WITECH: Jurnal Teknologi Rekayasa Komputer dan Jaringan
Vol. 2 (No. 1), 2026: 35-46
https://journal.uwais.ac.id/index.php/witech/article/view/41

A Systematic Review of Security Challenges in Distributed Cloud Computing Based on the CIA Triad

Tinjauan Sistematis Tantangan Keamanan pada Cloud Computing Terdistribusi Berbasis CIA Triad

Dian Puspita Sari Andri[1], Rahmaniar[2]

[1]Universitas Negeri Makassar, Makassar, Indonesia; Email: dianpuspitasariandri@gmail.com
[2]Universitas Negeri Makassar, Makassar, Indonesia; Email: rahmaniarzahraqueen@unm.ac.id

Article History
Received: 2026-04-04
Revised: 2026-04-15
Accepted: 2026-04-20
Published: 2026-04-30

Keywords:
Distributed Systems;
System Security;
Confidentiality;
Availability;
Systematic Literature Review

Corresponding author:
rahmaniarzahraqueen@unm.ac.id

Paper type:
Research paper

POLITEKNIK WAHDAH ISLAMIYAH MAKASSAR
Program Studi Teknologi Rekayasa Komputer dan Jaringan, Politeknik Wahdah Islamiyah Makassar, Indonesia

Abstract

This study aims to identify and classify security challenges in distributed cloud computing systems based on the aspects of Confidentiality, Integrity, and Availability (CIA). The research employs a Systematic Literature Review with a narrative analysis of articles published between 2021 and 2026, resulting in 15 selected studies through a structured inclusion and exclusion process. The findings indicate that confidentiality challenges include data breaches, unauthorized access, and data leakage, primarily driven by multi-tenancy and weak access control. In terms of integrity, the main risks involve data manipulation, misconfiguration, and limitations in verification mechanisms within distributed systems. Meanwhile, availability is threatened by Distributed Denial of Service (DDoS) attacks, node failures, and architectural complexity. Various security methods have been proposed, including encryption, access control, intrusion detection systems, as well as advanced approaches such as risk assessment, Trusted Execution Environments, Information Flow Tracking, and Zero Trust Architecture.

Abstrak

Penelitian ini bertujuan mengidentifikasi dan mengklasifikasikan tantangan keamanan pada sistem cloud computing terdistribusi berdasarkan aspek Confidentiality, Integrity, dan Availability (CIA). Metode yang digunakan adalah Systematic Literature Review dengan analisis naratif terhadap artikel periode 2021–2026, menghasilkan 15 studi terpilih melalui proses seleksi berbasis kriteria inklusi dan eksklusi. Hasil menunjukkan bahwa tantangan confidentiality meliputi data breach, unauthorized access, dan data leakage akibat multi-tenancy dan lemahnya kontrol akses. Pada integrity, risiko utama adalah manipulasi data, kesalahan konfigurasi, dan keterbatasan verifikasi dalam sistem terdistribusi. Sementara itu, availability terancam oleh serangan Distributed Denial of Service (DDoS), kegagalan node, dan kompleksitas arsitektur. Berbagai metode keamanan diusulkan, termasuk enkripsi, kontrol akses, intrusion detection system, serta pendekatan lanjutan seperti risk assessment, Trusted Execution Environment, Information Flow Tracking, dan Zero Trust Architecture.

Cite this article:
Dian Puspita Sari Andri, Rahmaniar. (2026). A Systematic Review of Security Challenges in Distributed Cloud Computing Based on the CIA Triad. *WITECH: Jurnal Teknologi Rekayasa Komputer dan Jaringan*, 2(1), 35-46. https://journal.uwais.ac.id/index.php/witech/article/view/41.

1. Introduction

The development of distributed systems has become a cornerstone of modern computing architecture, particularly in cloud computing, distributed storage systems, and large-scale multi-party applications. According to Aloraini & Hammoudeh (2017), Distributing data and services across multiple nodes increases the system's flexibility, but also broadens the attack surface. This complexity is exacerbated by Mendez Mena et al. (2018), which shows that distributed systems are inherently more vulnerable to attacks due to the heterogeneity and openness of the network.

In efforts to protect distributed systems, the most commonly used security framework is Confidentiality, Integrity and Availability (CIA). The CIA triad is regarded as the cornerstone of information system security (Yee & Zolkipli, 2021). Furthermore, Sharma & Singh (2025) argue that failure to uphold any component of the CIA triad may directly compromise the reliability and service continuity within distributed computing environments.

In the context of cloud computing as the most dominant form of distributed systems, confidentiality challenges arise due to multi-tenant environments and the use of insecure Application Programming Interfaces (API). A study by Kausalye & Kumar Sharma (2021), indicates that data leakage remains a major risk in cloud storage. Furthermore, weak authentication mechanisms and inadequate access control also contribute to privacy breaches (Mandal & Khan, 2021). Beyond confidentiality, data integrity becomes a critical challenge in distributed systems, as data is replicated and processed across multiple distributed nodes. According to Brandenburger (2021) This condition increases the risk of data manipulation and data tampering attacks. These findings are consistent with the study by Tyagi et al.(2019), which states that conventional security mechanisms are often insufficient to ensure comprehensive data consistency and integrity in large-scale distributed environments.

Beyond the CIA triad, trust management also represents a fundamental challenge in distributed systems, particularly in multi-party and cross-organizational environments. The absence of a central authority in such distributed systems complicates the establishment of trust among participating entities, making trust a critical issue that necessitates the implementation of reliable decentralized security mechanisms (Howard et al., 2023). The availability aspect is equally critical in distributed systems. Distributed Denial of Service (DDoS) attacks and resource exhaustion significantly threaten service continuity (Mahato et al., 2024). In addition to cyberattacks, node failures and network disruptions also contribute to reduced service availability in distributed systems (Dorogovs, 2016).

Although numerous studies have examined security challenges in distributed systems from specific perspectives, research that systematically integrates and compares fundamental security challenges remains limited. Therefore, this study conducts a Systematic Literature Review (SLR) to identify and classify security challenges in distributed systems, with a focus on Confidentiality, Integrity, and Availability as the basis for analysis.

2. Literature Review

2.1. Distributed Systems and Security Implications

According to Tanenbaum & Van Steen, (2017), a distributed system is a collection of autonomous computers that communicate through a network and collaborate to achieve a common goal, appearing as a single integrated system to users. The main characteristics of distributed systems, such as concurrency, lack of a global clock, and

independent failures, require the system to operate without fully centralized control. This condition directly increases the complexity of designing security mechanisms, as a failure or compromise in one component can impact other components within the system.

In practice, these characteristics make distributed systems more vulnerable to security threats compared to centralized systems. A study by Tyagi et al. (2019) shows that the distribution of data and processes across multiple nodes expands the attack surface and complicates the implementation of consistent security policies. This finding is reinforced by Dashti et al. (2020), who state that infrastructure heterogeneity and network openness in distributed cloud environments increase the potential for exploiting security vulnerabilities. Furthermore Aloraini & Hammoudeh, (2017) emphasize that without well-coordinated security mechanisms, distributed systems are more likely to face higher risks of data leakage and security breaches.

2.2. The CIA Triad as a Fundamental Security Challenge

In the context of distributed system security, Tanenbaum and Van Steen emphasize that the primary objective of security is to protect system resources from unauthorized access, data manipulation, and service disruption, which directly reflects the principles of Confidentiality, Integrity, and Availability (CIA). The CIA triad is regarded as a fundamental framework for evaluating the security of modern information systems, including large-scale distributed systems.

Numerous studies indicate that most security issues in cloud computing and distributed systems can be traced back to failures in maintaining one or more aspects of the CIA triad. Mandal & Khan, (2021) identify CIA as a dominant framework for classifying cloud security threats, while distributed systems continue to evolve. Cloud security challenges are fundamentally manifestations of violations of CIA principles. This view is reinforced by recent studies that recognize the CIA triad as a core framework for analyzing security challenges in cloud computing(Paiman et al., 2025; Ali et al., 2026)

2.3. Confidentiality Challenges in Distributed Systems

Confidentiality is one of the most prominent challenges in distributed systems, as data is stored and accessed through shared infrastructures that are dynamic and open in nature. Aloraini & Hammoudeh, (2017) emphasize that multi-tenant environments in cloud computing increase the risk of data leakage due to resource sharing among users. Furthermore, Kausalye & Kumar Sharma, (2021), argue that the use of insecure APIs, along with weak identity management and access control mechanisms, constitutes a primary cause of confidentiality breaches in cloud storage systems.

The complexity of this challenge is further amplified in multi-party systems, where enforcing uniform security policies across organizations becomes difficult. This is consistent with the findings of Dashti et al., (2020) which indicate that differences in policies and trust levels among participating entities increase the risk of data confidentiality violations.

2.4 Challenges of Integrity, Availability and Trust in Distributed Systems

Integrity and availability represent major security challenges in distributed systems, as data and services are replicated and processed across multiple nodes that do not always operate within the same trust domain. Data replication, the absence of a global clock, and partial failures increase the risk of data manipulation, inconsistencies among nodes, and service disruptions, including Distributed Denial of Service (DDoS) attacks and resource exhaustion (Tyagi et al., 2019; Brandenburger, 2021; Mahato et al., 2024).

Beyond these technical challenges, multi-party distributed systems also face issues related to trust management due to the absence of a central authority. This condition complicates the establishment of trust among entities and necessitates the implementation of decentralized security mechanisms to ensure system reliability (Howard et al., 2023).

3. Research Method

3.1. Research Design and Literature Search Strategy

This study employs a Systematic Literature Review (SLR) approach with narrative analysis to identify and classify security challenges in cloud computing within distributed systems. This approach is chosen as it enables thematic synthesis of heterogeneous and conceptual literature, as recommended in prior methodological studies (Baumeister & Leary, 1997; Rother, 2007).

The literature search process was conducted systematically using the Publish or Perish software by retrieving scholarly articles indexed in the Scopus and Google Scholar databases. The search focused on publications published within the 2021–2026 timeframe. In addition, supplementary references were obtained from books relevant to the research topic. The keywords used in the search process were designed to identify studies addressing security challenges in cloud computing, particularly those related to the CIA Triad (confidentiality, integrity, and availability). The detailed search strings used for each database are presented in Table 1.

Table 1. Search Strings

Keywords	Scopus	Google Scholars
security challenges OR security threats	100	
confidentiality OR integrity OR availability OR CIA TRIAD	50	50
Total Articles	150	50

After the literature search process was completed, the next stage involved screening to determine articles relevant to the research topic. The screening was conducted based on eligibility criteria, including study characteristics, research population, interventions, context, and relevance to cloud computing security. The inclusion and exclusion criteria used in the literature selection process are presented in Table 2.

Table 2. Eligibility Criteria for Selecting Literature

Kriteria	Inclusion	Exclusion
Study Characteristic	Journal 2021–2026, English	Book
Population	Cloud computing systems, distributed cloud	Non-cloud systems
Intervention	Cloud security CIA triad Security threats	Non-security topics
Context	Distributed cloud environment	Traditional standalone systems
Outcome	Security challenges	No security analysis
Other	Relevant to CIA security in cloud	Duplicate or irrelevant studies

3.2. Study Selection

The literature selection process in this study follows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, as illustrated in

Figure 1. In the identification stage, a total of 200 articles were retrieved from searches across various databases and research registers. Subsequently, a deduplication process was conducted, during which 20 duplicate articles were manually removed, resulting in 180 articles for the initial screening stage. During the screening phase, these 180 articles were assessed based on their titles and abstracts to determine their relevance to the inclusion criteria.

The screening results indicated that 150 articles were excluded due to irrelevance to the research topic or failure to meet the predefined criteria. Consequently, 30 articles were advanced to the full-text retrieval stage. All identified articles at this stage were successfully obtained, with no inaccessible records. An eligibility assessment was then conducted on the 30 full-text articles. Based on this evaluation, 15 articles were excluded for several reasons: 10 articles were not aligned with the research focus, 1 article reported outcomes that did not match the study objectives, and 4 articles were published as books or conference proceedings that did not meet the inclusion criteria.

After completing all selection stages, a total of 15 articles met all inclusion criteria and were included in the systematic review. Furthermore, no ongoing studies or studies awaiting classification were identified at the final stage of the literature selection process.

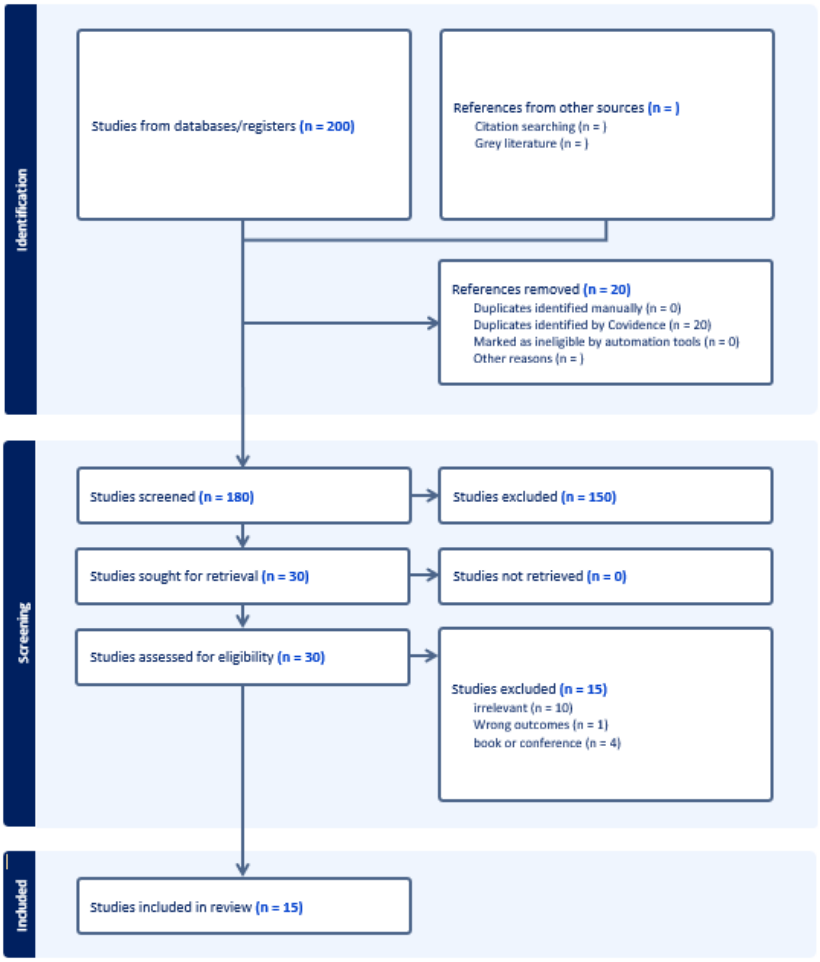

Figure 1. PRISMA Literature Review

3.3. **Research Questions**

The research methodology is designed to address the following research questions:

Research Question (RQ1):

What security challenges or threats affect the aspects of Confidentiality, Integrity, and Availability (CIA Triad) in distributed cloud computing systems?

Research Question (RQ2):

What security methods have been proposed in the literature to address security challenges in cloud computing systems based on the CIA Triad?

4. Results and Discussion

4.1. Results

Based on the results of the systematic literature analysis, security challenges in distributed systems can be classified into several main topics. Table 3 presents a summary of the selected studies based on the Systematic Literature Review criteria.

Table 3. Summary Table of Selected Studies Based on SLR Criteria

No	Author and Year	Title	Security Challenges	Findings
1	Payling-Nyhuus, (2025)	Recent Challenges and Solutions in Cloud Data Security	Unauthorised access, data exposure and inadequate monitoring	Confidentiality, Integrity, Availability
2	Neoaz, (2024)	A Comprehensive Review of Information Assurance in Cloud Computing Environments	Data breach, insider threat, DDoS, data loss, misconfiguration, shared responsibility issue	Cloud computing presents various security risks due to its distributed nature. Encryption, access control, monitoring and risk management are required to safeguard the CIA triad. The shared responsibility model and compliance are also key factors in cloud security.
3	Francis Ikenga-Metuh & Yeboah-Ofori, (2026)	Blockchain Security Using CIA for Secure Communication	MEV/BEV attacks, cross-chain exploit, cryptographic weaknesses, consensus attacks	The CIA triad is used to secure the blockchain through ECDSA, SHA-3 and distributed architecture. Modern threats such as MEV and bridge exploits highlight vulnerabilities in confidentiality, integrity and availability
4	Howard et al, (2023)	Confidential consortium framework: Secure multiparty applications with confidentiality, integrity, and high availability	Untrusted infrastructure, data exposure, integrity risk, node failure	The CCF framework demonstrates that CIA security in the cloud can be enhanced by reducing reliance on cloud providers through TEEs, immutable ledgers and consensus mechanisms, thereby ensuring confidentiality, integrity and availability in untrusted distributed cloud environments.

5	Devalla, (2024)	Continuous Verification of CIA in Microservices	API abuse, trust issues, dynamic scaling risk	The continuous verification approach enables real-time enforcement of the CIA principles through service meshes, API gateways and orchestration, thereby enhancing cloud security against dynamic threats such as API abuse and container exploits using a Zero Trust approach and anomaly detection
6	Ali et al., (2026)	Risk Assessment Methods in Cloud Computing	Data breach, DDoS, phishing, data leakage, multi-tenancy risk, unauthorized access	This study demonstrates that a variety of risk assessment methods are required to manage cloud security risks systematically, using a CIA triad-based approach to identify and mitigate security threats
7	Ahmadi, (2023)	Cloud Security Metrics and Measurement	Data breach, unauthorized access, multi-tenant risk, lack of standard metrics, dynamic environment	This study demonstrates that CIA-based cloud security assessment requires quantitative approaches such as encryption metrics, probabilistic models, and compliance frameworks such as ISO, NIST and CSA to systematically evaluate and enhance security within dynamic cloud environments.
8	Abdulsalam & Hedabou, (2021)	Security and Privacy in Cloud Computing: Technical Review	Data leakage, malicious insider, DDoS, API vulnerability, account hijacking, multi-tenancy risk	This study demonstrates that cloud security is affected by various threats modelled through the STRIDE framework, and requires adaptive approaches such as encryption, identity management, intrusion detection, and privacy-preserving techniques to comprehensively safeguard the CIA triad in a dynamic cloud environment.
9	Qasim et al., (2024)	Data Management Challenges in Cloud	Data security, privacy, data transfer issues, multi-cloud complexity	This study shows that the main challenges in cloud computing lie in data security and management, with solutions such as encryption, access control and multi-cloud strategies being necessary to enhance data security and efficiency within complex and dynamic cloud environments
10	Kumar et al., (2023)	SecureCloudX: Threshold Cryptography for Cloud	Unauthorized access, single point of failure	The SecureCloudX approach demonstrates that a combination of threshold cryptography and the Digital Signature Algorithm (DSA) can

				enhance cloud security by eliminating single points of failure and strengthening access controls and data integrity through key distribution and digital signatures.
11	Rahmika et al. (2025)	Cloud Governance Frameworks: CIA-Based Security and Compliance	Data breach, data leakage, API vulnerability, multi-tenancy, misconfiguration	The integration of the ISO/IEC 27001 and NIST CSF frameworks with the CIA approach enables adaptive cloud governance, enhancing security through risk-based policies, compliance and controls tailored to the type of cloud (public, private, hybrid)
12	Bhattacharjya (2022)	A Holistic Study on the Use of Blockchain Technology in CPS and IoT Architectures Maintaining the CIA Triad in Data Communication	DDoS, ARP spoofing, phishing, network congestion, single point of failure, privacy issues	Blockchain enhances CIA through decentralisation, cryptography and consensus mechanisms, but faces challenges such as scalability, resource constraints and governance
13	Kuštelega & Mekovec. (2024)	Migrating Data to the Cloud: An Analysis of Cloud Storage Privacy and Security Issues and Solutions	Data leakage, unauthorized access, DDoS, inference attack, side-channel attack, monitoring issue, trust issue, multi-cloud complexity	Cloud security requires a comprehensive approach based on the CIA triad, utilising encryption, access control, auditing, blockchain and privacy-preserving techniques. The main challenges stem from trust in cloud providers and the complexity of cloud systems
14	Alqahtani et al. (2024)	Cloud Security Using Fine-Grained Efficient Information Flow Tracking	Data leakage, unauthorized access, insider misuse, multi-tenancy risk, lack of trust, data flow vulnerability	The Information Flow Tracking (IFT) approach, delivered via the CloudMonitor framework, enhances cloud security by monitoring data flows, preventing data breaches, and strengthening confidentiality and integrity through data tagging and policy enforcement
15	Mehboob et al. (2024)	Detection of DDoS/DoS Attack Methodologies in Cloud Computing Network: A Survey	DDoS/DoS Attack Methodologies in Cloud Computing Network, a Survey DDoS/DoS, data leakage, data insecurity, network unavailability	DDoS attacks are a major threat to cloud availability. Various methods, such as machine learning, neural networks and intrusion detection systems (IDS), are used to detect and mitigate attacks in cloud environments

Table 3 presents a summary of the selected studies that have undergone the selection process based on the inclusion and exclusion criteria in the Systematic Literature Review (SLR). A total of fifteen relevant articles were analyzed to provide an

overview of various security challenges and key findings related to the implementation of Confidentiality, Integrity, and Availability (CIA triad) in cloud computing systems.

Based on the table, it can be observed that commonly identified security challenges include data breaches, unauthorized access, Distributed Denial of Service (DDoS) attacks, insider threats, as well as the complexity of multi-tenancy and dynamic cloud environments. In addition, several studies highlight risks such as misconfiguration, API vulnerabilities, and single points of failure that may affect the overall security of cloud systems. In terms of findings, most studies emphasize the importance of implementing security mechanisms such as encryption, access control, intrusion detection systems, as well as approaches based on risk assessment and security metrics. Furthermore, some studies propose advanced methods, including Trusted Execution Environments (TEE), threshold cryptography, digital signatures, and Zero Trust architecture to enhance security in distributed cloud environments.

4.2. Discussion

Based on the results presented in the table, the subsequent discussion is structured in accordance with the research questions.

Research Question (RQ1):
What security challenges or threats affect the aspects of Confidentiality, Integrity, and Availability (CIA Triad) in distributed cloud computing systems?

Based on the analysis of the fifteen selected studies, security challenges in distributed cloud computing systems can be classified into the aspects of Confidentiality, Integrity, and Availability (CIA triad). In terms of confidentiality, several studies indicate that the primary threats include data breaches, unauthorized access, and data leakage.

A study by Payling-Nyhuus, (2025) identifies weak monitoring mechanisms and access control as the main factors contributing to increased risks of data exposure in cloud environments. Furthermore, research by Alqahtani et al. (2024) emphasizes that data leakage and data misuse are major challenges in cloud computing due to the complexity of data flows across services and multi-tenant environments. This demonstrates that the shared-resource nature of cloud computing significantly increases risks to confidentiality.

Regarding integrity, several studies highlight that the main threats are related to data manipulation, misconfiguration, and weak data verification mechanisms. Howard et al. (2023) explain that maintaining data integrity in cloud environments is more challenging because data is processed on infrastructures that are not fully trusted (untrusted infrastructure), thereby requiring additional mechanisms to ensure data correctness. In addition, Ali et al. (2026) emphasize that the complexity of cloud systems, including virtualization and multi-tenancy, increases risks to data integrity and necessitates systematic risk assessment approaches to identify potential threats.

Meanwhile, in terms of availability, the most dominant threat is Distributed Denial of Service (DDoS) attacks, which can disrupt the availability of cloud services. Mehboob et al. (2024) state that DDoS attacks are among the primary threats in cloud computing, directly affecting service availability and potentially causing significant operational losses. Moreover, node failures and the complexity of distributed architectures can also lead to service disruptions, particularly in dynamic multi-cloud environments. The analysis indicates that security challenges in cloud computing arise not only from external attacks but also from internal system complexities such as multi-tenancy, virtualization, and the dynamic nature of cloud environments.

Research Question (RQ2):

What security methods have been proposed in the literature to address security challenges in cloud computing systems based on the CIA Triad?

Based on the analyzed studies, various security methods have been proposed to address security challenges in cloud computing using a CIA triad-based approach. One of the most commonly applied methods is the use of cryptographic and encryption techniques to ensure data confidentiality and integrity. Research by Francis Ikenga-Metuh and Yeboah-Ofori (2026) demonstrates that the use of cryptographic algorithms such as ECDSA and SHA-3 can enhance communication security in distributed systems by preserving data integrity and confidentiality. In addition, threshold cryptography is also employed to reduce the risk of a single point of failure in cloud systems.

Access control and authentication mechanisms are key solutions for addressing unauthorized access. A study by Payling-Nyhuus (2025) emphasizes the importance of implementing access control and authentication as part of an effective cloud security strategy. This approach aims to ensure that only authorized users can access data, thereby reducing the risk of confidentiality breaches. Furthermore, security framework-based approaches and risk assessment methods are widely utilized. Research by Ali et al. (2026) indicates that frameworks such as ISO/IEC 27001, NIST, and OCTAVE can support systematic and structured cloud security risk management Advanced approaches have also emerged, including Trusted Execution Environment (TEE), Information Flow Tracking (IFT), and Zero Trust Architecture. Alqahtani et al. (2024) how that IFT is effective in monitoring data flows and preventing data leakage, while Howard et al. (2023) highlight that TEE and immutable ledger technologies can enhance security in untrusted cloud infrastructures.

Overall, no single method is capable of addressing all cloud security challenges; therefore, a multi-layered security approach is required, integrating encryption, access control, monitoring, and risk management in a comprehensive manner.

5. Conclusion

Based on the results of the Systematic Literature Review (SLR) of fifteen studies, it can be concluded that security in distributed cloud computing systems is a complex and multidimensional issue influenced by various technical and architectural factors. The analysis of Research Question 1 (RQ1) indicates that the primary challenges in cloud computing are related to the aspects of Confidentiality, Integrity, and Availability (CIA triad), where threats such as data breaches, unauthorized access, data leakage, and Distributed Denial of Service (DDoS) attacks emerge as dominant issues. In addition, cloud characteristics such as multi-tenancy, virtualization, and dynamic environments further increase system vulnerabilities.

Furthermore, the analysis of Research Question 2 (RQ2) reveals that various security methods have been proposed to address these challenges, ranging from conventional approaches such as encryption, access control, and intrusion detection systems to advanced approaches such as risk assessment frameworks, Trusted Execution Environments (TEE), Information Flow Tracking (IFT), and Zero Trust Architecture. These findings indicate that no single method is sufficient to ensure comprehensive security, thereby necessitating a multi-layered security approach that integrates various techniques and frameworks in a comprehensive manner.

Overall, the CIA triad remains a fundamental foundation for ensuring security in cloud computing. However, to address continuously evolving threats, adaptive, integrated, and technology-driven approaches are required. Therefore, future research

should focus on developing more intelligent security solutions capable of adapting to the increasingly complex dynamics of cloud environments.

References

Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: Technical review. *Future Internet*, *14*(1), 11.

Ahmadi, S. (2023). Cloud security metrics and measurement. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (Online)*, *2*(1), 93–107.

Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2026). Information security risk assessment methods in cloud computing: Comprehensive review. *Journal of Computer Information Systems*, *66*(1), 123–150.

Aloraini, A., & Hammoudeh, M. (2017). A survey on data confidentiality and privacy in cloud computing. *Proceedings of the International Conference on Future Networks and Distributed Systems*, 1–7.

Alqahtani, F., Almutairi, M., & Sheldon, F. T. (2024). Cloud Security Using Fine-Grained Efficient Information Flow Tracking. *Future Internet*, *16*(4), 110. https://doi.org/10.3390/fi16040110

Baumeister, R. F., & Leary, M. R. (1997). Writing Narrative Literature Reviews. *Review of General Psychology*, *1*(3), 311–320. https://doi.org/10.1037/1089-2680.1.3.311

Bhattacharjya, A. (2022). A holistic study on the use of blockchain technology in CPS and IoT architectures maintaining the CIA triad in data communication. *International Journal of Applied Mathematics and Computer Science*, *32*(3), 403–413. https://doi.org/10.34768/amcs-2022-0029

Brandenburger, M. (2021). *Securing Data Integrity from Cloud Storage to Blockchains* [PhD Thesis]. Dissertation, Braunschweig, Technische Universität Braunschweig, 2020.

Dashti, W., Qureshi, A., Jahangeer, A., & Zafar, A. (2020). Security challenges over cloud environment from service provider prospective. *Cloud Computing and Data Science*, *1*(1), 12–20.

Devalla, S. (2024). From principles to practice: Continuous verification of the CIA triad in distributed microservice system. *Journal of Recent Trends in Computer Science and Engineering (JRTCSE)*, *12*(2), 82–97.

Dorogovs, P. (2016). E-Service Security Challenges: Availability, Integrity, Confidentiality. *Baltic Journal of Modern Computing*, *4*(1).

Francis Ikenga-Metuh, C., & Yeboah-Ofori, A. (2026). Blockchain security using confidentiality, integrity, and availability for secure communication. *Blockchains*, *4*(1).

Howard, H., Alder, F., Ashton, E., Chamayou, A., Clebsch, S., Costa, M., Delignat-Lavaud, A., Fournet, C., Jeffery, A., Kerner, M., & others. (2023). Confidential consortium framework: Secure multiparty applications with confidentiality, integrity, and high availability. *arXiv Preprint arXiv:2310.11559*.

Kausalye, S. S., & Kumar Sharma, S. (2021). Data confidentiality in cloud storage. A survey. *Recent Trends in Intensive Computing*, 653–660.

Kumar, S., Chuli, A., Raj, S., Jain, A., & Aju, D. (2023). SecureCloudX: An Innovative Approach to Enhance Data Security Through Advanced File Encryption. *International Conference on Optimization and Data Science in Industrial Engineering*, 77–97.

Kuštelega, M., & Mekovec, R. (2024). Migrating data to the cloud: An analysis of cloud storage privacy and security issues and solutions. *CroDiM: International Journal of Marketing Science*, *7*(1), 89–98.

Mahato, S., Sah, R., & Sapkota, S. (2024). Cybersecurity Challenges and Threats: The Risks in Digital World. *International Journal of Advanced Research in Science, Communication and Technology*, 651–655.

Mandal, S., & Khan, D. A. (2021). Comprehensive Survey of Security Issues & Framework in Data-Centric Cloud Applications. *Journal of Engineering Science & Technology Review*, *14*(1).

Mehboob, T., Sumra, I. A., & Shahzadi, I. (2024). Detection of DDoS/DoS Attack Methodologies in Cloud Computing Network: A Survey. *Journal of Computing & Biomedical Informatics*, *8*(01). https://jcbi.org/index.php/Main/article/view/191

Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, *27*(3), 162–182.

Neoaz, N. (2024). A Comprehensive Review of Information Assurance in Cloud Computing Environments. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(6), 715–725.

Paiman, M. A., Afghan, S., & Himmat, A. K. (2025). A Comprehensive Study of Information Security Principles, Threats, and Organizational Protection Measures. *LogicLink: Journal of Artificial Intelligence and Multimedia in Informatics*, *2*(2), 198–206. https://doi.org/10.28918/logiclink.v2i2.13154

Payling-Nyhuus, S. (2025). *Recent challenges and solutions in cloud data security: A literature review*.

Qasim, A., Rahim, R., Bodnar, B., Salman, M., & Mustafa, M. (2024). Data management challenges and solutions in cloud-based environments. *Internet*.

Rahmika, A. R., Akbar, M., Jayanto, D. L., & Bu'tu, J. R. (2025). Cloud Governance Frameworks: CIA-Based Security and Compliance. *Journal of Embedded Systems, Security and Intelligent Systems*, *6*(3), 379–389. https://doi.org/10.59562/jessi.v6i3.9541

Rother, E. T. (2007). Revisão sistemática X revisão narrativa. *Acta Paulista de Enfermagem*, *20*(2), v–vi. https://doi.org/10.1590/S0103-21002007000200001

Sharma, R. K., & Singh, A. (2025). Cloud Security: An In-Depth Examination of Confidentiality, Integrity, and Availability Challenges and Future Trends. *Journal of Survey in Fisheries Sciences*. https://doi.org/10.53555/hp4eqw19

Tanenbaum, A. S., & Van Steen, M. (2017). *Distributed systems*. CreateSpace Independent Publishing Platform.

Tyagi, M., Manoria, M., & Mishra, B. (2019). Survey and Analysis for Achieving the Security of Data in Cloud. *International Journal of Applied Engineering Research*, *14*(20), 3954. https://doi.org/10.37622/IJAER/14.20.2019.3954-3959

Yee, C. K., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, *8*(2), 34–42.