International journal of statistics (2051-8285)

Federated AI-Driven Intrusion Detection Framework for DDoS Mitigation in Cloud Networks

Nguyen Thanh Son
Faculty of Information and Communication Technology, Vietnam

ABSTRACT

The rapid expansion of cloud computing infrastructures has intensified exposure to distributed denial-of-service (DDoS) attacks, creating significant challenges for service availability, security resilience, and operational continuity. Traditional centralized intrusion detection approaches often face limitations related to data privacy, communication overhead, scalability, and delayed threat response. This research presents a Federated AI-Driven Intrusion Detection Framework for DDoS Mitigation in Cloud Networks that integrates federated learning principles with intelligent anomaly detection mechanisms to enable decentralized and privacy-preserving security operations. The proposed framework distributes model training across cloud nodes while maintaining local data ownership, allowing collaborative threat intelligence generation without transferring sensitive network information. The research conceptually combines deep learning-based attack recognition, adaptive federated aggregation, and edge-enabled security intelligence for improving real-time DDoS detection capabilities. Existing studies demonstrate the effectiveness of artificial intelligence and federated learning in identifying network anomalies; however, challenges remain regarding communication efficiency, model adaptability, and cross-domain security coordination. The proposed framework addresses these limitations by introducing a collaborative security architecture capable of learning from heterogeneous cloud environments. The analysis highlights that federated AI-based intrusion detection can improve scalability, privacy preservation, and proactive defense against evolving DDoS attack patterns. The framework also aligns with emerging secure edge intelligence paradigms where distributed intelligence supports reliable next-generation communication systems (Varanasi et al., 2026). The findings indicate that federated AI security models provide a promising direction for developing resilient cloud infrastructures with enhanced autonomous threat mitigation capabilities.

Keywords: Federated Learning, Artificial Intelligence, DDoS Detection, Cloud Security, Intrusion Detection System, Deep Learning, Edge Intelligence, Cybersecurity Framework.

INTRODUCTION

Background

Cloud computing has become a fundamental infrastructure model for modern digital services by providing scalable computing resources, flexible deployment environments, and distributed service availability. However, the openness and interconnected nature of cloud platforms have increased their vulnerability to sophisticated cyber threats, particularly distributed denial-of-service (DDoS) attacks. These attacks overwhelm computational resources, network bandwidth, and application services through coordinated malicious traffic generation, resulting in service degradation or complete availability failure. Recent research emphasizes that protecting cloud environments requires intelligent and adaptive security mechanisms capable of detecting complex attack behaviors beyond traditional rule-based approaches (Alauthman et al., 2025).

Artificial intelligence (AI)-based security solutions have demonstrated strong potential in identifying abnormal traffic patterns through machine learning and deep learning models. Deep learning-driven approaches can analyze high-dimensional network characteristics and recognize previously unseen attack patterns. However, conventional AI security systems frequently depend on centralized data collection, where network information from multiple sources is transmitted to a central server for training. This approach introduces privacy concerns, communication bottlenecks, and scalability limitations, especially in large-scale cloud ecosystems (Kumar et al., 2024).

Federated learning provides an alternative paradigm by enabling distributed model training among multiple participating nodes without requiring raw data exchange. In cybersecurity applications, federated learning allows organizations and cloud entities to collaboratively improve threat detection models while maintaining data confidentiality. Research on federated cybersecurity indicates that decentralized learning approaches can strengthen security intelligence across heterogeneous environments while reducing dependency on centralized infrastructures (Ghimire & Rawat, 2022).

The integration of federated learning with AI-driven intrusion detection represents a significant advancement for cloud security. Instead of relying on isolated detection systems, federated frameworks enable multiple cloud nodes to contribute knowledge through shared model updates. Such collaborative intelligence is particularly valuable for DDoS mitigation because attack patterns often span multiple networks and geographical regions. Secure edge intelligence and cross-domain standardization further support this direction by enabling coordinated decision-making across distributed communication environments (Varanasi et al., 2026).

Problem Statement

Although existing DDoS detection approaches have achieved considerable progress, several critical limitations remain. Traditional centralized detection systems require continuous transmission of network data, increasing communication overhead and creating potential privacy risks. Additionally, rapidly evolving DDoS techniques reduce the effectiveness of static detection models because attackers continuously modify traffic characteristics to bypass security mechanisms.

Deep learning-based DDoS defense strategies provide improved detection accuracy but often require large-scale datasets and centralized computational resources. Afraji et al. (2025) highlighted the growing importance of intelligent defense mechanisms for mitigating cloud-based DDoS attacks; however, practical deployment challenges remain regarding scalability and real-time adaptability.

Federated learning-based solutions address some privacy issues but introduce new challenges, including communication efficiency, heterogeneous client behavior, and model synchronization. Asad et al. (2023) identified communication cost as a major limitation in federated learning environments, particularly when numerous distributed participants exchange frequent model updates.

Therefore, there is a need for an integrated framework that combines AI-driven intrusion detection with federated intelligence to achieve efficient, scalable, and privacy-preserving DDoS mitigation in cloud networks.

Research Relevance

The increasing dependence on cloud-based applications requires security architectures capable of operating across distributed infrastructures. Modern cloud environments involve multiple service providers, edge devices, virtual machines, and geographically dispersed data centers. A centralized security model is insufficient for such complex ecosystems because threats can emerge simultaneously across multiple domains.

The development of federated AI-driven security frameworks contributes to next-generation cybersecurity by enabling collaborative defense mechanisms without compromising sensitive information. This approach supports the evolution toward intelligent distributed security systems where local detection capabilities are enhanced through collective knowledge sharing.

The relationship between federated intelligence and secure edge computing is increasingly important for future communication infrastructures. Varanasi et al. (2026) emphasized the significance of secure edge intelligence and standardized cross-domain coordination for real-time digital environments, demonstrating the importance of distributed intelligence architectures.

Objectives

This research aims to:

1. Develop a conceptual federated AI-driven intrusion detection framework for DDoS mitigation in cloud networks.

2. Analyze the integration of deep learning models with federated learning mechanisms for decentralized threat detection.

3. Examine how privacy preservation and distributed intelligence improve cloud security resilience.

4. Identify operational challenges associated with federated cybersecurity architectures.

5. Evaluate the potential impact of adaptive AI security frameworks on future cloud infrastructures.

Scope and Significance

The scope of this research focuses on AI-enabled federated intrusion detection mechanisms specifically designed for cloud-based DDoS mitigation. The proposed framework considers distributed cloud nodes as collaborative participants that locally analyze network behavior and contribute model improvements through federated aggregation.

The significance of this research lies in addressing the limitations of conventional centralized security models. By combining artificial intelligence, federated learning, and secure distributed intelligence, the proposed approach provides a foundation for resilient cloud environments capable of proactive threat identification and adaptive defense.

LITERATURE REVIEW

The increasing complexity of DDoS attacks has encouraged researchers to explore intelligent detection and mitigation strategies. Abdullayeva (2022) investigated distributed denial-of-service attack detection in cloud environments using data clustering techniques. The study demonstrated that intelligent classification methods can improve identification of abnormal traffic behavior; however, clustering-based approaches may face difficulties when dealing with rapidly changing attack characteristics.

Alauthman et al. (2025) presented a systematic survey of information theory-based DDoS detection approaches in cloud computing. Their analysis highlighted the importance of feature extraction, entropy-based monitoring, and adaptive detection mechanisms. However, the study identified persistent challenges related to scalability, dynamic attack evolution, and future-oriented intelligent defense models.

Deep learning approaches have become increasingly important for DDoS mitigation due to their ability to learn complex patterns from large network datasets. Kumar et al. (2024) examined AI-enabled defense mechanisms for securing cloud services and emphasized that artificial intelligence improves detection capability through automated feature learning. Nevertheless, dependence on centralized training environments remains a major limitation.

Afraji et al. (2025) analyzed deep learning-driven defense strategies and emphasized the role of intelligent models in improving cloud security performance. Their findings suggest that AI-based approaches can provide stronger protection against sophisticated attacks, although practical deployment requires addressing computational requirements and adaptability concerns.

Transformer-based models have also been explored for detecting specific DDoS attack categories. Kirubavathi et al. (2025) proposed an attention-based model for TCP-based DDoS attack detection, demonstrating the effectiveness of advanced neural architectures in capturing complex traffic relationships. However, such models typically require centralized datasets and significant computational resources.

Federated learning has emerged as an important solution for decentralized cybersecurity. Ghimire and Rawat (2022) investigated recent developments in federated learning for cybersecurity applications and highlighted its ability to support collaborative security intelligence while maintaining data privacy. Their work establishes federated learning as a promising foundation for distributed intrusion detection.

Doriguzzi-Corin and Siracusa (2022) introduced FLAD, an adaptive federated learning approach for DDoS attack detection. The study demonstrated that federated models can effectively support decentralized detection; however, challenges related to communication efficiency and model adaptation remain significant.

Alhasawi and Alghamdi (2024) explored federated learning for decentralized DDoS detection in IoT networks. Their findings indicate that federated approaches improve privacy preservation and collaborative learning, although network heterogeneity affects model performance.

Asad et al. (2023) investigated communication limitations in federated learning systems. Their research identified communication cost as a critical factor influencing scalability, emphasizing the need for optimized aggregation mechanisms in large distributed environments.

Ouhssini et al. (2024) provided a comprehensive review of DDoS prevention and mitigation approaches in cloud environments. Their analysis revealed a research gap between intelligent detection techniques and practical large-scale deployment requirements.

The reviewed studies demonstrate that AI-based and federated approaches individually provide significant advantages; however, an integrated framework combining adaptive deep learning, federated intelligence, and secure distributed coordination remains insufficiently explored. This research addresses this gap by proposing a federated AI-driven intrusion detection framework designed specifically for scalable DDoS mitigation in cloud networks.

METHODOLOGY

3.1 Research Design and Framework Overview

This research adopts a conceptual framework development methodology to design a Federated AI-Driven Intrusion Detection Framework for DDoS Mitigation in Cloud Networks. The methodology integrates artificial intelligence-based anomaly detection, federated learning mechanisms, cloud security principles, and distributed intelligence concepts into a unified security architecture.

The proposed framework is designed around the principle that cloud security should move from centralized monitoring toward collaborative intelligence-based protection. Instead of transferring raw network traffic data to centralized servers, participating cloud nodes independently analyze local traffic patterns and share only optimized model parameters. This approach enhances privacy preservation while enabling collective learning across distributed environments.

The framework consists of five major functional layers:

1. Cloud Network Data Acquisition Layer
2. Local AI-Based Intrusion Detection Layer
3. Federated Learning Intelligence Layer
4. Adaptive DDoS Decision and Mitigation Layer
5. Secure Edge-Cloud Coordination Layer

The architecture follows the concept of distributed intelligence where individual nodes maintain autonomous detection capabilities while contributing to a global security model. Such decentralized intelligence aligns with emerging secure edge computing environments where real-time decision-making is required across interconnected systems (Varanasi et al., 2026).

3.2 Cloud Network Data Acquisition Layer

The first component of the framework is responsible for collecting network-related information from distributed cloud resources. Modern cloud infrastructures generate heterogeneous security data including traffic flows, packet characteristics, service requests, resource utilization patterns, and communication behaviors.

Unlike conventional centralized intrusion detection systems, the proposed approach maintains data locally within each cloud node. Each participating entity, such as a virtual machine cluster, edge gateway, or cloud service component, functions as an independent learning client.

The collected features may include:

- Traffic volume variations
- Packet transmission frequency
- Source-destination communication patterns
- Protocol behavior
- Request-response abnormalities
- Resource consumption indicators

This distributed data collection strategy reduces exposure of sensitive operational information. In a practical cloud environment, multiple organizations using shared cloud infrastructure can collaboratively improve DDoS detection without revealing confidential traffic records.

Abdullayeva (2022) demonstrated that intelligent analysis of traffic characteristics can improve DDoS detection performance; however, traditional approaches often depend on centralized processing. The proposed framework extends this concept by introducing decentralized intelligence through federated learning.

3.3 Local AI-Based Intrusion Detection Layer

The second layer applies artificial intelligence models to analyze local network behavior. Each cloud participant trains an intrusion detection model using its own security data without transferring raw information externally.

The local AI model performs three primary functions:

Feature Learning

Deep learning mechanisms automatically identify important traffic characteristics associated with malicious behavior. Unlike manually engineered security rules, neural models can discover complex relationships between multiple network parameters.

Anomaly Classification

The trained model classifies incoming traffic into normal and suspicious categories. DDoS attacks typically produce abnormal patterns such as excessive connection attempts, unusual traffic concentration, or abnormal request distribution.

Continuous Model Adaptation

The local model continuously updates based on newly observed network behavior. This capability is essential because attackers frequently modify their strategies to bypass conventional detection systems.

Deep learning-based security mechanisms have demonstrated strong potential in identifying complex attack patterns. Afraji et al. (2025) emphasized that AI-driven defense strategies improve DDoS mitigation capabilities by enabling automated recognition of evolving threats.

Similarly, transformer-based approaches have shown effectiveness in capturing complex dependencies within network traffic. Kirubavathi et al. (2025) demonstrated that attention mechanisms can improve detection accuracy for TCP-based DDoS attacks by analyzing relationships among traffic characteristics.

However, centralized AI systems face limitations related to data privacy and scalability. The proposed framework addresses these issues by combining local AI detection with federated intelligence.

3.4 Federated Learning Intelligence Layer

The core innovation of the proposed framework is the integration of federated learning for collaborative security model development.

Federated learning enables multiple cloud nodes to participate in model improvement without sharing original datasets. The process follows four major stages:

Local Training

Each participating cloud node trains its intrusion detection model using locally available security data.

Model Update Generation

After training, nodes generate model parameters representing learned security patterns. These updates contain intelligence information but do not expose original traffic records.

Federated Aggregation

A secure aggregation mechanism combines updates from multiple nodes to create an improved global intrusion detection model.

Global Model Distribution

The optimized model is redistributed to participating nodes, allowing every client to benefit from collective security intelligence.

The federated approach provides significant advantages for cloud security because attack information is often distributed across multiple locations. A DDoS attack targeting different cloud services may generate partial indicators at individual nodes. Federated learning enables these distributed observations to contribute toward a comprehensive detection capability.

Doriguzzi-Corin and Siracusa (2022) demonstrated the effectiveness of adaptive federated learning for DDoS detection, highlighting the potential of decentralized security intelligence. Similarly, Alhasawi and Alghamdi (2024) showed that federated learning can support decentralized DDoS detection while preserving data privacy.

Despite these advantages, federated systems face communication challenges. Asad et al. (2023) identified communication cost as a major limitation because frequent model exchange can increase network overhead. Therefore, the proposed framework incorporates adaptive aggregation strategies that reduce unnecessary communication while maintaining detection accuracy.

3.5 Adaptive DDoS Decision and Mitigation Layer

After detecting suspicious activities, the framework performs intelligent mitigation decisions. The mitigation layer converts AI-generated predictions into security responses.

The decision mechanism includes:

Threat Classification

Detected traffic is categorized according to attack severity. Low-level anomalies may require monitoring, while high-confidence DDoS activities trigger immediate defensive actions.

Dynamic Resource Protection

The system can adjust cloud resource allocation by controlling suspicious traffic flows, isolating malicious sources, or modifying service access policies.

Automated Response Execution

AI-driven mitigation enables rapid response without requiring continuous human intervention. This capability is particularly important for large-scale cloud environments where attack volumes can exceed manual

response capacity.

Kumar et al. (2024) emphasized that AI-enabled defense mechanisms improve cloud security by providing automated and adaptive protection against emerging threats. However, excessive automation may introduce risks if incorrect predictions result in unnecessary blocking of legitimate users. Therefore, the proposed framework requires balanced decision thresholds and continuous model validation.

3.6 Secure Edge-Cloud Coordination Layer

The final layer establishes coordination between edge intelligence and cloud security services. Modern cloud ecosystems increasingly depend on edge computing components that require rapid security decisions closer to data sources.

Secure edge intelligence enables faster detection because preliminary analysis occurs near network entry points rather than relying entirely on distant cloud servers. This reduces latency and improves response efficiency.

The importance of standardized and secure distributed intelligence has become increasingly significant for next-generation communication environments. Varanasi et al. (2026) highlighted the role of secure edge intelligence and cross-domain coordination in supporting reliable digital infrastructures. The proposed framework extends this principle by applying collaborative intelligence to DDoS mitigation.

The integration of edge and cloud intelligence provides several advantages:

- Reduced detection latency
- Improved scalability
- Faster threat response
- Enhanced distributed learning capability

However, maintaining trust among multiple participating nodes remains a challenge. Malicious participants could attempt to manipulate model updates through poisoning attacks. Therefore, future implementations require additional verification mechanisms for federated model integrity.

RESULTS

The conceptual evaluation of the proposed Federated AI-Driven Intrusion Detection Framework indicates several important outcomes regarding cloud security enhancement. The first major finding is that integrating federated learning with AI-based intrusion detection provides a more scalable alternative to centralized security architectures. By distributing training operations among cloud nodes, the framework reduces dependency on centralized data collection while maintaining collaborative threat intelligence.

The analysis demonstrates that privacy preservation represents a significant advantage of the proposed model. Traditional cloud security systems require network information to be transferred to centralized servers, creating potential confidentiality concerns. Federated learning eliminates this requirement by exchanging model knowledge rather than raw security data. This characteristic is particularly valuable in multi-tenant cloud environments where organizations must protect sensitive operational information.

The second finding relates to improved adaptability against evolving DDoS attack patterns. Conventional rule-based systems often struggle when attackers introduce new traffic strategies. The proposed AI-driven framework continuously learns from distributed observations, enabling more dynamic detection capabilities. Existing research supports this observation, as deep learning approaches have demonstrated improved capability in recognizing complex attack behaviors (Afraji et al., 2025; Kumar et al., 2024).

Another significant finding is the importance of communication optimization in federated security systems. Although federated learning improves privacy, frequent exchange of model updates can increase communication requirements. The framework therefore emphasizes adaptive aggregation strategies that balance learning performance and network efficiency. This finding corresponds with communication challenges identified in federated learning research (Asad et al., 2023).

The framework also reveals the importance of integrating edge intelligence with cloud security operations. Distributed edge-cloud coordination enables faster threat identification and reduces response delays. Secure edge intelligence principles provide a foundation for real-time cybersecurity decision-making in next-generation communication systems (Varanasi et al., 2026).

Furthermore, the analysis identifies that combining multiple security capabilities produces stronger protection than isolated approaches. Federated learning contributes decentralized collaboration, artificial intelligence provides adaptive detection, and edge

intelligence supports rapid response. Together, these components create a comprehensive security ecosystem for cloud networks.

However, the findings also highlight several limitations. Federated models may experience reduced performance when participating nodes possess highly different data distributions. Additionally, malicious clients may attempt to compromise the learning process through manipulated updates. These challenges require future research on secure aggregation, trust evaluation, and robust federated optimization techniques.

Overall, the findings indicate that federated AI-driven intrusion detection represents a promising approach for strengthening cloud security. The framework provides a foundation for developing autonomous, privacy-preserving, and scalable DDoS mitigation systems capable of supporting future distributed computing environments.

DISCUSSION

The proposed Federated AI-Driven Intrusion Detection Framework for DDoS Mitigation in Cloud Networks represents a shift from conventional centralized cybersecurity mechanisms toward decentralized and collaborative defense architectures. The findings indicate that integrating artificial intelligence with federated learning provides a balanced approach to addressing the primary limitations of existing cloud security systems, including privacy concerns, scalability challenges, and delayed response capabilities.

A major theoretical implication of this research is the extension of distributed intelligence principles into cybersecurity operations. Traditional intrusion detection systems generally assume that centralized analysis produces better security outcomes because larger datasets can be processed collectively. However, this approach creates dependency on centralized infrastructures and increases risks associated with data exposure. Federated learning challenges this assumption by demonstrating that security intelligence can be collaboratively developed while maintaining local data ownership. This theoretical foundation aligns with the broader movement toward secure edge intelligence, where distributed systems cooperate to achieve intelligent decision-making capabilities (Varanasi et al., 2026).

From a practical perspective, the proposed framework offers significant benefits for cloud service providers, enterprise networks, and multi-cloud environments. In a large-scale cloud infrastructure, DDoS attacks rarely originate from a single location. Instead, attack patterns may appear across different geographical regions, network segments, or service platforms. A federated approach allows these distributed components to collectively identify emerging threats without requiring direct exchange of sensitive network information. This capability improves both security collaboration and operational independence.

The framework also provides advantages in terms of adaptive threat detection. Existing studies indicate that AI-based approaches improve the identification of complex attack patterns because they can automatically learn relationships among network features. Deep learning-driven security models have demonstrated improved performance in recognizing sophisticated DDoS behaviors compared with traditional detection approaches (Afraji et al., 2025). However, the effectiveness of these models depends heavily on data quality, computational resources, and continuous adaptation. The proposed framework addresses these challenges by enabling distributed model improvement through federated learning.

The integration of federated learning introduces important trade-offs. While decentralized training improves privacy protection, it increases system complexity. Each participating node must maintain local computational capability, perform model updates, and communicate securely with the aggregation mechanism. Asad et al. (2023) highlighted that communication cost remains one of the primary challenges affecting federated learning scalability. Therefore, although federated architectures reduce raw data transmission, inefficient model synchronization may still create performance limitations.

Another critical consideration is the impact of heterogeneous cloud environments. Different cloud nodes may generate different traffic characteristics due to variations in applications, users, geographical locations, and infrastructure configurations. Such non-uniform data distributions can negatively influence global model performance. Federated learning systems must therefore incorporate adaptive optimization techniques capable of handling diverse security environments.

The framework also raises concerns regarding trust and reliability. Since multiple participants contribute model updates, attackers may attempt to manipulate the learning process through malicious contributions. A compromised participant could introduce inaccurate information into the global model, reducing detection accuracy. Future implementations require robust verification mechanisms, anomaly detection for model updates, and secure aggregation strategies.

Comparatively, existing DDoS detection studies have focused mainly on improving detection algorithms rather than developing comprehensive distributed security ecosystems. Abdullayeva (2022) explored clustering-based detection methods, while Alauthman et al. (2025) analyzed information theory-based approaches for cloud DDoS detection. These studies provide valuable insights into attack identification; however, they do not fully address the challenges of privacy-preserving collaborative security. The proposed framework extends previous research by combining intelligent detection with decentralized knowledge sharing.

Federated cybersecurity research further supports this direction. Ghimire and Rawat (2022) identified federated learning as an emerging solution for cybersecurity applications by enabling collaborative defense without centralized data exchange. Similarly, Doriguzzi-Corin and Siracusa (2022) demonstrated the feasibility of federated approaches for DDoS detection, while Alhasawi and Alghamdi (2024) confirmed their applicability in decentralized network environments.

The proposed framework also complements emerging secure communication architectures. As next-generation digital infrastructures increasingly depend on interconnected edge and cloud resources, security mechanisms must operate across multiple domains. Secure edge intelligence provides the foundation for real-time threat analysis and coordinated protection strategies (Varanasi et al., 2026). Therefore, federated AI-driven security frameworks represent an important pathway toward future autonomous cybersecurity ecosystems.

Despite its advantages, the framework has limitations. First, the research presents a conceptual architecture rather than an experimental implementation, meaning practical performance evaluation requires future simulation and real-world testing. Second, the framework depends on reliable communication channels between participating nodes. Third, computational requirements associated with AI models may create deployment challenges in resource-constrained environments.

Overall, the discussion demonstrates that federated AI-driven intrusion detection provides a balanced solution between security intelligence, privacy preservation, and scalability. While challenges remain regarding communication efficiency, trust management, and heterogeneous environments, the framework establishes a strong foundation for future cloud security research.

CONCLUSION

The increasing sophistication of DDoS attacks requires cloud security architectures capable of operating beyond traditional centralized defense mechanisms. This research proposed a Federated AI-Driven Intrusion Detection Framework for DDoS Mitigation in Cloud Networks by integrating artificial intelligence, federated learning, and secure edge-cloud coordination.

The framework addresses critical limitations of existing security approaches by enabling collaborative threat intelligence generation without requiring raw data exchange. Through distributed AI-based detection, cloud nodes can independently analyze malicious activities while contributing knowledge toward a shared security model. This approach improves privacy protection, scalability, and adaptability against evolving DDoS attack strategies.

The literature analysis demonstrated that deep learning approaches provide strong capabilities for identifying complex attack behaviors, while federated learning introduces opportunities for decentralized cybersecurity collaboration. However, existing approaches often address these technologies independently. The proposed framework contributes by combining them into a unified architecture designed specifically for cloud-based DDoS mitigation.

The research findings indicate that federated AI security models can improve real-time threat detection and support more resilient cloud infrastructures. The integration of secure edge intelligence further strengthens the framework by reducing response latency and enabling distributed decision-making capabilities. Such approaches are increasingly relevant for future communication and digital infrastructure environments where intelligent coordination across domains is essential (Varanasi et al., 2026).

Nevertheless, several challenges require further investigation. Communication optimization, malicious model updates, heterogeneous data distributions, and computational requirements remain important research issues. Future studies should focus on implementing the proposed framework in simulated and real cloud environments, evaluating performance metrics such as detection accuracy, false positive rates, communication efficiency, and response time.

Future research may also explore advanced privacy-preserving mechanisms, blockchain-assisted federated security, adaptive reinforcement learning, and autonomous threat response systems. By addressing these

challenges, federated AI-driven intrusion detection can become a key component of next-generation cloud cybersecurity frameworks.

REFERENCES

1. D. M. A. A. Afraji, J. Lloret, and L. Pe˜nalver, “Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments,” Cyber Secur. Appl., vol. 3, p. 100085, 2025.

2. M. Alauthman, A. Almomani, M. Alarqan, B. Belaton, M. Al-Betar, and V. Arya, “Information theory-based DDoS attack detection in cloud computing: a systematic survey of approaches, challenges, and future directions,” Int. J. Cloud Appl. Comput., vol. 15, no. 1, pp. 1–38, 2025.

3. Y. Alhasawi and S. Alghamdi, “Federated learning for decentralized DDoS attack detection in IoT networks,” IEEE Access, vol. 12, pp. 42357–42368, 2024.

4. M. Asad, S. Shaukat, D. Hu, Z. Wang, E. Javanmardi, J. Nakazato, and M. Tsukada, “Limitations and future aspects of communication costs in federated learning: a survey,” Sensors, vol. 23, no. 17, p. 7358, 2023.

5. F. J. Abdullayeva, “Distributed denial of service attack detection in E-government cloud via data clustering,” Array, vol. 15, p. 100229, 2022.

6. R. Doriguzzi-Corin and D. Siracusa, “FLAD: adaptive federated learning for DDoS attack detection,” arXiv preprint arXiv:2205.06661, 2022.

7. B. Ghimire and D. B. Rawat, “Recent advances in federated learning for cybersecurity and cybersecurity for the internet of things,” IEEE Internet Things J., vol. 9, no. 11, pp. 8229–8249, 2022.

8. G. Kirubavathi, I. R. Sumathi, J. Mahalakshmi, and D. Srivastava, “Detection and mitigation of TCP-based DDoS attacks in cloud environments using a self-attention and intersample attention transformer model,” J. Supercomput., vol. 81, no. 3, p. 474, 2025.

9. S. Kumar, M. Dwivedi, M. Kumar, and S. S. Gill, “A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services,” Comput. Sci. Rev., vol. 53, p. 100661, 2024.

10. M. Ouhssini, K. Afdel, M. Akouhar, E. Agherrabi, and A. Abarda, “Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: a comprehensive systematic review of state-of-the-art approaches,” Egypt. Inform. J., vol. 27, p. 100517, 2024.

11. Kishore Subramanya Hebbar, Jaykumar Ambadas Maheshkar, “Intelligent Ml-Based Workload Placement In Hybrid Clouds: Optimizing Cost And Sla In Modernized Systems”, AS, vol. 27, no. 1, pp. 84–101, Dec. 2025, doi: 10.22178/acta.27.1.8

12. S. R. Varanasi, S. S. S. Valiveti, M. Adnan, M. I. Faruk, M. J. Hossain and M. M. T. G. Manik, "Cross-Domain Standardization and Secure Edge Intelligence for Real-Time Digital Twin Deployments in Next-Generation Communication Systems," in IEEE Communications Standards Magazine, doi: 10.1109/MCOMSTD.2026.3662187.