IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154200

A SURVEY OF AI-DRIVEN INTRUSION DETECTION SYSTEMS FOR CLOUD AND EDGE COMPUTING: TECHNIQUES, CHALLENGES, AND FUTURE DIRECTIONS

Abdulrahman Mohammed Saba[1], Alfa Muhammad[2], Sayuti Musa Shafi'i[3]

Department of Networking and Cloud Computing, The Federal Polytechnic Bida, Nigeria[1]

Department of Cyber Security and Data Protection, The Federal Polytechnic Bida, Nigeria[2]

Department of Information Technology, Continental Transfert Technique Limited, Abuja, Nigeria[3]

Abstract: The research presents a comprehensive survey of AI-driven intrusion detection systems designed for cloud and edge computing environments. The review systematically analyses recent research developments between 2015 and 2025, focusing on the application of supervised, unsupervised, semi-supervised, and hybrid learning techniques for network intrusion detection. It examines widely used algorithms such as Support Vector Machines, Random Forests, Convolutional Neural Networks, Recurrent Neural Networks, and emerging models including Transformer architectures and Graph Neural Networks. In addition, the survey evaluates commonly used benchmark datasets, such as NSL-KDD, CIC-IDS2017, and UNSW-NB15, which are widely employed to assess detection performance and model generalization. AI-driven intrusion detection systems represent a promising direction for strengthening cybersecurity in distributed cloud and edge computing ecosystems. By integrating advanced machine learning techniques with scalable and privacy-aware architectures, future IDS solutions can provide more intelligent, resilient, and proactive defence mechanisms against increasingly sophisticated cyber threats.

Keywords: Application, Algorithms, Models, Datasets.

I. INTRODUCTION

Over the past two decades, cloud computing has significantly transformed the digital landscape. It has evolved from basic virtualization into a complex ecosystem supporting sophisticated technologies such as artificial intelligence, machine learning, and edge computing [13]. Edge computing and cloud-native technologies have become key paradigms for meeting the growing demands of real-time, low-latency applications [12]. By integrating cloud and edge infrastructure, a modern, highly distributed computing framework has been built. This architecture is crucial for supporting demanding new applications such as real-time analytics and autonomous systems, but the resulting complexity also increases the difficulty of security oversight and cyberattack defence.

[12] categorized vulnerabilities into four areas: data, network, application, and user-related issues, highlighting the ineffectiveness of traditional security tools. [8], emphasized that resource-constrained IoT devices are a key driver of attacks, particularly DDoS attacks and malware intrusions. [25], based on literature, pointed out that IoT vulnerabilities are caused by resource-constrained devices and invalid authentication frameworks. Other studies have also analyzed and acknowledged the threats existing between the cloud and IoT; for example, [29] revealed systemic threats arising from data in transit, device heterogeneity, and the lack of standardized security mechanisms. All these studies indicate that flawed security models, interoperability issues, and the lack of adaptive defence mechanisms are significant causes of IoT vulnerabilities in the cloud.

Traditional intrusion detection mechanisms, especially signature-based systems, face numerous challenges in this environment. While signature-based matching and rule-based methods are effective against known static attacks, they fail to detect novel, polymorphic, or covert attacks and often exhibit high false negative rates in dynamic environments [14]). Furthermore, centralized intrusion detection system architectures introduce unacceptable latency and bandwidth costs when monitoring geographically dispersed edge nodes or managing encrypted streams and short-lived cloud instances. These limitations have prompted a shift from signature-based detection to adaptive, behavior-based techniques to better identify patterns of benign and malicious activity.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154200

Artificial intelligence (AI), encompassing traditional machine learning (ML) and modern deep learning (DL), has become a key driver for next-generation intrusion detection systems (IDS), enabling near real-time adaptive threat detection across cloud and edge infrastructures. ML/DL methods can learn complex feature representations from high-dimensional telemetry data (network traffic, logs, system calls), detecting anomalies without explicit signatures and adapting to attackers' evolving strategies [16; 28]. Meanwhile, distributed learning paradigms, such as federated learning, allow for collaborative model training without centralizing sensitive data, which is highly attractive for privacy-conscious edge deployments [42]. However, the application of AI in cloud/edge IDS also presents new technical challenges (data heterogeneity, conceptual drift, resource limitations, interpretability, adversarial manipulation) that must be addressed to achieve robust and deployable systems [55].

Given the increasing role of cloud and edge computing, and the evolving threat landscape, there is an urgent need to analyze and summarize the latest advancements in AI-driven intrusion detection technologies for these environments. A comprehensive analysis can illuminate existing technologies (feature engineering, machine learning/deep learning models, distributed and privacy-preserving learning), highlight operational and research challenges (scalability, power and bandwidth limitations, adversarial threats, interpretability), and point to promising future directions (lightweight on-device models, adaptive continuous learning, secure federated approaches). This is the starting point of this paper: "Analysis of AI-Driven Intrusion Detection Systems for Cloud and Edge Computing: Technologies, Challenges, and Future Directions." This paper aims to integrate existing technologies and provide a roadmap for researchers and practitioners seeking resilient and practical intrusion detection system solutions suitable for distributed cloud edge ecosystems.

II. SCOPE AND CONTRIBUTIONS

The review systematically examines AI-based intrusion detection systems (AI-IDS) specifically designed for cloud and edge computing environments, focusing on literature published between 2015 and 2025. Cloud and edge environments have become an integral part of modern distributed applications, but due to their scalability, heterogeneity, and decentralized management, they remain highly vulnerable to sophisticated cyberattacks [4; 56]. Traditional signature-based intrusion detection systems often fail to detect emerging, zero-day, and dynamic threats [31]. Therefore, artificial intelligence technologies, particularly machine learning (ML), deep learning (DL), and collaborative learning frameworks, are being adopted to improve detection accuracy and adaptability [38].

The scope of this review encompasses various AI methodologies, including supervised learning, anomaly detection, ensemble models, deep architectures (e.g., CNNs, RNNs, Transformers), and distributed learning paradigms such as federated learning for privacy-preserving intrusion detection systems (IDS) [61]. It also examines cloud-based, edge, and hybrid IDS architectures with respect to latency, privacy, power constraints, scalability, and detection performance [9]. Evaluation practices, datasets (e.g., NSL-KDD, CICIDS2017, UNSW-NB15), adversarial robustness, and explainability are analyzed to assess current maturity and gaps in the field [27].

The research makes the following four main contributions:

i. A Comprehensive Classification of Artificial Intelligence Technologies in Intrusion Detection Systems (IDS)
We develop a structured classification system to categorize machine learning/deep learning (ML/DL) methods used in cloud/edge IDS, highlighting their computational advantages and disadvantages, detection capabilities, and feasibility in resource-constrained environments [38].

Table 1: CLASSIFICATION OF AI TECHNOLOGIES IN IDS

AI Methodology	Core Function	Common Techniques	Key Datasets
Supervised Learning	Classifies traffic into “benign” or “malicious” using labelled data.	SVM, Random Forest, CNN, RNN [cite: 303-305]	[cite_start]KDD’99, NSL-KDD, CIC-IDS2017
Unsupervised Learning	Identifies anomalies by detecting deviations from normal behavior.	K-Means, DBSCAN, Isolation Forest, Autoencoders.	CIC-IDS2017, UNSW-NB15.
Semi-Supervised/Hybrid	Combines labelled and unlabelled data to refine detection boundaries.	One-class SVM, Graph-based SVM, Hybrid CNN-RNN.	CIC-IDS2017.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154200

Deep Learning	Extracts complex spatiotemporal patterns from high-dimensional data.	CNN, LSTM, Transformers, GNNs [cite: 326-328].	[cite_start]CIC-IDS2017, UNSW-NB15.

ii. A Comparative Analysis of Cloud and Edge IDS Architectures
We analyze architectural design schemes (centralized analytics in the cloud and distributed inference at the edge), considering latency sensitivity, bandwidth consumption, privacy, and collaboration between infrastructure layers [9].

TABLE 2: COMPARATIVE ANALYSIS OF CLOUD AND EDGE IDS ARCHITECTURES

Architecture	Description	Key Advantages	Major Limitations
Centralized (Cloud)	Data is aggregated on high-capacity cloud servers for analysis.	Global visibility, supports complex AI models.	High latency, bandwidth costs, privacy risks.
Edge-Based	Decisions are made locally on gateways or IoT devices.	Near real-time response, improved privacy.	Limited CPU/Memory, restricted model complexity.
Hybrid	Combines edge inference with cloud-based model training.	Balances low latency with high-precision analysis.	Design complexity, orchestration overhead.
Federated (FIDS)	Nodes collaboratively train models without sharing raw data.	Enhanced privacy, compliant with regulations.	Communication overhead, model divergence.

iii. Identifying Key Challenges and Research Gaps
We addressed several limitations, including a lack of interpretability [51], privacy risks in collaborative training [46], model vulnerability to adversary and poisoning attacks [51], and insufficient real-world datasets and inadequate evaluation rigor [49].

iv. Future Research Roadmap
We proposed future research directions, including lightweight and efficient models, robust adversary-trained intrusion detection systems, interpretable learning mechanisms, concept drift detection, and standardized multi-platform benchmarks to enhance reliability and operational readiness [56].

By combining architectural analysis, AI method classification, and security-oriented evaluation, this review provides a unified and forward-looking reference for researchers and practitioners dedicated to improving network resilience in cloud and edge environments.

2.1 Supervised Learning in Intrusion Detection Systems

Intrusion detection systems (IDS) are essential for the protection of advanced communication networks. These systems were primarily designed to identify particular patterns, signatures, and rule violations. Machine Learning and Deep Learning approaches have been used in recent years in the field of network intrusion detection to provide promising alternatives. These approaches can discriminate between normal and anomalous patterns. In this paper, the NSL-KDD (Network Security Laboratory Knowledge Discovery and Data Mining) benchmark data set has been used to evaluate Network Intrusion Detection Systems (NIDS) by using different machine learning algorithms such as Support Vector Machine, J48, Random Forest, and Naïve Bytes with both binary and multi-class classification [60]. Traditional decision tree algorithms are susceptible to bias when certain classes dominate the dataset and prone to overfitting, particularly if they are not pruned. Previous studies have shown that combining several models can mitigate these issues by improving predictive accuracy and robustness. In the study, a novel approach was proposed to address these challenges by constructing multiple selective decision trees using the entirety of the input dataset and employing a majority voting scheme for output forecasting. The method outperforms competing algorithms, including KNN, Decision Trees, Random Forest, Bagging, XGB, Gradient Boost, and ExtraTrees, achieving superior accuracy in five out of ten datasets. This practical exploration highlights the effectiveness of our approach in enhancing decision tree performance across diverse datasets [44]. Deep Learning (DL) has recently emerged as a transformative approach for NIDS by learning complex representations of normal and malicious traffic patterns without the need for extensive manual feature engineering. The survey provides a review of recent progress in DL for NIDS and introduces a taxonomy with four categories. These include reconstruction and generative models that detect anomalies, Transformer-based sequence models for capturing

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154200

temporal dependencies, convolutional and deep neural networks for supervised classification, and hybrid or deployment-oriented approaches that combine techniques or support real-world deployment needs. The survey reviews 31 studies published between 2020 and 2025, covering their datasets, feature sets, model architectures, and reported performance. A comparative analysis highlights common practices and emerging trends [44].

Zero-day attacks pose a significant challenge in cybersecurity, as they exploit previously unknown vulnerabilities and circumvent traditional signature-based defenses. By combining machine learning, deep learning, and behavioral analytics, the framework detects abnormal system behavior and identifies malicious activity in real-time. Unsupervised anomaly detection, sequence-based neural models, and AI-supported threat intelligence are employed to forecast potential weaknesses and predict exploit trajectories before active exploitation occurs. Observations from experimental analysis demonstrate that AI-enabled defenses reduce false alarms, accelerate response time, and improve proactive security. The study confirms that intelligent, data-driven systems significantly enhance resilience against previously unknown and rapidly evolving cyber threats [11]. Therefore, while supervised learning is excellent for detecting misuse, its practical applications largely depend on adaptive training strategies, automated labelling processes, and integration with complementary anomaly-based methods.

2.2 Unsupervised Learning for Intrusion Detection Systems

Unsupervised learning plays an essential role in anomaly-based IDS, as it identifies deviations from the network's learned normal behavior without relying on labelled attack samples. Cluster-based methods, such as K-Means and DBSCAN, have been used extensively to group similar traffic patterns and isolate outliers as potential attacks, providing good detection capabilities for new threats [2]. Density-based methods improve the detection of irregular attack behavior that does not fit traditional cluster shapes [24]. Isolation Forest has gained popularity due to its efficiency with high-dimensional data and its ability to directly score anomalies using a random tree structure, making it suitable for large-scale cloud traffic monitoring [33]. Recent advances include unsupervised deep models such as autoencoders, variational autoencoders (VAEs), and generative adversarial networks (GANs) to learn compact latent representations of normal network activity, leading to improved detection on modern datasets such as CIC-IDS2017 and UNSW-NB15 [43]. However, unsupervised detectors often suffer from high false positive rates, as changes in legitimate usage patterns (e.g., workload spikes or new services in a cloud environment) can be incorrectly flagged as malicious [49]. Furthermore, their effectiveness relies heavily on feature engineering, normalization, and threshold tuning, which can be challenging in dynamic edge networks with limited computational resources. Despite these drawbacks, unsupervised learning remains a fundamental approach to zero-day intrusion detection and remains essential where labelled data is scarce or impractical.

2.3 Semi-Supervised and Hybrid Learning for Intrusion Detection Systems

Semi-supervised learning has become increasingly important in IDS because tagged attack data is often sparse or incomplete in real-world implementations. These methods use a large amount of untagged traffic to learn a reference model of normal activity generally considered mostly harmless as well as a small tagged subset to refine the classification boundary [19]. One-class and graph-based semi-supervised SVM techniques have proven effective in identifying anomalies in dynamic cloud and IoT environments, where manual tagging is not practical [56]. On the other hand, hybrid IDS architectures combine supervised misuse detection with unsupervised anomaly detection to balance detection coverage and operational reliability. Common designs involve training signature-based classifiers to detect known attacks, while routing uncertain or new patterns to an anomaly-based module, thereby reducing false positives and improving zero-day detection [57]. Recent hybrid deep learning frameworks integrate autoencoders with CNN or RNN layers, enabling automatic feature extraction and robust classification on cloud traffic datasets such as CIC-IDS2017 [30]. Despite their excellent performance, semi-supervised and hybrid models introduce operational difficulties: decision fusion, alert prioritization, and synchronized retraining on distributed edge nodes can be expensive, and performance can still degrade under conceptual drift or adversarial manipulation [44]. However, their ability to reduce tagging requirements while improving new intrusion detection makes them an attractive direction for scalable cloud-edge IDS deployments.

2.4 Applications of Deep Learning in Intrusion Detection Systems

Deep learning (DL) has become a major research direction in the field of intrusion detection systems (IDS) due to its ability to automatically extract complex spatiotemporal patterns from high-dimensional network traffic. Convolutional neural networks (CNNs) have been widely used in packet- and flow-based intrusion detection because they can effectively capture structural dependencies in traffic feature maps, thereby improving the accuracy of detecting modern attack vectors on datasets such as CIC-IDS2017 and UNSW-NB15 [40]. Recurrent architectures, such as Long Short-Term Memory (LSTM) networks and Closed Recurrent Units (GRUs), can capture time-dependent attack behaviors, such as DDoS burst attacks and slow botnet propagation, and have demonstrated robust modeling capabilities for sequential traffic data in IoT and cloud systems [3]. In recent years, Transformer-based encoders and graph neural

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154200

networks (GNNs) have attracted significant attention due to their scalability and ability to model long-range interactions and topological behaviors in distributed networks [21].

Generative machine learning models, such as Auto Encoders (AEs), vibrational auto encoders (VAEs), and generative adversarial networks (GANs), further enhance anomaly-based detection capabilities by learning latent representations of normal network states and labelling deviations to detect potential zero-day threats [7]. However, deploying machine learning-based intrusion detection systems (IDS) in resource-constrained edge environments remains challenging due to high computational and memory costs and latency issues [59]. To overcome these limitations, lightweight deep learning techniques (network pruning, quantization, attention mechanism simplification, and knowledge distillation) are being integrated into models to compress them while maintaining detection accuracy [64]. However, deep learning methods are sometimes considered a "black box," hindering trust in incident response and operational security workflows [30]. Adversarial machine learning attacks can also threaten model integrity through shielding or poisoning strategies, requiring robust training and defence mechanisms [49].

Despite these challenges, deep learning continues to advance in detection generalization capabilities and adaptability to evolving cloud edge environments, making it a key driver for next-generation intelligent intrusion detection system (IDS) solutions.

III. RESOURCE-AWARE IMPLEMENTATION: CLOUD VS. EDGE CONSIDERATIONS

The deployment architecture of an IDS significantly impacts the selection and performance of AI techniques, especially as organizations increasingly distribute computing across the cloud and edge layers. Cloud-based IDSs benefit from nearly elastic computing resources, enabling the use of deep neural architectures and large-scale batch analysis for traffic classification and threat intelligence aggregation [63]. However, centralized processing introduces latency, bandwidth overhead, and privacy concerns by continuously streaming large volumes of traffic from distributed nodes to the cloud [29]. On the other hand, edge-based IDSs process data locally, closer to the source (e.g., IoT devices or edge gateways), improving responsiveness and autonomy in scenarios requiring near-real-time detection [1]. However, memory, CPU, and energy budget constraints reduce model complexity, requiring lightweight inference strategies such as model pruning, quantization, knowledge distillation, and online learning [29]. Federated learning has emerged as an attractive approach to address the cloud-to-edge tradeoff by jointly training global models on decentralized data sources without sharing raw traffic, thereby enhancing privacy and maintaining scalability [46]. Despite their advantages, federated IDSs can suffer from model divergence and increased communication overhead between different nodes, requiring robust aggregation schemes and compression techniques [39]. Adaptive hybrid architectures where the cloud handles training and global coordination, while the edge performs optimized inference are increasingly recognized as a practical deployment model for secure and scalable AI-based intrusion detection systems (IDS) in modern distributed systems [4].

Overall, the cloud provides advanced intelligence capabilities, while the edge provides fast and privacy-preserving threat detection; therefore, aligning AI model design with deployment constraints remains an important research and engineering priority.

IV. KEY CHALLENGES AND RESEARCH GAPS IN AI-DRIVEN INTRUSION DETECTION SYSTEMS FOR CLOUD AND EDGE COMPUTING

While AI-driven intrusion detection systems (IDS) have demonstrated significant potential for threat detection, several unresolved challenges limit their deployment effectiveness in cloud-edge ecosystems. These challenges encompass multiple aspects, including computational resource constraints, model robustness, data quality, privacy protection, and deployment scalability.

4.1 Resource Constraints and Optimization

AI-driven IDS (especially deep neural networks) require substantial computational resources for training and inference. Edge devices typically have limited CPU capacity, memory, and battery power; therefore, without optimization, deploying large-scale machine learning models will be difficult [39; 64]. Techniques such as model pruning, quantization, and lightweight architectures are being explored, but these techniques often reduce detection accuracy or generalization performance [59]. Furthermore, real-time intrusion detection imposes strict latency constraints, posing a challenge to the feasibility of resource-intensive models on heterogeneous edge nodes [18]. Ensuring efficient scaling of models across thousands of distributed devices remains an open research topic.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154200

4.2 Adversarial Vulnerabilities and Model Robustness

AI models used in intrusion detection systems (IDS) are vulnerable to adversarial machine learning (AML) attacks, where attackers craft malicious inputs to evade detection [21]. In federated networks, attackers may inject malicious gradients (data poisoning) or manipulate local model updates to degrade global performance. Moreover, due to insufficient understanding of normal network behavior, evasion attacks against anomaly detectors remain difficult to defend against [32]. Defence strategies such as robust aggregation, adversarial training, and authentication detection are still under development and lack comprehensive evaluation in real-world cloud-edge deployments.

4.3 Data Quality and Threat Imbalance

Training reliable intrusion detection system (IDS) models requires high-quality labelled datasets. However, real-world network environments typically provide noisy, unlabelled, and highly imbalanced data, with normal traffic far exceeding attack traffic [26; 44]. Therefore, supervised learning methods struggle to detect zero-day attacks or rare attack patterns. Using generative adversarial networks (GANs) and data augmentation techniques to generate synthetic data can help, but may introduce bias or unrealistic traffic distributions [6]. Furthermore, cloud-hosted applications generate constantly changing traffic patterns, which, unless continuously updated, can lead to concept drift and degraded model performance [46].

4.4 Privacy and Data Confidentiality Issues

Cloud-based intrusion detection systems (IDS) often require centralized aggregation of network traffic logs, which exposes sensitive user information and presents compliance challenges under data protection regulations [1]. Federated learning and edge learning improve privacy by keeping data locally, but metadata exchange (e.g., gradients or feature statistics) still carries the risk of information leakage through inference attacks [53]. Secure sharing mechanisms such as differential privacy, cryptographic model updates, and blockchain-based trust management remain computationally expensive or difficult to scale reliably.

4.5 Scalability, Interoperability and Deployment Management

Cloud edge environments consist of diverse hardware, communication protocols, and network policies. Coordinating intrusion detection in such heterogeneous environments presents significant compatibility challenges [29]. Large-scale deployments also incur high communication overhead, especially in collaborative or federated intrusion detection system frameworks requiring continuous synchronization [46]. The dynamic nature of edge networks frequent node joining, leaving, or moving further increases the complexity of centralized orchestration and adds to the configuration burden on system administrators.

Based on the identified challenges, the following gaps remain:
i. Lack of standard benchmarks and real-world deployment test platforms for cloud edge intrusion detection systems (IDS).
ii. Limited cross-layer intelligent fusion for collaborative detection.
iii. Lack of accurate, understandable AI models for the resource-constrained edge.
iv. Weak defenses against poisoning and adversarial attacks in federated IDS.
v. Need for lifelong adaptive learning to correct conceptual drift in changing networks.
Addressing these gaps is crucial to achieving secure, intelligent, and sustainable cloud edge IDS solutions.

V. CONCLUSION

In conclusion, the survey has provided a comprehensive analysis of AI-driven Intrusion Detection Systems (IDS) designed for cloud and edge computing environments. The review examined recent developments in artificial intelligence techniques, including supervised, unsupervised, semi-supervised, and deep learning models, and assessed their applicability in detecting modern cyber threats across distributed infrastructures. The study highlighted that traditional signature-based intrusion detection mechanisms are increasingly inadequate in highly dynamic cloud-edge ecosystems due to their inability to detect zero-day and evolving attacks. In contrast, AI-based approaches demonstrate strong potential in improving detection accuracy, adaptability, and real-time threat identification by learning complex behavioural patterns from large-scale network data.

The review also compared different deployment architectures, including centralized cloud-based IDS, edge-based IDS, hybrid models, and federated intrusion detection frameworks. Each architecture offers distinct advantages and limitations depending on factors such as latency requirements, computational resources, privacy constraints, and scalability. Hybrid and federated approaches appear particularly promising because they combine the computational power of the cloud with the responsiveness and privacy benefits of edge environments.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154200

Despite significant advancements, several critical challenges remain. These include resource limitations in edge devices, vulnerability of AI models to adversarial attacks, insufficient high-quality datasets, privacy risks associated with centralized data collection, and the lack of standardized evaluation benchmarks. Addressing these issues is essential for the successful deployment of reliable AI-driven IDS in real-world cloud-edge infrastructures.

Future research should therefore focus on developing lightweight and interpretable AI models, improving adversarial robustness, enhancing privacy-preserving learning techniques such as federated learning, and establishing standardized datasets and evaluation frameworks. Additionally, adaptive and continuous learning mechanisms capable of handling concept drift in dynamic network environments will be crucial for maintaining long-term detection performance.

Overall, AI-driven intrusion detection systems represent a promising direction for strengthening cybersecurity in distributed cloud and edge computing ecosystems. By integrating advanced machine learning techniques with scalable and privacy-aware architectures, future IDS solutions can provide more intelligent, resilient, and proactive defence mechanisms against increasingly sophisticated cyber threats.

REFERENCES

[1] Abouelmehdi, K., Beni-Hssane, A., & Khaloufi, H. (2018). Big data security and privacy in healthcare: A review. Procedia Computer Science, 113, 73–80.
[2] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.
[3] Almiani, M., AbuGhazaleh, A., Alauthman, M., Jararweh, Y., & Ridhawi, I. (2020). Deep recurrent neural network for IoT intrusion detection system. Simulation Modelling Practice and Theory, 101, 102031.
[4] Almiani, M., AbuGhazleh, A., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. Future Generation Computer Systems, 110, 141–150.
[5] Aloqaily, M., Otoum, S., Al Ridhawi, I., & Jararweh, Y. (2021). Design of autonomous and secure edge computing frameworks: Opportunities and challenges. IEEE Network, 35(2), 246–253.
[6] Alqahtani, S., Altamimi, A., & Alhussein, M. (2021). GAN-based cyber-attack detection in IoT environments. IEEE Access, 9, 85472–85483.
[7] Al-Rawashdeh, K., & Al-Sultan, A. (2019). Anomaly-based intrusion detection system using deep learning. Procedia Computer Science, 151, 100–107.
[8] Alsamiri, J., & Alsubhi, K. (2023). Federated learning based intrusion detection systems in Internet of Vehicles: A literature survey. Future Internet, 15, 403.
[9] Ammar, M., Russello, G., & Crispo, B. (2021). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 58, 102718.
[10] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2020). On the effectiveness of ML for cyber security. Computers & Security, 92, 101747.
[11] Archana, P., Kumaravel, S., & Gayathri, D. K. (2026). Artificial intelligence-based zero-day attack detection and proactive mitigation strategies: A literature review. International Research Journal on Advanced Engineering Hub, 4(2), 474–480.
[12] Arivola. (2021). Edge computing and cloud-native technologies: Synergies for real-time, low-latency application. International Journal of Computer Engineering and Technology, 12(1), 114–125.
[13] Awaluddin, M., & Windiarti, I. S. (2025). Cloud computing technology and its development in the last 20 years: Trends, challenges, and future directions. Jurnal Ilmiah Universitas Muhammadiyah Buton, 11(3), 673–686.
[14] Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy (Technical Report). Chalmers University of Technology.
[15] Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.
[16] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
[17] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599–616.
[18] Can Bertin, M. A., Wang, S., & Haider, S. A. (2022). Federated learning for intrusion detection in IoT: Concepts, challenges and future directions. Future Internet, 14(2), 49.
[19] Chapelle, O., Schölkopf, B., & Zien, A. (2006). Semi-Supervised Learning. MIT Press.
[20] Chen, Q., Li, Y., & Wen, S. (2019). A collaborative intrusion detection mechanism against DDoS attacks in cloud computing. IEEE Access, 7, 41925–41933.

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154200

[21] Cheng, L., Deng, J., & Wang, Y. (2023). Graph neural networks for network intrusion detection: A survey. Computers & Security, 124, 103036.
[22] Derhab, A., Guerroumi, M., Belaoued, M., & Ghazali, R. (2022). Deep learning for intrusion detection systems: Taxonomy, challenges, and solutions. IEEE Access, 10, 11034–11054.
[23] Dhanabal, L., & Shantharajah, S. P. (2015). A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. International Journal of Advanced Research in Computer and Communication Engineering, 4(6), 446–452.
[24] Ertöz, L., Steinbach, M., & Kumar, V. (2003). Finding clusters of different sizes, shapes, and densities in noisy, high dimensional data. In SDM (pp. 47–58). SIAM.
[25] Fei, W., Ohno, H., & Sampalli, S. (2023). A systematic review of IoT security: Research potential, challenges, and future directions. ACM Computing Surveys, 56(5), 1–40.
[26] Ferrag, M. A., Maglaras, L., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 54, 102526.
[27] Garcia-Teodoro, P., Maciá-Fernández, G., Díaz-Verdejo, J., & Estepa, A. (2022). Network anomaly detection: Evolution, challenges, and research opportunities. Computer Communications, 190, 324–343.
[28] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
[29] Hameed, S., & Alomari, E. (2020). Cybersecurity challenges in cloud computing: State of the art and future directions. Cluster Computing, 23, 1961–1984.
[30] Hindy, H., Brosset, D., Bayne, E., Seeam, A., Atkinson, R., & Tachtatzis, C. (2020). A taxonomy and survey of intrusion detection system design techniques, network threats and datasets. IEEE Communications Surveys & Tutorials, 22(3), 2416–2451.
[31] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2017). Threat analysis of IoT networks using AI-based IDS. IEEE CSR, 375–382.
[32] Hussain, F., Hussain, R., & Kim, H. (2022). Adversarial attacks and defenses in distributed AI systems: A survey. IEEE Access, 10, 44191–44215.
[33] Kabir, S., Shufian, A., & Zishan, S. R. (2023). Isolation Forest-based anomaly detection and fault localization for solar PV system. ICREST Conference, Dhaka.
[34] Khan, R. U., Zhang, X., Kumar, R., Sharif, A., & Tareen, A. K. (2019). Network intrusion detection system using machine learning. International Journal of Advanced Computer Science and Applications, 10(5), 402–411.
[35] Kim, J., Kim, J., Kim, H., & Kim, H. (2016). Long short-term memory recurrent neural network classifier for intrusion detection. International Conference on Platform Technology and Service, 1–5.
[36] Liang, W., Guo, Y., Li, J., & Wang, K. (2020). Deep semi-supervised learning for network intrusion detection. IEEE Access, 8, 111113–111122.
[37] Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. In ICDM (pp. 413–422). IEEE.
[38] Liu, H., Zhang, Y., & Chen, Z. (2023). Deep learning for network intrusion detection in distributed environments. IEEE Access, 11, 24645–24660.
[39] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 37(3), 50–60.
[40] Lopez-Martin, M., Carro, B., & Sanchez-Esguevillas, A. (2020). Deep learning for end-to-end network traffic classification. IEEE Communications Surveys & Tutorials, 22(3), 1777–1801.
[41] MacQueen, J. (1967). Some methods for classification and analysis of multivariate observations. In Fifth Berkeley Symposium (pp. 281–297).
[42] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. AISTATS.
[43] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. NDSS Symposium.
[44] Moustafa, N., Janicke, H., & Sitnikova, E. (2019). Addressing concept drift for effective cyber-security. Future Generation Computer Systems, 97, 443–454.
[45] Otoum, S., Kantarci, B., & Mouftah, H. (2020). On the feasibility of AI-based intrusion detection in fog computing. IEEE Internet of Things Journal, 7(7), 7428–7438.
[46] Pokhrel, S. R., & Choi, J. (2020). Federated learning with blockchain for IoT. IEEE Internet of Things Journal, 7(10), 9466–9480.
[47] Revathi, S., & Malathi, A. (2013). A detailed analysis on NSL-KDD dataset using various machine learning techniques. International Journal of Engineering Research & Technology, 2(12), 1848–1853.
[48] Rigaki, M., & Garcia, S. (2020). A survey of adversarial machine learning in network intrusion detection systems. ACM Computing Surveys, 53(4), 1–33.
[49] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167.

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154200

[50] Sharma, A., & Mittal, A. (2021). Anomaly detection in network traffic using isolation forest. Procedia Computer Science, 189, 222–229.
[51] Sharma, T., Gupta, S., & Shukla, A. (2022). Explainable AI in cybersecurity: A survey. ACM Computing Surveys, 55(11), 1–38.
[52] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646.
[53] Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. IEEE Symposium on Security and Privacy, 3–18.
[54] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.
[55] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.
[56] Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A., & Ghogho, M. (2022). Deep learning approaches for network intrusion detection. IEEE S&P Workshops, 95–102.
[57] Thakkar, A., & Lohiya, R. (2020). A survey on intrusion detection in Internet of Things. Sensors, 20(16), 4369.
[58] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Al-Nemrat, A. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550.
[59] Xu, J., & Saad, W. (2019). Latency minimization for efficient federated learning in edge computing. IEEE GLOBECOM, 1–6.
[60] Yasmeen, S. A., Bader, A., & Amr, A. M. (2022). Network intrusion detection using machine learning techniques. Advances in Science and Technology Research Journal, 16(3), 193–206.
[61] Zahoor, Z., Ali, S., & Kim, H. (2023). Federated deep learning for edge IDS: A comprehensive review. IEEE Communications Surveys & Tutorials, 25(1), 548–572.
[62] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service flooding attacks. IEEE Communications Surveys & Tutorials, 15(4), 2046–2069.
[63] Zhang, Y., Carlinet, E., Montessuit, R., & Lacoste-Julien, S. (2021). Scalable neural-network-based intrusion detection systems for high-speed networks. IEEE Transactions on Network and Service Management, 18(1), 265–279.
[64] Zhao, L., Pan, Z., Liu, Y., & Tang, Y. (2021). Lightweight deep learning models for intrusion detection in IoT environments. IEEE Internet of Things Journal, 8(14), 11145–11154.
[65] Zhu, X. (2005). Semi-supervised learning literature survey. Technical Report, University of Wisconsin–Madison.

 This work is licensed under a Creative Commons Attribution 4.0 International License