AI-Powered Intrusion Detection and Prevention Systems for the Next Generation Network

Temitope Damilola Elijah [1], **Akinsola Akintunde Samuel** [2], **Olayemi Babawole Familusi** [3]

[1] *Georgia Southern University*
1332 Southern Drive, Statesboro, GA 30458, USA

[2] *Sheffield Hallam University*
Howard Street, Sheffield, S1 1WB, UK

[3] *University of Ibadan*
Oduduwa Road, 200132, Ibadan, Nigeria

DOI: 10.22178/pos.123-3

LCC Subject Category: T1-995

Received 16.09.2025
Accepted 27.10.2025
Published online 31.10.2025

Corresponding Author:
Temitope Damilola Elijah

Abstract. The rapid evolution of next-generation networks (NGNs), driven by 5G, IoT, edge computing, and software-defined networking, has introduced new opportunities alongside complex security challenges. Traditional intrusion detection and prevention systems (IDS), built on signature-based and anomaly-based methods, struggle to cope with the scale, heterogeneity, and dynamic threat landscape of NGNs. In response, artificial intelligence (AI) has emerged as a powerful enabler of modern IDPS. This review surveys AI-powered approaches, beginning with classical machine learning methods such as decision trees, support vector machines, and random forests, and then examining deep learning architectures including convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory networks (LSTMs), and autoencoders. It further analyses hybrid frameworks that integrate ensemble learning, federated learning, and meta-learning, as well as specialised methods tailored for SDN, IoT, edge, and cloud/5G environments. Benchmark datasets, including NSL-KDD, CICIDS2017, UNSW-NB15, Bot-IoT, IoT-23, and TON_IoT, are reviewed, highlighting their contributions and limitations. The paper identifies key challenges, including dataset scarcity, generalisation gaps, computational overhead, adversarial robustness, explainability, and privacy. Future directions emphasise the need for realistic NGN datasets, lightweight yet accurate architectures, privacy-preserving and federated frameworks, and integrated detection and prevention mechanisms. Overall, AI-powered IDPS demonstrate significant potential to secure NGNs, but realising this vision will require advances that balance accuracy, efficiency, interpretability, and resilience.

Keywords: Artificial intelligence; Intrusion detection and prevention systems (IDPS); Next generation networks (NGNs); Deep learning.

INTRODUCTION

The rise of modern communication infrastructure, including 5G, edge computing, the Internet of Things (IoT), and software-defined networking (SDN), marks a paradigm shift in how devices connect, communicate, and share data. These next-generation networks (NGNs) promise ultra-low latency, massive device connectivity, high throughput, and dynamic service provisioning. However, they also introduce expanded attack surfaces, novel vulnerabilities, and complex threat landscapes that traditional security mechanisms struggle to handle. In this context, Intrusion Detection and Prevention Systems (IDPS) become critical components of network defence. Leveraging Artificial Intelligence (AI), machine learning (ML), deep learning (DL), hybrid models, and related techniques offers powerful new tools to detect, prevent, and adapt to evolving threats. This review aims to synthesise recent developments in AI-powered IDPS for NGNs,

compare their capabilities, identify gaps, and outline future research directions.

Traditionally, IDPS systems have been built on signature-based models, anomaly-based detection, or a combination of the two. Signature-based systems rely on known attack patterns; they are effective against recognised threats but fail to detect zero-day attacks or variants of malware whose signatures are not in the database. Anomaly-based systems detect deviations from learned normal behaviour; while more adaptive, they often suffer from high false-positive rates, difficulties defining "normal" behaviour in dynamic networks, and challenges scaling to high data volumes. As NGNs grow in scale, heterogeneity, and speed owing to IoT endpoints, edge nodes, virtualised functions, and mobile devices, these traditional approaches confront significant limitations, including a lack of adaptability, slow response to new threats, inefficiencies under high loads, and an inability to preserve privacy in distributed settings.

AI-based methods have sought to address many of those shortcomings. In recent years, machine learning (ML) models, such as decision trees, random forests, support vector machines, and ensemble classifiers, have been applied to intrusion detection tasks, often combining signature-based and anomaly-based features to enhance the detection of both known and novel threats [1]. Deep learning approaches (e.g., convolutional neural networks, recurrent neural networks, LSTM, autoencoders) have been shown to achieve stronger performance in analysing complex, high-dimensional data such as network traffic, system logs, and time-series flows [2]. These methods can uncover subtle patterns and temporal correlations that are invisible to simpler models. For example, recent surveys emphasise that deep learning-based IDS (DL IDS) have improved generalizability in detecting zero-day intrusions or attacks with minimal prior knowledge [2, 3].

Nevertheless, even AI-based systems face challenges in NGN contexts. Key issues include real-time processing requirements, resource constraints in edge and IoT devices, non-independent and identically distributed (non-IID) data across distributed nodes, privacy concerns, and adversarial attacks targeting the detection systems themselves. Federated learning and privacy-preserving ML have emerged to address some of these issues, enabling collaborative model training without sharing raw data between endpoints (as in edge computing for 5G) [4]. Graph neural networks (GNNs) have also been investigated for capturing relational structures in network traffic or IoT topologies, enabling more nuanced detection of intrusion across connected entities (e.g., device groups) [5].

At the same time, practical deployment reveals further constraints. For example, real-time IDS/IPS in 5G networks must maintain very low latency and high throughput under heavy loads; many AI models that perform well in offline or benchmark settings degrade under real network traffic, especially when facing encrypted traffic, bursty traffic, or resource-constrained edge nodes (Security trade-offs) [6]. Furthermore, maintaining model interpretability, minimising false positives, and ensuring reliability under adversarial conditions are still open problems.

Given the above, hybrid AI-powered IDPS systems that combine multiple AI techniques (e.g., ML + DL or ensemble + federated learning), exploit both centralised and edge computing, integrate prevention (not just detection), and address privacy, efficiency, and robustness are emerging as promising solutions. These systems aim to leverage the strengths of various AI methods, compensate for individual weaknesses, and better align with the demanding requirements of NGNs. This review paper, therefore, focuses on hybrid and advanced AI approaches for intrusion detection and prevention in next-generation networks.

The objectives of this review are:

1) to survey the state of the art AI-powered IDPS techniques in NGN settings (5G, IoT, edge, SDN),

2) to compare their detection, prevention, efficiency, scalability, and privacy properties,

3) to identify significant challenges and gaps in current research, and

4) to suggest directions for future work.

RESULTS AND DISCUSSION

Background and Concepts. Following-generation networks (FGNs) represent a significant evolution in communication infrastructure, marked by features such as ultra-low latency, massive device connectivity, software-defined networking (SDN), network function virtualisation (NFV), edge computing, and the rapid expansion of the

Internet of Things (IoT). These characteristics enable flexible, programmable, and scalable services but simultaneously introduce complex security challenges. Traditional Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), while long considered critical components of cybersecurity defence, were not originally designed to operate in the dynamic, heterogeneous environments of NGNs. Researchers must carefully consider the foundations of IDS/IPS, their limitations, and the emerging role of artificial intelligence (AI) to contextualise recent research in this area.

Historically, intrusion detection systems have been categorised into two primary approaches: signature-based and anomaly-based. Signature-based systems detect intrusions by comparing network traffic or system behaviour with a database of known attack patterns. These systems are highly efficient at identifying threats with established signatures but fail to detect novel or zero-day attacks. By contrast, anomaly-based IDSs construct models of "normal" network behaviour and flag deviations as potential threats. Although they are more adaptable to unseen intrusions, anomaly-based systems often suffer from high false-positive rates and the difficulty of defining what constitutes "normal" behaviour in dynamic environments [7]. Hybrid detection methods aim to integrate both approaches to balance detection coverage and false alarm rates. Many studies suggest that hybrid systems are particularly effective in IoT-enabled NGNs [8]. Intrusion prevention systems extend the capabilities of IDS by actively blocking or mitigating detected intrusions. In NGNs, IPS solutions must operate in near real time, which places stringent demands on computational efficiency and latency.

The transition to NGNs exacerbates the limitations of traditional IDS/IPS. Networks in the 5G and IoT era are more heterogeneous, supporting billions of devices with diverse hardware and software capabilities. This scale increases both the attack surface and the variability of traffic patterns. Moreover, NGNs demand ultra-low latency and high throughput, leaving little tolerance for detection delays. Nonstationary environments arise from dynamic behaviours, such as mobile devices frequently joining and leaving networks or traffic patterns evolving with changing applications, which in turn undermine static detection models. Resource constraints on edge and IoT devices also limit the feasibility of deploying computationally intensive detection systems locally. At the same time, privacy concerns often restrict centralised data aggregation for training [9]. Finally, adversaries have begun designing evasive attacks specifically to exploit vulnerabilities in both traditional and AI-driven IDS models, further complicating detection in NGNs.

Researchers and developers have increasingly adopted AI-driven methods as the foundation of modern IDPS to address these challenges. While early applications of AI in intrusion detection used machine learning techniques such as decision trees, support vector machines, and random forests, the rise of deep learning has significantly expanded capabilities. Deep models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory networks (LSTMs) have demonstrated strong performance in analysing high-dimensional, sequential traffic data [2]. These architectures can capture subtle spatial and temporal patterns in network traffic that would otherwise go undetected.

Graph neural networks (GNNs) have emerged as promising tools for NGN intrusion detection due to their ability to capture the relational structures inherent in network traffic and device interactions. Systems such as E GraphSAGE demonstrated how graph embeddings can enhance anomaly detection across complex topologies [10]. At the same time, Anomal E showed that self-supervised GNNs can identify attacks without requiring extensive labelled data [11]. More advanced approaches, including BS GAT, incorporated graph attention mechanisms to enhance classification accuracy in edge computing environments [12]. Similarly, elastic GNNs (EL GNNs) were proposed to address catastrophic forgetting in continual learning scenarios, enabling intrusion detection systems to adapt to evolving threats without sacrificing performance on previously learned attack types [13].

The trend toward hybrid approaches is another notable development. By combining multiple AI methods — such as machine learning and deep learning, CNNs and LSTMs, or GNNs and transformers — researchers have sought to exploit the strengths of each technique while mitigating their weaknesses. These hybrid models have shown improved accuracy, robustness, and adaptability compared to single-method approaches, particularly under adversarial conditions and in highly dynamic NGN environments [12].

Survey of AI-Powered IDPS Methods. Artificial intelligence has become central to modern intrusion detection and prevention systems (IDPS), particularly in next-generation networks (NGNs). Classical machine learning (ML) methods, including decision trees, support vector machines (SVMs), and random forests, were among the first approaches applied to intrusion detection. These models relied heavily on feature engineering but achieved strong results on datasets such as NSL-KDD and CICIDS2017 [14, 15]. For example, authors [1] demonstrated that random forest classifiers achieved detection accuracies above 95%, highlighting the potential of ML-based systems. Nonetheless, their reliance on manually extracted features and difficulties with scalability limited their applicability to dynamic, large-scale NGNs.

Researchers subsequently introduced deep learning (DL) methods to overcome these shortcomings. Convolutional neural networks (CNNs) learn spatial relationships within network traffic data. In contrast, recurrent neural networks (RNNs) and long short-term memory (LSTM) models captured temporal dependencies in sequential traffic flows [2, 3]. Autoencoders were also widely applied for anomaly detection by reconstructing standard traffic patterns and identifying deviations. These methods consistently outperformed traditional ML-based approaches, especially in detecting zero-day attacks. However, their computational demands limit deployment in resource-constrained environments, such as IoT and edge devices.

Hybrid AI methods emerged to address the limitations of individual models. By combining CNNs with LSTMs, researchers demonstrated improved detection accuracy by leveraging both spatial and temporal features [16]. Ensemble approaches that fused multiple classifiers achieved greater robustness and reduced false positives, even under adversarial conditions [17]. Federated learning extended these hybrid concepts by enabling distributed training while preserving privacy, making it especially suitable for 5G and IoT scenarios [1]. Emerging research on meta learning has further suggested that models could adapt more quickly to new attack patterns in highly dynamic NGNs.

Specialised methods have also been developed for distinct NGN environments. In software-defined networks (SDN), where centralised controllers are highly vulnerable, AI-based IDPSs analyse flow statistics and achieve strong detection performance on benchmark datasets, such as UNSW NB15 [6]. IoT and edge computing contexts emphasised lightweight models capable of functioning under resource constraints. Graph neural networks (GNNs) proved particularly effective in this domain, with BS GAT achieving high accuracy by capturing relational patterns among IoT devices [12]. In cloud and 5G infrastructures, where traffic volumes are massive and latency requirements are stringent, researchers applied federated and transfer learning, as well as deep reinforcement learning, to develop scalable, adaptive IDPS frameworks [2].

The literature reveals a progression from interpretable but limited ML methods to more sophisticated DL models, and increasingly toward hybrid and specialised AI-powered IDPS. While ML methods remain useful for lightweight detection tasks, DL and hybrid approaches dominate in terms of accuracy and adaptability, particularly in complex NGN environments. Specialised solutions for SDN, IoT, and 5G further highlight the need to tailor IDPS architectures to specific network conditions.

Table 1 – Comparison of AI-Powered IDPS Methods

Category	Techniques	Datasets Used	Strengths	Weaknesses
ML-based IDPS	Decision Trees, SVM, RF	NSL KDD, CICIDS2017	Interpretable, low cost	Requires feature engineering, poor zero-day detection
DL based IDPS	CNN, RNN, LSTM, Autoencoders	CICIDS2017, UNSW NB15	Learns features automatically, with high accuracy	High computational cost, limited edge deployment
Hybrid AI Methods	CNN+LSTM, Ensembles, FL, Meta	CICIDS2017, UNSW NB15	Robust, adaptable, lower false positives	Complexity, adversarial vulnerabilities
SDN-based detection	CNN RNN, DL classifiers	UNSW NB15	High accuracy for controller traffic	Centralised attack target, latency issues
IoT/Edge Security	GNNs (BS GAT), lightweight DL	Bot IoT, IoT 23	Handles heterogeneity, relational analysis	Resource constraints, limited datasets
Cloud/5G Detection	FL, TL, RL-based IDPS	CICIDS2017, 5G traffic	Scalable, low-latency, adaptive prevention	High complexity, privacy concerns

Datasets and Benchmarks. The evaluation of intrusion detection and prevention systems (IDPS) has historically relied on benchmark datasets that capture network traffic and attack scenarios. These datasets play a crucial role in training, testing, and comparing AI-based models, as their quality and representativeness directly impact system performance. Early datasets, such as KDD'99 and its refined version, NSL-KDD, have been widely used for traditional machine learning models. While they are easy to use and remain popular in academic research, they are now considered outdated because they lack realistic NGN traffic characteristics and include redundant samples that bias detection performance.

More recent datasets, such as UNSW NB15 and CICIDS2017, were designed to address some of these limitations by incorporating modern attack types, diverse traffic flows, and more balanced distributions of benign and malicious data. UNSW NB15 contains nine attack categories, including exploits and denial-of-service (DoS) attacks, captured using realistic traffic emulation. CICIDS2017 includes botnet, DDoS, brute-force, and web-based attacks, making it one of the most comprehensive benchmarks for modern intrusion detection research. These datasets have been instrumental in advancing deep learning methods that leverage large, complex traffic patterns for feature learning.

For IoT and edge environments, specialised datasets have emerged. Researchers created the Bot IoT dataset to reflect IoT attack traffic, including distributed denial-of-service (DDoS) and information theft scenarios, generated in a realistic network testbed. Similarly, IoT 23, published by Stratosphere Laboratory, contains real IoT device traffic infected with malware, including the Mirai and Gafgyt botnets, making it highly valuable for AI-powered IDPS targeting IoT environments. However, both datasets are limited in terms of device diversity and attack variety compared to real-world deployments [18].

More recently, the TON_IoT dataset has been introduced to capture telemetry and flow data from IoT and industrial environments. TON_IoT includes logs from sensors, devices, and network traffic, providing a broader perspective on attacks targeting innovative environments. Despite its comprehensiveness, challenges such as data imbalance and the complexity of preprocessing remain. In 5G and NGN research, the availability of benchmark datasets is still limited. Some studies have relied on extensions of existing datasets, such as CICDDoS2019 for distributed denial-of-service attacks, or on synthetic 5G traffic generated in controlled testbeds [19]. The lack of standardised, publicly available NGN datasets is a significant research gap, as it hinders the evaluation of detection systems under realistic 5G, SDN, or edge conditions.

The benchmark datasets for IDPS have evolved from legacy KDD-based corpora to more realistic, domain-specific collections such as CICIDS2017, UNSW NB15, Bot IoT, and TON_IoT. Nevertheless, gaps remain, especially regarding comprehensive NGN-specific datasets that reflect the scale, heterogeneity, and adversarial conditions of modern network environments. The absence of such datasets remains a barrier to evaluating AI-powered IDPS in real-world scenarios.

Table 2 provides a comparative summary of commonly used datasets for AI-powered IDPS.

Table 2 – Commonly Used IDPS Datasets and Their Characteristics

Dataset	Year	Domain/ Scope	Strengths	Weaknesses
KDD'99	1999	Legacy TCP/IP traffic	Widely used, large-scale, and easy for baseline evaluation	Outdated, redundant samples, unrealistic attack mixes
NSL KDD	2009	Improved KDD'99	Removes redundancy, balanced dataset	Still outdated, lacks modern NGN traffic
UNSW NB15	2015	General network traffic	Includes nine attack types, realistic traffic emulation	Data imbalance in some attack classes
CICIDS 2017	2017	Enterprise networks	Rich modern attacks (botnet, brute force, web, DDoS)	High preprocessing complexity, large file sizes
CICDDoS 2019	2019	DDoS traffic	Focused on volumetric attacks, useful for DL models	Narrow scope, only DDoS attacks
Bot IoT	2018	IoT networks	Realistic IoT testbed, IoT-specific attacks	Limited device variety, lab-based traffic
IoT 23	2020	IoT malware traffic	Contains Mirai, Gafgyt, and other IoT botnets	Imbalanced classes, a small set of devices
TON_IoT	2021	IoT & Industrial IoT	Multisource telemetry, sensors, logs, and flows	Complex preprocessing, high imbalance

Challenges and Research Gaps. Although artificial intelligence has significantly advanced intrusion detection and prevention systems, several persistent challenges remain in next-generation networks (NGNs). Researchers identify these challenges as stemming from both the technical limitations of current approaches and the practical realities of NGN deployments, and they highlight several research gaps that must be addressed to build reliable and scalable solutions. One of the most pressing issues is the lack of standardised, realistic datasets for NGNs. While benchmark datasets such as NSL-KDD, CICID2017, UNSW-NB15, Bot-IoT, and TON_IoT have enabled rapid progress in AI-based IDPS research, they are limited in scope and do not fully capture the scale, heterogeneity, and adversarial complexity of real-world NGNs [2, 20, 21]. Most datasets are collected in controlled testbeds, which restricts diversity and introduces biases that hinder model generalisation. Furthermore, NGN-specific datasets that reflect traffic in 5G, SDN, and large-scale IoT ecosystems are scarce, leaving a gap between experimental evaluation and real-world applicability.

A second major challenge involves the generalisation and adaptability of AI models. Machine learning and deep learning models often achieve high accuracy on specific datasets but degrade substantially when applied to unseen environments. This lack of transferability arises from differences in traffic patterns, network configurations, and evolving attack strategies [3]. In dynamic NGNs, where new devices and services constantly alter traffic characteristics, static models quickly become outdated. Although approaches such as transfer learning, meta learning, and continual learning have been proposed, they remain underexplored in IDPS research and require further development to ensure robust performance across diverse scenarios. The computational overhead of deep and hybrid models is another barrier to deployment, especially in IoT and edge computing environments. Models such as CNNs, LSTMs, and transformers require significant processing power and memory, which may not be available on resource-constrained devices [12]. While lightweight architectures and model compression techniques have been explored, achieving a balance between detection accuracy and real-time efficiency remains an open problem. This challenge is particularly acute in 5G and edge settings, where latency requirements are stringent and delays in detection could compromise system reliability.

An additional research gap concerns the resilience of AI-powered IDPSs to adversarial attacks. Recent studies show that adversaries can deliberately craft inputs designed to evade detection models by exploiting their vulnerabilities. For example, carefully manipulated traffic features or adversarial perturbations can cause misclassification in both ML and DL models, raising concerns about robustness [17]. Despite growing awareness of this issue, relatively few IDPS solutions incorporate adversarial training or defensive mechanisms, leaving many systems vulnerable to targeted attacks.

The interpretability and explainability of AI-driven IDPS also remain unresolved challenges. Deep learning models, in particular, operate as black boxes, offering little transparency into their decision-making processes [2]. In high-stakes domains such as NGNs, where intrusion detection may inform legal, financial, or national security decisions, stakeholders require interpretable results to validate system outputs. Explainable AI (XAI) techniques are still underutilised in this field, representing a critical research opportunity. Privacy and data protection concerns add another dimension of complexity. Federated learning has been proposed as a means to mitigate risks by training models across distributed nodes without sharing raw data. Still, it introduces issues such as model poisoning, communication overhead, and synchronisation delays [1]. Researchers have not yet fully achieved the delicate balance between ensuring privacy and maintaining detection accuracy in large-scale NGNs.

Researchers have not yet comprehensively addressed the integration of detection with prevention. While many studies focus on improving detection accuracy, fewer examine automated prevention mechanisms that can operate safely in real time. Deep reinforcement learning and adaptive rule-based systems have shown promise for dynamic prevention in cloud and 5G networks, but these approaches remain experimental and require further validation before deployment [6]. The main research gaps in AI-powered IDPS for NGNs include the scarcity of realistic datasets, the limited generalisation and adaptability of models, the computational costs of deep learning architectures, vulnerability to adversarial attacks, the lack of interpretability, unresolved privacy issues, and insufficient focus on integrated

prevention. Addressing these gaps will require developing more diverse datasets, lightweight and adaptive AI architectures, adversarially robust models, explainable AI frameworks, and end-to-end detection and prevention systems.

Future Research Directions. The challenges and gaps identified in Section 6 highlight several critical directions for future research on AI-powered intrusion detection and prevention systems (IDPS) for next-generation networks (NGNs). Addressing these directions will be essential for developing systems that are not only accurate but also scalable, explainable, and resilient in real-world deployment. A priority area is the development of realistic and standardised NGN datasets. Future datasets should reflect the scale, heterogeneity, and dynamic conditions of 5G, IoT, SDN, and edge networks, including the capture of encrypted traffic, multimodal data (such as telemetry, logs, and flows), and adversarially generated intrusions. Collaborative initiatives among academia, industry, and government agencies could facilitate the generation of large-scale datasets, ensuring diversity across benign and malicious traffic. Researchers must also establish benchmarking standards to enable fair comparisons of models across studies, as fragmented evaluation practices currently hinder such comparisons [2, 20]. Another promising direction is the design of lightweight, efficient AI architectures for IoT and edge devices. Model compression, pruning, quantisation, and knowledge distillation could help reduce computational overhead while preserving detection accuracy [12]. Edge AI accelerators and hardware-aware neural architectures may also help make real-time intrusion detection feasible under strict latency constraints. In parallel, scalable cloud-based IDPS solutions will remain essential for heavy data processing, necessitating hybrid architectures that intelligently distribute workloads between edge and cloud environments.

Enhancing generalisation and adaptability is another critical goal. Researchers should further explore transfer learning, meta-learning, and continual learning approaches to develop IDPS that can adapt rapidly to new environments and evolving threats. For example, meta-learning techniques may allow a system to generalise across attack types and then fine-tune quickly to specific contexts. At the same time, continual learning methods can mitigate catastrophic forgetting when models are updated incrementally [3]. This adaptability will be crucial in NGNs, where traffic characteristics change frequently due to the dynamic nature of connected devices and services. Future research must also address the robustness of IDPS against adversarial attacks. Adversarial machine learning has shown that carefully crafted inputs can mislead even highly accurate deep learning models. Integrating adversarial training, defensive distillation, and anomaly-aware regularisation techniques into IDPS could significantly improve resilience. Furthermore, combining detection with moving-target defence strategies, in which system configurations dynamically change to confuse attackers, offers a promising but underexplored approach [17].

The incorporation of explainable AI (XAI) into IDPS represents another vital avenue. As deep learning and hybrid models become increasingly complex, explainability will be crucial to building trust among security analysts, operators, and decision-makers. Future systems should include interpretable layers or post hoc explanation modules that can highlight which features or flows contributed to a decision [2]; this not only improves transparency but also assists in forensic analysis, compliance, and legal validation of intrusion evidence. Privacy-preserving learning frameworks will continue to gain importance. Federated learning (FL) has demonstrated potential for distributed NGNs by enabling model training without sharing raw data. Still, future work must address challenges such as communication overhead, model poisoning attacks, and secure aggregation protocols [1]. Combining FL with blockchain-based provenance and auditing systems may offer an effective way to secure both training and deployment pipelines. Such integration could also enable collaborative intrusion detection across organisations while maintaining strict data confidentiality.

Finally, the future of IDPS lies in holistic detection and prevention frameworks that go beyond identifying intrusions to autonomously responding in real-time. Researchers could harness deep reinforcement learning to optimise adaptive prevention strategies, such as dynamically adjusting access controls or reconfiguring network topologies in response to detected threats [6]. Researchers should explore how to safely integrate these proactive mechanisms with detection models to minimise collateral damage and maintain service continuity in mission-critical NGN applications.

The research on AI-powered IDPS must focus on creating adaptive, efficient, interpretable, and privacy-preserving systems that can withstand adversarial manipulation and operate effectively across diverse NGN environments. Achieving these objectives will require multidisciplinary collaboration across AI research, cybersecurity, telecommunications, and regulatory domains. By addressing these directions, the research community can move toward building IDPS frameworks that are not only technically advanced but also trustworthy, practical, and socially responsible.

CONCLUSIONS

This review examines the role of artificial intelligence in enhancing intrusion detection and prevention systems (IDPS) for next-generation networks (NGNs). It showed that while classical machine learning methods laid the foundation, deep learning and hybrid approaches now dominate due to their superior adaptability and accuracy. Specialised models tailored to SDN, IoT, edge, and 5G environments further highlight the need for context-aware solutions. Despite significant progress, key challenges remain, including the limited availability of realistic datasets, computational overhead, a lack of explainability, and vulnerability to adversarial attacks. Addressing these gaps through lightweight architectures, adversarially robust models, explainable AI, and integrated detection prevention frameworks will be critical. Overall, AI-powered IDPS hold strong potential to provide scalable and trustworthy protection for NGNs, provided that future research focuses on balancing accuracy, efficiency, and resilience.

REFERENCES

1. Noor, K., Imoize, A. L., Li, C., & Weng, C. (2025). A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond. *Mathematics, 13*(7), 1088. doi: 10.3390/math13071088

2. Xu, Z., Wu, Y., Wang, S., Gao, J., Qiu, T., Wang, Z., Wan, H., & Zhao, X. (2025). Deep learning-based Intrusion Detection Systems: a survey. *arXiv (Cornell University).* doi: 10.48550/arxiv.2504.07839

3. Hemalatha, S., Mahalakshmi, M., Vignesh, V., Geethalakshmi, M., Balasubramanian, D., & Anand, J. A. (2023). Deep Learning Approaches for Intrusion Detection in the Face of Emerging Cybersecurity Challenges. *International Conference on Sustainable Communication Networks and Application (ICSCNA)*, 1522–1529. doi: 10.1109/icscna58489.2023.10370556

4. Kum, k. B., Amaechi, A., & Tonye, E. (2025). AI-Driven Intrusion Detection System for 5G Edge Networks Using Federated Learning: The case of Cameroon Regulatory, Technical & Real-World Relevance. *International Journal of Research in Engineering and Science (IJRES), 13*(6), 30-47.

5. Zhong, M., Lin, M., Zhang, C., & Xu, Z. (2024). A survey on graph neural networks for intrusion detection systems: Methods, trends and challenges. *Computers & Security, 141*, 103821. doi: 10.1016/j.cose.2024.103821

6. Bocu, R., & Iavich, M. (2022). Real-Time Intrusion Detection and Prevention System for 5G and beyond Software-Defined Networks. *Symmetry, 15*(1), 110. doi: 10.3390/sym15010110

7. Rahman, M. M., Shakil, S. A., & Mustakim, M. R. (2024). A survey on intrusion detection systems in IoT networks. *Cyber Security and Applications, 3*, 100082. doi: 10.1016/j.csa.2024.100082

8. Alnasser, O., Muhtadi, J. A., Saleem, K., & Shrestha, S. (2025). Signature- and anomaly-based intrusion detection system for secure IoTs and V2G communication. *Alexandria Engineering Journal, 125*, 424–440. doi: 10.1016/j.aej.2025.03.068

9. Lazim, S., & Ali, Q., I. (2025). Machine Learning-Based Intrusion Detection and Prevention System for IIOT Smart Metering Networks: Challenges and Solutions. *arXiv (Cornell University)*. doi: 10.48550/arxiv.2502.11138

10. Lo, W. W., Layeghy, S., Sarhan, M., Gallagher, M., & Portmann, M. (2022). E-GraphSAGE: A Graph Neural Network-based Intrusion Detection System for IoT. *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium,* 1–9. doi: 10.1109/noms54207.2022.9789878

11. Caville, E., Lo, W. W., Layeghy, S., & Portmann, M. (2022). Anomal-E: A self-supervised network intrusion detection system based on graph neural networks. *Knowledge-Based Systems, 258*, 110030. doi: 10.1016/j.knosys.2022.110030

12. Wang, Y., Han, Z., Du, Y., Li, J., & He, X. (2025). BS-GAT: a network intrusion detection system based on a graph neural network for edge computing. *Cybersecurity, 8*(1). doi: 10.1186/s42400-024-00296-8

13. Nguyen, T., & Park, M. (2025). EL-GNN: A Continual-Learning-Based Graph Neural Network for Task-Incremental Intrusion Detection Systems. *Electronics, 14*(14), 2756. doi: 10.3390/electronics14142756

14. KDD (1999). KDD Cup 1999 Computer network intrusion detection. Retrieved from https://www.kdd.org/kdd-cup/view/kdd-cup-1999/Tasks

15. Canadian Institute for Cybersecurity. (n. d.). Intrusion Detection Evaluation Dataset (CIC-IDS2017). Retrieved from https://www.unb.ca/cic/datasets/ids-2017.html

16. Saikia, P., Dholaria, D., Yadav, P., Patel, V., & Roy, M. (2022b). A Hybrid CNN-LSTM model for Video Deepfake Detection by Leveraging Optical Flow Features. *arXiv (Cornell University).* doi: 10.48550/arxiv.2208.00788

17. Khan, S. A., Artusi, A., & Dai, H. (2022). Adversarially robust deepfake media detection using fused convolutional neural network predictions. *arXiv (Cornell University).* doi: 10.48550/arxiv.2102.05950

18. Garcia, S., Parmisano, A., & Erquiaga, M. J. (2021). IoT-23: A labelled dataset with malicious and benign IoT network traffic. In *Zenodo (CERN European Organisation for Nuclear Research).* doi: 10.5281/zenodo.4743746

19. Canadian Institute for Cybersecurity. (n. d.). DDoS evaluation dataset (CIC-DDoS2019). Retrieved from https://www.unb.ca/cic/datasets/ddos-2019.html

20. Moustafa, N. (2019). The Bot-IoT dataset. In *IEEE DataPort.* doi: 10.21227/r7v2-x988

21. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT Telemetry Dataset: A new generation dataset of IoT and IIOT for Data-Driven Intrusion Detection Systems. *IEEE Access, 8*, 165130–165150. doi: 10.1109/access.2020.3022862