

A Review of Cyberattacks and Their Recent Defense Methods in the Cloud Computing Environment

Ahmed Thamer Ahmed 

Directorate of Education in Diyala, Ministry of Education, Diyala, 32001, Iraq

ahmed.aladly1988@gmail.com

Abstract

Cloud computing has quietly become part and parcel of modern digital infrastructure. It supports a wide range of Internet of Things (IoT), enterprise, and web applications. However, as they become more prevalent, cloud environments are becoming a prime target for advanced cyberattacks such as Distributed Denial-of-Service (DDoS), Advanced Persistent Threats (APTs), phishing, and privacy-related attacks. This paper presents a structured review of recent advances in cloud cybersecurity, based on peer-reviewed studies published in scientific databases between 2022 and 2025. The review highlights new defense technologies like artificial intelligence (AI), deep learning (DL), cloud-edge collaborative security, privacy-preserving methods, blockchain-based trust management, and post-quantum cryptography. The reviewed studies are compared and contrasted to identify trends, strengths, limitations, and gaps in securing cloud computing environments. The results show a clear shift from signature-based security to intelligent, adaptive, and decentralized security architectures that offer better detection precision, faster response, and stronger privacy protection. This review provides an overview of recent advances. It summarizes existing research gaps and directions for future work to achieve secure and resilient cloud services.

Keywords: Cloud Security, Artificial Intelligence, Deep Learning, Cloud-Edge Computing, Privacy-Preserving Technologies, Blockchain, Post-Quantum Cryptography

Article history: Received: 11 Mar 2026, Accepted: 4 Jul 2026, Published: 15 Sep 2026.

This article is open-access under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Cyber attacks on cloud computing are very common these days. It is even normal for penetration testing to start with the cloud. Because it is a single point of connection between users and a website. In modern IoT, the cloud is essential because it provides users with on-demand access. In addition, a third party manages the cloud server, making it scalable and flexible. The rapid expansion of cloud computing has revolutionized modern technology by providing scalable and on-demand resources, significantly increasing the scale and complexity of these environments [1], [2], [3], and [4].

As a result, cyberattacks in this environment have become more complex and are evolving rapidly. Traditional security systems commonly rely on firewalls and signature-based intrusion detection

systems (IDS). This is not suitable for cloud infrastructures, as the cloud virtual machines, containers, and services are often created, moved, and removed. This makes the static cyber defense system ineffective. Consequently, traditional security models often fail to address the dynamic and evolving nature of these cyber threats, rendering reliance on them insufficient [5], [6], [7], and [8].

This is also a major privacy concern, as attackers can access sensitive user data. They can easily expose it to 3rd party service providers and leak user information. Furthermore, such attacks pose a critical threat to sensitive data and system assets, necessitating robust measures to prevent unauthorized access [9] and [10]. The most common attack type is a Distributed Denial of Service (DDoS). A DDoS attack remains the most persistent and

damaging. Modern DDoS attacks have shifted from simple high-volume traffic floods to low-rate, stealthy application-layer attacks. They are designed to bypass older cyber detection systems while exhausting system resources.

This evolution reflects a broader trend where traditional defense strategies and risk management frameworks are proving increasingly inadequate against dynamic, complex threats targeting cloud infrastructure [11], [12], and [13]. These challenges scale further when resources are intertwined across multiple sectors. Traditional security measures often fail to identify and respond effectively to evolving threats in these distributed environments, where massive amounts of private data are exposed to risks such as unauthorized access and inference attacks [15] and [16], leaving the administration domain at high risk. Cyber-Physical Systems (CPS) are directly affected and can lead to catastrophic failure.

Given the evolving nature of cyberattacks, traditional signal-based and threshold-based Intrusion Detection Systems (IDS) often fail. Because these attacks are always evolving, the system may be breached and undetected for months or years, leaking sensitive data. The rapid expansion of cloud computing and Internet of Things (IoT) infrastructures has introduced complex security vulnerabilities, where traditional defense mechanisms often prove inadequate against the escalating volume and sophistication of modern cyber threats targeting data confidentiality and service availability [17], [18], [19], and [20]. Cyber Defense not only detects threats but is also required to minimize the maximum amount of damage. This helps keep the service active and uninterrupted. Mitigation is one of them.

Geopolitical factors also matter; some attacks are carried out to identify weaknesses or to get sensitive information, such as military intelligence backed by foreign advisors. A single point of failure can trigger a cascading effect because IoT devices are highly interconnected. With the rapid development of intelligent transportation systems and connected vehicles, modern vehicles have been increasingly endowed with enhanced computing, storage, sensing, and communication capabilities [21]. This makes them a large attack surface that is very complex to

detect. In short, if one communication channel is compromised, the whole system is compromised.

While research on cloud cybersecurity is gaining momentum, current research mostly focuses on a specific defense technology, such as cloud-edge collaboration, privacy-preserving techniques, blockchain-based security, or artificial intelligence-based intrusion detection, without considering other technologies. Thus, a comprehensive review is needed to bring together these new defense mechanisms systematically, reflect on their merits and constraints, and discuss their potential application in today's cloud computing scenario. As cyberattacks become increasingly complex and sophisticated, a common perspective is needed to understand current research trends and opportunities.

This paper provides an overview of recent developments in cloud cybersecurity by surveying recent literature on new defense technologies. The review focuses on AI and deep learning architectures, cloud-edge collaborative security, privacy-preserving mechanisms, post-quantum cryptographic solutions, and blockchain-based trust models. This review not only summarizes current trends but also provides an overview of the approaches used, identifies research gaps and hurdles, and proposes future research directions for developing a resilient cloud security framework.

The rest of this paper is organized as follows. Section 2 presents the methodology used to select and analyze the literature. Section 3 discusses recent progress in AI and deep learning architectures in the context of cloud security. Section 3 discusses recent developments in AI and deep learning architectures for cloud security. Section 4 examines cloud-edge collaborative security approaches, and Section 5 explores advanced threat scenarios. Section 6 examines privacy-respecting technologies, and Section 7 explores new technologies, such as blockchain and quantum-secure technologies. Section 8 presents the comparative analysis and discussion, and Section 9 provides the conclusions and outlines future research directions.

2. Review Methodology

The review follows a typical literature review methodology where the relevant literature is

identified, reviewed, and analyzed. To ensure the literature was recent, relevant, and high quality, it was collected by searching for defined keywords and screening against defined selection criteria in major scientific databases. Table 1 summarizes the review methodology.

Table 1: Review methodology.

Component	Description
Review Type	Structured literature review
Objective	To review recent cyberattack defense methods and emerging security technologies for cloud computing environments
Databases	IEEE Xplore, Scopus, ScienceDirect, SpringerLink, and MDPI
Publication Period	2022–2025
Document Type	Peer-reviewed journal articles
Language	English
Search Keywords	Cloud security, cyber attacks, cloud computing, intrusion detection, artificial intelligence, deep learning, blockchain, federated learning, privacy-preserving technologies, post-quantum cryptography, DDoS detection
Inclusion Criteria	Studies focusing on cloud security, AI/DL-based defense, cloud-edge security, blockchain, privacy-preserving methods, or quantum-resistant security with sufficient technical details
Exclusion Criteria	Duplicate papers, conference abstracts, editorials, unpublished manuscripts, non-English publications, and studies not directly related to cloud cybersecurity
Analysis Criteria	Defense technique, attack type, employed technologies, advantages, limitations, and future research directions

3. Progress in AI and DL Architectures

There has been a major shift away from single-algorithm detection systems toward hybrid systems. Deep learning models help reduce false positives. Research shows that these integrated approaches overcome the inherent deficiencies of traditional methods by improving detection accuracy and significantly minimizing false alarm rates [22], [23]. These approaches are powered by spatial, temporal, and contextual feature extraction.

3.1 Hybrid Models as the Standard

Single-model architectures are largely outdated, and hybrid models are the new standard. From hybrid convolutional neural networks to fog security models and swarm optimization-grounded methods, these works collectively advance the state of the art in IoT security [24]. They can capture multidimensional data. There are a few types of hybrid models:

- Agentic Intelligence Self-Adaptive Framework (AISAF): Uses CNNs to extract specific features. It uses LSTMs for temporal dependencies and Transformers for contextual reasoning.
- DeepLG SecNet model: This model merges Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU) to enhance detection efficiency.
- AE-CIAM framework: This combines an Attention-enhanced Autoencoder with a CNN Inception model to detect low-rate DDoS attacks.

The hybrid design lets the system learn patterns. These are multiscale, spatiotemporal, and often paired CNNs with BiLSTM networks. This optimizes time-series analysis and helps the model learn patterns that single-architecture models often miss.

3.2 Attention Mechanisms

This is considered the core of cyber defense. This technique works by identifying the most important data through the network. So far, it has proven to be essential in modern systems. The self-attention and intersimple attention transformer (SAINT) is a DDoS detection system used mainly for TCP. Distributed Denial-of-Service (DDoS) attacks disrupt operations by overwhelming services and represent a major security challenge in modern cloud and industrial environments [25], [26]. This attention system uses a dual-attention technique to capture both inner-flow dependencies and interactions. Attention models are mainly built inside autoencoders and CNNs to interpret data. This makes it context-relevant and more accurate within cloud infrastructure traffic.

3.3 Handling Class Imbalance

While cloud computing has become an essential platform for on-demand services, it is inherently vulnerable to various security threats. It requires

robust mechanisms to ensure data protection and resource confidentiality [27], [28], [29]. To avoid high false-positive feedback from risky traffic, handling class imbalance is key. This helps increase recall. The Synthetic Minority Over-sampling Technique (SMOTE) is used in most datasets for minority classes. The key is always identifying the important features. For that, attention-enhanced Autoencoders, undersampling, or balancing training data can work similarly. As in DeepLG SecNet Ensemble Bagged Trees Detection (EBTD), which is reliable for predicting uneven cyber-attacks, stratified aggregation and parallel data sampling are widely used.

3.4 The Shift to Cloud-Edge Collaboration

From the research review, the main concern common among them is transferring data, more specifically, from the centralized cloud to security intelligence, then from security intelligence to the network edge. Latency becomes an issue with this decentralized approach. In Industrial Internet of Things (IIoT) and Cyber-Physical Systems (CPS), it is a very critical component.

▪ Latency and Bandwidth Optimization:

Ensuring real-time processing capabilities while minimizing computational costs and response delays is a fundamental challenge in dynamic computing environments [30], [31]. To reduce latency, edge computing requires processing data near the source. This maximizes bandwidth. By processing data closer to the source, edge computing helps reduce latency and maximize bandwidth. Edge servers use only simple models. This sends encrypted data instead of raw data. This reduces the resource load. For industrial IoT applications, this method provides real-time intrusion alerts. This also avoids the long delays found in traditional cloud-based systems. To mitigate this delay, an adaptive encryption technique has been introduced. It can dynamically adjust encryption strength on the transmission channel. This balances the security requirements with low latency.

▪ Collaborative Architectures:

This architecture is being incorporated into many modern defense systems. This extends to the cloud, edge, and terminal layers. This allows quick responses to IoT requests and pulling from vast

resources. Cloud computing offers scalability and flexibility but still suffers from critical security and privacy challenges [32], [33]. These architectures enable secure data exchange under cloud-based supervision. They use upstream and downstream enterprises to facilitate this. To analyze network traffic across the cloud edge, supervised models are used. Combined with an integrated framework and clustering algorithms, these models enable effective analysis. The most common algorithms are K-means and DBSCAN.

3.5 Dynamic Heterogeneous Redundancy (DHR)

It is used to increase resilience to fight against common types of attacks. In recent research, the hybrid event-time has been added to the ICS in the cloud edge. This adaptation of DHS is used for triggering scheduling. This resolves issues with traditional event-triggered scheduling. Event-triggered scheduling is vulnerable in resource-constrained environments. Optimizing resource utilization through efficient task scheduling and capacity planning is critical in these dynamic cloud and edge environments to prevent system instability and performance bottlenecks [34], [35]. This is why it introduces credibility and heterogeneity metrics. To reduce the risk, keeping control over compromised edge nodes is essential.

4. Advanced Threat Scenarios

Modern cyberattacks are often slow but persistent, designed to drain system resources. The distributed nature of cloud computing environments inherently exposes them to critical security challenges and evolving threats that aim to disrupt service availability and reliability [36], [37]. Previously, DDoS attacks were often high-volume traffic meant to take down the server.

• Low-Rate DDoS (LDDoS):

It is considered one of the most dangerous types of cyber threats today. Because it is very hard to detect, it can target specific sections like TCP. From the outside, it looks like normal user behavior, making it undetectable with a normal DDoS attack preventer. This is why the AE-CIAM framework is built. This framework is specifically designed to target stealthy attacks. The core of this framework is an attention mechanism that identifies diversion in network

traffic. Normal DDoS attacks overload the bandwidth. LDDoS degrades service quality over time. To identify and remove LDDoS, a specialized deep learning model is used to discern patterns. This allows detection of novel and unknown attacks by leveraging machine learning and deep learning models' ability to learn intricate traffic patterns and accurately pinpoint the nature of the attack [38].

- **Advanced Persistent Threats (APTs):**

The latest defense method against these cyberattacks goes beyond static data analysis. These are highly stealthy and remain active for extended periods. With the rise of artificial intelligence, applying it to cyber environments to detect and respond to cyberattacks automatically has begun to gain attention [39]. One proposed model for this kind of threat is Grouped Multiagent Deep Reinforcement Learning (GMADRLD). It allows the defender to gather resources and get used to the new strategy.

- **TCP-Based Vulnerabilities:**

Current cloud and IoT architectures face significant security risks and malicious attacks in the ever-evolving cyber landscape, necessitating robust defense mechanisms to safeguard data integrity and privacy [40], [41], [42]. A common attack exploits the TCP three-way handshake by mimicking legitimate connection requests. This makes the standard defenses ineffective. The SAINT model can detect it by learning patterns. It analyzes interflow and interaction to identify malicious TCP patterns. This allows it to distinguish real traffic. These cyberattacks can happen at any time, faster than human response. Hence, the autonomous agent-based defense systems (CDA-CLOUD) use LSTM models for rapid classification. In high-speed cloud networks, delay is not an option.

5. Privacy-Preserving Technologies

Privacy is a key focus of this research. Data shifts from the cloud to the edge. With the high demand for cloud computing, the security of network communication is also an important consideration [43]. Maintaining user privacy during this shift is a key area of study. Allowing calculations on encrypted data without leakage is not simple.

- **5.1 Federated Learning (FL)**

This technique lets the model train on decentralized edge devices without sharing raw data. This method enables collaborative learning by sharing only model updates rather than raw data, eliminating the need to send personal data to central servers [44]. It is also the most dominant approach for preserving privacy. This minimizes data exposure. Also, consider collaborative learning in heterogeneous networks. Furthermore, the distributed nature of cloud-edge architectures has prompted the development of federated learning-based detection mechanisms, where multiple edge nodes collaboratively perform anomaly detection while preserving data privacy through parameter sharing rather than raw data exchange [45]. FL is often combined with other security measures in the CloudEdge framework. The CDA-CLOUD system uses FL to allow agents to learn from local environments. It also maintains data privacy with decentralized model updates.

- **5.2 Adaptive Privacy Budgets**

This privacy-focused model takes action based on the threat level. It does so by maintaining usefulness while adding noise to the data. The noise allocation is proportional to the threat level. In the cloud-edge setting, this noise helps optimize the trade-off between model accuracy and privacy protection. It is also similar to cloud-edge collaborative learning. The dynamic Gaussian noise allocation is used to optimize the trade-off between accuracy and privacy.

5.3 Hybrid Encryption

Hybrid encryption combines symmetric and asymmetric encryption. Hybrid encryption is favored for its efficiency and security. In a multi-step algorithm integrating DES, RSA, and Blowfish with biometric-derived keys, it is essential for secure cloud storage. Adaptive encryption uses homomorphic encryption for privacy-preserving computations. This is used in collaborative industrial systems. Because of its ability to do secret sharing for level processing at the cloud edge. The Outsourcable Hybrid Proxy Re-Encryption (OHPRE) takes secure data sharing one step ahead. It does so by combining public-key and attribute-based encryption and achieving superior access control. The statements, opinions, and data contained in all publications are solely those of the individual

author(s) and contributor(s) and not of MDPI and/or the editor(s) [46], [47], [48].

6. Emerging Technologies: Blockchain and Quantum Resilience

As cyberattacks evolve, so does the defense against these attacks. Bleeding-edge technology has already begun to play a role in modern systems. With blockchain and quantum resilience, the fight is over who has more computing resources.

6.1 Blockchain for Trust:

Blockchain trust is a core principle of blockchain contracts. It is integrated into security frameworks to establish decentralized trust. Companies need comprehensive security solutions to maintain stable company operations, ensure customer trust, and raise security awareness [49]. A blockchain records agent helps prevent tampering through security logs. This is very effective in multi-agent defense systems. It also supports decentralized identity (DID) management. This allows authentication without reliance on central servers. It is important for scalable IoE ecosystems. Also, blockchain-based cybersecurity trust models provide a dynamic framework. These models are used to evaluate the reliability of cloud service providers and verify data integrity.

6.2 Quantum-Resilient Cryptography

Advances in quantum computing threaten classical encryption. Against a quantum cyber-attack, even blockchain-based trust can also be broken. Traditional approaches often struggle to adapt to the diverse and evolving traffic patterns in industrial IoT networks, making them less effective against sophisticated cyberattack strategies [50]. This makes it increasingly necessary to implement quantum-resilient cryptography to protect against foreign adversaries. Quantum Key Distribution (QKD) is being added to multi-risk protection models. This ensures unconditional security for data transmission. Research is also prioritizing post-quantum cryptography (PQC) algorithms. Lattice-based and

hash-based signatures are being used to future-proof networks against quantum attacks. These technologies aim to secure long-term data confidentiality and integrity in the quantum computing era.

7. Results and Discussion

This section presents the review and results for all the technologies mentioned.

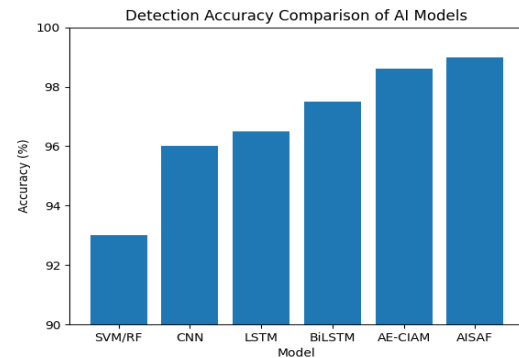


Fig. 1 Detection Accuracy Comparison of AI Models

The results show major changes in cyberattacks and recent defense methods in the Cloud Computing Environment. They are slowly moving away from traditional security systems in favor of adaptive AI-based security systems. Table 2 and Fig. 1 show that hybrid models outperform traditional models. This holds for all tested attack cases. Among them, models with an attention system perform especially well. For example, AE-CIAM and AISAF reached 98% accuracy. This proves that hybrid models are more effective against slow and hidden attacks. Traditional intrusion detection systems cannot detect these attacks.

Table 3 and Fig. 2 show that cloud-only security systems experience higher detection latency. This is due to network bandwidth delay. Edge-only solutions respond faster, but they lack scalability. This is why hybrid cloud-edge architectures were introduced. They allow real-time threat detection at the edge. They also use cloud resources for global intelligence sharing and long-term model training. The analysis highlights the importance of collaboration between the cloud and the edge.

Table 2: Comparative performance of AI-driven intrusion detection models

Model	Attack Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score	Key Strength
-------	-------------	--------------	---------------	------------	----------	--------------

SVM / RF	Volumetric DDoS	91–94	90	89	89.5	Low complexity
CNN	DDoS	95–97	94	96	95	Spatial feature learning
LSTM	LDDoS	96–97	95	96	95.5	Temporal modeling
BiLSTM	Phishing	97–98	97	98	97.5	Bidirectional context
AE-CIAM	LDDoS	98.6	98.2	98.9	98.5	Attention-based anomaly detection
AISAF (Agentic)	Multi-vector	99+	99	99	99	Self-adaptive intelligence

Table 3: Comparative analysis of cloud security deployment models

Architecture	Latency	Bandwidth Usage	Privacy Risk	Scalability	Detection Speed
Cloud-only	High	High	Medium	Very High	Medium
Edge-only	Very Low	Very Low	Low	Limited	High
Cloud-Edge Hybrid	Low	Optimized	Low	High	Very High

Table 5: Evaluation of privacy-preserving and governance-aware security mechanisms

Technique	Privacy Level	Computational Cost	Regulatory Compliance	Suitability for IIoT
AES/RSA	Medium	Low	Medium	High
Homomorphic Encryption	Very High	Very High	High	Medium
Federated Learning	High	Medium	High	Very High
Blockchain Auditing	High	Medium	Very High	High
Hybrid (FL + Blockchain)	Very High	Medium-High	Very High	Excellent

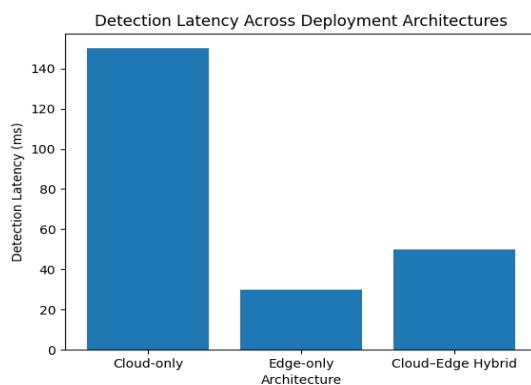


Fig. 2 Detection Latency Across Deployment Architectures

Table 4 and Fig. 3 present the advanced threat coverage results. Traditional intrusion detection systems cannot detect sophisticated attacks like low-rate DDoS and Advanced Persistent Threats (APTs), where Agentic and reinforcement learning-based defense systems perform better. They adapt by learning attacker behavior. They also dynamically adjust mitigation strategies. This adaptability is very

important in modern IoT environments. Attack patterns in these environments change rapidly.

From Table 5 and Fig. 4, federated learning and blockchain-assisted frameworks provide strong privacy guarantees. However, the cost increase is very substantial. However, implementing these technologies presents obstacles, such as blockchain's substantial resource requirements, FL's vulnerability to hostile attacks like MITM, and increased system complexity [51]. So, future research needs to focus on optimizing energy efficiency and scalability without compromising security.

Table 4: Effectiveness of AI models against advanced cyber threats

Threat Type	Traditional IDS	DL-based IDS	Agentic / RL-based Defense
Volumetric DDoS	High	Very High	Very High
Low-rate DDoS	Low	High	Very High
Phishing	Medium	High	Very High

APTs	Very Low	Medium	High
TCP Exploits	Low	High	Very High

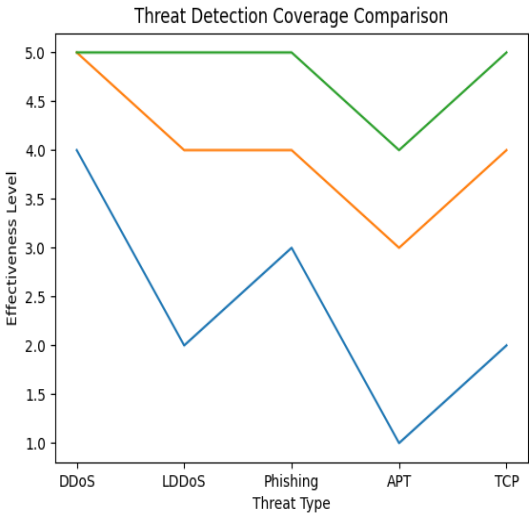


Fig. 3 Threat Detection Coverage Comparison

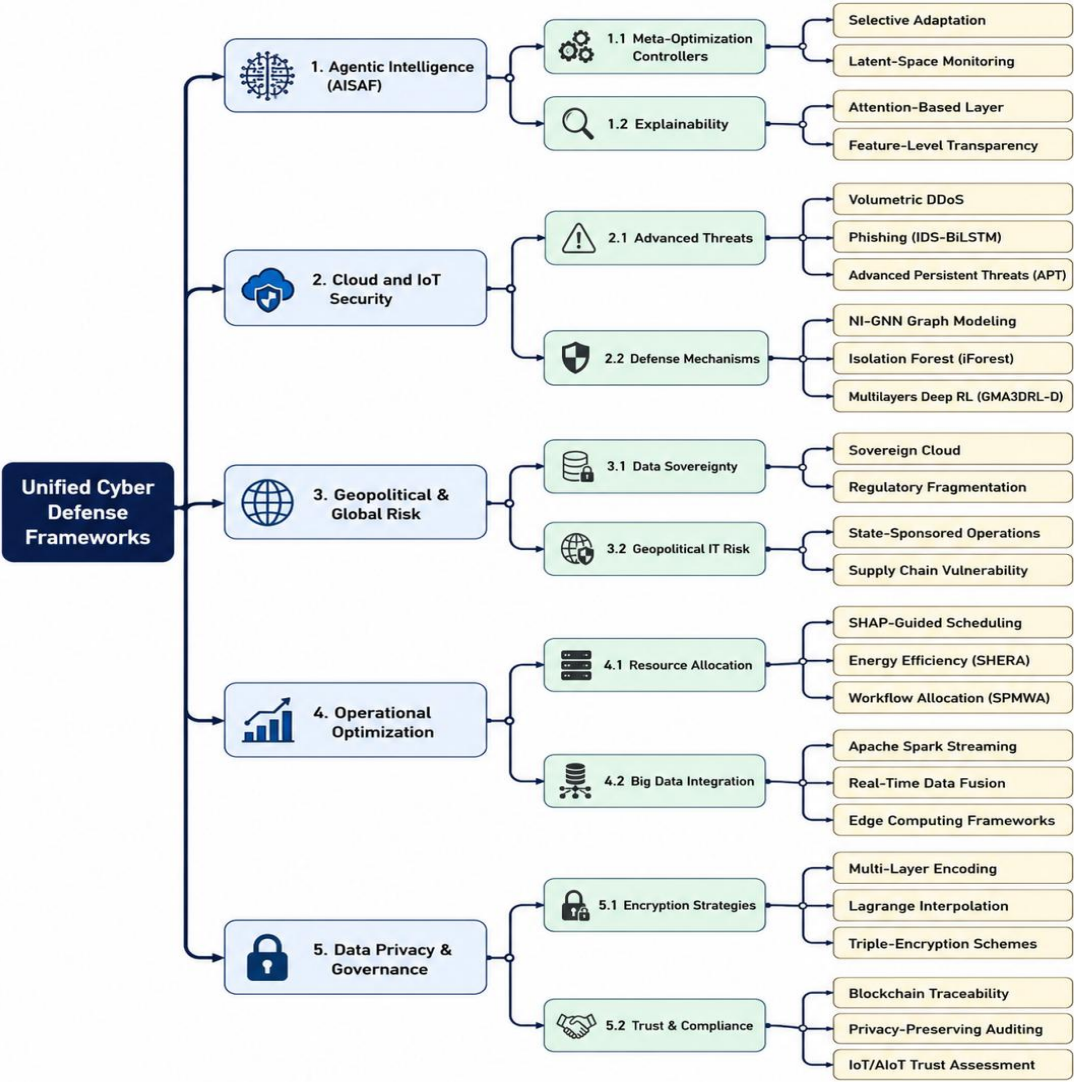


Fig. 4 Mind map

7. Conclusion

The complexity, size, and sophistication of cyberattacks are increasing, and cybersecurity strategies need to stay a step ahead to safeguard sensitive information, protect user privacy, and maintain the security and resilience of cloud computing environments. The reviewed studies show that cloud-edge collaborative architectures, privacy-preserving computing techniques, hybrid AI systems, and deep learning models are significantly improving the ability to detect, mitigate, and respond to modern cyber threats. Even with these advances, several challenges remain, including the development of explainable AI, scalable privacy-preserving mechanisms, and quantum-resistant cryptographic solutions to address future security challenges. Therefore, future research is needed to create intelligent, adaptive, and trustworthy security frameworks and to encourage interdisciplinary research partnerships between academia, industry, and government agencies to spur innovation and enhance the cybersecurity resilience of next-generation cloud computing systems.

Acknowledgements

The authors thank their respective institutions for providing the resources and academic environment that supported the completion of this work.

Conflict of interest

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

References

- [1] Vijetha, B. (2026). Agentic Intelligence for Unified Cyber Defense: A Self-Adaptive Framework for Threat Detection Across Cloud, Edge, and IoT Systems. *IEEE Access*, 14, 5104-5118.
- [2] Wang, F., & Xie, S. (2025). Cybersecurity in cloud computing: AI-driven intrusion detection and mitigation strategies. *IEEE Access*, 13, 108051-108058.
- [3] Slathia, A. S., Sharma, A., Krishna, P. B., Anand, S., Rath, A., Joseph, L., & Gao, X. Z. (2025). SHERA: SHAP-enhanced resource allocation for VM scheduling and efficient cloud computing. *IEEE Access*.
- [4] El Skafi, M. A., Yunis, M. M., Zekri, A., & Daher, J. B. (2025). The confluence of big data and cloud computing in SME adoption strategies. *IEEE Access*, 13, 37789-37811.
- [5] Gatti, G., Valero, J. M. J., Pérez, M. G., & Basile, C. (2025). Holistic Cyber Risk Assessment in the Cloud Continuum: A Multi-Layer, Multi-Domain Approach. *IEEE Access*.
- [6] Al Mazroa, A., Albogamy, F. R., Ishak, M. K., & Mostafa, S. M. (2025). Boosting cyberattack detection using binary metaheuristics with deep learning on cyber-physical system environment. *IEEE Access*, 13, 11280-11294.
- [7] Chaganti, K. C., Inta, S. R., Bandla, S. L., Chilukuri, R., Paidy, P., Muthuveeran, S., & Dulam, N. (2025). Cyber Threats in the Pharmaceutical Industry: A Deep Dive into Recent Attacks and Future Implications. *IEEE Access*.
- [8] Khurshid, F., Noor, U., & Rashid, Z. (2025). Cyber Attack Mitigation Framework for Denial of Service (DoS) Attacks in Fog Computing. *arXiv preprint arXiv:2509.11668*.
- [9] Ahmad, Z., Ahmad, M., & Ahmad, B. (2025). DDoS Attacks in Cloud Computing: Detection and Prevention. *arXiv preprint arXiv:2508.13522*.
- [10] Mollah, M. B., Wang, H., & Fang, H. (2026, February). Evaluating vulnerabilities of connected vehicles under cyber attacks by attack-defense tree. In *2026 International Conference on Computing, Networking and Communications (ICNC)* (pp. 1-6). IEEE.
- [11] Zou, Y. (2025). Design and Implementation of a Cloud Computing Security Assessment Model Based on Hierarchical Analysis and Fuzzy Comprehensive Evaluation. *arXiv preprint arXiv:2511.05049*.
- [12] Malikussaid and Sutiyo, "The impact of the Russia-Ukraine conflict on the cloud computing risk landscape," School of Computing, Telkom Univ., Bandung, Indonesia.
- [13] Chen, J., Lan, X., Zhang, Q., Ma, W., Fang, W., & He, J. (2025). Defending against APT attacks in cloud computing environments using grouped multiagent deep reinforcement learning. *IEEE Internet of Things Journal*.
- [14] Rishiwal, V., Agarwal, U., Yadav, M., Tanwar, S., Garg, D., & Guizani, M. (2025). A new alliance of machine learning and quantum computing: concepts, attacks, and challenges in IoT networks. *IEEE Internet of Things Journal*.
- [15] Yang, W., Wang, H., Li, Z., Niu, Z., Wu, L., Wei, X., ... & Susilo, W. (2024). Privacy-preserving machine learning in cloud-edge-end collaborative environments. *IEEE Internet of Things Journal*, 12(1), 419-434.
- [16] Mamidala, V., Yallamelli, A. R. G., Devarajan, M. V., Ganesan, T., Yalla, R. K. M. K., & Sambas, A. (2025). Hybrid anomaly-based cloud security and machine learning-based behavioral analysis for

- threat intelligence detection in cloud environment. *Cluster Computing*, 28(8), 485.
- [17] Aydin, H., & Aydin, M. A. (2025). A multi-agent-based DDoS detection and defense system design with federated learning and blockchain in public cloud network environment. *Cluster Computing*, 28(16), 1018.
- [18] Kumar, A., & Agarwal, M. (2025). A multi-level DDoS defense mechanism in container-based cloud environment. *Cluster Computing*, 28(5), 306.
- [19] Natarajan, D. R., Narla, S., Kethu, S. S., Peddi, S., Valivarathi, D. T., & Purandhar, N. (2025). Device-aware phishing attack detection in cloud environments using an enhanced DBS-BiLSTM model. *Cluster Computing*, 28(12), 761.
- [20] Ling, J., & Duan, R. (2025). Privacy-preserving technology for data sharing in cloud-assisted Internet of medical things. *Cluster Computing*, 28(7), 447.
- [21] Guo, F., Luo, X., Liu, X., & Luo, Y. (2025). A mobility-aware task offloading approach for vehicles in cloud-edge collaborative environments. *Cluster Computing*, 28(14), 886.
- [22] Abid, A., Jemili, F., & Korbaa, O. (2024). Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques. *Cluster Computing*, 27(2), 2217-2238.
- [23] Mohy-Eddine, M., Guezaz, A., Benkirane, S., & Azrou, M. (2024). Malicious detection model with artificial neural network in IoT-based smart farming security. *Cluster Computing*, 27(6), 7307-7322.
- [24] Nanjappan, M., Pradeep, K., Natesan, G., Samydurai, A., & Premalatha, G. (2024). DeepLG SecNet: Utilizing deep LSTM and GRU with a secure network for enhanced intrusion detection in IoT environments. *Cluster Computing*, 27(4), 5459-5471.
- [25] Souri, A., Norouzi, M., & Alsenani, Y. (2024). A new cloud-based cyber-attack detection architecture for hyper-automation process in industrial Internet of Things. *Cluster Computing*, 27(3), 3639-3655.
- [26] Ammi, M., Adedugbe, O., Alharby, F. M., & Benkhelifa, E. (2022). Leveraging a cloud-native architecture to enable semantic interconnectedness of data for cyber threat intelligence. *Cluster Computing*, 25(5), 3629-3640.
- [27] Sreelatha, G., Babu, A. V., & Midhunchakkaravarthy, D. (2022). Improved security in cloud using Sandpiper and extended equilibrium deep transfer learning-based intrusion detection. *Cluster Computing*, 25(5), 3129-3144.
- [28] Kamble, T., Ghuge, M., Jain, R., & Sarbhukan Bodade, V. (2025). Secure data transmission in cloud computing using a cyber-security trust model with multi-risk protection scheme in smart IOT application. *Cluster Computing*, 28(2), 79.
- [29] Alam, M., Shahid, M., & Mustajab, S. (2024). Security-prioritized multiple workflow allocation model under precedence constraints in cloud computing environment. *Cluster Computing*, 27(1), 341-376.
- [30]
- [31] Najar, A. A., & Manohar Naik, S. (2025). AE-CIAM: a hybrid AI-enabled framework for low-rate DDoS attack detection in cloud computing. *Cluster Computing*, 28(2), 103.
- [32] Safi-Esfahani, F., Larian, H., Saeedi Mobarakeh, S., & Mirjalili, S. (2025). Dynamic scheduling of independent tasks in a cloud computing environment applying improved chicken swarm optimization and differential evolution—*The Journal of Supercomputing*, 81(8), 867.
- [33] Al-Musawi, M. J. H., Navabifar, F., & HAMMOOD MZEDAWEE, H. K. (2025). Providing a multi-step algorithm based on biometric information and hybrid encryption for secure data storage in cloud computing. *The Journal of Supercomputing*, 81(16), 1-40.
- [34] Kirubavathi, G., Sumathi, I. R., Mahalakshmi, J., & Srivastava, D. (2025). Detection and mitigation of TCP-based DDoS attacks in cloud environments using a self-attention and intersample attention transformer model: KG et al—*The Journal of Supercomputing*, 81(3), 474.
- [35] Alsheavi, A. N., Alhusaini, N., Wang, X., Farhan, S., Aziz, S. A., Ahmed, I. A., ... & Ismail, A. S. (2025). Efficient load balancing in cloud computing using hybrid ant colony optimization and crow search strategies: AN Alsheavi et al—*The Journal of Supercomputing*, 81(10), 1146.
- [36] Pereira, P., Araujo, J., Torquato, M., Dantas, J., Melo, C., & Maciel, P. (2020). Stochastic performance model for web server capacity planning in fog computing: P. Pereira et al. *The Journal of Supercomputing*, 76(12), 9533-9557.
- [37] Alam, M., Shahid, M., & Mustajab, S. (2024). Security challenges for workflow allocation model in cloud computing environment: a comprehensive survey, framework, taxonomy, open issues, and future directions. *The Journal of Supercomputing*, 80(8), 11491-11555.
- [38] Alam, M., Shahid, M., & Mustajab, S. (2024). Security challenges for workflow allocation model in cloud computing environment: a comprehensive survey, framework, taxonomy, open issues, and future directions. *The Journal of Supercomputing*, 80(8), 11491-11555.
- [39] Aljuaid, W. A. H., & Alshamrani, S. S. (2024). A deep learning approach for intrusion detection systems in cloud computing environments. *Applied sciences*, 14(13), 5381.
- [40] Jeong, M., Park, J., & Oh, S. H. (2025). Cyber Environment Test Framework for Simulating Command and Control Attack Methods with Reinforcement Learning. *Applied Sciences*, 15(4), 2120.
- [41] Alabdulatif, A., & Thilakarathne, N. N. (2024). A novel cloud-enabled cyber threat hunting platform

- for evaluating the cyber risks associated with smart health ecosystems. *Applied Sciences*, 14(20), 9567.
- [42] Tan, A., Dong, C., Wang, Y., Wang, C., & Xia, C. (2024). Intelligent and Secure Cloud–Edge Collaborative Industrial Information Encryption Strategy Based on Credibility Assessment. *Applied Sciences*, 14(19), 8812.
- [43] Mishra, K. N., Lal, R. K., Barwal, P. N., & Mishra, A. (2025). Advancing Data Privacy in Cloud Storage: A Novel Multi-Layer Encoding Framework. *Applied Sciences*, 15(13), 7485.
- [44] Sathaporn, P., Krungseanmuang, W., Chaowalittawin, V., Benjangkaprasert, C., & Purahong, B. (2025). DDoS detection using a hybrid CNN–RNN model enhanced with multi-head attention for cloud infrastructure. *Applied Sciences*, 15(21), 11567.
- [45] Eren, H., Karaduman, Ö., & Gençoglu, M. T. (2025). Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions. *Applied Sciences*, 15(15), 8704.
- [46] Niu, Y., Han, X., He, C., Wang, Y., Cao, Z., & Zhou, D. (2025). A Privacy-Preserving Polymorphic Heterogeneous Security Architecture for Cloud–Edge Collaboration Industrial Control Systems. *Applied Sciences*, 15(14), 8032.
- [47] Abbas, Z., & Myeong, S. (2023). Enhancing industrial cyber security, focusing on formulating a practical strategy for making predictions through machine learning tools in a cloud computing environment. *Electronics*, 12(12), 2650.
- [48] Z. Chen, C. Deng, X. Gao, X. Li, and H. Hu, "Malicious cloud service traffic detection based on multi-feature fusion," *Electronics*, vol. 14, no—11, p. 2190, 2025.
- [49] Almosti, A. M., & Rahman, M. H. (2025). Analysis of Data Privacy Breaches Using Deep Learning in Cloud Environments: A Review. *Electronics*, 14(13), 2727.
- [50] Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2025). Cybersecurity analytics for the enterprise environment: A systematic literature review. *Electronics*, 14(11), 2252.
- [51] Zhukabayeva, T., Ahmad, Z., Adamova, A., Karabayev, N., & Abdildayeva, A. (2025). An edge-computing-based integrated framework for network traffic analysis and intrusion detection to enhance cyber–physical system security in industrial IoT. *Sensors*, 25(8), 2395.
- [52] Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial Internet of things–edge computing integration: Challenges, threats, and future directions. *Sensors*, 25(1), 213.