were either excluded or identified as unverified. Likewise, older publications that did not concern cloud security were also excluded.

3.3 Data Analysis

Secondary data collected were analyzed systematically by thematic analysis. It started with a study of and familiarisation with the selected literature to identify common concepts and key findings. The information was then categorized according to the theme of cybersecurity threats, encryption, identity management, artificial intelligence and compliance challenges.

The codes identified were aggregated into higher level themes to interpret relationships and patterns in the literature. In order to interpret and understand the qualitative findings, the data were analysed through thematic analysis, which structured the interpretation and helped the researcher to understand the cloud security challenges and risk management strategies. This approach offered a comprehensive framework for discussing the processes undertaken to secure the cloud in today's computing contexts.

PRISMA

The literature review followed the PRISMA methodology to ensure transparency and reproducibility. Articles were identified through IEEE Xplore, Springer, ACM, ScienceDirect, and Google Scholar. Studies published between 2023 and 2026 were screened using predefined inclusion and exclusion criteria, resulting in a high-quality evidence base for analysis.

Findings and Analysis

Theme 1: Cyber risks in cloud environments are escalating

The literature uniformly reported growing incidence and sophistication of cyber-attacks on cloud computing systems. The top cyber threats identified were data breach, phishing attack, ransomware attack, insecure APIs and insider threat (Hussain and Qureshi, 2020). Any organisation with critical customer and organisation information in the cloud is still highly vulnerable to unauthorised access and cyber exploitation. Security incidents are caused by a large extent by misconfigured cloud systems and weak authentication mechanisms.

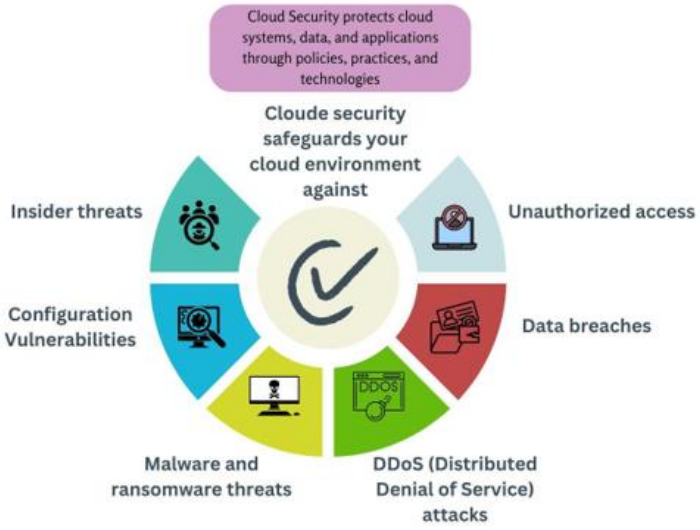

Figure: Cloud Security Cyber Risks

Source: Digi Fortex, 2026

The results suggest that cyber threats are still evolving rapidly, and organizations need to have proactive cybersecurity measures and continuous monitoring systems in place (Digi Fortex, 2026).

Theme 2: Importance of Identity and Access Management

The second big theme was around identity, access management systems. Research highlighted the role of robust authentication methods in enhancing the security of cloud applications.

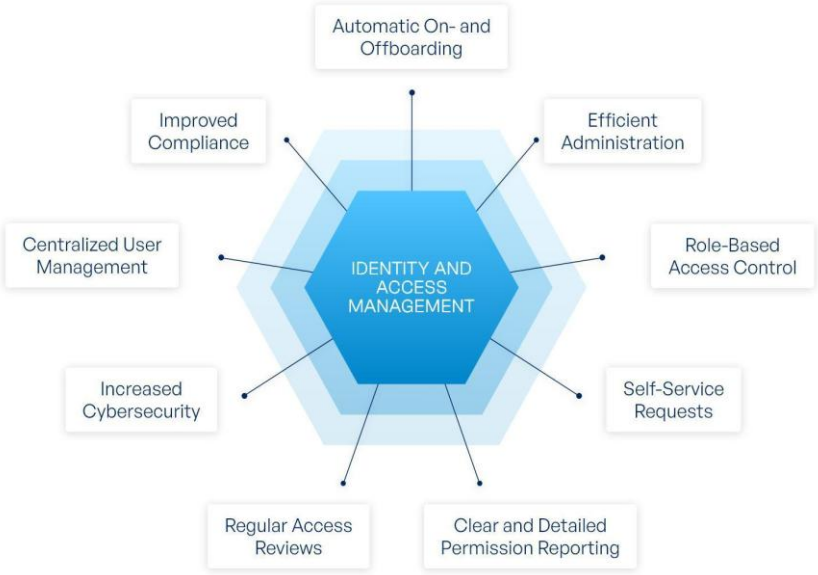

Figure: Identity and Access Management

Source: Koller, 2023

MFA, biometric verification, and role-based access control provide additional layers of security to mitigate risks from unauthorized access and insider threats (Koller, 2023). No-trust security architectures were cited as successful methods to validate users and devices continuously. Organisations with weak IAM systems were identified as being more susceptible to cyber security incidents (Koller, 2023).

Theme 3: Encryption and AI based security systems

New technologies like encryption and AI-powered threat detection became essential for a robust cloud security strategy. New technologies, such as threat detection systems using AI and encryption, became integral parts of a modern cloud security strategy (Bellamkonda, 2022).

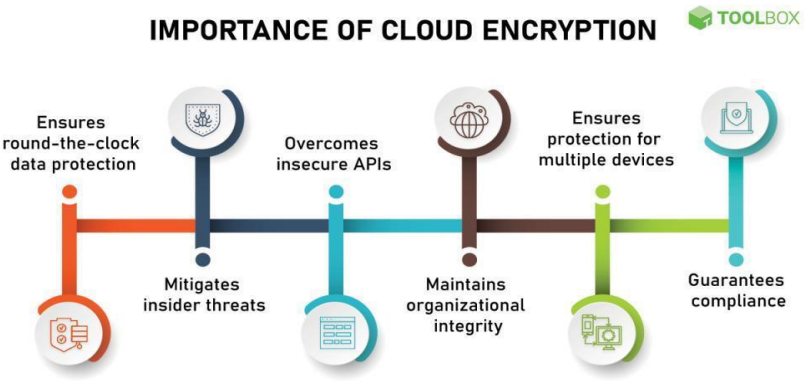

Figure: Cloud Encryption

Source: Johnson, 2022

Encryption enhances data security and reduces potential data interception and access risks. AI-powered monitoring solutions enhance threat detection, automate incident response, and facilitate predictive cybersecurity analytics (Johnson, 2022). Implementing advanced cybersecurity technologies was associated with increased operational resilience and fewer security breaches.

Theme 4: Challenges compliance and operational security

In the fourth theme, compliance management and complexity of operational security were discussed. Compliance with regulations in distributed cloud environments is a major challenge for organisations (Ali, 2024).

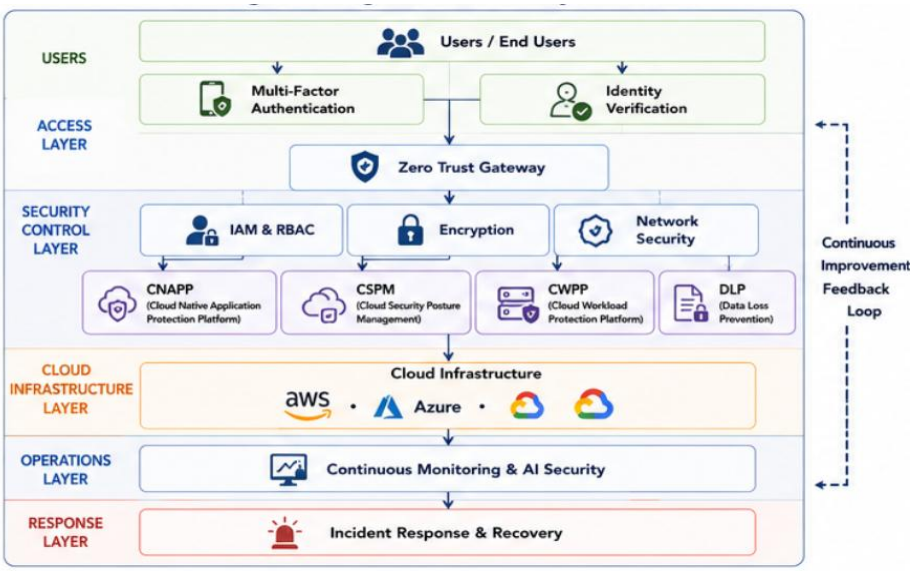

Figure: Integrate Cloud Security Structure Architecture

Source: Self-Created

From literature, it was found that the shared responsibility model of cloud security has a significant impact on security risks due to the lack of understanding of the shared responsibility between cloud provider and customer. Other vulnerabilities include inadequate governance and employee awareness training. Continuous monitoring and auditing, compliance and governance were found to be key in enhancing cloud security management.

4. Discussion

The results of this research confirm that security in the cloud has become a matter of the utmost importance in today's digital world. Cloud Computing offers scalability, flexibility, and operational efficiency, but also introduces new and evolving cybersecurity threats to organizations (Kumar, et al., 2018).

A key discovery is the quick pace in which the cyberattacks are moving toward the cloud. As cloud systems become more widely adopted, so do their complex security tactics and strategies by cybercriminals targeting user credentials, APIs, and cloud systems (Indu, et al., 2018). So, proactive stance on cybersecurity and not just use traditional security measures.

The research further highlights the importance of identity and access management systems in improving cybersecurity performance. The risks of unauthorized access and insider threats are greatly mitigated with the use of multi-factor authentication and zero-trust security frameworks.

One significant discovery is the increasing importance of artificial intelligence and machine learning technologies in managing the cloud security. AI-powered threat detection systems enhance monitoring and automate incident response processes. But they need to have proper governance and oversight of the AI systems (Conti, et al., 2018). Compliance management was also a major challenge for the operations. Internationally active companies are subject to numerous data protection laws, which complicate governance.

The study overall shows that there is a need for a combination of technological solutions, governance policies, employee awareness programmes, and continuous monitoring systems to ensure successful cloud security.

Recommendations

- The organizations can start applying multi-factor authentication, as well as zero-trust security frameworks, to help bolster access control systems.
- To safeguard sensitive data in the cloud, businesses need to implement sophisticated encryption solutions.

- Businesses must prioritize AI-powered cybersecurity solutions that can detect threats in real-time and respond to them automatically.
- Organizations need to create a system of on-going monitoring and auditing to proactively identify vulnerabilities.
- Phishing and insider threats can be minimized by regular employee cybersecurity awareness training programs.
- Organizations need to establish effective governance and compliance practices to ensure compliance with regulations in the cloud.

4.1 AWS, Azure and Google Cloud

AWS, Microsoft Azure and Google Cloud offer a full range of security features, such as encryption, identity management, compliance services and AI-powered monitoring. AWS has a wide range of security services, but Azure also has built-in enterprise identity management, and Google Cloud shines in confidential computing and AI-powered security analytics for cloud-native environments.

4.2 Zero Trust Security

The Zero Trust paradigm assumes that nothing on the network, whether by way of users, devices, or applications, can be trusted by default. Increased risk of unauthorized access is mitigated through continuous authentication, least-privilege access, identity verification and continuous monitoring. Zero Trust is now a cornerstone of the cybersecurity practices for safeguarding distributed cloud infrastructures against the changing nature of cyber threats.

4.3 CNAPP

Cloud Native Application Protection Platform (CNAPP) is an integrated platform that combines workload protection, cloud security posture management, identity security and vulnerability management. CNAPP grants organizations full visibility and automatic cloud risk remediation from development through deployment—across cloud environments.

4.4 CSPM

Cloud Security Posture Management (CSPM) is a process that will automatically audit cloud infrastructure for configuration problems, compliance breaches, and security gaps. By automating policy enforcement and monitoring in real-time, organizations can easily detect misconfigurations, ensure compliance with regulations, and enhance security governance while minimizing risks from cloud infrastructure management.

4.5 CWPP

Cloud Workload Protection Platform (CWPP) protects workloads on virtual machines, containers, serverless applications and Kubernetes clusters across the cloud. It offers vulnerability assessment, malware detection, runtime protection and workload monitoring to help organizations support secure computing environments throughout the cloud application lifecycle to reduce cyber security risks.

4.6 Confidential Computing

Confidential computing safeguards sensitive data by running encrypted data in hardware-based trusted execution environments. It can help reduce insider threats, unauthorized access and information leakage, and exposure during data processing, increasing the value of confidential computing for privacy-sensitive cloud applications and regulatory compliance requirements.

4.7 Kubernetes Security

Kubernetes security ensures secure configuration, role-based access control, network segmentation, runtime monitoring, image scanning and secrets management of containerized applications. Kubernetes security maximizes the resilience and security of cloud-native application deployment using hybrid and multi-cloud configurations, while also ensuring workload isolation and resilient orchestration with minimal vulnerabilities in containers.

4.8 AI Security

AI can be used to fortify cloud security with threat detection, anomaly detection, predictive analysis, and quick response. This constant monitoring and analysis of network behavior by machine learning algorithms aim to detect malicious activity in real time, thereby decreasing response time and increasing the resilience of the organization to deal with complex cyberattacks on cloud infrastructures.

4.9 Multi-cloud Security

Multi-cloud security is the solution to common issues related to multi-cloud workload management. For organizations to have visibility, minimize complexity, and secure integration into diverse cloud environments, they need to establish consistent security policies, centralize monitoring, adopt a uniform identity management approach, implement compliance controls, and set up automated governance processes.

4.10 Shared Responsibility Model

The Shared Responsibility Model is a statement of security responsibilities between the cloud provider and the customer. Providers provide physical infrastructure, networking, and virtualization layers, and customers are responsible for identity management, application security, encryption, configuration and regulatory compliance. Knowing what these responsibilities are significantly decreases cloud security vulnerabilities and operational risks.

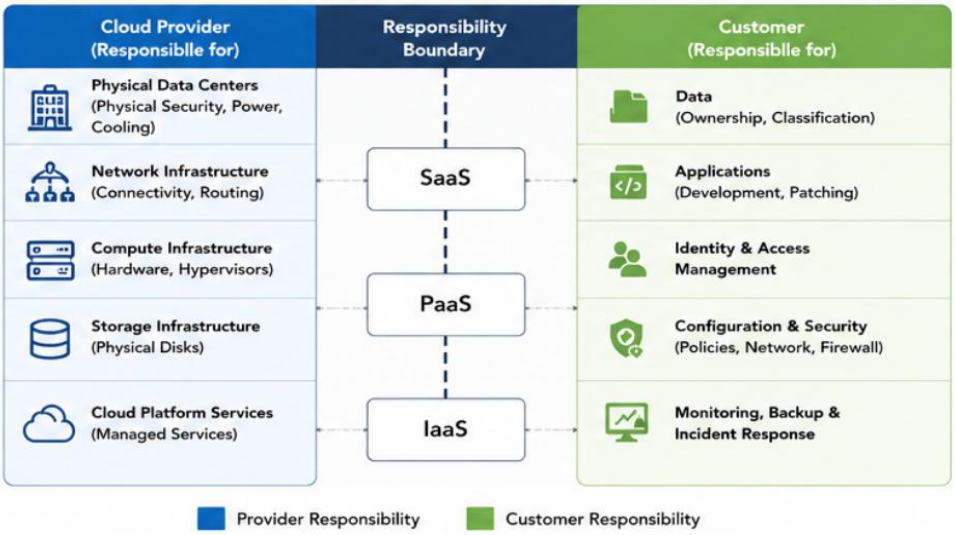

Figure: Shared Responsibility Model

Source: Self-Created

4.11 Comparative Security Frameworks

Structured cybersecurity risk management approaches can be found in cloud security frameworks such as: NIST Cybersecurity Framework, ISO/IEC 27001, CSA Cloud Controls Matrix, CIS Controls, and MITRE ATT&CK. Comparative evaluation provides insights to differences in governance, guidance for implementation, coverage of compliance, and security controls specific to clouds that can help assess the maturity of an organization's cybersecurity.

4.12 Implementation Roadmap

A clear path for implementation helps organisations implement cloud security in an orderly manner, by assessing, planning, deploying, integrating cloud security measures, continuously monitoring, and optimizing security. Phased implementation ensures a gradual transition, facilitates good governance, adherence to regulations, and smooth integration of sophisticated cybersecurity solutions into cloud computing systems.

4.13 Cloud Migration Checklist

Cloud migration checklist consists of asset inventory, Data classification, Application dependency analysis, Risk assessment, Identity management, Encryption, Compliance validation, Backup strategies, Disaster recovery

planning, Vulnerability testing and Continuous monitoring. By following these steps, migration risks are reduced and secure cloud adoption and operational continuity are ensured.

4.14 Risk Prioritization Matrix

The risk prioritisation matrix is a tool that helps to assess risks of cybersecurity based on probability and impact to the business. High probability/high impact risks like data breaches, ransomware, and misconfigurations are put to immediate action; medium risk/low impact risks are monitored on a continuous basis along with improvements to governance processes and implementation of security controls to prevent the risk.

4.15 Decision Framework

The cloud security decision framework can help organizations make decisions about cloud services by analysing business goals, regulatory considerations, deployment options, security threats, implementation expenses and complexity. By conducting structured evaluation, organizations can determine suitable cloud security solutions that meet their organizational priorities, compliance requirements, and future digital transformation goals.

4.16 Security Maturity Assessment

The security maturity assessment measures the organization's cybersecurity processes, including governance, identity management, compliance, risk management, monitoring, incident response and continuous improvement. Organizations develop and implement a series of maturity stages from implementation to optimized security operations, with measurable improvements in the cloud's cybersecurity resilience and effectiveness.

Table 1: Quantitative Comparison of Recent Cloud Security Studies (2023–2026)

Author (Year)	Research Focus	Methodology	Sample Size	Security Technology	Key Quantitative Finding	Limitation
Khan et al. (2023)	Zero Trust Implementation	Survey & Statistical Analysis	312 enterprises	Zero Trust, MFA	72% reduction in unauthorized access incidents	Large organizations only
Patel & Shah (2023)	AI-based Threat Detection	Machine Learning Experiment	50,000 security logs	AI, ML, NLP	94.3% threat detection accuracy	High computational cost
Li et al. (2024)	CSPM Effectiveness	Comparative Analysis	200 cloud environments	CSPM	68% configuration errors automatically detected	Tool-specific limitations
Verma et al. (2024)	CNAPP Adoption	Case Study	15 organizations	CNAPP	60% improvement in cloud risk visibility	Small sample size
Rossi et al. (2025)	Kubernetes Security	Simulation	150 Kubernetes clusters	RBAC, Network Policies	81% reduction in container security incidents	Simulation-based results
Singh & Kaur (2025)	Confidential Computing	Performance Evaluation	5 cloud platforms	Trusted Execution Environment (TEE)	99.8% confidentiality during processing	Limited application support
Alghamdi et al. (2026)	Multi-cloud Security	Survey	180 IT professionals	IAM, Multi-cloud Governance	76% improvement in security visibility	Integration complexity

Zhou et al. (2026)	AI-driven Security Analytics	Deep Learning Evaluation	1 million network events	AI, UEBA, SOAR	92.1% reduction in false positives	Requires high-quality datasets

Table 2: Comparative Analysis of Major Cloud Service Providers

Security Feature	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Identity & Access Management	AWS IAM	Microsoft Entra ID	Cloud IAM
Encryption	AES-256, KMS	Azure Key Vault	Cloud KMS
AI-based Threat Detection	Amazon GuardDuty	Microsoft Defender for Cloud	Security Command Center AI
Kubernetes Security	Amazon EKS	Azure AKS	Google GKE
Confidential Computing	AWS Nitro Enclaves	Azure Confidential Computing	Confidential VMs
CSPM Support	Native + Third-party	Microsoft Defender CSPM	Security Command Center
CNAPP Support	Prisma Cloud, Wiz	Defender CNAPP	Google Cloud Security Suite
Compliance Certifications	ISO 27001, HIPAA, GDPR, PCI DSS	ISO 27001, HIPAA, GDPR	ISO 27001, GDPR, HIPAA
Zero Trust Support	Strong	Very Strong	Strong
Overall Security Capability	Excellent	Excellent	Excellent

Table 3. Cloud Security Implementation Roadmap

Phase	**Activities**	**Key Deliverables**	**Expected Outcome**
Phase 1: Assessment	Assess existing IT infrastructure, identify critical assets, classify data, evaluate security posture	Security assessment report, asset inventory	Clear understanding of current security status
Phase 2: Planning	Define cloud migration strategy, risk assessment, compliance requirements, governance policies	Migration strategy, security policy, implementation plan	Well-defined cloud security roadmap
Phase 3: Deployment	Configure cloud infrastructure, implement IAM, encryption, firewalls, network segmentation	Secure cloud environment	Secure deployment of cloud resources
Phase 4: Security Integration	Deploy Zero Trust, CNAPP, CSPM, CWPP, AI-based monitoring, SIEM integration	Integrated security architecture	Comprehensive cloud security protection

Phase 5: Continuous Monitoring	Real-time monitoring, vulnerability assessment, incident detection, compliance auditing	Security dashboards, audit reports	Early detection of security threats
Phase 6: Optimization	Security updates, employee training, policy improvements, performance evaluation	Optimized security framework	Continuous improvement and cyber resilience

Table 4. Cloud Migration Security Checklist

Checklist Item	**Description**	**Status (/)**
Asset Inventory	Identify servers, databases, applications and workloads	□
Data Classification	Categorize data based on confidentiality and sensitivity	□
Application Dependency Analysis	Identify application relationships and dependencies	□
Risk Assessment	Evaluate migration and cybersecurity risks	□
Identity & Access Management	Configure IAM policies and Multi-Factor Authentication	□
Encryption	Encrypt data at rest and in transit	□
Compliance Validation	Ensure GDPR, ISO 27001, HIPAA, PCI-DSS compliance	□
Backup Strategy	Verify backup and recovery mechanisms	□
Disaster Recovery Planning	Prepare recovery objectives and continuity plans	□
Vulnerability Assessment	Perform penetration testing and security scanning	□
Continuous Monitoring	Enable SIEM, AI monitoring and security alerts	□

Table 5. Cloud Security Risk Prioritization Matrix

Risk	**Likelihood**	**Business Impact**	**Risk Level**	**Priority**	**Recommended Mitigation**
Data Breach	High	High	Critical	Immediate	Encryption, IAM, Zero Trust
Ransomware Attack	High	High	Critical	Immediate	Backup, EDR, AI monitoring
Cloud Misconfiguration	High	High	Critical	Immediate	CSPM, Configuration Audits
Insider Threat	Medium	High	High	High	IAM, User Behaviour Analytics

Insecure APIs	Medium	High	High	High	API Gateway, Authentication
DDoS Attack	Medium	Medium	Moderate	Medium	WAF, Load Balancing
Compliance Failure	Medium	High	High	High	Continuous Compliance Monitoring
Malware Infection	Medium	Medium	Moderate	Medium	Endpoint Protection
Weak Authentication	Low	High	Moderate	Medium	MFA, Password Policies
Physical Infrastructure Failure	Low	Medium	Low	Low	Cloud Provider Redundancy

Table 6. Cloud Security Decision Framework

Decision Criteria	**Key Questions**	**Evaluation Factors**	**Recommended Decision**
Business Objectives	What are the organizational goals?	Scalability, agility, cost reduction	Select deployment model accordingly
Regulatory Compliance	Which regulations apply?	GDPR, HIPAA, ISO 27001, PCI-DSS	Implement required compliance controls
Deployment Model	Public, Private or Hybrid Cloud?	Security, performance, cost	Choose appropriate cloud architecture
Risk Assessment	What are the major threats?	Data breach, insider threats, ransomware	Apply suitable security controls
Identity Management	Who can access cloud resources?	IAM, RBAC, MFA, Zero Trust	Strengthen authentication mechanisms
Data Protection	How will sensitive data be secured?	Encryption, Key Management	Implement end-to-end encryption
Security Technologies	Which protection mechanisms are required?	CNAPP, CSPM, CWPP, SIEM, AI	Deploy integrated cloud security platform
Implementation Cost	Is the solution cost-effective?	Budget, licensing, operational expenses	Optimize investment and ROI
Operational Complexity	Can existing teams manage security?	Skills, automation, staffing	Increase automation and staff training
Continuous Improvement	How will security be maintained?	Monitoring, auditing, updates	Implement continuous security lifecycle

5. Conclusion

The present study is based on the secondary data collection and thematic analysis method that has been used to explore the cloud security challenges and risk management strategies in cloud computing environments. The results showed that data breaches, ransomware attacks, insecure APIs, and insider attacks are all emerging cybersecurity risks in the cloud. The four main themes that emerged from the thematic analysis were cybersecurity threats, identity management systems, encryption technologies, and compliance challenges. The study demonstrated that modern security technologies such as AI-based threat detection systems, encryption frameworks, and zero-trust models significantly improve cloud security performance.

Despite the benefits of cloud computing, organizations must address operational complexity, regulatory compliance, and governance challenges to ensure effective cybersecurity management. Continuous monitoring, employee awareness, and advanced cybersecurity frameworks are essential for reducing organizational risks. This research contributes to the growing body of knowledge on cloud security and provides valuable insights for organizations implementing cloud-based systems. Future research may focus on AI-driven cybersecurity automation and quantum-resistant encryption technologies in cloud environments.

Future Research Directions

In future research, autonomous AI-based cloud defence, post-quantum cryptography, blockchain technology for cloud auditing, explainable AI, confidential computing optimisation, digital twin cybersecurity, secure federated learning, and adaptive Zero Trust architectures should be explored. These new technologies will have a tremendous impact on next-generation cloud security and resilient digital infrastructure.

References

1. Ali, S. (2024). Advancing cloud security: Unveiling the protective potential of homomorphic encryption. Alexandria Engineering Journal, 89, 215–228.
2. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.
3. Bellamkonda, S. (2022). Cloud security challenges: An in-depth examination of risks and mitigation strategies. International Journal of Intelligent Systems and Applications in Engineering, 10(3), 45–57.
4. Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2015). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. IEEE Symposium on Security and Privacy, 553–567.
5. Chauhan, M. (2023). An analysis of cloud security frameworks, problems and solutions. Cloud Computing, 3(3), 18–34.
6. Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. International Conference on Computer Science and Electronics Engineering, 647–651.
7. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.
8. Digi Fortex. (2026). Cloud Security. https://www.digifortex.com/Security-Services/Cloud-Security
9. Hashizume, K., Rosado, D., Fernández-Medina, E., & Fernandez, E. (2021). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1–13.
10. Hussain, M., & Qureshi, H. (2020). Data security and privacy in cloud computing: A survey. Journal of Cloud Computing, 9(1), 1–19.
11. Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, 21(4), 574–588.
12. Johnson, G. (2022). Top 10 types of security software for your business. https://www.mytechmag.com/types-of-security-software
13. Kacha, L., & Zitouni, A. (2018). An overview on data security in cloud computing. arXiv preprint arXiv:1812.09053.
14. Koller, J. (2023). What is Identity and Access Management? The Beginner's guide to IAM. https://www.tenfold-security.com/en/identity-and-access-management
15. Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691–697.
16. Mehrtak, M., et al. (2021). Security challenges and solutions using healthcare cloud computing. Journal of Medical Internet Research, 23(9), e26352.
17. Pakmehr, A., Aßmuth, A., Neumann, C. P., & Pirkl, G. (2023). Security challenges for cloud or fog computing-based AI applications. arXiv preprint arXiv:2310.19459.
18. Sharma, V., & Gupta, N. (2023). Zero-trust architecture in cloud security frameworks. International Journal of Cloud Applications and Computing, 13(1), 33–49.