



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

Privacy and security in cloud computing- A review of various attacks and mitigation strategies

Dr. Reghunath K

Associate Professor, Computer Applications, Marian Academy of Management Studies, Kothamangalam

Abstract

Cloud computing has transformed the process and storage of data in terms of scalability, flexibility, and affordability. Nonetheless, its shared and distributed character brings up serious questions of privacy and security. The current review considers the recent events during 2020-25, the largest cloud-based attacks, their effect, and the mitigation techniques. It discusses the development of privacy-enhancing methods, such as homomorphic encryption, federated learning, and blockchain authentication, and security models, such as Zero Trust Architecture and ISO/IEC standards. Such issues as multi-cloud complexity, regulatory compliance, and performance trade-offs are also assessed during the study. Through the integration of the developments and the research gaps, the paper points to the future research directions that address the concept of AI-based threat detection, confidential computing, and post-quantum cryptography. Altogether, the review highlights the significance of combining privacy and security processes to obtain resilient, adaptive and trustworthy cloud infrastructures.

Keywords: Cloud Computing, Privacy, Security Frameworks, Cybersecurity, Mitigation Strategies

1. Introduction

1.1 Background

Cloud computing has taken root as a paradigm in the current information infrastructure and is now the means of on-demand computing, storage, and application services that is scalable and can be accessibly achieved via the internet (Cloud Security Alliance, 2025). The critical model service paradigms, "Infrastructure as a Service (IaaS)", Platform as a Service (PaaS) and Software as a Service (SaaS), along with deployment options public, private, hybrid, and multi-cloud, provide companies with unparalleled flexibility, cost-efficiency, and global coverage. Nevertheless, the same characteristics, which make cloud computing appealing, namely, multi-tenancy, resource pooling, ubiquity of access, and abstraction of physical infrastructure, pose a thorny privacy and security threat, as well. As an illustration, the survey of cloud computing security and privacy concerns reveals that the transition to remote, distributed, virtualised environments presents new threats with respect to data leaks, unmanaged data replications, and users not having control over the location and lifecycle of their data (Rahdari et al., 2025). The actual scale of such issues is emphasised in empirical evidence. These trends indicate that despite adoption, the cloud computing ecosystem still requires fundamental security controls, such as server-side encryption, disk encryption, and block storage, and enablement of block public access, and that despite the growth, 84% of organizations operate two or more cloud environments, 75% operate in particular to simplify multi-cloud security (dcurwin, 2025). Privacy-wise, clouds create serious concerns about ownership, control, and sovereignty of data: the data can live in other jurisdictions, flow through intermediary nodes, or run on third-party services, and then it is awkward to comply with such regulations as the General Data Protection Regulation (GDPR) or the new regulations in other states. Overall, the architectural advantages of cloud computing naturally create a larger attack surface, and the combination of big-data analytics, artificial intelligence loads, and a multi-tenant deployment only exacerbates the urgency of sound security and privacy systems.

1.2 Motivation

The reason behind this literature review is threefold. First, the growing pace of cloud computing, which is stimulated by the digital transformation, big data analytics, integration of the Internet of Things (IoT) and international business growth, suggests that more and more volumes of critical and sensitive data are being stored, processed, and transferred over cloud computing infrastructures. This ubiquity makes cyber-attackers find cloud systems more attractive targets, and privacy and security issues are no longer marginal, indeed, being of central strategic importance. As an example, the 2023 CSA survey points to the fact that organisations

are struggling not only with large-scale multi-cloud deployment but also with the natural complexity of protecting them, which makes the newer paradigms of protection necessary (Jain, 2024). Second, as it is widely used, various industry and scholarly studies have reported that there are still many cloud deployments that are vulnerable due to improper configuration, lack of encryption, poor access controls, and lack of governance. The 2021 CIO survey revealed that most cloud storage providers do not have the necessary security controls in place, a fact that indicates that the cloud migration is way ahead of security maturity (CIO, 2021). The risk profile related to cloud computing is becoming increasingly steep, considering that financial loss, regulatory fines, reputational damage, and national-level cyber incursion are on the rise. Third, although an increasing literature exists covering the individual security and privacy problems in cloud computing, there has been a haphazard world of attacks, mitigation, frameworks, and performance trade-offs, particularly since 2020-2025. The topic of privacy-enhancing and trust-centric cloud-native security techniques demonstrates that a systematic survey of the attack types, mitigation measures, and the landscape of gaps is currently being developed, but remains to be released to the researchers, practitioners, and policy-makers (Arif et al., 2025). It is with this inspiration that this review will attempt to consolidate the current trends in cloud security and privacy, discern common trends with respect to assault and defence, and reveal unresolved issues and prospects. This way, it helps to improve the overall capacity of building safe and privacy-conscious cloud computing in the age of big data.

1.3 Aim and Objectives

- Examine the evolution of privacy and security threats in cloud computing from 2020–2025.
- Identify and evaluate existing protection and mitigation strategies.
- Highlight gaps, challenges, and potential directions for future research in cloud security frameworks

1.4 Research Questions

- RQ1: What are the most common privacy and security threats in cloud computing environments and their impact?
- RQ2: What protection and mitigation strategies have been proposed to address these threats?
- RQ3: What are the key challenges, limitations, and future research directions in current cloud security frameworks?

1.5 Structure of the Paper

The paper will be divided into six major sections. Section 1 presents the research background, motivation, objectives, and questions. Section 2 is an account of the literature review, which describes chronological developments and attack classifications. In section 3, there is a discussion of important security technologies and mitigation strategies. Section 4 looks into privacy and security frameworks. Section 5 contains difficulties, constraints, and prospects. Lastly, Section 6 gives the general summary and conclusions of the review.

2. Literature Review

2.1 Chronological Review

Cloud computing has been experiencing a fast evolution within the past decade, changing the traditional computing infrastructures by way of virtualization, scalability, and distributed resources. The recent advances in cloud computing privacy and security research since 2020 to 2025 have highlighted the importance of protecting, securing, and controlling access to data. Early 2020 was primarily focused on DDoS and insider attack detection solutions, which were based on intrusion detection systems and heuristic methods (Jayakrishna and Prasanth, 2025). Nonetheless, the increase in hybrid cloud implementations brought about new security challenges, such as multi-tenancy and inter-cloud interactions, and identity control. Between 2021 and 2023, researchers began utilizing artificial intelligence (AI) and blockchain mechanisms to detect and prevent threats. The identity verification systems, which utilise blockchain technology, were proposed to resolve the issue of trust and authentication in the multi-cloud frameworks. At the same time, machine learning (ML) models have contributed to improved anomaly detection and predictive threat analysis (Mohamed, 2025). Furthermore, homomorphic encryption, safe multiparty computation took the center stage in the maintenance of data confidentiality without affecting the performance. Further on, in 2024 and later, it became about zero-trust architecture (ZTA) and privacy-preserving federated learning models. ZTA points out that continuous verification and micro-segmentation should be encouraged by assuming that no user or device can be trusted (Mushtaq et al., 2025). Likewise, federated learning has been proposed as an encouraging trend toward models of training ML without aggregated data in a centralized place, facilitating the minimization of privacy leaks (Kaul and Khurana 2021). It is also emphasized in the literature that there is a growing need to rely on cloud-native security solutions that can be combined with containerized and microservice-based applications, therefore, ensuring scalability without compromising the global privacy standards like GDPR and ISO/IEC 27018. The chronological development shows that the reactive detection systems have evolved into

proactive and smart systems that are aimed at predicting, preventing, and mitigating threats in a dynamic manner.

2.2 Type of Attacks

Cloud computing environments are prone to numerous types of attacks because they are distributed and shared. The most evident ones are data breaches, account hijacking, insider threats, DDoS attacks, vulnerabilities in virtualization, and API exploitation. Cloud computing environments are prone to numerous types of attacks because they are distributed and shared. The most evident ones are data breaches, account hijacking, insider threats, DDoS attacks, vulnerabilities in virtualization, and API exploitation. One of the threats recently reported in cloud ecosystems is a data breach. The types of attacks include weak encryption or improperly configured storage, or poorly secured APIs that attackers use to obtain sensitive data (Ramcharan, 2025). Cloud vendors such as AWS and Google Cloud have had to deal with many cases of data leakage due to poor identity and access management IAM settings. Account hijacking is the process by which attackers obtain access to user accounts in an unauthorized way by means of phishing, malware, or lax password practices. By getting into the machines, attackers may compromise data, interfere with services, or escalate privileges within the virtual machines. To reduce this risk, researchers have suggested multifactor authentication (MFA), identity federation, and identity of zero-trust models.

Table 1: Common Types of Attacks and Mitigation Strategies in Cloud Computing

Type of Attack	Description	Impact on Cloud Environment	Mitigation / Defense Strategies
Data Breaches	Occur due to weak encryption, misconfigured storage, or insecure APIs allowing attackers to access sensitive data.	Exposure of confidential data, regulatory non-compliance, and reputational damage.	Strong encryption, secure API management, improved IAM configurations.
Account Hijacking	Unauthorized access to user credentials via phishing, malware, or weak passwords.	Unauthorized data manipulation, service disruption, and privilege escalation.	Multi-Factor Authentication (MFA), identity federation, and Zero Trust Architecture.
Insider Threats	Privileged users misuse their access for malicious purposes, making detection difficult.	Data theft, service disruption, and internal system compromise.	Behavioral analytics, Role-Based Access Control (RBAC), and continuous user monitoring.
Distributed Denial of Service (DDoS)	Attackers overload servers with excessive traffic, disrupting service availability.	System downtime, degraded performance, and financial losses.	Adaptive rate-limiting, ML-based anomaly detection for real-time monitoring.
Virtualization / Hypervisor Attacks	Exploit vulnerabilities in virtual infrastructure to gain control over multiple VMs.	Full system compromise, unauthorized access to co-hosted tenants.	Micro-hypervisors, secure enclave technologies, isolation of workloads.
API and Interface Attacks	Exploit insecure APIs that expose cloud resources and communication channels.	Unauthorized access, data manipulation, service abuse.	Token-based authentication, encryption, and continuous monitoring of APIs.

The biggest threat that is still present is insider threats, as they are caused by the misuse of privileges by authorised users. These attacks are sometimes hard to notice since they utilise authorised points of access. In response, behavioral analytics-based and role-based access control (RBAC)-based monitoring tools are going to be implemented to monitor user anomalies (Abshari and Sridhar, 2025). DDoS attacks disrupt the availability of cloud services, as they flood servers with excessive traffic that causes malicious congestion. As a response, cloud service providers have added rate-limiting algorithms that are dynamically adjusted, as well as anomaly detection algorithms that are machine learning-based to detect suspicious traffic patterns in real time (Chatterjee and Ahmed, 2022). Attacks of virtualisation and hypervisor-level leverage weaknesses of the

underlying virtual infrastructure. The goal of attackers is to attack hypervisors to get control over several virtual machines at the same time. The technology of micro-hypervisors and secure enclaves is also being developed by researchers to isolate the workloads in an efficient way (Boubakri and Zouari, 2025). Finally, API and interface attacks are based on the exploitation of insecure APIs that reveal cloud resources. Since APIs are at the centre of communication in clouds, their security with the help of encryption, authentication based on the use of tokens, and constant monitoring has become a necessity. The cumulative effect of these attacks is that the threat environment of cloud environments is complex and dynamic. A combination of AI, blockchain, and frameworks of secure architecture is crucial in ensuring the balance of performance, scalability, and protection.

2.3 Database Sources

The literature review applied in this study was made based on several academic and technical databases to guarantee extensive coverage of cloud computing privacy and security studies. Major sources are IEEE Xplore, ScienceDirect (Elsevier), SpringerLink, ACM Digital Library, Scopus and Google Scholar. These databases were chosen because they have high-quality peer-reviewed publications and are also relevant to the emerging cloud computing technologies. Priorities were put on articles published in Future Generation Computer Systems, Journal of Cloud Computing, IEEE Transactions on Cloud Computing, and Computer Networks because they consistently present the state-of-the-art results in the context of cloud security, privacy-preserving computation, and threat mitigation models. Keywords used in search queries included the following: cloud security threats, data privacy in cloud computing, attack detection in cloud systems, blockchain security in cloud, and privacy-preserving frameworks. The criteria of the literature selection were as follows: (a) the publication date of the article should not exceed 2025, (b) the article should include practical mitigation frameworks, and (c) the article should speak about the measurable increase in the metrics of cloud security performance. Papers that dealt with outdated/proprietary cloud systems were filtered out to keep up to date with prevailing standards. The synthesis of thematic and chronological analyses of the research papers collected aimed to reveal the trends, innovations, and gaps in the research. The synthesis shows that privacy is getting better with the help of AI-based intrusion detection and encryption mechanisms; however, real-time adaptability and interoperability are not yet well-developed. Through these scholarly databases, the review will guarantee coverage of both the base research and technological breakthroughs to give a fair understanding of the trend on privacy and security in cloud computing.

3. Techniques and Technologies

The rise of cloud computing has transformed how we store and process data by providing scalability, cost-effectiveness, and flexibility. At the same time, these advantages come with increased worries related to data confidentiality, integrity, and availability. In order to solve these issues, a variety of solutions and technologies have been created that improve privacy and security in cloud-based environments. These solutions include encryption algorithms, authentication models, data integrity assurance, access control policies, and resilience measures to promote data availability.

1. Encryption Methods for Data Confidentiality

Encryption is the foundation of cloud data security. It transforms sensitive data into incomprehensible ciphertext so that unauthorized individuals cannot read or alter it. Symmetric encryption techniques, such as the Advanced Encryption Standard (AES), are often used because they are relatively fast to compute, while also providing strong security properties (Abdulsalam and Hedabou, 2021). AES-256 can be used to encrypt data at rest (being stored), while Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols can be used to transmit data in transit. These are end-to-end encryption protocols that help protect data during transportation and against interception and man-in-the-middle (MITM) attacks (Vellela et al., 2022).

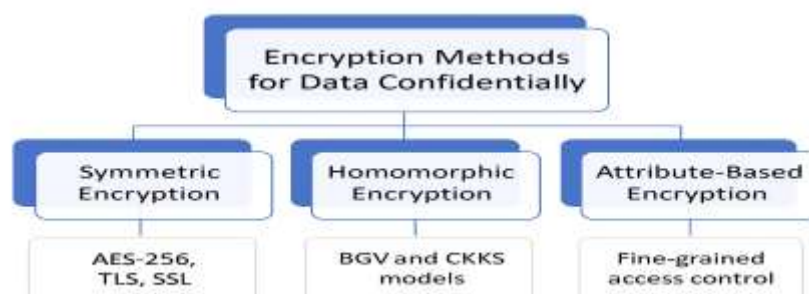


Figure 1. Encryption Methods for Data Confidentiality

In addition to traditional encryption methods, advanced techniques such as Homomorphic Encryption (HE) support data processing without decryption (Alenizi et al., 2021). This is particularly relevant in the cloud, where third-party servers host data processing. HE remains a computationally expensive operation; advances in partially homomorphic and fully homomorphic encryption schemes such as BGV and CKKS models, have made HE computationally feasible for limited cases (Chetlapalli et al., 2021). A newer, innovative method is to use Attribute-Based Encryption (ABE), whereby the encryption process utilizes user attributes or roles. ABE provides a strong method for fine-grained access control, enabling confidentiality while preserving usability in a multi-tenant cloud environment.

2. Authentication and Access Control Mechanisms

Strong authentication is needed to avoid compromise of cloud resources by unauthorized users. Multi-Factor Authentication (MFA) supports traditional username–password systems with additional layers of verification, which include biometrics, one-time passwords (OTPs), hardware tokens, etc (Zarichuk, 2024). Federated Identity Management (FIM) systems and Single Sign-On (SSO) systems allow users to authenticate securely across several cloud platforms without requiring users to tamper or curate their many cloud accesses. Token-based authorization systems (e.g., OAuth 2.0, OpenID Connect) are a lot more secure than verifying credentials, which are easily stolen or hijacked.

Access control methods govern how users can interact with their cloud resources; the two most commonly used are Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). RBAC permits users to access data resources depending on predetermined roles in the organization, which restricts users to accessing only data that are necessary for the roles they perform (Lo'ai and Saldamli, 2021). ABAC advances RBAC by incorporating dynamic attributes, for example, location, time, and whether the device is secured. Recently, Zero Trust Architecture (ZTA) has emerged, promoting the principle of “never trust, always verify.” ZTA provides a constant validation of every access request, even inside the network, which provides higher assurance against insider threats.

3. Data Integrity and Verification Technologies

In a cloud environment, verifying the integrity of stored and transmitted data is critical because users don't have physical control over the storage platform. Provable Data Possession (PDP) and Proof of Retrievability (PoR) are two popular techniques that allow users the ability to verify their data stored on the cloud without the need to download everything (Abba Ari et al., 2024). The major difference is that PDP generates cryptographic proofs that demonstrate integrity, while PoR ensures that the user can fully retrieve the data if requested. Another technique that is frequently found in cloud storage platforms is the use of Merkle Hash Trees, which are an efficient way to verify the integrity of the stored blocks of data in a scalable method (Thabit et al., 2021).

Blockchain technology has become a highly effective means of providing transparency and integrity of data. Data and transnational activities can be logged in a decentralized ledger through a tamper-proof process, and data integrity is not dependent upon a single source of truth (Joshi et al., 2022). Cloud service providers are beginning to implement blockchain-based audit capabilities to enhance accountability and traceability in distributed environments.

Hence, to summarize, data confidentiality and availability in the cloud are ensured through an integrated application of mechanisms, including encryption, authentication, integrity checking, and redundancy. Although the technologies available today guard data with great strength, continued innovation must occur to respond to cyber threats that will only continue to evolve. The combination of AI, blockchain, and confidential computing represents a new era moving forward to secure, resilient, and privacy-preserving cloud environments.

4. Role of Privacy and Security Frameworks in Cloud Computing

With the spread of cloud computing, powerful privacy and security frameworks are vital in organising the controls, system implementation, and compliance assurance. These frameworks are useful in more than one way: they normalise the best practices, aid in governance and in auditability, offer architectural patterns, and allow organisations to react to any emerging threat in the cloud.

Techniques of Privacy Preservation

Privacy preservation is one of the dimensions of the framework landscape. Such methods as anonymisation, data-masking, secure multi-party computation, differential privacy and homomorphic encryption are typically integrated into frameworks so that sensitive data stored and processed in the cloud are secure. To take a specific case, a recent study that compared different privacy-saving approaches in cloud computing identified cryptography, anonymisation and access control as important pillars that were evaluated on the basis of scalability and practical deployment performance (Kambala 2025). In addition, studies on cloud-based image processing reveal the use of adversarial perturbation and obfuscation tools in privacy models to counter the use of facial recognition in cloud computing (Chen et al., 2025). Such privacy models are inclined to plot the

cloud lifecycle, including data collection, storage, sharing, processing, and deletion, against stages in which particular controls are introduced. Through this, organisations would be able to embrace systematic privacy-by-design principles as opposed to ad-hoc protection. On the governance front, privacy frameworks tend to be in line with data protection policies (e.g., GDPR, HIPAA) as they define roles, data flow models, data minimisation techniques, and audit logs. Such frameworks are valuable because they enable the privacy controls to be repeatable, measurable, and verifiable in the cloud.

Regarding security, information security standards and guidelines such as Cloud Security Alliance (CSA) guidelines, implementation of the “Zero Trust Architecture (ZTA)” model, and standards such as ISO/IEC 27017 on cloud security offer structured frameworks on threat mitigation, identity and access controls, network segmentation, and workload security. Just as an example, according to a 2024 research article, Zero Trust in cloud networks minimises lateral movement, enhances micro-segmentation, and bolsters identity and access management (IAM) in the cloud (Ahmadi, 2024). In 2024, the CSA released a press statement about Zero Trust guidance to critical infrastructure, which shows the framework is being adjusted to support the cloud with hybrid clouds, edges, IoT, and OT/ICS (Cloud Security Alliance, 2024). Security frameworks help organisations to do the definition of the protected surface, data flows mapping, policy enforcement, monitoring, and constant adjustments. Indicatively, there are five steps that are described by CSA in the Zero Trust to discover the protected surface, flow mapping, building architecture, policy creation, and finally, monitor and maintain the network. The frameworks assist in the translation of high-level concepts (e.g., least-privilege, continuous verification, micro-segmentation) into operational controls and metrics. The studies indicate that organisations that adopt the Zero Trust models can realise a high level of incident reduction at the cost of performance and scalability.

The intersection between privacy and security models in cloud computing is becoming more critical. Traditional guarded boundaries are becoming unclear in modern cloud systems and frameworks that consider data-in-use (confidential computing), data-in-transit and data-at-rest along with identity, workload and network protections are needed. Indicatively, in a 2025 article in CSA, the author notes that in cloud-native, serverless, multi-cloud environments, Zero Trust is no longer adequate: organisations now need to embrace adaptive trust, confidential computing and decentralised identity systems as components of a security + privacy architecture (Cloud Security Alliance, 2025b). Through integrating privacy-sensitive methods (like secure multi-party computation, differential privacy) with security networks (like Zero Trust and micro-segmentation), cloud providers and consumers can be in a better position to mitigate the threat of insider attacks, side-channel attacks, misconfigurations and data exfiltration. There must be frameworks defining the interplay between privacy controls (masking, anonymisation, encryption) and security controls (IAM, segmentation, monitoring) and vice versa. As an example, the storage of encryption keys can be a privacy control (key confidentiality) as well as a security control (key access control). Frameworks are valuable in that they bring about uniformity, facilitate auditing, increase trust between vendors and clients, as well as aid with regulatory adherence. The latter enables mapping of controls to cloud service models (IaaS, PaaS, SaaS) and deployment modes (public, private, hybrid). With that said, there are practical constraints: most organisations have difficulties in scaling frameworks to large multi-cloud workloads, addressing legacy systems, or cross-integrating hybrid environments. Indicatively, a study about Zero Trust in cloud computing shows that scalability, performance overhead, and compatibility with the existing systems are problematic (Oladimeji, 2024). The considerations related to implementation are organisational alignment (process, people, governance), vendor interoperability, the definition of metrics (KPIs of maturity of framework), and ongoing adaptation in case of threat evolution. Frameworks should be dynamic, and they cannot be deployed using static controls because of the dynamic nature of the cloud. Future framework roadmap indicates the direction toward the integration of AI/ML to enforce adaptive policies, confidential computing to protect data-in-use, and decentralised identity solutions to distribute trust.

5. Challenges, Limitations and Future Directions

Although remarkable progress has been made in the field of security and privacy of cloud computing, there are still a number of ongoing challenges and limitations to effective protection, and they outline the future research direction. A significant issue is misconfiguration and gaps of shared responsibility: cloud services generally assume that some controls are managed by the provider, and other controls are managed by the user, which creates a lack of clarity and results in exposures. Indicatively, cloud services are reported to be left unconfigured, which is one of the greatest contributors to the twenty-first-century cloud attacks. The other weakness is the complexity of multi-cloud and hybrid-cloud ecosystems. With the implementation of an organisation across different providers, there is a friction in governance, visibility, identity and access management (IAM), and uniformity in policy enforcement. Research indicates that multi-cloud environments exacerbate interoperability issues, hamper consolidated threat tracking, and make responding to incidents

difficult (Almutairi and Sheldon, 2025). Even more advanced mitigation techniques homomorphic encryption, secure multi-party computation, or real-time AI-driven monitoring, are limited to production cloud computing by performance and scalability constraints. These are commonly computationally, latency or cost-intensive techniques, which prevent widespread use. As an example, a recent survey of Zero Trust in the cloud environment has pointed to scalability and performance trade-offs at large scale. In the privacy front, there are questions of data sovereignty, legal/ regulatory compliance, transparency, and trust, which are still to be addressed. Cloud information can physically be located in other jurisdictions, in transit, and be processed by third-party systems, so aligning regulation with regulations such as the GDPR or future data-protection legislation can be difficult (Fatima et al., 2024).

The research has several promising directions in the future:

- One of the problems associated with the emergence of quantum-enabled cloud architectures is the emergence of new security risks (e.g., quantum side-channel attacks, cryptographic breakage) and hence necessitate post-quantum cryptographic frameworks and quantum-aware resource management (Coupel and Farheen 2025).
- The application of AI/ML to dynamic threat detection and coordination has not been thoroughly studied in multi-cloud environments with heterogeneity; privacy-aware AI (federated learning, encrypted inference) is increasingly in demand for cloud monitoring and intrusion data.

As numerous mitigation measures are in place, viable constraints (cost, performance, complexity), emerging threats (quantum, AI-driven attacks), and systemic gaps (governance, multi-cloud interoperability) need to be further addressed. Subsequent studies should focus on scalable, efficient, and adaptive privacy-security infrastructure, which has the ability to operate in clouds, edges, and new quantum infrastructure.

6. Summary

This review critically analysed the dynamic situation surrounding privacy and security in cloud computing, and some of the threats, mitigation measures and emerging frameworks in 2020-25. The discussion has followed the timeline of security model evolution that started with the simple encryption and access control tools to more advanced systems like Zero Trust Architecture, blockchain-based authentication, and AI-based intrusion detection. It examined various attack vectors, data breaches, insider threats, virtualisation vulnerabilities and DDoS attacks that undermine confidentiality, integrity and availability in the cloud. The review has highlighted the importance of privacy-protecting approaches, including homomorphic encryption, differential privacy, and federated learning, as well as well-developed security models, including CSA guidelines and the ISO/IEC 27017. Irrespective of the significant progress, there are issues that still exist, especially with multi-cloud interoperability, regulatory compliance and performance scalability. Going forward, privacy and security frameworks should be combined with AI, confidential computing, and post-quantum cryptography in future studies because it is necessary to have adaptive, intelligent, and compliant cloud infrastructures. Broadly, this study has found out that maintaining privacy and security in cloud computing is an ongoing innovation, standard governance and shared implementation of the next generation protective models that balance usability, efficiency and trust in digital ecosystems.

References

1. Barcellos-Paula, L., Castro-Rezende, A. and Gil-Lafuente, A.M. (2024) 'Application of the Affinities Theory to the environmental sustainability of tourist destinations: the case of Ljubljana', *Cleaner and Responsible Consumption*, 14, 100216. <https://doi.org/10.1016/j.clrc.2024.100216>
2. Coupel, J. and Farheen, T. (2025) 'Security vulnerabilities in quantum cloud systems: a survey on emerging threats', *arXiv [Preprint]*, arXiv:2504.19064. <https://doi.org/10.48550/arXiv.2504.19064>
3. Davidson, S. (2025) 'Industry update: tourist destination management in Scotland set to suffer following the removal of funding – SkyeConnect National DMO Survey', *Scottish Tourism Alliance*. <https://scottishtourismalliance.co.uk/industry-update-tourist-destination-management-in-scotland-set-to-suffer-following-the-removal-of-funding-skyeconnect-national-dmo-survey/>
4. Faheem, A.L. (2023) 'IMTM successfully concludes the fourth edition of Sustainable Tourism Forum', *Visit Maldives Corporation*. <https://corporate.visitmaldives.com/news/imtm-successfully-concludes-the-fourth-edition-of-sustainable-tourism-forum/>
5. Fatima, E., Sumra, I.A. and Naveed, R. (2024) 'A comprehensive survey on security threats and challenges in cloud computing models (SaaS, PaaS and IaaS)', *Journal of Computing and Biomedical Informatics*, 7(1), pp. 537–544.
6. Gordon, R. (2025) 'Edinburgh crowned world's most sustainable travel destination', *The City of Edinburgh Council*. <https://www.edinburgh.gov.uk/news/article/13872/edinburgh-crowned-world-s-most-sustainable-travel-destination>

7. Government of India, Ministry of Tourism (2022) National strategy for sustainable tourism. New Delhi: Ministry of Tourism.
https://tourism.gov.in/sites/default/files/202205/National%20Strategy%20for%20Sustainable%20tourism_0.pdf
8. Hakone Tourist Association (2021) 'Hakone DMO certified guide training | Hakone Sustainable Tourism', Hakone-japan.com. <https://hakone-japan.com/sustainable-tourism/activity/530/>
9. Jackson, L.A. (2025) 'Community-based tourism: a catalyst for achieving the United Nations Sustainable Development Goals One and Eight', *Tourism and Hospitality*, 6(1), 29.
<https://doi.org/10.3390/tourhosp6010029>
10. Japan Tourism Agency (2024) 'The Tourism Nation Promotion Basic Plan | Tourism Nation Promotion Basic Law', Japan Tourism Agency.
<https://www.mlit.go.jp/kankocho/en/kankorikkoku/kihonkeikaku.html>
11. Kambala, G. (2025) 'Data privacy in cloud computing: a comparative study of privacy preserving techniques', *International Journal of Scientific Research and Management*, 13(1), pp. 1299–1316.
12. Kaul, D. and Khurana, R. (2021) 'AI to detect and mitigate security vulnerabilities in APIs: encryption, authentication, and anomaly detection in enterprise-level distributed systems', *Eigenpub Review of Science and Technology*, 5(1), pp. 34–62.
13. Lalli, M. (2024) 'The evolving role of DMOs in shaping tourism: superpowers required?', LinkedIn.
<https://www.linkedin.com/pulse/evolving-role-dmos-shaping-tourism-superpowers-required-mirko-lalli-vgpjf/>
14. MacEachern, J., MacInnis, B., MacLeod, D., Munkres, R., Jaspal, S.K., Kinay, P. and Wang, X. (2024) 'Destination management organizations' roles in sustainable tourism in the face of climate change: an overview of Prince Edward Island', *Sustainability*, 16(7), 3049. <https://doi.org/10.3390/su16073049>
15. McGuire, M.A. (2022) 'Today's destination management organization (DMO)', *Introduction to Hospitality*. <https://openwa.pressbooks.pub/introhospitality1/chapter/wa3-2/>
16. Mteti, S.H., Mpambije, C.J. and Manyerere, D.J. (2025) 'Unlocking cultural tourism: local community awareness and perceptions of cultural heritage resources in Katavi Region in southern circuit of Tanzania', *Social Sciences & Humanities Open*, 11, 101295.
<https://doi.org/10.1016/j.ssaho.2025.101295>
17. Rahdari, A., Keshavarz, E., Nowroozi, E., Taheri, R., Hajizadeh, M., Mohammadi, M., Sinaei, S. and Bauschert, T. (2025) 'A survey on privacy and security in distributed cloud computing: exploring federated learning and beyond', *IEEE Open Journal of the Communications Society*, 6, pp. 3710–3744.
<https://doi.org/10.1109/OJCOMS.2025.3560034>
18. Scotland (2024) Scotland Starts Here: A Responsible Tourism Strategy for the South of Scotland 2024–2034. South of Scotland Destination Alliance.
19. https://www.ssdalliance.com/wpcontent/uploads/2024/06/Tourism_Strategy_Final_v3.2_reduced.pdf
20. South African Government (2021) 'Tourism', South African Government. <https://www.gov.za/about-sa/tourism>
21. South of Scotland Destination Alliance (2025) 'Our current work'.
<https://www.ssdalliance.com/about-the-ssda/current-work/>
22. South of Scotland Destination Alliance (2025) 'Responsible Tourism Strategy'.
<https://www.ssdalliance.com/about-the-ssda/responsible-tourism-strategy/>
23. ST Costa Rica (2025) 'ST Costa Rica DMC strengthens its commitment to sustainability', Destination Management Company. <https://stcostaricadmc.com/st-costa-rica-dmc-strengthens-its-commitment-to-sustainability/>
24. UNCTAD (2025) Guiding principles for sustainable investment in tourism. UN Trade and Development. <https://unctad.org/publication/guiding-principles-sustainable-investment-tourism>
25. UNWTO (2023) Tourism: a driver for shared prosperity: key insights. World Tourism Organization. <https://www.wta-web.org/wp-content/uploads/2023/11/TOURISM-A-DRIVER-FOR-SHARED-PROSPERITY-Key-Insights.pdf>
26. UNWTO (2023) World Tourism Barometer: September 2023. UNWTO.
<https://en.unwto-ap.org/news/tourism-barometer-september-2023/>
27. UNWTO (2025) Guiding principles for sustainable investment in tourism: jointly developed by UN Trade and Development (UNCTAD) and the World Tourism Organization (UN Tourism). UN Trade and Development. <https://unctad.org/publication/guiding-principles-sustainable-investment-tourism>

28. Wagenseil, U., Wyss, M. and Huck, L. (2022) 'The case of sustainable tourism development in Alpine destinations: importance, implementation, and the role of the local DMO', *Tourism Planning & Development*, 21(6), pp. 659–681. <https://doi.org/10.1080/21568316.2022.2107561>
29. World, C. (2025) 'Maldives celebrates World Tourism Day 2025 with focus on sustainable transformation', *Maldives News Network*. <https://mnn.mv/featured/4521>