Open Access Research Journal of
Multidisciplinary Studies
Journals home page: https://oarjpublication/journals/oarjms/
ISSN: 2783-0268 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(REVIEW ARTICLE)

Check for updates

A Systematic Review of Artificial Intelligence, Cloud and Security Technologies

Ibrahim Rashid Abdullahi *

Faculty of Science, department of computer science Somali National university.

Open Access Research Journal of Multidisciplinary Studies, 2026, 11(01), 014-025

Publication history: Received on 20 December 2025; revised on 25 January 2026; accepted on 28 January 2026

Article DOI: https://doi.org/10.53022/oarjms.2026.11.1.0015

Abstract

The widespread use of the cloud computing and artificial intelligence has changed the contemporary digital infrastructures and exposed them to the complex cyber security threats at the same time. The review is the synthesis of the recent studies on artificial intelligence, cloud computing, and security technologies, in particular, the use of AI-based mechanisms in protecting the cloud infrastructure. The review examines articles published in the year 2025-2026 that reflect AI techniques in cloud settings, developing cloud architectures, and security issues and intelligent defense systems. The results denote that the machine learning and deep learning models have a profound impact on the performance of cloud through predictive analytics, resource optimization, and real-time threat detection. The use of advanced security mechanisms, such as Zero Trust models, closed-loop defense mechanisms, multimodal telemetry fusion, and AI-integrated cryptographic techniques, is always effective in dynamic and distributed cloud environments than the traditional perimeter-based models. Nonetheless, the issues concerning governance, standardization, explainability, and AI models protection remain. On the whole, the review demonstrates the obvious tendency towards adaptive and intelligent and integrated security models needed to develop resilient and trustful cloud ecosystems and outlines major trends in the future research and practice.

Keywords: Artificial Intelligence; Cloud Computing; Cybersecurity; AI-Driven Security; Cloud Infrastructure

1. Introduction

The high rate of digital technology development has fundamentally changed contemporary information systems by reconstituting the manner in which organizations handle data, provide services and the manner in which they guard digital assets [1]. Three key issues have become important parts of modern digital infrastructures artificial intelligence (AI), cloud computing, and cybersecurity. Cloud computing provides scalable, flexible, and cost-effective computing capability and AI can be used to perform intelligent automation, enhanced analytics, and adaptive decision making [2]. Meanwhile, security technologies are crucial in securing cloud-based systems against highly advanced cyber-attacks. The intersection of AI, cloud, and security technologies has thus become the major focus of the resiliency and reliability of the contemporary digital ecosystems [3].

The use of cloud computing has become popular in a wide variety of industries including healthcare, finance, education, manufacturing and government because it has the potential to aid in the digital transformation and innovation. Nonetheless, the transfer of applications and data to the public, private, and hybrid cloud environments has greatly increased the cyberattack surface [4]. The threats to cloud infrastructures are numerous, and they include data breaches, misconfigurations, insider attacks, distributed denial-of-service (DDoS) attacks, and advanced persistent threats. Conventional security methods that use static rules and network borders have failed to effectively deal with such risks in dynamic and distributed cloud systems [5].

* Corresponding author: Ibrahim Rashid Abdullahi

1.1. Convergence of Artificial Intelligence, Cloud, and Security Technologies

Artificial intelligence has been gradually incorporated in cloud security solutions to overcome the weaknesses of the traditional security measures. Machine learning and deep learning, which are AI-based solutions, have facilitated automatic threat detection, anomaly detection, predictive risk assessment, and dynamic incident response [6]. AI-based security models can also learn on large amounts of data, detect intricate attack patterns, and evolve to different threat landscapes unlike rule-based systems. Consequently, artificial intelligence has been extensively used in intrusion detection systems, threat intelligence systems, identity and access management, encryption systems, and security orchestration and response automation systems within cloud-based systems [7].

Although these benefits exist, the use of AI in the cloud environment has brought new security and privacy issues. The threats of data poisoning, adversarial attacks, model inversion, and unauthorized access are also directed at AI systems themselves [8]. Moreover, the mass gathering, storage, and processing of sensitive information to train AI and make inferences is a major issue that attracts critical concerns of confidentiality, integrity, availability, and regulatory compliance. These difficulties have motivated research in to secure AI architectures, privacy-preserving computation, blockchain-based verification mechanisms, and quantum-resistant cryptographic solutions to build more trust in cloud-based AI systems [9].

The combination of AI, cloud computing, and security technologies has thus emerged as an eminent research topic. Many papers have put forward innovative solutions, such as Zero Trust Architectures, AI-improved threat intelligence, the lightweight detection models of resource-constrained architectures, block chain-based data protection systems, and adaptive closed-loop security systems [10]. Nonetheless, the current literature is still rather fragmented, with a variety of methodologies, evaluation measures, and situations of application. It is this fragmentation that may support the systematic review as a means of uniting the findings, pinpointing the gaps in research and offering a more global perspective of what is going on.

This paper, therefore, provides a review of the artificial intelligence, cloud and security technologies and specifically AI-assisted security controls of cloud infrastructure. The purpose of the review is to review current frameworks and models, their effectiveness, as well as highlight the emerging tendencies and directions of research in the future. This review has the potential to assist researchers, practitioners, and policymakers in developing secure, intelligent, and resilient cloud-based systems that could overcome the transforming cybersecurity scenario by synthesizing existing knowledge.

2. Literature review

2.1. Artificial Intelligence Techniques and Their Applications in Cloud Environments

The use of artificial intelligence in cloud-based environments allows processing of data, automation and making decisions using intelligent computing resources that are available on a scale. The cloud platforms can host AI applications that include machine learning, deep learning, predictive analytics, and intelligent resource management and enable the efficient processing of big data and real-time services. The research papers that had been published recently had proven the increased significance of artificial intelligence in prediction, automation, and optimization of performance in cloud, edge, and data-intensive systems. By suggesting a hybrid model consisting of SelectKBest feature selection, GRU-based sequence model prediction, and machine learning packs (RF, KNN, and SVM), Aldomi et al., (2026) [11] had highlighted proactive predictability of failure in cloud computing with high multi-class prediction accuracy on Google cluster traces. Simultaneously, articles by Tarapder et al., (2026) [12] and Carlisle et al., (2026) [13,14] had demonstrated that hybrid AI instances comprising deep learning, anomaly detection, graph-based reasoning, fog cloud computing, and blockchain had demonstrated much better intrusion detection accuracy, scalability, and auditability in IoT and healthcare settings. On top of cloud and security applications, Jesus et al., (2026) [15] and Cai et al., (2026) [16] had already implemented deep learning and machine learning algorithms, including YOLO, PointNet++, and random forest regression, to industrial material monitoring and global methane emission analysis, allowing the proper estimation of volume, identification of hotspots, and policy-relevant environmental data in accordance with Industry 4.0 and sustainability goals.

In addition to these technical contributions, a number of authors had also noted the significance of architectural maturity, system integration and governance as the key enablers of successful AI deployment. Ajayi et al., (2026) [17] had established that industrial robot Ultra-low-latency control performance had been strongly predicted by Edge AI automation maturity especially local inference, controller integration, and reliability or failover preparedness. Within the healthcare sector, Ponnumani et al., (2026) [18] had already introduced a generative AI pipeline that had effectively

retrieved structured clinical information in electronic health records at scale without jeopardizing or sacrificing its cost-efficiency. Institutional and strategic Views, both Baranyi et al., (2026) [19] and Habib Zadeh Khiyaban et al., (2026) [20] had examined the ethical, organizational, and governance aspects of AI adoption on academic research and banking, highlighting the necessity of policy preparation, transparency, and human-oriented design. Taken together, these studies had sugg

ested that there was a move towards integrated, trustworthy, and ethically sound AI architectures that took into account a balance between technical performance and organizational preparedness and societal responsibility. Table 1 shows the summary of above studies.

Table 1 Overview of AI-based studies across multiple application domains

Ref.	Authors	Domain / Context	Methodology / Framework	Dataset / Sample	Key Findings
[1]	Aldomi et al., (2026)	Cloud Computing	SelectKBest + GRU feature extraction with RF, KNN, and SVM classifiers	Google Cluster Traces	The proposed GRU-based framework achieved 97.7% accuracy, with GRU–RF yielding the best performance (RMSE = 0.1415, Fail-class F1 = 0.99, AUC > 0.98), enabling early and accurate task failure prediction.
[2]	Tarapder et al., (2026)	Edge AI in Industrial Robotics	Quantitative, cross-sectional regression analysis	N = 162 practitioners	Edge AI automation maturity significantly predicted ultra-low-latency control performance (R^2 = 0.46), with local inference, controller integration, and reliability identified as key contributors.
[3]	Carlisle et al., (2026)	Healthcare / Clinical Informatics	Generative AI pipeline (UODBLLM) using XML prompts and LLM integration	1,800 MRI reports	The system achieved 100% completion with low processing cost and time, successfully extracting 16 structured clinical elements while maintaining HIPAA-compliant security.
[4]	Jesus et al., (2026)	Academic Research	Qualitative exploratory study using thematic analysis	Faculty and researchers (Philippines)	The study developed a conceptual framework highlighting ethical, strategic, and institutional dimensions required for responsible AI integration in academic research.
[5]	Cai et al., (2026)	Construction / Industry 4.0	Hybrid RGB camera + LiDAR with YOLOv5 and PointNet++	On-site bulk material datasets	The proposed method achieved 81.6% object recognition precision and less than 8% volume estimation error, outperforming traditional measurement techniques.
[6]	Ajayi et al., (2026)	Environmental Monitoring	Random forest regression with geospatial and time-series analytics	Global and U.S. methane datasets	The model achieved MAE = 2.71 and R^2 = 0.81, identifying the energy sector as the dominant methane contributor and supporting AI-driven mitigation strategies.

[7]	Ponnumani et al., (2026)	IoT Security	VAE + Isolation Forest + GAT hybrid framework	CIC IoT-DIAD 2024	The framework achieved 99.08% accuracy and 98.03% F1-score, demonstrating superior scalability, interpretability, and multi-class intrusion detection performance.
[8]	Baranyi et al., (2026)	Smart Rehabilitation	AIRS framework using RT-3DR and Vision-Language Models	263 rehabilitation videos	The system provided accurate 3D and language-based feedback for home rehabilitation, improving compliance, privacy, and adaptability across rehabilitation scenarios.
[9]	Habib Zadeh Khiyaban et al., (2026)	Banking Sector	Systematic literature review (2020–2025)	21 peer-reviewed studies	AI adoption enhanced efficiency, personalization, and risk management, while challenges related to governance, transparency, and cybersecurity persisted.

The figure 1 presented a comparative analysis of the performance of the artificial intelligence models in various domains of application. Predicting the cloud failures, IoT intrusion detection, and healthcare IoT intrusion detection had very high predictive capabilities with accuracy levels near or above 97 which showcases the strength of AI-based models to predict in a structured and security-prone setting. Conversely, prediction of methane emissions displayed relatively inferior performance which demonstrates the complexity as well as variability of environmental data. In general, the figure demonstrated the efficiency of AI methods in various fields and showed differences in performance in domains.

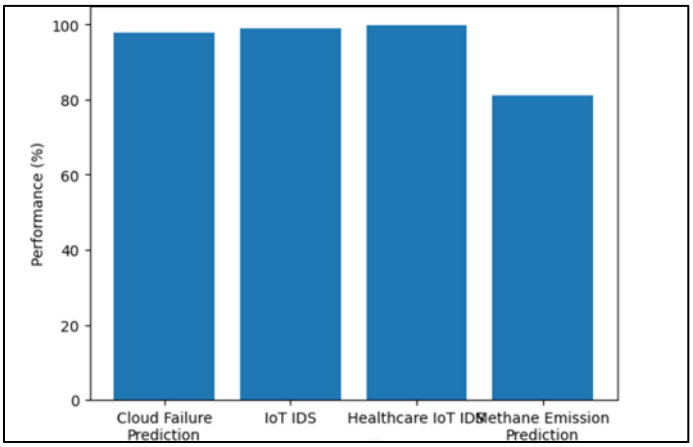

Figure 1 Comparative Performance of AI Models Across Studies

The figure 2 showed the distribution of the reviewed studies by the domains of applications. The topic of IoT security became the most popular aspect to be examined meaning that there is high research interest in the field of connected system protection. The next was Healthcare and Industry 4.0, which shows an increasing level of interest in intelligent automation and data-driven decision-making. Cloud computing, environmental applications, academia, and banking, in turn, were less represented in the studies. This distribution implied an uneven distribution of the available research interest and the possibilities of the further research of the unexplored areas.

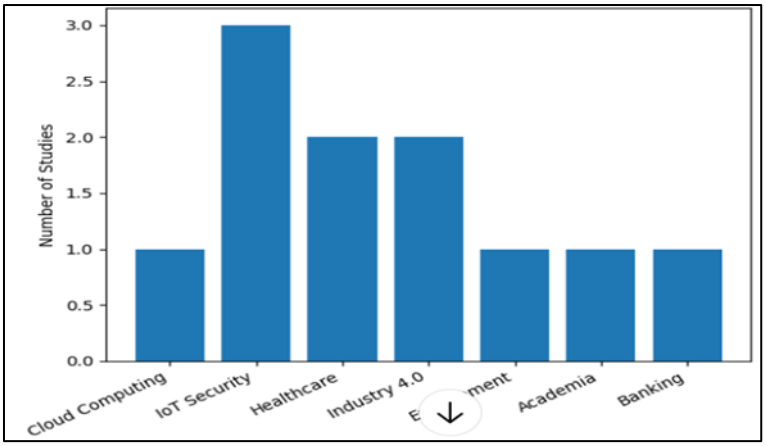

Figure 2 Distribution of Application Domains in Reviewed Literature

2.2. Cloud Computing Architectures and Emerging Security Challenges

Cloud computing models have been developed to accommodate scalability and flexibility by endorsing single-cloud models to heritage multi-cloud and hybrid, edge-integrated multi-cloud models. Nevertheless, this development has brought forth new security issues like privacy threats of data, complexities in identity and access controls, cross-platform threats, and compliance concerns of the regulations. The dynamic and distributed characteristics of contemporary cloud facilities are an additional factor that exposes the system to cyber threats necessitating advanced security protocols and consistent monitoring. The recent research on cloud computing was mainly aimed at enhancing security, privacy preservation and intrusion detection in the becoming complicated cloud set ups. Cyril (2026) [21] introduced a multi-tenant cloud storage model with homomorphic encrypted data with a verification approach that allows verification using blockchain to guarantee integrity of data without exposing sensitive data, which contributes to tenant isolation and confidentiality issues. On the same note, Olusesi et al., (2026) [22] came up with a new intrusion detection system based on Support vector machine in collaboration with Fast firefly algorithm, which improved the relationship between the packets delivery, throughput, energy consumption, and detection rate in cloud networks. Suresh et al., (2026) [23] continued to develop the field of cloud security by proposing an unsupervised intrusion diagnosis model built upon the representation learning using autoencoders and the density-based clustering, which are effective in processing high-dimensional, unbalanced traffic and providing high levels of anomaly detection and multiclass classification. The research as a whole proved that sophisticated cryptographic algorithms and smart learning systems contributed greatly to the safety and stability of clouds in the face of dynamic cyber attacks.

Besides security mechanisms, some studies focused specifically on clouds' adoption, resources' optimization, and new models of deployment. The intentions of the users concerning the adoption of premium clouds' resources were examined by Diunugala et al., (2026) [24], and the results indicated that influences are given when focusing on usefulness, trust, subjective norms, and attitudes; meanwhile, concerns about privacy positively affected attitudes. Moreover, the emerging trends of clouds and some of their issues, such as multi-cloud computing, hybrid clouds, serverless computing, and AI within clouds, are presented and discussed by Ware et al. (2025) [25], concerning issues such as data privacy and compliance with laws and lock-in. Yedalla and Jayasudha (2025) [26] highlighted the importance of the security framework in the cloud environment, mentioning the key security features, namely, identity management, encryption services, and AI-enabled threat protection. Further, the article presented by Chaudhary et al., (2025) [27] introduced AI-based resource management using model order reduction techniques combined with queuing theory techniques, reflecting better response time, throughput, energy consumption, and reliability in the system design. Finally, the article presented by Younus et al., (2025) [28] presented the application of cloud technology in the e-government system, highlighting the growing focus on cloud technology in the domain due to better scalability features in the services rendered in the system, despite the security challenges faced in terms of data security and privacy.

Table 2 Summary of Literature on Cloud Computing

Ref. No.	Author(s) & Year	Focus Area	Methodology / Technique Used	Key Findings / Contributions
[11]	Cyril (2026)	Data privacy and integrity in multi-tenant cloud storage	CKKS homomorphic encryption combined with blockchain-based verification	Achieved strong privacy preservation (score 9.7) with efficient integrity verification, ensured tenant isolation, and provided cryptographic guarantees suitable for enterprise-scale deployments
[12]	Olusesi et al., (2026)	Intrusion detection in cloud environments	Support Vector Machine with Fast Firefly Algorithm (SVM–FFA)	Improved packet delivery ratio, throughput, energy efficiency, and detection accuracy compared to existing IDS methods
[13]	Suresh et al., (2026)	Unsupervised cloud intrusion diagnosis	Dual-stage autoencoder and density-based clustering	Achieved 99.46% anomaly detection accuracy and 98.79% multiclass classification accuracy under highly imbalanced cloud traffic
[14]	Diunugala et al., (2026)	User adoption of premium cloud services	CV-SEM and Artificial Neural Networks (ANN)	Identified perceived usefulness, trust, subjective norms, and attitudes as key predictors of adoption; ANN achieved over 88% prediction accuracy
[15]	Ware et al., (2025)	Emerging cloud computing trends and challenges	Conceptual and analytical review	Highlighted trends such as multi-cloud, hybrid cloud, serverless computing, and AI integration, while identifying privacy, compliance, and vendor lock-in as key challenges
[16]	Yedalla & Jayasudha (2025)	Application security in multi-cloud environments	Critical literature analysis	Emphasized IAM, encryption, AI-driven threat detection, and regulatory compliance as essential for improving multi-cloud security
[17]	Chaudhary et al., (2025)	AI-driven resource management in cloud computing	AI integration with model order reduction and queueing theory	Reduced response time by 50%, improved throughput and energy efficiency, and achieved high system reliability (99.99% uptime)
[18]	Younus et al., (2025)	Cloud computing in e-government services	Systematic literature review with bibliometric analysis (CiteSpace)	Demonstrated growing adoption of cloud computing in e-government due to scalability and efficiency, despite ongoing data security and privacy concerns

Figure 3 depicted the distribution of the highlighted studies of cloud computing, published in 2025 and 2026. It was observed that slightly more research studies in the field of cloud computing were published in 2025 in comparison to the research studies published in 2026. However, this demonstrated constant scholarly interest in the field of cloud computing during both periods, including the associated issues of security, privacy, and optimization, and the adoption of associated challenges pertaining to the field of cloud computing.

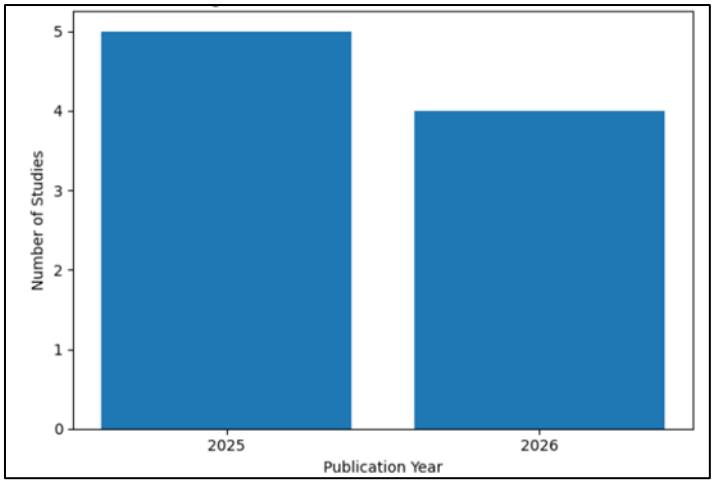

Figure 3 Year Wise Distribution of Studies

2.3. AI-Driven Security Mechanisms for Cloud Infrastructure Protection

AI-based security mechanisms for protecting cloud infrastructures incorporate artificial intelligence, machine learning, and deep learning models to keep cloud infrastructures under constant surveillance, analysis, and instant response to cybersecurity threats. The mechanisms have also improved the detection of security threats, anomalies, and adaptive security responses, all within the ever-changing environments of cloud infrastructures. Thus, AI-based security mechanisms have improved cloud security through the integration of AI with various security models. The various research papers examined have all highlighted the need, even through consensus, that perimeter-based security mechanisms are not effective for protecting AI-based, cloud-infrastructure-based cyber infrastructures. Maqbool et al., (2026) [29] had also proven in their research that the incorporation of Zero Trust Architecture with AI threat intelligence and secure hybrid cloud design can overcome the challenges of access governance, lateral movement, and operational resiliency very effectively in the hybrid cloud environment. Ang et al., (2026) [30] had also proposed a multilayered adaptive framework of security in the banking industry, where the combination of next-generation firewalls, hybrid intrusion, and AI analytics resulted in high accuracy and minimum false positives in detecting and preventing cyberattacks, which were in adherence to the current industry standards and regulations. Mollah et al., (2025) [31] had again demonstrated the importance of AI-based closed-loop defense capabilities in the cloud environment by showing that the implementation of multimodal telemetry, hybrid ensemble, and AI-based recalibration improved the accuracy of threat detection, minimised the response time, and resulted in stability in the endpoint environment. Kezron et al., (2025) [32] had further demonstrated the importance of AI, Zero Trust, and scalable industry-standard-based CSI in SMEs by showing that the incorporation of scalable industry-standard CSI resulted in improved threat detection and response capabilities, despite the problems associated with limited resources and threat environment.

In parallel, several publications aimed to improve data protection schemes by leveraging sophisticated AI systems, along with cryptographic schemes, for data protection schemes and real-time detection systems for AI systems and cloud environments. In one relevant direction, Chen et al., (2026) [33] proposed a Secure AI DST scheme based on a combination of a hybrid approach, a blockchain scheme, and deep learning intrusion classification, achieving high integrity, restricted access, and low computational overhead. Additionally, real-time AI schemes for improving light-weight AI systems were examined by Alzaylaee et al., (2026) [34], where the effectiveness of AI architectures, such as MobileNetV2, Optimized CNN-LSTM, and SHAP, was also examined. Moreover, Patel et al., (2025) [35] focused on improving future-proofing for various AI and cloud environments by proposing various AI-driven schemes for improving data encryption schemes, achieving better performances than traditional cryptography schemes. Finally, Surya et al., (2025) [36] demonstrated the superiority of deep learning multi-layer AI schemes for improving data detection schemes, compared to traditional machine learning schemes, for various complex AI schemes, achieving better performances than traditional machine learning schemes for distinct AI system environments.

Table 3 Summary of Related Cybersecurity Studies

Ref. No.	Author(s) & Year	Focus Area / Context	Methodology / Framework	Key Findings	Key Contribution
[19]	Maqbool et al. (2026)	Cloud-centric & AI-driven infrastructures	Zero Trust Architecture integrated with AI-driven threat intelligence	Improved access governance, reduced lateral movement, enhanced operational resilience in hybrid cloud environments	Demonstrated the effectiveness of combining Zero Trust and AI for modern cloud security
[20]	Ang et al. (2026)	Banking sector cybersecurity	Multilayer adaptive security framework (next-generation firewalls, hybrid IDS, AI analytics)	Achieved high detection accuracy with minimal false positives while maintaining regulatory compliance	Validated adaptive, AI-based security architectures for regulated financial systems
[21]	Mollah et al. (2025)	AI-driven cloud defense	Closed-loop security using multimodal telemetry fusion and hybrid ensemble models	Improved threat detection accuracy, reduced response time, and stabilized performance under evolving threats	Highlighted the importance of drift-aware, self-adaptive cloud security mechanisms
[22]	Kezron et al. (2025)	Cybersecurity for SMEs	Scalable, standards-aligned Zero Trust and AI lifecycle security architecture	Enhanced detection capability, response efficiency, and regulatory compliance despite resource constraints	Extended advanced AI–Zero Trust security models to small and medium enterprises
[23]	Chen et al. (2026)	Secure AI data storage and transmission	Secure AI-DST framework integrating hybrid encryption, blockchain, and deep learning-based intrusion detection	Ensured high data integrity, reduced unauthorized access, and maintained low computational overhead	Integrated cryptography, blockchain, and AI for secure cloud-based AI systems
[24]	Alzaylaee et al. (2026)	Real-time AI-based cybersecurity	Lightweight AI models (MobileNetV2, optimized CNN–LSTM) with SHAP-based interpretability	Enabled efficient real-time detection with reduced resource usage and improved model transparency	Addressed efficiency and explainability challenges in AI-driven security
[25]	Patel et al. (2025)	Future-proof cloud security	AI-driven encryption with dynamic key management and quantum-resistant cryptography	Demonstrated superior scalability and resilience compared to traditional encryption techniques	Proposed quantum-ready, AI-enhanced cryptographic security solutions
[26]	Surya et al. (2025)	Cloud threat detection	Deep learning-based multi-layer security models	Outperformed conventional machine learning methods in detecting complex and evolving cyber threats	Confirmed the superiority of deep learning for dynamic cloud security environments

The figure 4 shows an illustration of year-wise distribution of studies included in the literature, which reflects research trends in cloud-based cybersecurity, especially incorporating AI technology. The figure reveals an equal distribution of recent research published in 2025 and 2026, reflecting an increasing research interest in advanced cybersecurity solutions. The figure equally represents research published in 2025 as well as in 2026, reflecting an equally increasing

research interest. This represents an increasing focus on advanced cybersecurity solutions in an ever-changing cybersecurity scenario.

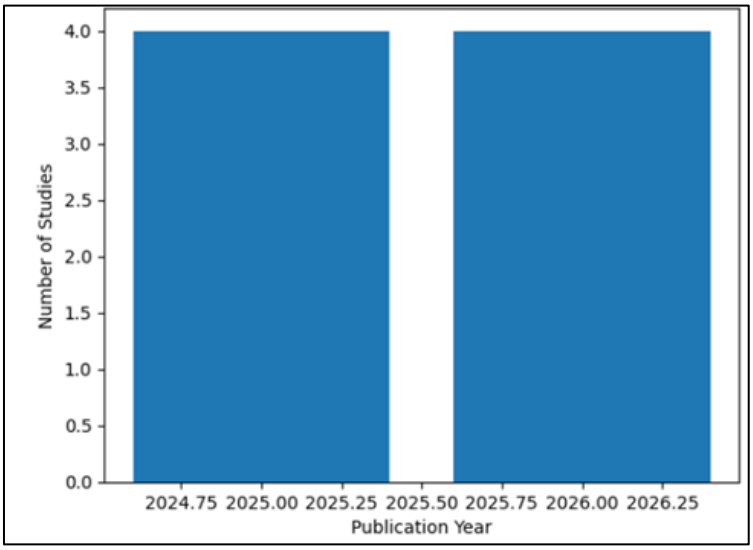

Figure 4 Year Wise Distribution of Literature Review Studies

3. Discussion

Overall, these reviewed studies collectively demonstrated how the advent and union of artificial intelligence, cloud computing, and security systems had revolutionized modern digital infrastructure by promoting intelligent automation, processing, and security systems. From the literature reviewed, it was clear how widely artificial intelligence systems are used in a wide range of cloud, edge, and data-centric environments for making predictions, optimizations, detecting intruders, and calling real-time decisions on systems or networks, with their high quality of outcomes and performance delivered even in structured or security-critical settings. Furthermore, it became understandable how the AI systems assisted cloud environments, which were utilized to improve upon failures, enhance management, and further develop reliability, where the deep learning architectures kept turning out to be increasingly effective for complex patterns, high data dimensionality, or evolving security concerns. From the literature, it was also clear how conventional, traditional, or non-traditional security systems or architectures were no longer considered good enough due to the fact that modern cloud environments inherently have become complex, different, complex, distributed, multi-user, and multi-environment. Advanced security mechanisms based on Zero Trust principles, closed-loop systems, multi-modal system telemeter's fusion, or flexible systems were also found more likely to provide better intrusion recognition. Likewise, the integration of cryptography, blockchain, or even artificial intelligence had served to further enhance the confidentiality, integrity, and trust values related to the data managed within the cloud-based AI system, ensuring that the values were within the appropriate range computationally. Notwithstanding the above, the domain-specific variation results related to the application of the developed models, based on the literature related to the field, were also found evident within the more recent studies related to the topic. Apart from the purely technical aspects, architectural maturity, ethics, or organizational willingness were found more clearly promoted within the literature as the key determinants related to the successful adoption of the related AI or even cloud-based security. All in all, the related literature was found providing evidence related to the clearly determined direction that the related studies within the field were taking. There was undeniable proof that outstanding developments were occurring within the field, even though evidence related to the existing gaps was found within the related literature.

4. Conclusion

This review article explored the scenario of artificial intelligence, cloud computing, and security technologies in development and emphasized their crucial role in building modern-day infrastructures. The existing research studies showed how AI-based technologies play a vital role in improving cloud computing services by offering intelligent automation, predictive analytics, efficient resource management, and real-time security. In the research studies, advanced technologies of machine learning and deep learning were observed to outperform traditional techniques while dealing with the ever-changing scenario of cloud infrastructures, particularly in regard to security-related issues. Traditional security technologies were also observed as being less effective for the building of modern cloud

infrastructures and thus promoted adaptive, zero-trust, and closed-loop security solutions. Moreover, it was claimed how the integration of AI systems with different kinds of cryptographic developments along with blockchain and privacy-preserving technologies helped enhance data confidentiality, integrity, and trust while maintaining efficiency. Further, based on aspects of governance, ethics, interpretability, and organizational readiness, it was highlighted in the literature how AI-driven cloud security systems were implemented successfully. However, it was clear how several challenges, based on standardization, scalability, and mitigations against emerging and evolving sophisticated cyber threats, were still pending for AI system-level protection. From here, it can be established how the current literature aimed to bring into focus the essence of a holistic, intelligent, and futuristic approach while integrating the AI systems into cloud infrastructure. Further, it is clear how the research findings of the current reviewed literature would play an essential role in the strategy and implementation phase during the development of future research work.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest exists among the Authors.

References

[1] Sharma, Himanshu. "The evolution of cybersecurity challenges and mitigation strategies in cloud computing systems." *International Journal of Computer Engineering and Technology* 15, no. 4 (2024): 118-127.

[2] Ang'udi, Janet Julia. "Security challenges in cloud computing: A comprehensive analysis." *World Journal of Advanced Engineering Technology and Sciences* 10, no. 2 (2023): 155-181.

[3] Ahmadi, Sina. "Systematic literature review on cloud computing security: Threats and mitigation strategies." *Ahmadi, S.(2024) Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Journal of Information Security* 15 (2024): 148-167.

[4] Sharma, Chetna, and Chandani Sharma. "Cloud Computing Security: Threats and Mitigation Strategies." In *2024 International Conference on Signal Processing and Advance Research in Computing (SPARC)*, vol. 1, pp. 1-6. IEEE, 2024.

[5] Awodele, O., C. Ogbonna, E. O. Ogu, J. O. Hinmikaiye, and J. E. T. Akinsola. "Characterization and risk assessment of cybersecurity threats in cloud computing: A comparative evaluation of mitigation techniques." *Acadlore Trans. Mach. Learn* 3, no. 2 (2024): 106-118.

[6] Bhumichai, Dhanasak, Christos Smiliotopoulos, Ryan Benton, Georgios Kambourakis, and Dimitrios Damopoulos. "The convergence of artificial intelligence and blockchain: The state of play and the road ahead." *Information* 15, no. 5 (2024): 268.

[7] Hashi, A. I., & Hashi, A. M. (2026). A Deep Learning Driven Cloud Edge Intelligence Framework for Real-Time Big Data Based Cyber-Security Threat Detection. International Journal of Computing and Engineering, 8(1), 13–44. https://doi.org/10.47941/ijce.3447

[8] Sharma, Ashutosh, Elizaveta Podoplelova, Gleb Shapovalov, Alexey Tselykh, and Alexander Tselykh. "Sustainable smart cities: convergence of artificial intelligence and blockchain." *Sustainability* 13, no. 23 (2021): 13076.

[9] Hashi, A. I., & Mohamed, A. H. (2025). Quantum Inspired Cryptographic Framework for Secure Federated Learning and Data Integrity in Large Scale IoT Ecosystems. SSRG International Journal of Computer Science and Engineering, 12(12), 8–24. https://doi.org/10.14445/23488387/IJCSE-V12I12P102

[10] Pandl, Konstantin D., Scott Thiebes, Manuel Schmidt-Kraepelin, and Ali Sunyaev. "On the convergence of artificial intelligence and distributed ledger technology: A scoping review and future research agenda." *IEEE access* 8 (2020): 57075-57095.

[11] Aldomi, Saba, Husam Suleiman, Ali Shatnawi, and Luay Alawneh. "A deep learning approach for early prediction of task failures in cloud computing environments." Systems and Soft Computing (2026): 200442.

[12] Tarapder, Shoflul Azam. "EDGE Artificial Intelligence Based Automation For Ultra-Low-Latency Control In Industrial Robotic Systems." Review of Applied Science and Technology 5, no. 01 (2026): 01-37.

[13] Carlisle, Marvin N., William A. Pace, Andrew W. Liu, Robert Krumm, Janet E. Cowan, Peter R. Carroll, Matthew R. Cooperberg, and Anobel Y. Odisho. "Development and Validation of a Generative Artificial Intelligence-Based

Pipeline for Automated Clinical Data Extraction From Electronic Health Records: Technical Implementation Study." JMIR Bioinformatics and Biotechnology 7, no. 1 (2026): e70708.

[14] Jesus, Jiomarie Balaquit, Mara Shaira Siega, Genevieve Tabornal Jacaban, Geraldine Sambrana, and Danilo Y. Patalinghug. "Future of Artificial Intelligence (AI) in academic research: A framework." Ho Chi Minh City Open University Journal of Science-Social Sciences (2026).

[15] Cai, Zhen, Ghaith Allah Chebil, Yuan Tan, Stephan Kessler, and Johannes Fottner. "Deep learning-based on-site identification and volume measurement of bulk material in construction industry." Engineering Applications of Artificial Intelligence 163 (2026): 112797.

[16] Ajayi, A. S., J. Abimbola, S. E. Segun, E. I. Ajayi, and A. D. Bodude. "Harnessing artificial intelligence for methane emissions control in industrial natural gas engines: Optimizing exhaust after treatment to advance US clean energy goals–A review." European Journal of Sustainable Development Research 10, no. 1 (2026).

[17] Ponnumani, Rajakumar, Nisha Vasudeva, Thenmozhi Elumalai, Prabu Kaliyaperumal, Balamurugan Balusamy, and Francesco Benedetto. "A multi-stage framework for scalable and context-aware intrusion detection in IoT-cloud systems using deep latent modeling and graph-based attack classification." Computers and Electrical Engineering 131 (2026): 110949.

[18] Baranyi, Gábor, Zs Csibi, Kristian Fenech, Áron Fóthi, Zs Gaál, Joul Skaf, and András Lőrincz. "Adaptive framework for ambient intelligence in rehabilitation assistance." Journal of Ambient Intelligence and Humanized Computing (2026): 1-12.

[19] Habib Zadeh Khiyaban, Simin, and Shoaib Sabbar. "Artificial Intelligence in Banking: Opportunities, Risks, and Ethical Imperatives." Code, Cognition & Society 1, no. 2 (2026): 1-12.

[20] Alamri, Malak, Noshina Tariq, Mamoona Humayun, and Menwa Alshammeri. "Energy-efficient threat detection in IoT healthcare using AI and blockchain-enhanced fog–cloud architecture." Cluster Computing 29, no. 2 (2026): 108.

[21] Hashi, A. I., & Mohamed, A. H. (2025). Quantum Inspired Cryptographic Framework for Secure Federated Learning and Data Integrity in Large Scale IoT Ecosystems. SSRG International Journal of Computer Science and Engineering, 12(12), 8–24. https://doi.org/10.14445/23488387/IJCSE-V12I12P102

[22] Olusesi, Ayobami Taiwo, Ignatius Kema Okakwu, Ayodeji Akinsoji Okubanjo, Ayo Isaac Oyedeji, and Oluwaseyi Olawale Bello. "Intrusion Detection in Cloud Computing Using Support Vector Machine and Fast Firefly Algorithm." AUIQ Technical Engineering Science 3, no. 1 (2026): 1.

[23] K. S, Suresh, Thenmozhi Elumalai, Radhakrishnan Rajamani, Anubhav Kumar, Balamurugan Balusamy, Sumendra Yogarayan, and Kaliyaperumal Prabu. "An Unsupervised Cloud-Centric Intrusion Diagnosis Framework Using Autoencoder and Density-Based Learning." Future Internet 18, no. 1 (2026): 54.

[24] Hashi, A. I. (2025). Digital Governance and Public Sector Innovation in Somalia: Enhancing Transparency, Efficiency, and Citizen Participation through Technology. European Journal of Information and Knowledge Management, 4(1), 1–24. https://doi.org/10.47941/ejikm.3124

[25] Hashi, A. I. (2025). A blockchain-enhanced zero-trust framework for privacy in Industrial IoT systems. International Journal on Science and Technology (IJSAT), 16(3), Article 8036. https://doi.org/10.71097/IJSAT.v16.i3.8036

[26] Yedalla, Jayasudha. "APPLICATION SECURITY PRACTICES ESSENTIAL FOR SECURITY OF APPLICATIONS HOSTED IN MULTI. CLOUD PLATFORMS." International Research Journal of Modernization in Engineering Technology and Science (IRJMETS) 7, no. 1 (2025): 6.

[27] Chaudhary, Himani, Geetanjali Sharma, Dinesh Kumar Nishad, and Saifullah Khalid. "Advanced queueing and scheduling techniques in cloud computing using AI-based model order reduction." Discover Computing 28, no. 1 (2025): 75.

[28] Younus, Muhammad, Eko Priyo Purnomo, Achmad Nurmandi, Dyah Mutiarin, Halimah Abdul Manaf, Fathiya Mumtaz, and Tiara Khairunnisa. "Analyzing the trend of government support for cloud computing usage in e-government architecture." Journal of Cloud Computing 14, no. 1 (2025): 14.

[29] Hashi, A. I., & Hashi, A. M. (2026). A Deep Learning Driven Cloud Edge Intelligence Framework for Real-Time Big Data Based Cyber-Security Threat Detection. International Journal of Computing and Engineering, 8(1), 13–44. https://doi.org/10.47941/ijce.3447

[30] Chen, Jiefei, Zhiliang Lu, Hua Zheng, Zhengguo Ren, Yuanfeng Chen, and Jianing Shang. "Data security storage and transmission framework for AI computing power platforms." Scientific Reports (2026).

[31] Alzaylaee, Mohammed K., Fahdah A. Almarshad, Ghada Abdalaziz Gashgari, Danah Algawiaz, and Abdullah IA Alzahrani. "Advancing Cybersecurity: AI-Driven Computer Vision and Machine Learning Models for Real-Time Threat Detection and Prevention." Journal of Engineering Research (2026).

[32] Ang, Sokroeurn, Mony Ho, Sopheatra Huy, and Midhunchakkaravarthy Janarthanan. "A Multi-Layered Adaptive Cybersecurity Framework for the Banking Sector Integrating Next-Gen Firewalls with AI-Driven IDPS." STAP Journal of Security Risk Management 2026, no. 1 (2026): 67-76.

[33] Mollah, Md Harun-Or-Rashid. "AI-DRIVEN THREAT DETECTION AND RESPONSE FRAMEWORK FOR CLOUD INFRASTRUCTURE SECURITY." American Journal of Scholarly Research and Innovation 4, no. 01 (2025): 494-535.

[34] Patel, Advait, Hariharan Ragothaman, Milavkumar Shah, Adit Sheth, Charit Upadhyay, Pravin Pandey, and Saai Krishnan Udayakumar. "AI-Powered Data Encryption Techniques: Safeguarding Cloud Infrastructure." In 2025 IEEE Conference on Artificial Intelligence (CAI), pp. 864-871. IEEE, 2025.

[35] Kezron, Isabirye Edward. "Cybersecurity framework for securing cloud and AI-driven services in small and medium-sized businesses." Journal of Tianjin University Science and Technology 58, no. 6 (2025).

[36] Surya, S., D. Santhakumar, Anuj Tyagi, Kiran Onapakala, VB Thurai Raaj, and N. Krishna Kumar. "AI-Driven Threat Detection: Implementing Multi-Layer Security Networks in Cloud Environments." In 2025 International Conference on Pervasive Computational Technologies (ICPCT), pp. 465-470. IEEE, 2025.