Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 02 (2026)

AI-Driven Intrusion Detection Systems For Next-Generation Networks: Techniques, Challenges And Future Directions

Dr. Vilas Ramrao Joshi[1], Dr. Brijesh Kumar Yadav[2], Dr. Prabhat Kumar Pallav[3], Deepak Kumar Sharma[4*]

[1]Professor, ISBMCOE Nande Pune University, SPPU, Pune, India,
Email: joshivilas131071@gmail.com
[2]Associate Professor, ISBMCOE Nande Pune University, SPPU, Pune, India,
Email: brijesh1243@gmail.com
[3]Assistant Professor, Siddhant COE Sudumbare Pune University, SPPU, Pune, India,
Email: prabhatpallav17@gmail.com
[4]Research Scholar, Electronics and Communication Engineering (ECE), Amity University, Noida,*
Email: deepak.kusharma99@gmail.com

Abstract:- The rapid evolution of next-generation networks, including 5G technology, emerging 6G technology, and large-scale Internet of Things ecosystems, has significantly increased the complexity and scale of cybersecurity threats. Traditional intrusion detection systems (IDS), primarily based on signature and rule-based techniques, are increasingly ineffective against sophisticated attacks such as zero-day exploits, polymorphic malware, and encrypted traffic anomalies. In this context, Artificial Intelligence (AI)-driven IDS has emerged as a promising solution for enhancing detection accuracy, adaptability, and real-time response capabilities. This paper presents a comprehensive analysis of AI-based intrusion detection mechanisms tailored for next-generation network environments. It explores the integration of machine learning (ML), deep learning (DL), and hybrid intelligent models for detecting both known and unknown threats. Specifically, techniques such as convolutional neural networks, recurrent neural networks, long short-term memory models, and generative adversarial networks are evaluated for their ability to capture complex traffic patterns and temporal dependencies. The study further examines widely used benchmark datasets, including NSL-KDD, UNSW-NB15, and CICIDS2017, to assess model performance across diverse attack scenarios..

Keywords: *Intrusion Detection System (IDS),Artificial Intelligence, Deep Learning, 5G/6G Networks , IoT Security ,Network Anomaly Detection*

2.1 Traditional IDS Approaches

Intrusion Detection Systems (IDS) have long been a cornerstone of network security, providing mechanisms to monitor, analyze, and detect malicious activities within network environments. Before the advent of intelligent and adaptive systems, traditional IDS approaches primarily relied on two fundamental methodologies: signature-based detection and anomaly-based detection. While both approaches have contributed significantly to cybersecurity, their inherent limitations have necessitated the transition toward more advanced, AI-driven solutions.

Signature-Based IDS

Signature-based IDS, also known as misuse detection systems, operate by comparing observed network traffic against a predefined database of known attack signatures. These signatures are essentially patterns or fingerprints derived from previously identified threats, such as specific byte sequences, malicious payload structures, or known exploit behaviors. When incoming traffic matches a stored signature, the system flags it as a potential intrusion.

One of the primary advantages of signature-based IDS is their high accuracy in detecting known attacks. Since these systems rely on well-defined patterns, they typically produce low false positive rates, making them reliable for identifying established threats.[1] Additionally, signature-based systems are relatively easy to implement and interpret, as the detection logic is straightforward and based on explicit rules. This makes them particularly useful in environments where compliance and auditability are important.

However, the effectiveness of signature-based IDS is inherently limited by the scope and timeliness of their signature databases. These systems are incapable of detecting new or unknown attacks, commonly referred to as zero-day threats, because no corresponding signatures exist for such exploits.[2] As cyber threats continue to evolve rapidly, maintaining an up-to-date signature database becomes a significant challenge, requiring continuous monitoring, analysis, and manual updates by security experts. Another limitation is their inability to handle polymorphic and metamorphic malware, which can modify their code structure to evade detection while retaining their malicious functionality. Signature-based systems often fail to recognize these variants, as even minor changes in the attack pattern can prevent a match. Furthermore, the increasing use of encryption in network communications reduces the visibility of payload data, making it more difficult for signature-based systems to identify malicious content.

In high-speed and large-scale networks, such as those enabled by 5G technology, signature-based IDS may also face performance bottlenecks due to the need to match traffic against extensive signature databases in real time. This can lead to increased latency and reduced efficiency, particularly in environments with massive data throughput.

Anomaly-Based IDS

Anomaly-based IDS were developed to address the limitations of signature-based systems, particularly their inability to detect unknown threats. Instead of relying on predefined attack patterns, anomaly-based systems establish a baseline of normal network behavior and identify deviations from this baseline as potential intrusions. These systems use statistical models, heuristics, or machine learning techniques to characterize normal activity based on features such as traffic volume, protocol usage, and user behavior. The key strength of anomaly-based IDS lies in their ability to detect previously unseen attacks. By focusing on deviations from normal behavior, these systems can identify novel threats, including zero-day exploits and insider attacks, which may not have known signatures.[3] This makes them particularly valuable in dynamic and complex network environments, where new attack vectors emerge frequently.

Anomaly-based IDS are also adaptable to different network conditions, as they can continuously update their understanding of normal behavior over time. This adaptability is crucial in modern network environments, including those involving the Internet of Things, where device behavior and traffic patterns can vary significantly. Despite these advantages, anomaly-based IDS are associated with several challenges. One of the most significant issues is the high rate of false positives. Since these systems flag any deviation from normal behavior as suspicious, they may incorrectly classify legitimate activities as malicious, leading to unnecessary alerts and increased workload for security analysts.[4] This problem is exacerbated in highly dynamic networks, where normal behavior can change frequently, making it difficult to establish an accurate baseline. Another limitation is the difficulty of defining what constitutes “normal” behavior. In large-scale and heterogeneous environments, such as cloud infrastructures or distributed systems, network traffic patterns can be highly variable and context-dependent. As a result, anomaly-based systems may struggle to maintain accurate and consistent models, reducing their effectiveness. Additionally, traditional anomaly-based IDS often rely on simplistic statistical methods that may not capture the complex and high-dimensional nature of modern network traffic. This can limit their ability to detect subtle or sophisticated attacks. While more advanced machine learning techniques have been introduced to enhance anomaly detection, early implementations lacked the computational power and data availability required for effective deployment.

Limitations of Traditional IDS Approaches

[1]Signature-based IDS are highly accurate for known attack detection with low false positives.
[2]These systems cannot detect zero-day or unknown attacks.
[3]Anomaly-based IDS can identify new and previously unseen threats.
[4]High false positive rates are a major limitation of anomaly detection systems.

While both signature-based and anomaly-based IDS have played a vital role in the evolution of network security, they share several overarching limitations that hinder their effectiveness in next-generation network environments.

Table 1: Comparative overview of traditional and AI-driven IDS approaches.

Approach	Detection basis	Strength	Major limitation
Signature-based IDS	Known attack patterns and rule/signature matching	High precision for previously identified threats	Cannot detect zero-day and polymorphic attacks effectively
Anomaly-based IDS	Deviation from established normal behaviour	Useful for detecting unknown or unusual behaviour	High false positive rate in dynamic networks
AI-driven IDS	Learned patterns from ML/DL models	Adaptive detection, scalable analysis and improved accuracy	Requires quality datasets, computing resources and interpretability controls

First, both approaches struggle to scale efficiently in modern networks characterized by high data volumes, dynamic topologies, and diverse device ecosystems. The increasing adoption of technologies such as cloud computing and Software-Defined Networking further complicates the detection process by introducing additional layers of abstraction and virtualization.[5] Traditional IDS are not well-equipped to handle these complexities, as they lack the flexibility and adaptability required for such environments.

Second, the reliance on manual configuration and expert knowledge poses a significant challenge. Signature-based systems require continuous updates, while anomaly-based systems depend on accurate baseline modelling. Both processes are time-consuming and prone to human error, limiting the responsiveness of these systems to emerging threats.

Third, traditional IDS are often unable to provide real-time detection and response in high-speed networks. The computational overhead associated with pattern matching or statistical analysis can lead to delays, reducing the effectiveness of intrusion prevention measures. This is particularly problematic in latency-sensitive applications, where timely detection is critical.

Finally, both approaches lack the ability to learn and evolve autonomously. In contrast to modern AI-driven systems, traditional IDS do not improve their performance over time based on new data or experiences. This makes them less effective in dealing withadaptive and intelligent adversaries who continuously modify their attack strategies. While traditional IDS approaches have laid the foundation for network security, their limitations in detecting unknown threats, handling complex data, and adapting to dynamic environments have driven the need for more advanced solutions. The integration of artificial intelligence and machine learning techniques represents a significant step forward in overcoming these challenges and enhancing the overall effectiveness of intrusion detection systems.

2.2 AI-Based IDS Evolution

The increasing sophistication and frequency of cyberattacks in modern network environments have necessitated the development of more intelligent and adaptive intrusion detection mechanisms. Traditional IDS approaches, while effective for known threats, lack the flexibility to handle dynamic and complex attack patterns. This has led to the integration of Artificial Intelligence (AI) techniques, particularly machine learning (ML) and deep learning (DL), into intrusion detection systems. AI-based IDS leverage data-driven models to automatically learn patterns from network traffic, enabling improved detection accuracy, adaptability, and scalability in next-generation environments such as 5G technology and the Internet of Things.

Machine Learning-Based IDS

Machine learning techniques represent one of the earliest applications of AI in intrusion detection. These methods rely on algorithms that can learn from labelled or unlabelled data to classify network traffic as either normal or malicious. ML-based IDS are generally categorized into supervised, unsupervised, and semi-supervised learning approaches. Among supervised learning techniques, Support Vector Machines (SVM), Random Forest (RF), and

[5]Modern network architectures increase the complexity of intrusion detection.

K-Nearest Neighbours (KNN) have been widely used due to their effectiveness in classification tasks. Support Vector Machines are particularly known for their ability to handle high-dimensional data and construct optimal hyperplanes for separating different classes of network traffic.Random Forest, an ensemble learning method, improves detection performance by combining multiple decision trees to reduce overfitting and increase generalization capability.[6] K-Nearest Neighbours is a simple yet effective classification algorithm that identifies the class of a data point based on the majority class of its nearest neighbors in the feature space.[7]

Unsupervised learning techniques, such as clustering and anomaly detection methods, are also employed in IDS to identify unusual patterns without requiring labeled data. These methods are particularly useful in detecting zero-day attacks, as they can identify deviations from normal behavior.[8] However, their effectiveness depends on feature representation and the ability to distinguish between legitimate and malicious anomalies. Despite their advantages, ML-based IDS face challenges such as dependence on labeled datasets, need for feature engineering, and limited capability in capturing temporal dependencies in network traffic.

Deep Learning-Based IDS

Deep learning has emerged as a powerful extension of machine learning, capable of automatically extracting hierarchical features from raw data. Unlike traditional ML methods, deep learning models can learn complex representations directly from network traffic, reducing the need for manual feature engineering.

Convolutional Neural Networks (CNNs) are widely used in IDS for their ability to capture spatial patterns in data. They can effectively identify correlations among features in network traffic and improve classification performance.[9] Recurrent Neural Networks (RNNs) are designed for sequential data analysis, making them suitable for modelling time-dependent network traffic behavior. Long Short-Term Memory (LSTM) networks, a specialized form of RNN, address the limitations of traditional RNNs by incorporating memory cells that retain long-term dependencies. This makes them highly effective in detecting sequential attack patterns such as distributed denial-of-service (DDoS) attacks. Autoencoders, another deep learning technique, are used for unsupervised anomaly detection by learning compressed representations of normal data and identifying deviations through reconstruction errors. Deep learning-based IDS offer advantages such as high detection accuracy, automatic feature extraction, and the ability to handle large-scale datasets. However, they require significant computational resources, large training datasets, and often lack interpretability, which can limit their deployment in real-world scenarios.[10]

Evolution and Integration

The transition from machine learning to deep learning in IDS reflects the need for more sophisticated and adaptive security solutions. While ML techniques provide efficient and interpretable models, deep learning approaches excel in handling complex and high-dimensional data. Recent research trends focus on hybrid models that combine ML and DL techniques to leverage their respective strengths and improve overall system performance. In conclusion, AI-based IDS represent a major advancement in intrusion detection, enabling more accurate and scalable security solutions for modern network environments. Continued research is required to address challenges such as data imbalance, model interpretability, and real-time deployment.

[6]Breiman, L. (2001). *Random forests*. Machine Learning, Springer.
[7]Cover, T., & Hart, P. (1967). *Nearest neighbor pattern classification*. IEEE Transactions on Information Theory.
[8]Chandola, V., Banerjee, A., & Kumar, V. (2009). *Anomaly detection: A survey*. ACM Computing Surveys.
[9]Sommer, R., & Paxson, V. (2010). *Outside the closed world: On using machine learning for network intrusion detection*. IEEE Symposium on Security and Privacy.
[10]Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). *A deep learning approach for network intrusion detection system*. EAI ICST.

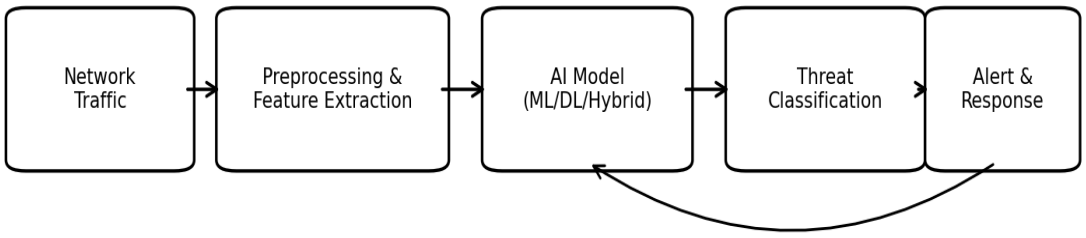

Figure 1: Workflow of an AI-driven intrusion detection system.

2.3 Review of Recent Studies

Recent advancements in Artificial Intelligence (AI)-driven Intrusion Detection Systems (IDS) have been extensively explored in the literature, with researchers focusing on improving detection accuracy, reducing false positives, and enhancing scalability in complex network environments. A critical review of recent studies reveals that most research efforts are centered around the use of benchmark datasets, advanced machine learning (ML) and deep learning (DL) techniques, and performance evaluation metrics such as accuracy, precision, recall, and F1-score. One of the most widely used datasets in IDS research is the CICIDS2017 dataset, developed to simulate real-world network traffic with both benign and malicious activities. It includes various modern attack types such as Distributed Denial of Service (DDoS), brute force, botnet, and web-based attacks, making it highly relevant for evaluating contemporary IDS models. Similarly, the UNSW-NB15 dataset was designed to overcome the limitations of older datasets like KDD99 by incorporating modern attack categories and realistic traffic features[11]. These datasets are frequently used in combination to validate the robustness and generalizability of IDS models across different environments.

Recent studies have demonstrated the effectiveness of machine learning techniques such as Random Forest, Decision Trees, and Support Vector Machines in achieving high detection accuracy. For instance, a study published in the *Journal of Big Data* reported that ensemble models, particularly Random Forest and Extra Trees, achieved accuracy rates as high as 99.95% on the UNSW-NB15 dataset and up to 99.99% on the CICIDS2017 dataset. These results highlight the capability of ensemble learning methods to handle large and complex datasets while maintaining high detection performance. In addition to traditional ML approaches, deep learning-based IDS models have gained significant attention due to their ability to automatically extract features and model complex patterns in network traffic. A hybrid deep learning model combining optimization techniques with convolutional architectures achieved near-perfect detection performance, with accuracy levels approaching 100% on CICIDS2017 and approximately 98.9% on UNSW-NB15.[12] These findings demonstrate the superiority of deep learning models in capturing both spatial and temporal characteristics of network data.

Another important trend in recent research is the use of feature selection and dimensionality reduction techniques to improve model efficiency. Studies have shown that reducing redundant features can significantly enhance detection accuracy while lowering computational overhead. For example, feature reduction techniques applied to datasets such as KDD99, UNSW-NB15, and CICIDS 2017 resulted in accuracy levels exceeding 99% for certain classifiers, particularly Random Forest. This indicates that effective feature engineering plays a crucial role in improving IDS performance. Despite these promising results, several limitations have been identified in recent studies. One of the major challenges is the issue of data imbalance, where certain attack categories are underrepresented in the dataset. This can lead to biased models that perform well on dominant classes but fail to detect rare attacks effectively. Additionally, many studies rely on offline datasets that may not accurately reflect real-world network conditions, limiting the applicability of the proposed models in practical scenarios[13].

Another limitation is the lack of reproducibility and standardization across studies. Variations in preprocessing techniques, feature selection methods, and evaluation metrics make it difficult to compare results objectively. For

[11]Moustafa, N., & Slay, J. (2015). *UNSW-NB15: A comprehensive data set for network intrusion detection systems*.
[12]SN Computer Science (2024). *Hybrid deep learning IDS performance study*.
[13]CICIDS2017 Dataset Analysis Study (2024).

instance, some studies achieve high accuracy by applying extensive data preprocessing or oversampling techniques, which may introduce bias and inflate performance metrics.[14] Furthermore, deep learning models often require high computational resources and large training datasets, making them less suitable for deployment in resource-constrained environments such as Internet of Things networks. In addition, the interpretability of AI-based IDS remains a significant concern. Many deep learning models operate as "black boxes," making it difficult for security analysts to understand the reasoning behind detection decisions. This lack of transparency can hinder trust and adoption in critical applications. Recent studies have begun exploring Explainable AI (XAI) techniques to address this issue, but further research is needed to achieve a balance between accuracy and interpretability.

Comparative Summary of Recent Studies

Table 2: Benchmark datasets commonly used for AI-based IDS evaluation.

Dataset	Traffic scope	Common use in IDS research	Key limitation
NSL-KDD	Refined version of KDD intrusion data	Baseline comparison for classical ML models	Older attack patterns and limited realism
UNSW-NB15	Modern benign and attack traffic	Evaluation of ML and hybrid IDS models	Class imbalance and environment-specific features
CICIDS2017	Benign traffic with DDoS, brute force, botnet and web attacks	Testing deep learning and feature-selection models	Offline dataset may not fully represent live networks

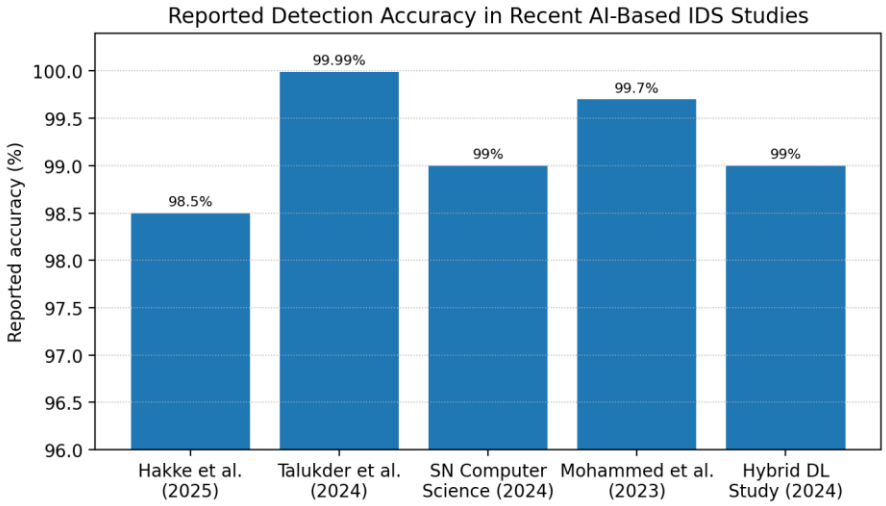

Figure 2: Reported detection accuracy across recent AI-based IDS studies.

Study	Dataset Used	Techniques	Accuracy	Limitations
Hakke et al. (2025)	NSL-KDD, UNSW-NB15, CICIDS2017	ML classifiers	~98–99%	Limited real-world validation
Talukder et al. (2024)	UNSW-NB15, CICIDS2017	RF, ET, XGBoost	Up to 99.99%	High computational complexity
SN Computer Science Study (2024)	CICIDS2017, UNSW-NB15	Hybrid DL (ResNet)	~98–100%	Resource intensive models
Mohammed et al. (2023)	KDD99, UNSW-NB15, CICIDS2017	ML + Feature Reduction	~99.7%	Feature dependency
Hybrid DL Study (2024)	CICIDS2017, UNSW-NB15	CNN + Optimization	~98–100%	Dataset bias

[14]Springer Study (2024). *Intrusion detection with unbalanced datasets*.

The comparative analysis clearly indicates that modern IDS models, particularly those based on ensemble learning and deep learning, achieve very high accuracy levels across standard benchmark datasets. However, these results must be interpreted with caution due to inherent limitations in datasets, evaluation methodologies, and experimental setups. While accuracy remains a key performance metric, it does not fully capture the effectiveness of IDS in real-world scenarios, where factors such as false positives, scalability, and adaptability are equally important. In conclusion, recent studies demonstrate significant progress in AI-based intrusion detection, but challenges such as dataset realism, model interpretability, and deployment constraints remain open research issues. Addressing these challenges will be critical for developing robust and practical IDS solutions for next-generation networks.

3. Next-Generation Network Environment

3.1 Characteristics

The evolution of communication technologies has led to the emergence of next-generation networks that are fundamentally different from traditional network infrastructures. These networks are designed to support a wide range of applications with diverse requirements, including enhanced mobile broadband, ultra-reliable low-latency communications, and massive machine-type communications. Key enabling technologies such as 5G technology and the emerging 6G technology are central to this transformation. The defining characteristics of next-generation networks include high bandwidth, ultra-low latency, and massive device connectivity, each of which introduces both opportunities and significant cybersecurity challenges.

Table 3: Characteristics of next-generation networks and IDS implications.

Network characteristic	Benefit	Security implication for IDS
High bandwidth	Supports heavy data throughput and advanced applications	Requires high-speed traffic inspection and scalable detection
Ultra-low latency	Enables real-time applications such as autonomous systems	Demands lightweight IDS models with minimal processing delay
Massive device connectivity	Supports dense IoT and smart infrastructure deployments	Expands attack surface and increases heterogeneous traffic patterns

High Bandwidth (5G/6G)

One of the most prominent features of next-generation networks is their ability to support extremely high data transmission rates. Fifth-generation (5G) networks offer peak data rates of up to 20 Gbps, while future sixth-generation (6G) networks are expected to exceed 100 Gbps, enabling unprecedented levels of data throughput.[15] This significant increase in bandwidth facilitates advanced applications such as high-definition video streaming, augmented and virtual reality, autonomous driving, and real-time industrial automation. The high bandwidth capability is achieved through the use of advanced technologies such as millimeter-wave (mmWave) communication, massive multiple-input multiple-output (MIMO) systems, and network densification. These technologies allow for efficient utilization of the radio spectrum and improved data transmission efficiency. However, the increased bandwidth also leads to a substantial rise in network traffic volume, making it more challenging to monitor and analyze data in real time.

From a security perspective, high bandwidth environments create opportunities for attackers to launch large-scale and high-speed attacks, such as Distributed Denial of Service (DDoS) attacks, with greater impact. Traditional security mechanisms may struggle to keep pace with the sheer volume of data, leading to potential blind spots in intrusion detection systems.[16] Moreover, the increased use of encrypted communication in high-speed networks further complicates traffic analysis, as it limits the visibility of packet contents. In addition, high bandwidth networks require efficient and scalable security solutions capable of processing large volumes of data without introducing significant latency. This has driven the adoption of AI-based intrusion detection systems, which can

[15]Andrews, J. G., et al. (2014). *What will 5G be?* IEEE Journal on Selected Areas in Communications.
[16]Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). *Machine learning in IoT security: Current solutions and future challenges*. IEEE Communications Surveys & Tutorials.

analyze high-dimensional data and identify patterns indicative of malicious activity. However, ensuring real-time detection in such environments remains a significant challenge.

Ultra-Low Latency

Another defining characteristic of next-generation networks is ultra-low latency, which refers to the minimal delay in data transmission between devices. 5G networks aim to achieve latency as low as 1 millisecond, while 6G networks are expected to reduce this further to sub-millisecond levels.[17] Ultra-low latency is critical for applications that require real-time responsiveness, such as remote surgery, autonomous vehicles, industrial control systems, and smart grid operations. The reduction in latency is made possible through innovations such as edge computing, network slicing, and optimized communication protocols. Edge computing, in particular, plays a crucial role by processing data closer to the source, thereby reducing the need for long-distance data transmission to centralized cloud servers. This distributed architecture enhances performance but also introduces new security challenges. In ultra-low latency environments, even minor delays in detecting and responding to cyber threats can have severe consequences.

For example, in autonomous driving systems, a delayed response to a malicious attack could result in catastrophic outcomes. Therefore, intrusion detection systems must operate in real time, with minimal computational overhead, to ensure timely threat mitigation.[18] However, achieving real-time detection in low-latency environments is challenging due to the trade-off between detection accuracy and processing speed. Complex detection algorithms, particularly those based on deep learning, may introduce additional latency, making them unsuitable for time-sensitive applications. This necessitates the development of lightweight and efficient AI models that can deliver high accuracy without compromising speed. Furthermore, the distributed nature of edge computing environments increases the attack surface, as multiple nodes must be secured simultaneously. Each edge device can serve as a potential entry point for attackers, making it essential to implement robust and decentralized security mechanisms.

Massive Device Connectivity

Next-generation networks are designed to support a massive number of connected devices, particularly within the Internet of Things ecosystem. It is estimated that 5G networks will support up to one million devices per square kilometer, enabling large-scale deployment of smart devices in applications such as smart cities, healthcare, agriculture, and industrial automation This .level of connectivity represents a significant shift from traditional networks, which were primarily designed for human-to-human communication. The proliferation of IoT devices introduces several challenges related to network management, data processing, and security. Many IoT devices are resource-constrained, with limited processing power, memory, and energy capacity. As a result, they often lack robust security mechanisms, making them vulnerable to various cyberattacks, including botnets, data breaches, and unauthorized access.[19] Massive device connectivity also leads to highly heterogeneous network environments, where devices with different capabilities, protocols, and communication standards coexist. This heterogeneity complicates the task of intrusion detection, as traditional IDS may not be able to effectively monitor and analyze diverse traffic patterns. Additionally, the dynamic nature of IoT networks, where devices frequently join and leave the network, makes it difficult to establish stable behavioral baselines.

Another significant concern is the potential for large-scale coordinated attacks. Compromised IoT devices can be used to form botnets, which can launch distributed attacks on network infrastructure or other targets. The Mirai botnet attack is a well-known example of how vulnerable IoT devices can be exploited to disrupt internet services on a global scale.[20] To address these challenges, advanced intrusion detection systems must be capable of handling large-scale, heterogeneous data while maintaining high detection accuracy. AI-based approaches, particularly those leveraging distributed and federated learning, offer promising solutions by enabling collaborative threat detection without compromising data privacy. However, the implementation of such systems requires careful

[17]Saad, W., Bennis, M., & Chen, M. (2019). *A vision of 6G wireless systems: Applications, trends, technologies, and open research problems*. IEEE Network.
[18]Taleb, T., et al. (2017). *On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture*. IEEE Communications Surveys & Tutorials
[19]Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). *Security, privacy and trust in Internet of Things*. Computer Networks (Elsevier).
[20]Antonakakis, M., et al. (2017). *Understanding the Mirai botnet*. USENIX Security Symposium.

consideration of scalability, communication overhead, and model synchronization. In summary, the defining characteristics of next-generation networks—high bandwidth, ultra-low latency, and massive device connectivity enable a wide range of innovative applications but also introduce significant cybersecurity challenges. These characteristics demand the development of advanced, intelligent, and scalable intrusion detection systems capable of operating efficiently in dynamic and complex environments. As network technologies continue to evolve, addressing these challenges will be critical to ensuring the security and reliability of next-generation communication infrastructures.

3.2 Security Challenges

Next-generation networks introduce a wide range of security challenges due to their dynamic, distributed, and heterogeneous nature. One of the primary concerns is the dynamic topology of modern networks, where nodes frequently join, leave, or change their communication patterns, especially in environments enabled by 5G technology and large-scale Internet of Things deployments. This constant change makes it difficult for traditional intrusion detection systems to maintain accurate network models and detect anomalies effectively. Another major challenge is the increasing use of encrypted traffic, which, while essential for ensuring data privacy and confidentiality, limits the visibility of network payloads and hinders deep packet inspection techniques commonly used in intrusion detection. As a result, detecting malicious activities within encrypted streams becomes significantly more complex and requires advanced behavioral and metadata-based analysis.

Furthermore, zero-day attacks pose a critical threat, as they exploit previously unknown vulnerabilities for which no signatures or patches exist, making them undetectable by traditional signature-based systems.[21] These attacks demand adaptive and intelligent detection mechanisms capable of identifying subtle deviations in network behavior. Additionally, the widespread deployment of resource-constrained IoT devices introduces further vulnerabilities, as these devices often lack sufficient computational power, memory, and built-in security features to defend against sophisticated attacks.[22] Their limited capabilities also restrict the implementation of complex security algorithms, making them easy targets for exploitation and inclusion in large-scale botnets. Collectively, these challenges highlight the need for scalable, intelligent, and lightweight intrusion detection solutions tailored to the unique requirements of next-generation network environments.

4. AI Techniques for Intrusion Detection

Artificial Intelligence (AI) techniques have significantly enhanced the effectiveness of intrusion detection systems by enabling automated learning, adaptability, and high accuracy in identifying complex attack patterns across modern network environments such as 5G technology and the Internet of Things. Within machine learning models, supervised learning approaches rely on labelled datasets to train classifiers such as Support Vector Machines, Random Forest, and Decision Trees, which have demonstrated high accuracy in distinguishing between normal and malicious traffic.[23] In contrast, unsupervised learning techniques, including clustering and anomaly detection methods, do not require labeled data and are particularly effective in identifying unknown or zero-day attacks by detecting deviations from normal behavior patterns.[24] Reinforcement learning, a relatively newer approach in IDS, enables systems to learn optimal detection strategies through interaction with the environment by maximizing cumulative rewards, making it suitable for adaptive and real-time intrusion detection scenarios.

Moving beyond traditional machine learning, deep learning models have gained prominence due to their ability to automatically extract complex features from high-dimensional network data. Convolutional Neural Networks (CNNs) are widely used for traffic classification tasks by capturing spatial correlations among network features, thereby improving detection accuracy.[25] Recurrent Neural Networks (RNNs) and their advanced variant, Long Short-Term Memory (LSTM) networks, are particularly effective for analyzing sequential data, as they can capture temporal dependencies in network traffic and detect evolving attack patterns such as distributed denial-of-service

[21]Sommer, R., & Paxson, V. (2010). *Outside the closed world: On using machine learning for network intrusion detection*. IEEE Symposium on Security and Privacy.
[22]Sicari, S., et al. (2015). *Security, privacy and trust in Internet of Things*. Computer Networks (Elsevier).
[23]Breiman, L. (2001). *Random forests*. Machine Learning, Springer.
[24]Chandola, V., Banerjee, A., & Kumar, V. (2009). *Anomaly detection: A survey*. ACM Computing Surveys.
[25]Kim, G., Lee, S., & Kim, S. (2014). *A novel hybrid intrusion detection method*. Expert Systems with Applications (Elsevier).

(DDoS) attacks.[26] Generative Adversarial Networks (GANs) have also been introduced in intrusion detection to simulate realistic attack scenarios and generate synthetic datasets, which help in improving model robustness and addressing data imbalance issues. In addition to individual techniques, hybrid models combining machine learning and deep learning approaches have shown promising results by leveraging the strengths of both paradigms. These models often integrate feature selection capabilities of ML with the representation learning power of DL to achieve improved detection performance and reduced false positives.Ensemble methods, which combine multiple classifiers to make final predictions, further enhance IDS performance by improving generalization and robustness against diverse attack types.[27]Overall, the integration of AI techniques into IDS has transformed traditional detection mechanisms into intelligent, scalable, and adaptive systems capable of addressing the complex security challenges of next-generation networks.

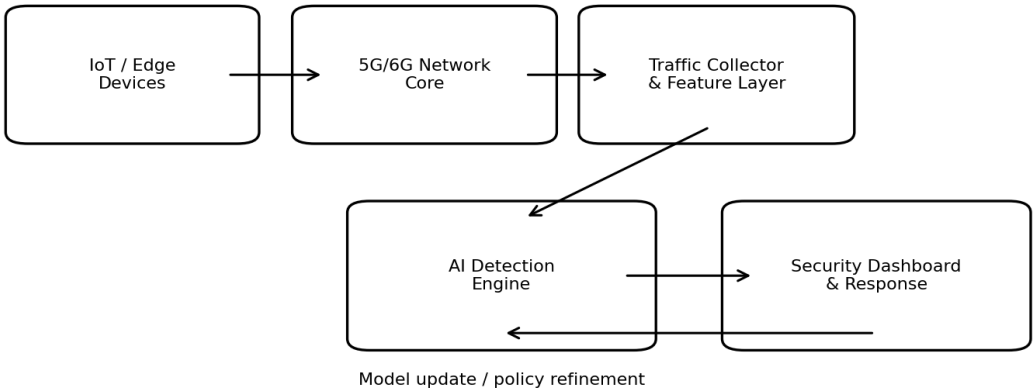

Figure 3: Conceptual architecture for AI-enabled IDS in next-generation networks.

5. Experimental Setup

The experimental setup for evaluating AI-driven intrusion detection systems (IDS) plays a crucial role in ensuring the reliability, reproducibility, and validity of results. Typically, experiments are conducted using a well-defined hardware and software environment that can support computationally intensive machine learning and deep learning models. A standard setup may include high-performance computing systems equipped with multi-core processors, sufficient RAM (e.g., 16–64 GB), and GPU acceleration (such as NVIDIA CUDA-enabled GPUs) to efficiently train deep learning models.On the software side, programming environments such as Python are widely used due to their extensive libraries and ease of implementation, along with frameworks like TensorFlow and Keras for building and training neural networks. Additional tools such as Scikit-learn are commonly employed for implementing traditional machine learning algorithms and preprocessing tasks.[28] The evaluation of IDS models is performed using standard performance metrics that provide insights into detection effectiveness.

Accuracy is the most commonly used metric, representing the proportion of correctly classified instances among the total samples; however, it may be misleading in imbalanced datasets. Precision measures the proportion of correctly identified positive instances among all predicted positives, indicating the system's ability to avoid false alarms. Recall, also known as detection rate, evaluates the proportion of actual attacks correctly identified by the system, reflecting its sensitivity to malicious activity. The F1-score, which is the harmonic mean of precision and recall, provides a balanced measure of model performance, especially in scenarios where both false positives and false negatives are critical.[29]Additionally, the False Positive Rate (FPR) is an important metric that quantifies the proportion of normal traffic incorrectly classified as malicious, which is crucial for minimizing unnecessary alerts and maintaining system efficiency.Together, these metrics provide a comprehensive evaluation framework for assessing the performance of IDS models in detecting both known and unknown cyber threats in next-generation network environments.

[26]Hochreiter, S., &Schmidhuber, J. (1997). *Long short-term memory*. Neural Computation.
[27]Zhou, Z. H. (2012). *Ensemble methods: Foundations and algorithms*. CRC Press.
[28]Pedregosa, F., et al. (2011). *Scikit-learn: Machine learning in Python*. Journal of Machine Learning Research.
[29] Sokolova, M., & Lapalme, G. (2009). *A systematic analysis of performance measures*. Information Processing & Management.

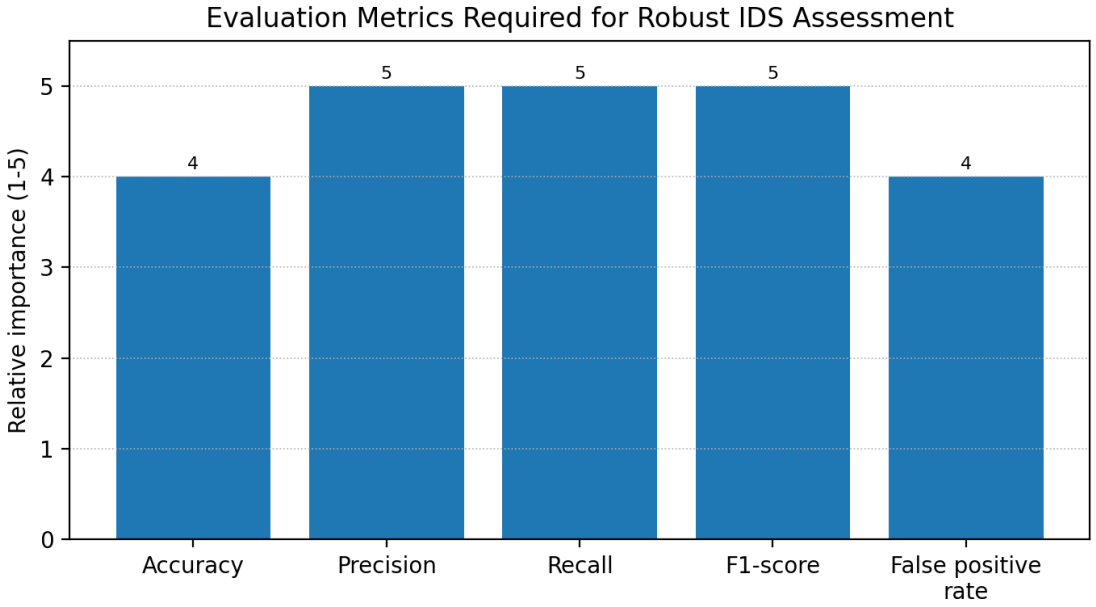

Figure 4: Relative importance of standard IDS evaluation metrics.

6. Challenges and Limitations

Despite the significant advancements in AI-driven intrusion detection systems, several challenges and limitations continue to hinder their effectiveness in real-world deployments. One of the most critical issues is data imbalance, where the number of normal traffic instances significantly outweighs malicious samples, leading to biased models that perform poorly in detecting rare but critical attacks. Additionally, the lack of real-world datasets poses a major limitation, as most publicly available datasets such as NSL-KDD or CICIDS2017 do not fully capture the complexity, diversity, and evolving nature of real network traffic, thereby affecting the generalizability of trained models.[30]Another serious concern is the vulnerability of AI models to adversarial attacks, where attackers deliberately manipulate input data to deceive machine learning algorithms and evade detection, compromising the reliability of IDS systems. Furthermore, scalability issues arise due to the increasing speed and size of network traffic in environments powered by 5G technology and large-scale Internet of Things deployments, making it challenging for AI models to process and analyze data efficiently in real time .These limitations highlight the need for robust, adaptive, and scalable solutions that can address the complexities of modern network infrastructures while maintaining high detection accuracy.

Table 4: Key challenges and mitigation strategies for AI-driven IDS.

Challenge	Impact on IDS performance	Suggested mitigation
Data imbalance	Poor detection of rare attack categories	Resampling, cost-sensitive learning and GAN-based synthetic data
Adversarial attacks	Manipulated traffic may evade AI classifiers	Adversarial training and robust validation
Scalability constraints	Latency and processing overload in high-speed networks	Edge deployment, model compression and federated learning
Limited interpretability	Reduced trust among analysts and administrators	Explainable AI and transparent feature attribution

7. Future Research Directions

Future research in AI-based intrusion detection systems is expected to focus on addressing existing limitations and enhancing system robustness through innovative approaches. One promising direction is the integration of Explainable AI (XAI), which aims to improve the transparency and interpretability of AI models, enabling security

[30]Sharafaldin, I., et al. (2018). *CICIDS2017 dataset and intrusion traffic characterization*.

analysts to better understand and trust detection decisions .Another important area is the adoption of federated learning, which allows multiple distributed devices to collaboratively train models without sharing raw data, thereby preserving privacy and enhancing security in decentralized environments .The role of AI in upcoming 6G technology is also gaining attention, as future networks will require highly intelligent and autonomous security mechanisms capable of handling extreme data rates and ultra-low latency requirements.[31] Additionally, real-time deployment challenges remain a key focus, as IDS must operate with minimal delay while maintaining high accuracy in dynamic and high-speed environments. This necessitates the development of lightweight, efficient, and scalable AI models that can be deployed at the edge or within distributed network architectures.[32] Overall, these research directions aim to create more resilient, adaptive, and trustworthy intrusion detection systems for next-generation networks.

Conclusion

This paper has presented a comprehensive analysis of AI-driven intrusion detection systems (IDS) within the context of next-generation network environments characterized by technologies such as 5G technology, emerging 6G technology, and the rapidly expanding Internet of Things. The study highlighted the limitations of traditional IDS approaches and demonstrated how the integration of Artificial Intelligence, including machine learning and deep learning techniques, significantly enhances the ability to detect both known and unknown cyber threats. Various AI models, including supervised, unsupervised, and deep learning architectures, were analyzed, showing their effectiveness in handling complex, high-dimensional network data and improving detection accuracy while reducing false positives. The key contributions of this work include a detailed review of existing IDS approaches, a comparative analysis of recent studies, and the identification of critical challenges such as data imbalance, lack of real-world datasets, adversarial threats, and scalability issues. Additionally, the paper emphasized the importance of adopting hybrid and ensemble models to leverage the strengths of multiple AI techniques. The proposed insights provide a structured understanding of how AI can be effectively utilized to build robust and adaptive IDS frameworks for modern network infrastructures.

From a practical perspective, the findings of this study have significant implications for cybersecurity practitioners, network administrators, and researchers. The adoption of AI-driven IDS can enhance real-time threat detection, improve network resilience, and support the secure deployment of emerging technologies such as smart cities, autonomous systems, and industrial IoT applications. However, successful implementation requires careful consideration of computational resources, model interpretability, and deployment constraints, particularly in resource-limited environments. In conclusion, while AI-based intrusion detection systems offer promising solutions to the evolving cybersecurity challenges in next-generation networks, further research is required to address existing limitations and ensure scalable, transparent, and real-time security solutions.

References

1. Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C. K., & Zhang, J. C. (2014). What will 5G be? *IEEE Journal on Selected Areas in Communications, 32*(6), 1065–1082.
2. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the Mirai botnet. *Proceedings of the 26th USENIX Security Symposium*, 1093–1110.
3. Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32.
4. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–58.
5. Cover, T., & Hart, P. (1967). Nearest neighbor pattern classification. *IEEE Transactions on Information Theory, 13*(1), 21–27.
6. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735–1780.
7. Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials, 22*(3), 1686–1721.

[31]Saad, W., et al. (2019). *A vision of 6G wireless systems*. IEEE Network.
[32]Taleb, T., et al. (2017). *Multi-access edge computing in 5G networks*. IEEE Communications Surveys & Tutorials.

8. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, 21–26.
9. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications, 41*(4), 1690–1700.
10. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. *Proceedings of the Military Communications and Information Systems Conference*, 1–6.
11. Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, É. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research, 12*, 2825–2830.
12. Saad, W., Bennis, M., & Chen, M. (2019). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Network, 34*(3), 134–142.
13. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 108–116.
14. for labour pain management: A systematic review and Bayesian network meta-analysis. *Journal of clinicalnursing*, *30*(23-24),3398-3414.
15. Henry, H., & Wells, C. (2021). Identification and management of dysfunctional breathing in primary care.
16. *Practice Nursing*, *32*(12), 474-479.
17. Hmwe, N. T. T., Browne, G., Mollart, L., Allanson, V., & Chan, S. W. C. (2020). Older people's perspectives on use of complementary and alternative medicine and acupressure: a qualitative study. *Complementary Therapies in Clinical Practice*, *39*(1), e101163.
18. Hofmeyr, G. J., & Singata-Madliki, M. (2020). The second stage of labour. *Best Practice & Research Clinical Obstetrics & Gynaecology*, *67*(1), 53-64.
19. Hosseini T. M., Keramat, A., Kolahdozan, S., Shahhosseini, Z., Moosazadeh, M., & Motaghi, Z. (2020).
20. Positive childbirth experience: A qualitative study. *Nursing Open*, *7*(4), 1233-1238.\
21. Hu, Y., Lu, H., Huang, J., & Zang, Y. (2021). Efficacy and safety of non-pharmacological interventions
22. Ibrahim, H. A. F., Alshahrani, M. S., Al-Qinnah, A. J., & Elgzar, W. T. (2024). Nonpharmacological pain relief for labour pain: knowledge, attitude, and barriers among obstetric care providers. *Peer Journal*, *12*(1), e16862.
23. Ingram, M. A., Brady, S., & Peacock, A. S. (2022). The barriers to offering non-pharmacological pain management as an initial option for labouring women: A review of the literature. *European Journal of Midwifery*, *6*(1), 37. https://doi.org/10.18332/ejm/149244.
24. Issac, A., Nayak, S., Priyadarshini, T., Balakrishnan, D., Halemani, K., Mishra, P., & Stephen, S. (2023). Effectiveness of breathing exercise on the duration of labour: A systematic review and meta-analysis. *Journal of Global Health*, 13(1), e1.
25. Ivan, U., Wang, J. K., Yancey, K., Mohammad, M., Jung, J. W., Berger, A. A., ... & Viswanath, O. (2021). Acupuncture for the management of low back pain. *Current Pain and Headache Reports*, *25*(1).
26. Jameei-Moghaddam, M., Goljaryan, S., Mohammad Alizadeh Charandabi, S., Taghavi, S., & Mirghafourvand, M. (2021). Effect of plantar reflexology on labour pain and childbirth experience: A randomized controlled clinical trial. *Journal of Obstetrics and Gynaecology Research, 47*(6), 2082-2092. https://doi.org/10.1111/jog.14755
27. Jha, S., Vyas, H., Nebhinani, M., Singh, P., & T D. (2023). The Effect of Birthing Ball Exercises on Labour Pain and Labour Outcome Among Primigravidae Parturient Mothers at a TertiaryCareHospital. *Cureus*, 15(3), e36088.
28. Konlan, K. D., Afaya, A., Mensah, E., Suuk, A. N., & Kombat, D. I. (2021). Non-pharmacological interventions of pain management used during labour; an exploratory descriptive qualitative study of puerperal women in Adidome Government Hospital of the Volta Region, Ghana. *Reproductive Health*, 18(1), 1-11.
29. Mueller, S., & Grunwald, M. (2021). Effects, side effects and contraindications of relaxation massage during pregnancy: a systematic review of randomized controlled trials. *Journal of Clinical Medicine*, *10*(16), 3485.
30. Mwakawanga, D. L., Mselle, L. T., Chikwala, V. Z., & Sirili, N. (2022). Use of non-pharmacological methods in managing labour pain: Experiences of nurse-midwives in two selected district hospitals in eastern

Tanzania. *BMC Pregnancy Childbirth, 22*(1), e376. https://doi.org/10.1186/s12884-022-04707-x.

31. Mwakawanga, D. L., Mselle, L. T., Chikwala, V. Z., & Sirili, N. (2022). Use of non-pharmacological methods in managing labour pain: Experiences of nurse-midwives in two selected district hospitals in eastern Tanzania. *BMC Pregnancy Childbirth,* 22(1), e376.
32. Polit, D. F., & Beck, C. T. (2020). *Nursing research: Generating and assessing evidence for nursingpractice.* LippincottWilliams&Wilkins.
33. Rosa, W. E., Kurth, A. E., Sullivan-Marx, E., et al. (2019). Nursing and midwifery advocacy to lead the United Nations Sustainable Development Agenda. *Nursing Outlook,* 67(6), 628-641.
34. Tolulope, E. D., Efemena Adugbo, J., Opeyemi Fawole, I., & Akingbade, O. (2023). Coping Experiences of Nigerian Women during Pregnancy and Labour: A Qualitative Study. *International Journal of Community Based Nursing and Midwifery,* 11(1), 23-33.
35. Türkmen, H., & Oran, N. T. (2021). Massage and heat application on labour pain and comfort: A quasi-randomized controlled experimental study. *Explore (NY), 17*(5), 438-445.
36. Wassihun, B., Alemayehu, Y., Gultie, T., Tekabe, B., & Gebeyehu, B. (2022). Non-pharmacological labour pain management practice and associated factors among skilled attendants working in public health facilities in Gamo and Gofa zone, Southern Ethiopia: A cross-sectional study. *PLoS One, 17*(4), e0266322.