International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(12s) 2026 pp. 407-427
https://doi.org/10.70917/ijcisim-2026-3915
Article

A Systematic Review of AI-Driven Intrusion Detection and Performance Optimization in Wireless Sensor Networks

Priyanka Sharma[1*], Mohd Suhaib Kidwai[2], Piyush Charan[3]

[1*]ECE Department, Integral University Lucknow, UP, India,
priyanka.sh30@gmail.com
[2]ECE Department, Integral University, Lucknow, UP, India, mskidwai@iul.ac.in
3ECE Department, Manav Rachna University, Faridabad, Haryana, piyushcharan@mru.edu.in

Abstract: The safety and reliability of Wireless Sensor Networks (WSNs) depend on the crucial function that Intrusion Detection Systems (IDS) perform in their operations. The current security systems face major obstacles because attackers continuously launch cyber operations against increasingly complex networks. Through the development of Artificial Intelligence (AI) technologies, which include Machine Learning (ML) and Deep Learning (DL) methods, IDS systems could now identify both standard and novel cyber threats. The study analyzes the most recent progress in ML and DL methods used to develop IDS that operate in WSNs through analysis of their primary algorithms and algorithmic combinations. The study conducted an extensive literature review by accessing the SCOPUS database to identify relevant studies published between 2021 and 2026. The systematic review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. As revealed by the results, the DL and hybrid approaches are superior to conventional ML algorithms in handling complicated and imbalanced datasets. Some of the accuracy rates observed are 99.94% when using KMeans-SMOTE, and 99.76% when using K-nearest neighbor (KNN). However, Deep Neural Networks (DNN) and Convolutional Neural Network–Long Short-Term Memory (CNN-LSTM) networks demonstrate relatively low accuracy levels of 96.23% and 97%, respectively. Most approaches use specific datasets, including WSN-DS and NSL-KDD, which makes the results environment-specific. Besides, issues such as high computational power, data imbalance, absence of standardized datasets, and implementation constraints underscore the need for a scalable and adaptable IDS for WSN.

Keywords: Artificial Intelligence (AI), Intrusion Detection System (IDS), Wireless Sensor Networks (WSNs), Machine Learning (ML), Deep Learning (DL)

1. Introduction

Wireless Sensor Network (WSN) functions as a basic sensing device network which can monitor parameter changes and transmit data across its designated operational area to support various applications, including target tracking, surveillance, and environmental monitoring [1,2]. WSNs have become a revolutionary technology that enables remote sensors to collect data and perform intelligent communication in multiple fields and smart infrastructure [3,4]. WSNs are used to collect real-time data using many sensor nodes placed in different locations. These nodes have limited resources but can sense data, process information, and transmit it wirelessly [5]. Cyber-physical systems and the Internet of Things (IoT) use these systems as essential components because they can function independently in unpredictable outdoor settings, which include rough weather conditions [6]. The growing size and complexity of these networks have made them essential for solving real-world problems that need ongoing observation and flexible solutions [7,8].

A standard WSN consists of essential components that work together to maintain network functionality. Each sensor node contains a data sensing unit, which collects environmental information, a processing unit that performs local computations, and a communication system that enables wireless data transmission. It also includes a power

system that typically operates on battery power, which determines the maximum operational time of the node [9,10]. The sink node establishes a connection between the sensor network and external systems by gathering information from the network while forwarding it to other systems for analysis, as demonstrated in Figure 1.

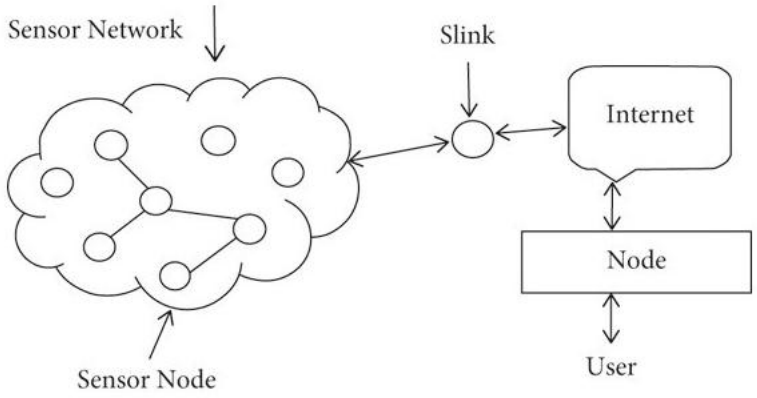

Figure 1: Communication architecture of WSNs [11]

The architectural design of WSNs exists in two primary categories, which include flat networking systems and hierarchical networking systems. All nodes in a flat architecture execute identical functions while using direct communication or multi-hop routing methods. But hierarchical and cluster-based systems create clusters of nodes that use cluster heads to perform data aggregation and communication tasks, which leads to improved energy efficiency and scalability [12,13]. The structured design of WSNs is shown in Figure 2.

Figure 2: Architecture of WSN [14]

The multiple functions of WSNs have led to their use in various critical mission operations. WSNs enable environmental monitoring through their ability to track temperature, humidity, and pollution levels in real time, which assists predictive models that support disaster management and climate analysis research [15,16]. Wearable sensor networks used in healthcare enable continuous patient monitoring while they use intelligent data analysis to identify early signs of anomalies. Industries use WSNs to predict equipment failures and detect faults while they optimize production processes, and smart agriculture systems use sensor data to improve irrigation effectiveness and increase crop yields [17,18]. WSNs deliver critical real-time sensing and communication functions, which enable both emergency response missions and smart city development projects to proceed. The different uses of WSNs

demonstrate their rising importance as a technology that allows automated intelligent systems to operate effectively [19,20].

The development of microelectronics in combination with wireless communications and information processing techniques has led to significant advancements in WSNs [21]. The modern sensors possess enhanced processing capabilities along with energy-efficient capabilities and can communicate with the help of advanced communications channels that allow for real-time analysis of information and collaborative computing operations [22]. The evolution in technology has transformed WSNs from being data acquisition devices to intelligent systems that adjust their communication techniques based on decisions made collectively while monitoring the environment. The increasing adoption of WSN systems for critical operations has introduced fresh security challenges because these systems function in open environments and possess limited capabilities while utilizing wireless connectivity [23,24].

1.1 Intrusion Detection in WSN

The built-in features of WSNs include their limited computational ability, their restricted memory capacity, their energy usage limits, and their dependence on wireless transmission. These features make the networks susceptible to multiple security dangers that exist in their operational environment [25]. The existing security measures cannot be used because of these restrictions, which result in WSNs being vulnerable to multiple types of attacks. The most common security threats to systems involve eavesdropping, together with data interception and spoofing attacks, as well as unauthorized access, which results in the loss of data confidentiality and integrity [26]. The advanced attack methods, which include Denial-of-Service (DoS) attacks, sinkhole attacks, wormhole attacks, Sybil attacks, and selective forwarding attacks, have the potential to cause major disruptions in network operations. The attacks might lower system performance and produce incorrect results in essential functions [27,28]. The security difficulties require IDS, which serve as essential elements within WSN security systems. IDS are designed to monitor network traffic and node behavior, as shown in Figure 3, to identify malicious activities or anomalies that indicate potential attacks [29,30]. The WSNs utilize various techniques that are used in the deployment of IDS. The techniques include centralized distributed systems as well as hybrid systems that enable various nodes to carry out detection tasks. The development of effective IDS is faced with various challenges, including three main obstacles that include limited resources as well as changing structures, with instant detection being required [31,32].

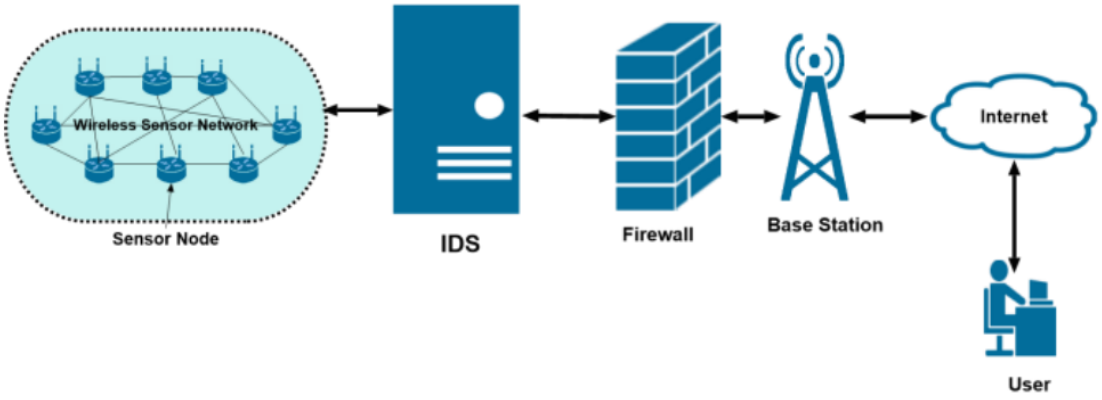

Figure 3: Intrusion Detection in WSN [33]

1.2 Role of AI in WSN

The implementation of AI technology in WSN intrusion detection systems has gained increasing recognition during the past several years, which includes ML and DL systems, the ability to learn from past data and recognize intricate patterns while adapting to new attack methods [34,35]. The ML algorithms that researchers use to build intelligent IDS models enhance detection performance while decreasing false alarm rates. The algorithms possess the ability to process extensive datasets while accurately determining whether network activities fall within acceptable limits or represent security threats [36,37].

DL, which exists as a branch of ML, improves IDS through its implementation of multilayer neural networks that extract features from unprocessed data. Advanced cyber-attack detection systems developed through the combination of Convolutional Neural Networks (CNNs) as well as Long Short-Term Memory (LSTM) networks have demonstrated superior performance compared to other methods [38-40]. The models exhibit strong capabilities for

real-time intrusion detection because they can study both time-based and location-based patterns in network traffic. The application of DL models to WSNs faces difficulties because these models need substantial processing power and energy consumption [41,42]. Researchers now investigate lightweight and hybrid AI solutions that establish a balance between detection performance and system resource usage to solve the existing problems. AI-based methods have transformed IDS systems in WSN environments by enhancing their performance facilities and ability to grow [43,44].

The security of WSN networks requires performance optimization because their sensor nodes have restricted energy, bandwidth, and computational capabilities. The network requires efficient resource management to achieve extended operational time, decreased network response time, and dependable data transmission [45,46]. The performance of WSN systems gets assessed through four key metrics, which include energy efficiency, throughput, packet delivery ratio, and network stability. The network performance optimization field has recently adopted AI methods, which support intelligent routing and adaptive resource distribution, energy-efficient communication, and fault prediction capabilities [47,48]. WSN performance optimization needs to include intrusion detection because this method enables complete security and efficiency improvements, which make WSN systems better suited for real-world use and mission-critical tasks [49,50].

The existing research on AI-based IDS lacks an all-encompassing evaluation that assesses the security and operational efficiency of all proposed methods [51]. The current research studies approach their analysis of algorithms through their main component without considering important elements, which include energy efficiency, scalability, and network lifetime, and real-world usage [52,53]. The research field has considered the way in which IDS combines with the performance optimization factors, such as latency, throughput, and resource utilization [54]. The research field has yet to explore the concept of hybrid AI models and lightweight approaches, which are applicable for resource-constrained sensor devices. The systematic review requires assessment of AI-based intrusion detection methods and their impact on network performance to attain a complete understanding of WSN efficiency.

1.3 Research Motivation and Contribution

The increasing adoption of WSN technology for vital sectors, including healthcare, military operations, and smart infrastructure systems, has established significant security challenges that endanger network security. Modern cyber threats require advanced detection systems that exceed the capabilities of standard intrusion detection methods. The use of AI methods enables organizations to improve their IDS through increased detection accuracy and better system performance. The requirement for research about AI-based IDS systems for WSN environments needs systematic evaluation methods for its fulfillment.

The main contributions of this study are summarized as follows:

- First, this study presents a comprehensive systematic review of AI-based IDS for WSNs, summarizing recent advancements, datasets, and methodologies. It provides a structured understanding of current trends and developments in AI-driven WSN security.
- Second, it analyzes and compares various ML and DL techniques used in IDS based on performance metrics such as accuracy, detection rate, and efficiency. This helps in identifying the most suitable techniques for different WSN scenarios.
- Third, the study identifies key challenges, including energy constraints, scalability issues, data imbalance, and computational overhead in WSN environments. These challenges highlight the limitations of existing approaches and the need for optimized solutions.
- Finally, it outlines future research directions focusing on lightweight models, hybrid AI approaches, and real-time IDS. It also emphasizes the integration of security with performance optimization for efficient WSN deployment.

The rest of the paper is as follows: Section 2 details the previous studies reviewed, and Section 3 uses the PRISMA model to show how the papers were chosen. Analyzing the literature reviews thematically based on the research questions is in Sections 4 and 5. Section 6 discusses the Challenges and the future opportunities, while Section 7 shows the discussion, and Section 8 delves into the study's conclusion.

2. Literature review

This section discusses the previous studies done by various authors based on the WSNs.

Munaye et al., (2026) [55] developed an IDS that specifically meets the needs of IoT environments that operate with WSNs. The proposed solution used the WSN-DS benchmark dataset together with the Adaptive Synthetic Sampling (ADASYN) method to address class imbalance problems. The system achieved 99.87% accuracy, which demonstrated its superior performance compared to base techniques.

Prasad et al. (2026) [56] proposed a technique that combined two metaheuristic optimization techniques through the Grasshopper Optimization Algorithm with Genetic Algorithm (GOA-GA) integration. After selecting appropriate features and completing training procedures, the ML classification algorithms successfully detected and classified four types of DoS attacks. The GOA-GA technique achieved a 95.51% recall and accuracy according to the experimental results.

Zhang et al., (2025) [57] created a Server-Client ML-based IDS (SC-MLIDS) system to enhance security protections for WSNs, which faced security threats because of their decentralized system design and their restricted operational capacity. The framework used a server-client system to efficiently process and analyze data that originated from the network's nodes and its gateways. The technology showed better performance than traditional methods because it reduced unnecessary data transmissions while improving detection precision. The proposed framework achieved F1-scores of 98.80% for the Majority Voting aggregation algorithm and 99.78% for the Weighted Score algorithm.

Hussain et al. (2025) [58] introduced a hybrid IDS that combined Deep Reinforcement Learning (DRL) with LSTM to protect WSNs from their complex security requirements. The proposed system achieved 99.1 percent accuracy with extremely low false positive rates, which allowed it to outperform existing models. The model's ensemble design enabled it to enhance detection capabilities while maintaining protection against evolving attack techniques through its ongoing learning process.

Sun et al., (2025) [59] developed an advanced IDS that used image classification networks for system security. This setup improved the performance of CNNs in their operations. The experimental results of multiclass classification testing showed that the proposed LeNet-based IDS system achieved an 89.97% test accuracy rate on NSL-KDD datasets.

Gowdhaman et al. (2024) [60] developed a Hybrid DL based IDS, designed for WSN by using the Inception model derived from the ResNet architecture. The researchers conducted their experiments using the NSL-KDD benchmark dataset, and they assessed the performance of their system by comparing it with existing IDS systems. The comparative analysis demonstrated that the proposed model's performance of 99.46% accuracy was better than traditional approaches.

Sadia et al. (2024) [61] proposed Deep Neural Networks (DNNs) to address the intricate challenges that arise from WSN data processing and to identify hidden security threats. The research developed a multiclass classification system through training a CNN-based method to achieve optimal results for WSN intrusion detection. The proposed model demonstrated a loss measurement of 0.14, which resulted in an outstanding accuracy of 97% while maintaining a low false alarm rate.

Sedhuramalingam et al., (2024) [62] designed an IDS that used an Improved DNN (IDNN) system to enhance its operational efficiency. The researchers applied a global search methodology and used both WSN-DS and KDDCup 99 datasets. The testing results demonstrated that DNNs outperformed standard ML classifiers in their ability to monitor network activity and host-level events during real-time operations. The experimental results showed a 95% improvement in the accuracy ratio using the proposed model.

Karthikeyan et al., (2024) [63] suggested the Firefly Algorithm (FA) in conjunction with ML to improve the accuracy of IDS of WSN-IoT. A maximum accuracy of 99.34% was attained when simulated using the NSL-KDD dataset, demonstrating the significant improvement of the FA-ML approach.

Talukder et al., (2024) [64] presented a novel method for intrusion detection that utilized ML approaches in conjunction with the Synthetic Minority Oversampling (SMOTE)-TomeLink algorithm. Using the WSN-DS dataset, which contained 374,661 records, the study determined the best model for WSN intrusion detection. Its accuracy rate was 99.78% in binary and 99.92% in multiclass classification.

Sharma et al., (2023) [65] worked with DNN to develop an IoT system that detects anomalies. The DNN model utilized the features retrieved from the filters. This DNN model was fed the strongly linked characteristics. To improve the DNN model's detection capabilities, its parameters were fine-tuned. Using the UNSW-NB15 dataset, the proposed model was examined and achieved an accuracy of 84%.

Awajan et al., (2023) [66] introduced an innovative IDS for IoT devices that was based on DNNs. Using a Fully Connected (FC) network, this smart system was able to identify fraudulent traffic that starts attacks on linked IoT devices. To simplify deployment, the suggested system was built to be independent of communication protocols. The results showed that the suggested system reliably performed against both real and simulated invasions, with an accuracy of 93.74%. Table 1 shows the summary of the above literature reviews.

Table 1: Summary of Literature Review

Author	Technique Used	Dataset Used	Outcomes	Limitations
Munaye et al. (2026) [55]	ADASYN	WSN-DS	Demonstrated 99.87% accuracy with effective handling of class imbalance	High computational cost due to boosting and sampling
Prasad et al. (2026) [56]	GOA-GA	WSN dataset	Reported 95.51% accuracy and recall, improving DoS attack detection	Complex optimization increases computation
Zhang et al. (2025) [57]	SC-MLIDS	Not specified	Produced F1-scores of 99.78%, while reducing redundant data transmission	High system complexity (server-client model)
Hussain et al. (2025) [58]	DRL + LSTM	UNSW-NB15	Reached 99.1% accuracy with reduced false positive rates	High computational and energy requirements
Sun et al. (2025) [59]	CNN - LeNet	NSL-KDD, CICIoV2024	Provided 89.97% accuracy, enhancing robustness through image-based processing	Data transformation overhead required.
Gowdhaman et al. (2024) [60]	ResNet	NSL-KDD	Reported 99.46% accuracy, outperforming traditional models	High model complexity
Sadia et al. (2024) [61]	DNN	Not specified	Demonstrated 97% accuracy with low FAR	Requires high computational resources
Sedhuramalingam et al. (2024) [62]	IDNN	KDDCup99, WSN-DS	Showed 95% accuracy, improving detection performance over ML methods	Requires parameter tuning and optimization
Karthikeyan et al. (2024) [63]	FA	NSL-KDD	Delivered 99.34% accuracy, enhancing IDS performance in WSN-IoT	Optimization overhead increases complexity
Talukder et al. (2024) [64]	SMOTE	WSN-DS	Attained 99.92% accuracy, improving detection in imbalanced datasets	Dataset dependency and preprocessing overhead
Sharma et al. (2023) [65]	DNN	UNSW-NB15	Produced ~84% detection accuracy, supporting anomaly-based detection	Lower accuracy compared to advanced models
Awajan et al. (2023) [66]	DNN - FC	IoT dataset	Demonstrated 93.74% accuracy, with protocol-independent detection capability	Moderate accuracy, limited scalability

3. Review Methodology

To screen and improve research, the PRISMA declaration is used. Using the SCOPUS database, which contains records published from 2021 to 2026, a comprehensive literature review on this phenomenon was carried out. All entries from the Scopus database that are classified as articles, journals, or publications are included in this study. Table 2 displays the search terms used in the Scopus database to locate relevant papers:

Table 2: Searching Keywords

Databases	**Keyword used**
Scopus	(TITLE-ABS-KEY (("wireless sensor network*" OR WSN)) AND TITLE-ABS-KEY (("intrusion detection" OR "anomaly detection")) OR TITLE-ABS-KEY (("machine learning" OR "deep learning" OR "artificial intelligence"))) AND PUBYEAR > 2020 AND PUBYEAR < 2027 AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "cr")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (PUBSTAGE , "final"))

Source: Author's own elaboration

When doing a literature review, only records that are classified as articles are taken into consideration for further analysis and evaluation. Only records that fulfilled the inclusion and exclusion criteria are shown in Table 3.

Table 3: The criteria for determining what is included and excluded

Criterion	**Inclusion**	**Exclusion**
Keywords	Studies discussing WSN, IDS, AI, ML, DL, and Network Security	Records where the variables do not correlate are not included.
Type of Literature	Peer-reviewed journal articles and review papers	Books, book series, book chapters, conference summaries, editorials, and thieses
Language	English	Publications in languages other than English
Timeframe	Studies published between 2021 and 2026	Studies published before 2021
Access Type	Open access	Articles without an accessible full text

Source: Author's own elaboration

3.1 Prisma Model

The "Preferred Reporting Items for Systematic Reviews and Meta-Analyses" publication outlines the PRISMA Statement, which governs conducting systematic reviews and meta-analyses. The PRISMA framework not only shows how high-quality the review is, but it also helps readers understand its pros and cons and how to do their own reviews. A detailed and organized procedure for data extraction is shown in Figure 4. Extracting research articles, analyzing sources, removing extraneous material according to predetermined criteria, and finally analyzing the content of the source research papers are all parts of this procedure. A comprehensive systematic literature evaluation to find relevant papers in the topic area has been scheduled to take place over the course of six years, from 2021 to 2026.

From the records identified through Scopus, a total of 11,107 records were initially obtained. Out of these,5524 results are excluded based on criteria that include year of publication and document type, which includes conference paper, article, conference review, review paper, and language. After screening,4969 records remain, which is more than 5000, which were initially used for testing. The total number of publications that meet the inclusion criteria stands at 30 after the screening process. The retrieved papers undergo two types of tests: language assessment and duplicate detection. The study exclusively focuses on works written in English, which results in 30 publications remaining after the filtering process ends.

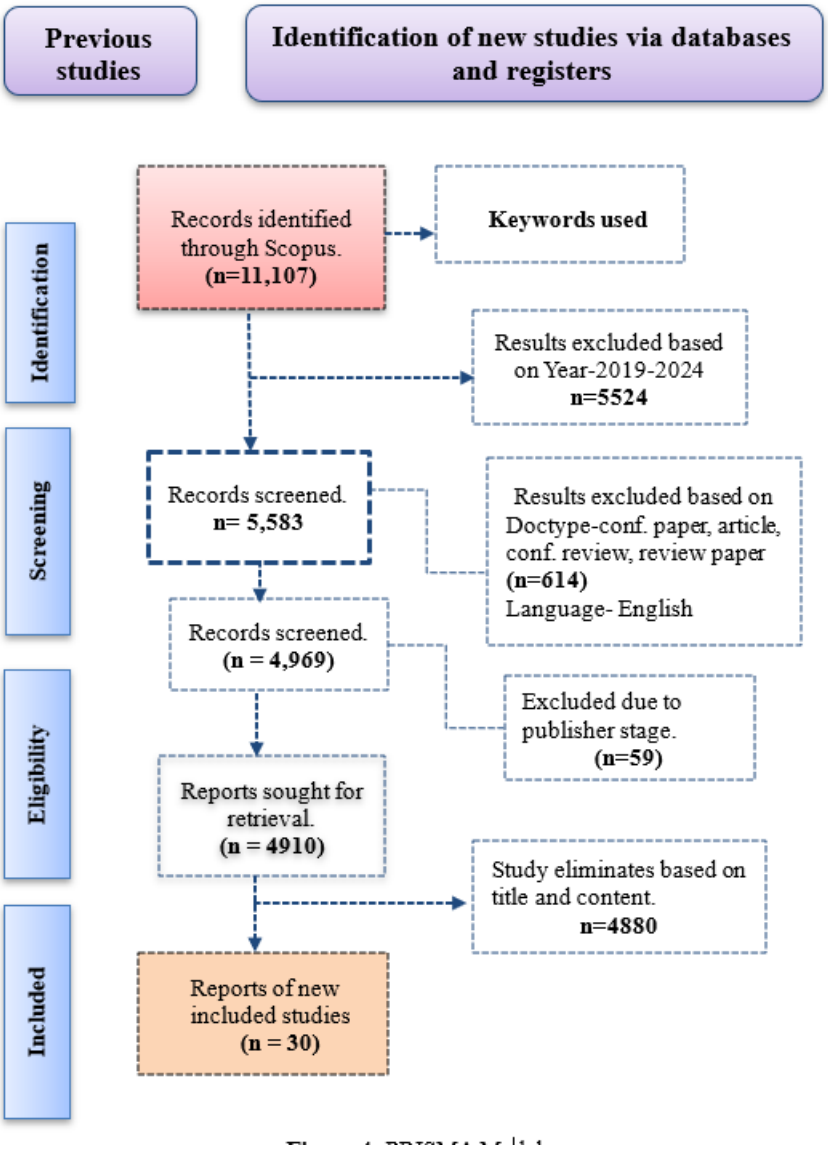

Figure 4: PRISMA Model

Figure 5 shows the distribution of publications across the top five subject areas. The highest number of publications comes from Computer Science, which has 3917 published works, while Engineering follows with 2959 published works. Mathematics contributes 995 publications, while Physics and Astronomy account for 706. Decision Sciences represents 665 publications. The research distribution indicates that AI-based intrusion detection for WSN research mainly originates from Computer Science and Engineering fields, with additional support from other interdisciplinary disciplines.

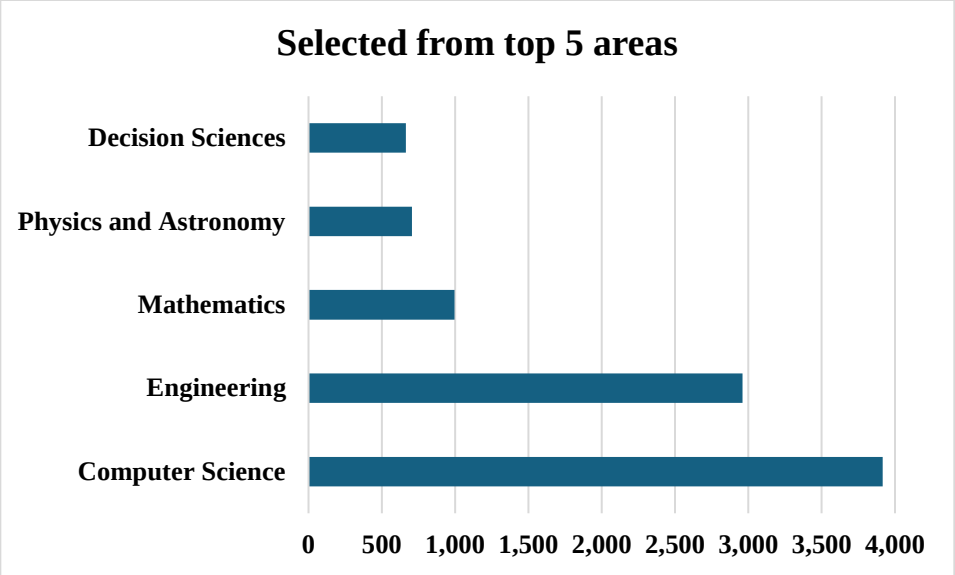

Figure 5: Selected papers from the top 5 Areas.

Source: Author's own elaboration

Figure 6 shows the main keywords that appear throughout the literature about AI-based IDSs designed for WSN. The WSN research field contains 2296 published papers, which demonstrate a strong interest in studying network design and data transmission methods and security systems that protect sensor networks. The 1243 ML papers show that researchers concentrate on using intelligent algorithms to find intrusions and traffic abnormalities in network systems. Research on node security, energy use, and data transfer systems in WSN is demonstrated through 1176 Sensor Nodes research papers. The 1081 DL research papers show that researchers increasingly study advanced neural network models to enhance their ability to detect intrusions and identify automated threats. The IoT research area contains 1019 papers that study how sensor networks connect to complete IoT systems and the security problems that emerge from this relationship. The research findings show multiple fields of study that support intrusion detection and security development for WSN through intelligent learning systems, network systems, and IoT applications.

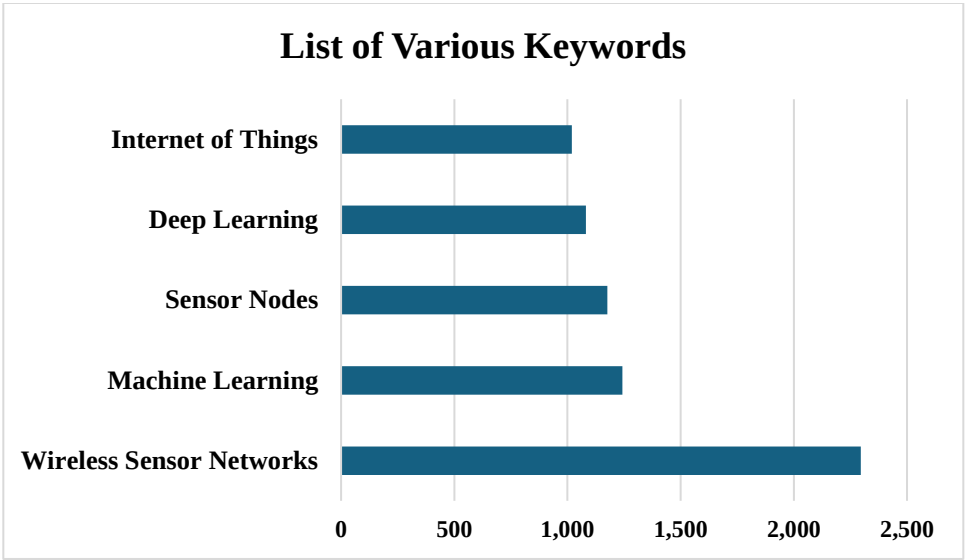

Figure 6: List of various Keywords.

Source: Author's own elaboration

The publication years of the studies are shown in Figure 7, which is an important piece of information. This systematic literature study aims to delve into the realm of AI-enabled IDSs in WSNs by carefully selecting search phrases.

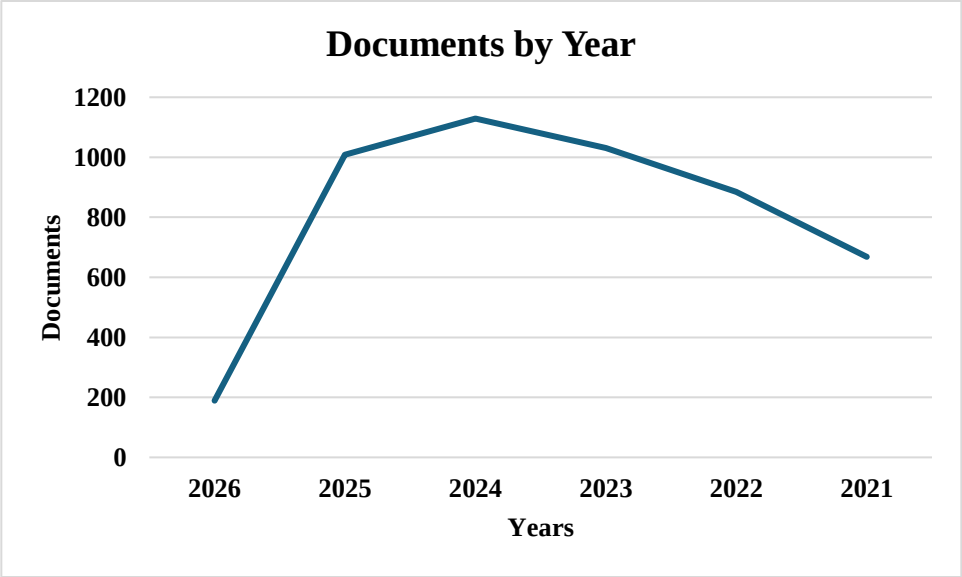

Figure 7: Trend in published papers.

Source: Author's own elaboration

Analytical Questions (**AQs**) that pertain to the objectives of this SR paper are thoroughly addressed:

AQ1. What are the traditional ML/DL algorithms used in WSN intrusion detection?

AQ2. What are the various datasets used in WSN environments?

AQ3. What are the key challenges and future opportunities for IDS in WSNs?

4. Traditional machine learning-based intrusion detection in WSNs

The following are the traditional intrusion detection techniques used in the WSNs, such as **Sirisha et al., (2026) [67],** who introduced the Dual Level Node Authentication Model along with Node Behavior Analysis (DLNA-NBA) for Intrusion Detection. The results showed that the proposed model greatly improved intrusion detection capabilities, achieved 98.9% accuracy in node authentication, 99.2% accuracy in intrusion detection, and decreased false alarms in WSN. Similarly, **Fares et al., (2025) [68]** created a novel method utilizing K-Nearest Neighbor (KNN) for the detection of network DoS assaults. The study used popular WSN-DS data that is tailored to DoS assaults. Accuracy and recall were two of the conventional measures used to assess the models' efficacy. After reaching a maximum accuracy of 99.76% in DoS detection, the experimental results proved that the KNN model was effective. However, **Shakya et al., (2025) [69]** suggested an intrusion detection system that relies on DNNs to boost efficiency. Using the cross-correlation method, researchers were able to choose the dataset's most useful features. The suggested model was tested and trained using the NSL-KDD intrusion dataset. The results of the experiment show that the proposed DNN outperforms the state-of-the-art ML models in terms of attack detection efficiency, with a score of 96.23%. Likewise, **Alomari et al., (2025) [70]** brought attention to the efficacy of various ML methods, including supervised as well as unsupervised learning, for WSN anomaly and intrusion detection. The main objective of the study was to make WSNs more secure by using an IDS based on ML techniques. The research found that ML models improved WSN security by increasing the efficiency of threat detection and retrieval in real time, with testing times ranging from 0.006 to 0.1249 and accuracy rates of 91% to 99.7 percent. Moreover, **Talukder et al., (2025) [71]** introduced a new hybrid ML model that uses the TON-IoT and WSN-DS datasets to assess its efficacy in dimensionality reduction and data balancing using KMeans-SMOTE (KMS). On the WSN-DS dataset, the suggested hybrid method accomplished outstanding results, with a precision of 99.94% and an F1-score of 99.94%.

Zhukabayeva et al., (2024) [72] put forward a design for enhancing the security of WSNs running on smart grids. The system efficiently identified cyber dangers by combining traffic analysis, node classification, and ML

algorithms. A thorough evaluation showed that WSN traffic load was accurately predicted using the Random Forest (RF), with a Mean Squared Error (MSE) of 2.772350. The RF model provided the best results in intrusion detection across all attack types, with a recall of 0.99, a precision of 0.99, and an F1 score of 0.98. Like this, **Gebremariam et al., (2023) [73]** devised a Multilayer Perceptron with Artificial Neural Network (MLPANN) to identify and pinpoint numerous assaults in WSNs. For training and testing the suggested system, four datasets were utilized. The method was designed to identify 10 attack types, including DoS attacks. Utilizing the WNS-DS dataset, the suggested method achieved an accuracy rate of 99.65%. Although **Elsadig et al., (2023) [74]** suggested a Decision Tree (DT) algorithm-based lightweight ML detection method for WSN DoS attack detection. By outperforming competing classifiers with a 99.5% accuracy rate and minimal overhead, the suggested method has demonstrated strong performance. The results showed that the suggested method was far superior to RF, with just 9.7 percent of the processing time required by RF. Moreover, **Salmi and Oughdir (2022) [75]** demonstrated a CNN-LSTM method for identifying and categorizing DoS intrusion assaults. This research utilized a WSN-DS dataset that was generated by computers. With a 97% success rate in classifying the provided attacks, the created model showed potential in the attack detection process. Lastly, **Alsulaiman and Al-Ahmadi (2021) [76]** tested a variety of ML algorithms to identify DoS assaults. Researchers trained and tested the models on the WSN-DS dataset. Compared to RF, J48 processed data faster (less than 9% of the time), and it obtained a higher accuracy (99.66%). These results showed that J48 was superior at overcoming the constraints of WSN. Table 4 and Figure 8 represent the previous studies done by various authors based on the ML techniques for IDS.

Table 4: ML techniques used in WSNs

Authors	**Algorithm**	**Accuracy (%)**	**Limitations**
Sirisha et al., (2026) [67]	DLNA-NBA	99.2	Increased system complexity due to multilayer architecture
Fares et al., (2025) [68]	KNN	99.76	High memory usage and slow with large datasets; sensitive to noise
Shakya et al., (2025) [69]	DNN	96.23	Performance affected by imbalanced data; high computational complexity
Talukder et al., (2025) [71]	KMS+ PCA	99.94	Increased model complexity; requires preprocessing and tuning
Zhukabayeva et al., (2024) [72]	RF	99.00	Limited generalization across datasets; depends on feature quality
Gebremariam et al., (2023) [73]	MLPANN	99.65	Requires large training data; prone to overfitting
Elsadig et al. (2023) [74]	DT	99.5	Less effective for complex and nonlinear attack patterns
Ravindra et al., (2023) [77]	Extreme Learning Machine (ELM)	96.90	Lower accuracy compared to ensemble and DL models
Alruwaili et al., (2023) [78]	Red kite optimization algorithm (RKOA)	98.94	Computational overhead due to the optimization process
Salmi and Oughdir (2022) [75]	CNN-LSTM	97.0	High computational cost; requires large datasets
Alsulaiman and Al-Ahmadi (2021) [76]	J48	99.66	Limited scalability and generalization
Meng et al., (2022) [79]	Light Gradient Boosting Machine **(**LightGBM)	99	Sensitive to parameter tuning

Putrada et al., (2022) [80]	eXtreme Gradient Boosting **(**XGBoost)	99.70	High computational cost and tuning complexity
Chandre et al., (2022) [81]	CNN	97	Requires large training data; computationally expensive
Dener et al., (2022) [82]	LightGBM	99.95	Might overfit without proper tuning
Ifzarne et al., (2021) [83]	Passive-aggressive (PA) Classifier	96	Lower accuracy compared to advanced ensemble models
Rezvi et al., (2021) [84]	ANN	98.56	Requires extensive training and hyperparameter tuning
Alruhaily et al., (2021) [85]	RF	97	Higher computational cost than simpler models

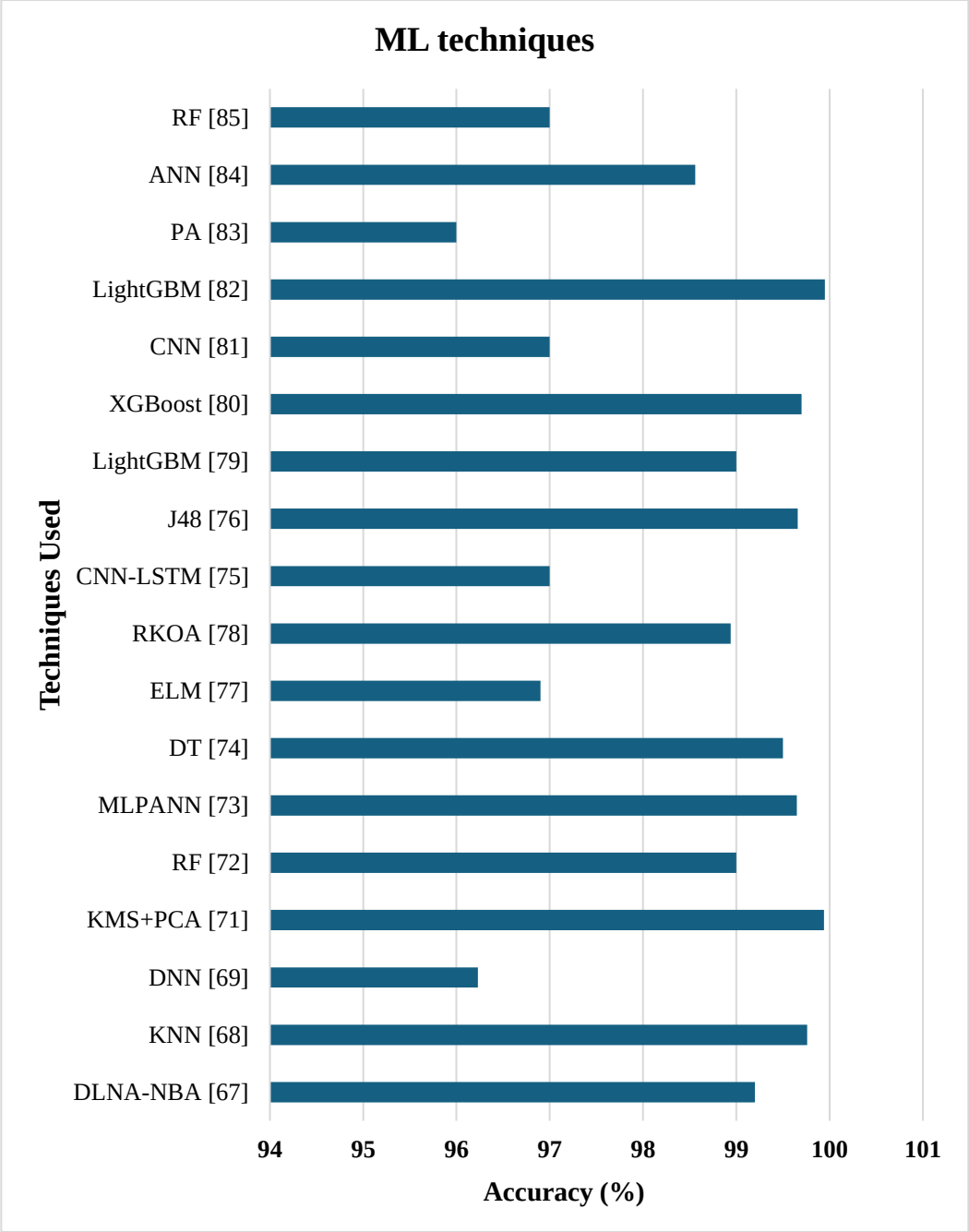

Figure 8: Comparative Analysis

5. Dataset used in the WSN for intrusion detection

The following are the mainly used datasets in WSNs:

- **WSN-DS Dataset**

The WSN-DS dataset has become one of the most popular datasets that researchers use to study intrusion detection methods for WSNs. The dataset uses simulated WSN environments to create its data, which centers on DoS attacks. The dataset provides researchers with access to normal and malicious traffic patterns, which they can use to test both binary and multiclass classification systems. Researchers have frequently used this dataset because it accurately represents actual WSN systems to test ML and DL algorithms, which include RL, LightGBM and hybrid

models [86]. The dataset enables researchers to investigate how nodes behave and communicate within systems that have limited available resources. It demonstrates its main drawback because it only focuses on specific types of attack, which do not represent the complete range of modern cyber threats that exist in diverse WSN and IoT environments [87].

- **NSL-KDD Dataset**

The NSL-KDD dataset serves as an advanced version of the KDD Cup 1999 dataset, which researchers use to evaluate IDS. The system was created to solve the problems that existed in its previous version by delivering a better assessment system. The dataset contains a structured set of features that represent network traffic and includes multiple categories of attacks, such as DoS [88]. The balanced structure of NSL-KDD, together with its accurate data labeling, makes it an ideal resource for training and testing ML and DL systems. The dataset has several restrictions because it fails to capture the actual behavior of WSN environments, and it contains outdated attack patterns that do not match current cybersecurity threats [89].

- **UNSW-NB15 Dataset**

The UNSW-NB15 dataset serves as a contemporary intrusion detection dataset, which was created to address the shortcomings found in previous datasets like NSL-KDD and KDD Cup 99 [90]. The data set was created through the simulation of real network traffic patterns, which occurred within a controlled cyber range environment, and it contains various modern attack methods, including exploits, fuzzers, worms, backdoors, and DoS attacks. The dataset contains a large number of features that capture both flow-based and packet-based characteristics, which make it appropriate for testing advanced ML and DL models [91]. Researchers use UNSW-NB15 to assess how well IDS models can identify current cyber threats through their ability to withstand different testing conditions. The dataset demands extensive preprocessing work together with feature selection activities and computational processing power because of its complex structure and multiple dimensions, which makes it difficult to use WSN systems with restricted resources [92].

- **CICIDS2017 Dataset**

The CICIDS2017 dataset stands as the most extensive and authentic dataset for the study of IDS [93]. It was created to simulate actual network traffic patterns, which include normal user behavior and all contemporary attack methods that include Distributed Denial-of-Service (DDoS) attacks, brute force attempts, botnet operations, and infiltration attempts. The dataset offers complete flow-based characteristics, which researchers extracted through network traffic investigation methods, making it ideal for DL model development [94]. The CICIDS2017 dataset was chosen due to the provision of quality data that can effectively simulate activities within networks, thus enabling researchers to validate advanced IDS within cloud computing and IoT-enabled WSNs. However, the huge amount of data and the high dimensionality call for efficient processing techniques prior to building the model [95]. Table 5 below presents the different types of datasets employed by researchers on WSNs.

Table 5: Dataset used

Authors (Year)	Technique used	Dataset(s)	Accuracy (%)
KVK and Reddy (2026) [96]	Enhanced Cheetah Optimization Algorithm (ECOA)	CICIDS2017 and UNSW-NB15	98.33, 97.52
Ileri et al., (2025) [97]	Particle Swarm Optimization **(**PSO)	Synthetically generated	99.9
Saleh et al., (2024) [98]	Gaussian Nave Bayes (GNB)	WSN-DS	96
Dharini et al., (2023) [99]	LightGBM	WSN DoS	99.16
Ismail et al. (2022) [100]	Naïve Bayes (NB)-LightGBM	WSN-DS	99.30
Mittal et al. (2021) [101]	Support Vector Machine (SVM)	NSL-KDD	96.15

Mahbooba et al. (2021) [102]	LSTM	WSN-DS	99.88
Yao et al. (2021) [103]	AutoEncoder(AE)-LightGBM	KDDCup'99	99.90
Ismail et al. (2021) [104]	LightGBM	WSN-DS	99.30
Pan et al. (2021) [105]	kNN-sine cosine algorithm (SCA)	NSL-KDD	99.33

6. Challenges and Future Opportunities

Despite the advancement in technology, the deployment of AI-based IDS for WSN faces several issues. The first issue, which is experienced by the WSN node, is attributed to its limited resource capabilities due to its energy, memory and computational abilities. The complex algorithms, such as the CNNs and LSTMs, and their combinations, need extensive computing capabilities, hence posing difficulties for their application in real-world time-critical cases [41–44]. In the experiments conducted, Hussain et al. (2025) [58] and Gowdhaman et al. (2024) [60] found that the DL models provide accurate results, but the models consume considerable energy and computation capacity. The dependency on the data set and data imbalances posed significant hurdles for the researcher working in this area. The WSN-DS data set, which is a universal data set, focuses on testing DoS attacks; hence, the trained model is biased against uncommon and unknown attacks [86–87]. Talukder et al. (2025) [71] solved the problem through SMOTE-based methods, but the preprocessing procedures made the model more difficult to use. Systems that use NSL-KDD or UNSW-NB15 datasets for training their models face challenges in achieving effective performance across multiple testing environments [90–92]. The high complexity of hybrid and optimization-based models also presents a major limitation. The detection accuracy improvements from GOA-GA [56], RKOA [78], and DRL-LSTM [58] come with new requirements for computational resources and system configuration. The system design hinders its ability to function as a real-time WSN deployment solution. The research faces challenges because there are no standardized datasets and benchmarking standards available for use. The absence of unified evaluation metrics makes it difficult to compare different IDS models effectively [51–54]. Most datasets fail to replicate actual WSN environments, which include changing network patterns, environmental disturbances and device malfunctions.

Future research should focus on creating IDS models that require less system resources and use minimal energy to meet WSN operational requirements. The model complexity reduction through pruning, quantization and knowledge distillation methods achieves accurate results according to research findings [78–80]. WSN environments gain better scalability and privacy protection through hybrid and distributed learning methods, which include federated learning as a viable solution for their development needs. The detection results can be enhanced through the combination of ML and DL models with optimization methods. Advanced data balancing and augmentation techniques, which include SMOTE, ADASYN and GAN-based methods, enable researchers to solve class imbalance problems while achieving better results in identifying minority attack types [55,71]. The creation of comprehensive WSN datasets that accurately represent actual WSN situations is necessary to enhance model performance in real-world conditions [90–92]. Future IDS systems should evaluate performance through energy efficiency, latency and network lifetime metrics, which would help systems operate effectively in actual time-sensitive situations [45–48].

7. Discussion

The analytical questions from this systematic review find their answers through a detailed examination of the data, methods, challenges, and future directions, which the previous sections provide. The research objectives receive assessment through a systematic evaluation of existing literature, which delivers complete solutions to all analytical questions. The literature review for AQ1, which examines the ML and DL algorithms applied to WSN intrusion detection, shows that traditional ML models, RF, LightGBM, KNN, DT, and SVMs receive widespread use because they deliver accurate results while requiring less computing power, which makes them ideal for WSN systems with limited resources [68,72,74,79]. DL models such as CNNs, LSTMs and DNNs have become increasingly popular because they automatically extract features while identifying hidden and complex attack patterns, although their operation necessitates more computational power [58,61,62]. Hybrid methods, which combine data balancing and dimensionality reduction and optimization algorithms, have shown better results for imbalanced datasets because they handle data imbalances better, but they add more complexity and require extra data preparation work [56,71]. In relation to AQ2, which investigates the datasets utilized in WSN environments, the study shows that WSN-DS is the most common dataset for WSN-based IDS evaluation, whereas NSL-KDD, UNSW-NB15, and CICIDS2017 have been utilized as benchmark and robustness testing datasets due to their diverse range of attacks [86–92]. However,

depending on individual datasets reduces the generality of the model. Regarding AQ3, which discusses the major problems and future directions, the findings suggest that there are several challenges faced when deploying IDS models in practical WSN environments, including imbalanced data sets, complex computation, inability to scale up, lack of generality, and nonexistence of benchmarked datasets, among others [51–54]. The results showed that although AI-based IDS achieves a high level of accuracy, more work needs to be done to create scalable and adaptable models for practical WSN environments.

8. Conclusion

The IDS is a crucial component of WSN since it protects data, ensures the integrity of the system and provides optimal performance of the network in mission-critical applications such as health care and military surveillance, and industrial sensing applications. The evolution of AI technology has significantly contributed to the intrusion detection process by utilizing ML and DL technologies that have been able to effectively detect complex attack methods that evolve with time in the WSN environment. The systematic review investigated different intrusion detection system methods by studying widely utilized datasets and analysis of ML and DL models, which included challenges and future research avenues. The study used structured review methods to select studies that had been published between 2021 and 2026 so that researchers could better understand ongoing research patterns. The research found that traditional ML models like random forest, LightGBM, KNN, and DT continue to be popular because they work well within WSN limitations, while DL models like CNN, LSTM, and DNN achieve better detection performance through their ability to recognize intricate intrusion behaviors. The combination of data balancing, feature selection and optimization techniques through hybrid methods shows better results when dealing with imbalanced datasets, which leads to better performance in intrusion detection system accuracy. The review shows that WSN-DS, NSL-KDD, UNSW-NB15, and CICIDS2017 serve as popular datasets for model evaluation, but their use of restricted and artificial datasets limits model generalization. The existing improvements face two main obstacles, which include expensive computational needs, imbalanced data and the absence of common datasets and challenges with real-time system operation. Future research needs to develop lightweight, energy-efficient and adaptive intrusion detection system models together with realistic datasets and standardized evaluation methods to enhance WSN security, scalability and reliability in changing environments.

References

1. Trigka, Maria, and Elias Dritsas. "Wireless sensor networks: From fundamentals and applications to innovations and future trends." Ieee Access (2025). https://doi.org/10.1109/ACCESS.2025.3572328
2. Mowla, Md Najmul, Neazmul Mowla, AFM Shahen Shah, Khaled M. Rabie, and Thokozani Shongwe. "Internet of Things and wireless sensor networks for smart agriculture applications: A survey." IEEE Access 11 (2023): 145813-145852. https://doi.org/10.1109/ACCESS.2023.3346299
3. Abdulhussain, Sadiq H., Basheera M. Mahmmod, Almuntadher Alwhelat, Dina Shehada, Zainab I. Shihab, Hala J. Mohammed, Tuqa H. Abdulameer et al. "A comprehensive review of sensor technologies in IOT: Technical aspects, challenges, and future directions." Computers 14, no. 8 (2025): 342. https://doi.org/10.3390/computers14080342
4. Sivasubramaniyam, Vigneselvan, Suganthi Ramasamy, Mohamed Shameer Peer, Tsega Yenew Melesse, and Gianluca Gatto. "Navigating wireless data transmission challenges in smart transportation: Technologies, sensor networks, and real-world applications." Electrical and Electronic Engineering 2025080707 (2025). https://doi.org/0.20944/preprints202508.0707.v1
5. Ashfaq, Muhammad, and Siti Nur. "IoT Sensor Networks-Orchestrating Connectivity, Efficiency, and Intelligence Across Diverse Domains." Int. J. Innov. Res. Comput. Sci. Technol 12, no. 3 (2024): 154-161. https://doi.org/10.55524/ijircst.2024.12.3.26
6. Aburukba, Raafat, and Khaled El Fakih. "Wireless Sensor Networks for Urban Development: A Study of Applications, Challenges, and Performance Metrics." Smart Cities 8, no. 3 (2025): 89. https://doi.org/10.3390/smartcities8030089
7. Hudda, Shreeram, and K. Haribabu. "A review on WSN-based resource-constrained smart IoT systems." Discover Internet of Things 5, no. 1 (2025): 56. https://doi.org/10.1007/s43926-025-00152-2
8. Pandey, Shivam, Mahi Chaudhary, and Zsolt Tóth. "An investigation on real-time insights: enhancing process control with IoT-enabled sensor networks." Discover Internet of Things 5, no. 1 (2025): 29. https://doi.org/10.1007/s43926-025-00124-6
9. Lata, Sonam, Shabana Mehfuz, and Shabana Urooj. "Secure and reliable WSN for Internet of Things: Challenges and enabling technologies." IEEE Access 9 (2021): 161103-161128. https://doi.org/10.1109/ACCESS.2021.3131367
10. Alomari, Mohammed F., Moamin A. Mahmoud, and Ramona Ramli. "A systematic review on the energy efficiency of dynamic clustering in a heterogeneous environment of wireless sensor networks (WSNs)." Electronics 11, no. 18 (2022): 2837. https://doi.org/10.3390/electronics11182837

11. Kavra, Radhika, Anjana Gupta, and Sangita Kansal. "Systematic study of topology control methods and routing techniques in wireless sensor networks." Peer-to-Peer Networking and Applications 15, no. 4 (2022): 1862-1922. https://doi.org/10.1007/s12083-022-01325-4
12. Vishwas, H. N., and T. K. Ramesh. "Recent trends in localization, routing, and security for wireless sensor networks." IEEE Access (2025). https://doi.org/10.1109/ACCESS.2025.3555280
13. Vikas, Charu Wahi, Bharat Bhushan Sagar, and Manisha Manjul. "Trusted energy-aware hierarchical routing (TEAHR) for wireless sensor networks." Sensors 25, no. 8 (2025): 2519. https://doi.org/10.3390/s25082519
14. Zhang, Bingtao, and Lingyan Meng. "Energy efficiency analysis of wireless sensor networks in precision agriculture economy." Scientific Programming 2021, no. 1 (2021): 8346708. https://doi.org/10.1155/2021/8346708
15. Maya Ramírez, Carlos Eliel, Tawanda Ashley Chari, and Ryman Shoko. "Significance of computational intelligence and genetic programming-based models for real-time disease monitoring in wireless sensor networks." Cogent Engineering 13, no. 1 (2026): 2605950. https://doi.org/10.1080/23311916.2025.2605950
16. Daousis, Spyridon, Nikolaos Peladarinos, Vasileios Cheimaras, Panagiotis Papageorgas, Dimitrios D. Piromalis, and Radu Adrian Munteanu. "Overview of protocols and standards for wireless sensor networks in critical infrastructures." Future Internet 16, no. 1 (2024): 33. https://doi.org/10.3390/fi16010033
17. Smith, John. "IoT-Enabled Wireless Sensor Networks for Environmental Sensing." American Journal of Sensor Networks and Wireless Communications 5, no. 5 (2024): 18-28. https://doi.org/10.71465/ajsnwc.3205
18. Rasoulpour, Fatemeh, and Muhammet Karabulut. "Advances in wireless sensor networks for IoT-enabled environmental monitoring and sustainable resource management." Smart City Insights 2, no. 3 (2025): 159-168. https://doi.org/10.22105/sci.v2i3.45
19. Selvam, Avines Panneer, and Safaa Najah Saud Al-Humairi. "The impact of iot and sensor integration on real-time weather monitoring systems: A systematic review." (2023). https://doi.org/10.21203/rs.3.rs-3579172/v1
20. Ali, Amir, Teodoro Montanaro, Ilaria Sergi, Simone Carrisi, Daniele Galli, Cosimo Distante, and Luigi Patrono. "An innovative iot and edge intelligence framework for monitoring elderly people using anomaly detection on data from non-wearable sensors." Sensors 25, no. 6 (2025): 1735. https://doi.org/10.3390/s25061735
21. Pavithra, D., T. Parameswaran, Mani Choudhry, S. Amrutha, T. Deepa, and R. Kiruthiga. "Application of LSTM networks for continuous patient monitoring and anomaly detection in wearable health devices." Indian J. Sci. Technol 17, no. 37 (2024): 3909-3921. https://doi.org/10.17485/IJST/v17i37.2600
22. Oztoprak, Ahmet, Reza Hassanpour, Aysegul Ozkan, and Kasim Oztoprak. "Security challenges, mitigation strategies, and future trends in wireless sensor networks: A review." ACM Computing Surveys 57, no. 4 (2024): 1-29. https://doi.org/10.1145/3706583
23. Faris, Mohammed, Mohd Nazri Mahmud, Mohd Fadzli Mohd Salleh, and Alhamzah Alnoor. "Wireless sensor network security: A recent review based on state-of-the-art works." International Journal of Engineering Business Management 15 (2023): 18479790231157220. https://doi.org/10.1177/18479790231157220
24. Ahmed, Akinsola, Ejiofor Oluomachi, Akinde Abdullah, and Njoku Tochukwu. "Enhancing data privacy in wireless sensor networks: Investigating techniques and protocols to protect privacy of data transmitted over wireless sensor networks in critical applications of healthcare and national security." arXiv preprint arXiv:2404.11388 (2024). https://doi.org/10.48550/arXiv.2404.11388
25. Zhukabayeva, Tamara, Lazzat Zholshiyeva, Yerik Mardenov, Atdhe Buja, Shafiullah Khan, and Noha Alnazzawi. "Real-Time Detection and Response to Wormhole and Sinkhole Attacks in Wireless Sensor Networks." Technologies 13, no. 8 (2025): 348. https://doi.org/10.3390/technologies13080348
26. Jae-Dong, Kim. "A comprehensive analysis of routing vulnerabilities and defense strategies in IoT networks." arXiv preprint arXiv:2410.13214 (2024). https://doi.org/10.48550/arXiv.2410.13214
27. Khokhar, Anjali. "A Comparative Analysis of Attacks on RPL in Internet of Things Networks." International Journal of Research & Technology 13, no. 3 (2025): 601-613. https://doi.org/10.64882/ijrt.v13.i3.765
28. Al-Anzi, Fawaz S. "Design and analysis of intrusion detection systems for wireless mesh networks." Digital Communications and Networks 8, no. 6 (2022): 1068-1076. https://doi.org/10.1016/j.dcan.2022.05.013
29. Al-Fuhaidi, Belal, Zainab Farae, Farouk Al-Fahaidy, Gawed Nagi, Abdullatif Ghallab, and Abdu Alameri. "Anomaly-Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms." Applied Computational Intelligence and Soft Computing 2024, no. 1 (2024): 2625922. https://doi.org/10.1155/2024/2625922
30. Heidari, Arash, and Mohammad Ali Jabraeil Jamali. "Internet of Things intrusion detection systems: a comprehensive review and future directions." Cluster Computing 26, no. 6 (2023): 3753-3780. https://doi.org/10.1007/s10586-022-03776-z
31. Jeffrey, Nicholas, Qing Tan, and José R. Villar. "A review of anomaly detection strategies to detect threats to cyber-physical systems." Electronics 12, no. 15 (2023): 3283. https://doi.org/10.3390/electronics12153283
32. Mikuláš, Matúš, and Ivan Kotuliak. "Review of intrusion detection systems taxonomy, techniques, methods, and future research directions." 2024 New Trends in Signal Processing (NTSP) (2024): 1-8. https://doi.org/10.23919/NTSP61680.2024.10726305
33. Kipongo, Joseph, Theo G. Swart, and Ebenezer Esenogho. "Design and implementation of intrusion detection systems using RPL and AOVD protocol-based wireless sensor networks." International Journal of Electronics and Telecommunications (2023): 309-318. https://doi.org/10.1109/ACCESS.2023.3347778

34. Zaimen, Khaoula, Laurent Moalic, Abdelhafid Abouaissa, and Lhassane Idoumghar. "A survey of artificial intelligence-based WSNs deployment techniques and related objectives modeling." IEEE Access 10 (2022): 113294-113329. https://doi.org/10.1109/ACCESS.2022.3217200
35. Masengo Wa Umba, Shimbi, Adnan M. Abu-Mahfouz, and Daniel Ramotsoela. "Artificial intelligence-driven intrusion detection in software-defined wireless sensor networks: Towards secure IoT-enabled healthcare systems." International journal of environmental research and public health 19, no. 9 (2022): 5367. https://doi.org/10.3390/ijerph19095367
36. Rana, Rachna, and Pankaj Bhambri. "Artificial Intelligence–Enabled Ad Hoc and Wireless Sensor Networks: Architectures, Challenges, and Applications." INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH 14, no. 1 (2026): 168-182. https://doi.org/10.56975/ijedr.v14i1.303958
37. Osamy, Walid, Ahmed M. Khedr, Ahmed Salim, Ahmed A. El-Sawy, Mohammed Alreshoodi, and Ibrahim Alsukayti. "Recent advances and prospects of using AI solutions for security, fault tolerance, and QoS challenges in WSNs." Electronics 11, no. 24 (2022): 4122. https://doi.org/10.3390/electronics11244122
38. Ahmad, Rami, Raniyah Wazirali, and Tarik Abu-Ain. "Machine learning for wireless sensor networks security: An overview of challenges and issues." Sensors 22, no. 13 (2022): 4730. https://doi.org/10.3390/s22134730
39. Ghadi, Yazeed Yasin, Tehseen Mazhar, Tamara Al Shloul, Tariq Shahzad, Umair Ahmad Salaria, Arfan Ahmed, and Habib Hamam. "Machine learning solutions for the security of wireless sensor networks: A review." Ieee Access 12 (2024): 12699-12719. https://doi.org/10.1109/ACCESS.2024.3355312
40. Al-Quayed, Fatima, Zulfiqar Ahmad, and Mamoona Humayun. "A situation-based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0." Ieee Access 12 (2024): 34800-34819. https://doi.org/10.1109/ACCESS.2024.3372187
41. Tamilselvi, S., Chin-Shiuh Shieh, Mong-Fong Horng, and N. R. Shanker. "Deep learning-based HTTP TRACE flood detection in wireless sensor network using deep spectral multilayer convolutional neural network." Scientific Reports (2026). https://doi.org/10.1038/s41598-026-42474-3
42. Johnson-Okonkwo, C. C., I. I. Ayogu, G. A. Chukwudebe, and J. N. Odii. "Harnessing machine learning for intelligent load balancing in wireless sensor networks: A review of strategies, challenges, and future directions." SSR Journal of Artificial Intelligence (SSRJAI) 2, no. 2 (2025): 86-106. https://doi.org/10.5281/zenodo.15831468
43. Menon, U. Vivek, Vinoth Babu Kumaravelu, C. Vinoth Kumar, A. Rammohan, Sunil Chinnadurai, Rajeshkumar Venkatesan, Han Hai, and Poongundran Selvaprabhu. "AI-powered IoT: A survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications." IEEE Access (2025). https://doi.org/10.1109/ACCESS.2025.3551750
44. Chaganti, Krishna C. "Advancing AI-driven threat detection in IoT ecosystems: Addressing scalability, resource constraints, and real-time adaptability." Authorea Preprints (2024). https://d197for5662m48.cloudfront.net/documents/publicationstatus/241747/preprint_pdf/6e15ff63f3f6d7387bbf96ee5167159a.pdf
45. Priyadarshi, Rahul, Ravi Ranjan Kumar, Rakesh Ranjan, and Padarti Vijaya Kumar. "AI-based routing algorithms improve energy efficiency, latency, and data reliability in wireless sensor networks." Scientific Reports 15, no. 1 (2025): 22292. https://doi.org/10.1038/s41598-025-08677-w
46. Saleh, Hadeel M., Hend Marouane, and Ahmed Fakhfakh. "A Comprehensive Analysis of Security Challenges and Countermeasures in Wireless Sensor Networks Enhanced by Machine Learning and Deep Learning Technologies." International Journal of Safety & Security Engineering 14, no. 2 (2024). https://doi.org/10.18280/ijsse.140206
47. Azizan, Adnan Helmi, Salama A. Mostafa, Aida Mustapha, Cik Feresa Mohd Foozy, Mohd Helmy Abd Wahab, Mazin Abed Mohammed, and Bashar Ahmad Khalaf. "A machine learning approach for improving the performance of network intrusion detection systems." Annals of Emerging Technologies in Computing (AETiC) 5, no. 5 (2021): 201-208. https://doi.org/10.33166/AETiC.2021.05.025
48. Ahmed, Quazi Warisha, Shruti Garg, Amrita Rai, Manikandan Ramachandran, Noor Zaman Jhanjhi, Mehedi Masud, and Mohammed Baz. "AI-based resource allocation techniques in wireless sensor internet of things networks in energy efficiency with data optimization." Electronics 11, no. 13 (2022): 2071. https://doi.org/10.3390/electronics11132071
49. Amutha, J., Sandeep Sharma, and Jaiprakash Nagar. "WSN strategies based on sensors, deployment, sensing models, coverage and energy efficiency: Review, approaches and open issues." Wireless Personal Communications 111, no. 2 (2020): 1089-1115. https://doi.org/10.1007/s11277-019-06903-z
50. Alsubaei, Faisal S. "Smart deep learning model for enhanced IoT intrusion detection." Scientific Reports 15, no. 1 (2025): 20577. https://doi.org/10.1038/s41598-025-06363-5
51. Raja, Muhammadu Sathik Raja Sathik. "The rise of AI-driven network intrusion detection systems: Innovations, challenges, and future directions." International Journal of AI, BigData, Computational and Management Studies 6, no. 1 (2025): 1-9. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I1P101
52. Sharma, Shashi Bhushan, and Amit Kumar Bairwa. "Leveraging AI for intrusion detection in IoT ecosystems: a comprehensive study." IEEE Access (2025). https://doi.org/10.1109/ACCESS.2025.3550392
53. Thakur, Sumendra, Nurul I. Sarkar, and Sira Yongchareon. "AI-Driven Energy-Efficient Routing in IoT-Based Wireless Sensor Networks: A Comprehensive Review." Sensors 25, no. 24 (2025): 7408. https://doi.org/10.3390/s25247408

54. Muneer, Salman, Umer Farooq, Atifa Athar, Muhammad Ahsan Raza, Taher M. Ghazal, and Shadman Sakib. "A critical review of artificial intelligence-based approaches in intrusion detection: A comprehensive analysis." Journal of Engineering 2024, no. 1 (2024): 3909173. https://doi.org/10.1155/2024/3909173
55. Munaye, Yirga Yayeh, Abebaw Demelash Gebeyehu, Li-Chia Tai, Zemenu Alem Abebe, Aeneas Bekele Workneh, Robel Berie Tarekegn, Yenework Belayneh Chekol, and Getaneh Berie Tarekegn. "Machine Learning-Driven Intrusion Detection for Securing IoT-Based Wireless Sensor Networks." Future Internet 18, no. 2 (2026): 113. https://doi.org/10.3390/fi18020113
56. Prasad, Ashwani, Karmel Arockiasamy, and Kanimozhi Gunasekaran. "A hybrid metaheuristic algorithm with machine learning for detecting denial-of-service attacks in wireless sensor networks." Frontiers in Artificial Intelligence 9 (2026): 1738152. https://doi.org/10.3389/frai.2026.1738152
57. Zhang, Hongwei, Darshana Upadhyay, Marzia Zaman, Achin Jain, and Srinivas Sampalli. "SC-MLIDS: Fusion-based Machine Learning Framework for Intrusion Detection in Wireless Sensor Networks." Ad Hoc Networks 175 (2025): 103871. https://doi.org/10.1016/j.adhoc.2025.103871
58. Hussain, Saqib, Jingsha He, Ala Saleh Alluhaidan, Nafei Zhu, Fahad Razaque Mughal, Sadique Ahmad, and Zulfiqar Ali Zardari. "MultiNet-IDS: an ensemble of DRL and LSTM for improved intrusion detection in wireless sensor networks." Scientific Reports 15, no. 1 (2025): 33420. https://doi.org/10.1038/s41598-025-18829-7
59. Sun, Yanxia, and Zenghui Wang. "Intrusion detection in IoT and wireless networks using image-based neural network classification." Applied Soft Computing 177 (2025): 113236. https://doi.org/10.1016/j.asoc.2025.113236
60. Gowdhaman, V., and R. Dhanapal. "Hybrid deep learning-based intrusion detection system for wireless sensor network." International Journal of Vehicle Information and Communication Systems 9, no. 3 (2024): 239-255. https://doi.org/10.1504/IJVICS.2024.139627
61. Sadia, Halima, Saima Farhan, Yasin Ul Haq, Rabia Sana, Tariq Mahmood, Saeed Ali Omer Bahaj, and Amjad Rehman Khan. "Intrusion detection system for wireless sensor networks: A machine learning-based approach." IEEE Access 12 (2024): 52565-52582. https://doi.org/10.1109/ACCESS.2024.3380014
62. Sedhuramalingam, K., and N. Saravanakumar. "A novel optimal deep learning approach for designing an intrusion detection system in wireless sensor networks." Egyptian Informatics Journal 27 (2024): 100522. https://doi.org/10.1016/j.eij.2024.100522
63. Karthikeyan, M., D. Manimegalai, and Karthikeyan RajaGopal. "Firefly algorithm-based WSN-IoT security enhancement with machine learning for intrusion detection," Scientific Reports 14, no. 1 (2024): 231. https://doi.org/10.1038/s41598-023-50554-x
64. Talukder, Md Alamin, Selina Sharmin, Md Ashraf Uddin, Md Manowarul Islam, and Sunil Aryal. "MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs." International Journal of Information Security 23, no. 3 (2024): 2139-2158. https://doi.org/10.1007/s10207-024-00833-z
65. Sharma, Bhawana, Lokesh Sharma, Chhagan Lal, and Satyabrata Roy. "Anomaly-based network intrusion detection for IoT attacks using deep learning technique." Computers and Electrical Engineering 107 (2023): 108626. https://doi.org/10.1016/j.compeleceng.2023.108626
66. Awajan, Albara. "A novel deep learning-based intrusion detection system for IOT networks." Computers 12, no. 2 (2023): 34. https://doi.org/10.3390/computers12020034
67. Sirisha, Aswadhati, and Kurra Sri. "Cluster head-based dual-level node authentication model with node pattern analysis for intrusion detection in wireless sensor networks using machine learning." Discover Computing 29, no. 1 (2026): 45. https://doi.org/10.1007/s10791-026-09948-4
68. Fares, Hajar, Amol D. Vibhute, Yassine Mouniane, and Habiba Bouijij. "Intrusion detection in wireless sensor networks using machine learning." Procedia Computer Science 252 (2025): 912-921. https://doi.org/10.1016/j.procs.2025.01.052
69. Shakya, Vandana, Jaytrilok Choudhary, and Dhirendra Pratap Singh. "Deep learning-based intrusion detection system for WSN." Procedia Computer Science 258 (2025): 2101-2106. https://doi.org/10.1016/j.procs.2025.04.460
70. Alomari, Esraa Saleh, Oday Ali Hassen, Wisam Makki Salim, Selvakumar Manickam, and Nur Azman Abu. "A New Descriptor Based on Machine Learning for Intrusion Detection in Wireless Sensor Networks (WSNs)." Journal of Intelligent Systems & Internet of Things 16, no. 1 (2025). https://doi.org/10.54216/JISIoT.160115
71. Talukder, Md Alamin, Majdi Khalid, and Nasrin Sultana. "A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction." Scientific Reports 15, no. 1 (2025): 4617. https://doi.org/10.1038/s41598-025-87028-1?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle
72. Zhukabayeva, Tamara, Aisha Pervez, Yerik Mardenov, Mohamed Othman, Nurdaulet Karabayev, and Zulfiqar Ahmad. "A traffic analysis and node categorization-aware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids." IEEE Access 12 (2024): 91715-91733. https://doi.org/10.1109/ACCESS.2024.3422077
73. Gebremariam, Gebrekiros Gebreyesus, J. Panda, and S. Indu. "Localization and detection of multiple attacks in wireless sensor networks using an artificial neural network." Wireless Communications and Mobile Computing 2023, no. 1 (2023): 2744706. https://doi.org/10.1155/2023/2744706?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle
74. Elsadig, Muawia A. "Detection of denial-of-service attack in wireless sensor networks: A lightweight machine learning approach." IEEe Access 11 (2023): 83537-83552. https://doi.org/10.1109/access.2023.3303113

75. Salmi, Salim, and Lahcen Oughdir. "Cnn-lstm based approach for DoS attacks detection in wireless sensor networks." International Journal of Advanced Computer Science and Applications 13, no. 4 (2022). https://doi.org/10.14569/IJACSA.2022.0130497
76. Alsulaiman, Lama, and Saad Al-Ahmadi. "Performance evaluation of machine learning techniques for DOS detection in wireless sensor network." arXiv preprint arXiv:2104.01963 (2021). https://doi.org/10.48550/arXiv.2104.01963
77. Ravindra, Chaya, Manjunath R. Kounte, Gangadharaiah Soralamavu Lakshmaiah, and V. Nuthan Prasad. "Etelmad: anomaly detection using enhanced transient extreme machine learning system in wireless sensor networks." Wireless Personal Communications 130, no. 1 (2023): 21-41. https://doi.org/10.1007/s11277-023-10271-0?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle
78. Alruwaili, Fahad F., Mashael M. Asiri, Fatma S. Alrayes, Sumayh S. Aljameel, Ahmed S. Salama, and Anwer Mustafa Hilal. "Red kite optimization algorithm with average ensemble model for intrusion detection for secure IoT." IEEE Access 11 (2023): 131749-131758. https://doi.org/10.1109/ACCESS.2023.3335124
79. Meng, Di, Hong Dai, Qiaochu Sun, Yao Xu, and Tianwei Shi. "Novel Wireless Sensor Network Intrusion Detection Method Based on LightGBM Model." IAENG International Journal of Applied Mathematics 52, no. 4 (2022). https://www.iaeng.org/IJAM/issues_v52/issue_4/IJAM_52_4_23.pdf
80. Putrada, Aji Gautama, Nur Alamsyah, Syafrial Fachri Pane, and Mohamad Nurkamal Fauzan. "Xgboost for IDS on WSN cyber attacks with imbalanced data." In the 2022 International Symposium on Electronics and Smart Devices (ISESD), pp. 1-7. IEEE, 2022. https://doi.org/10.1109/ISESD56103.2022.9980630
81. Chandre, Pankaj Ramchandra, Parikshit Mahalle, and Gitanjali Shinde. "Intrusion prevention system using a convolutional neural network for wireless sensor network." IAES International Journal of Artificial Intelligence 11, no. 2 (2022): 504. http://doi.org/10.11591/ijai.v11.i2.pp504-515
82. Dener, Murat, Samed Al, and Abdullah Orman. "STLGBM-DDS: An efficient data balanced DoS detection system for wireless sensor networks on big data environment." IEEE Access 10 (2022): 92931-92945. http://doi.org/10.1109/access.2022.3202807
83. Ifzarne, Samir, Hiba Tabbaa, Imad Hafidi, and Nidal Lamghari. "Anomaly detection using machine learning techniques in wireless sensor networks." In Journal of Physics: Conference Series, vol. 1743, no. 1, p. 012021. IOP Publishing, 2021. http://doi.org/10.1088/1742-6596/1743/1/012021
84. Rezvi, Md Alauddin, Sidratul Moontaha, Khadija Akter, Trisha, Shamse Tasnim, Cynthia, and Shamim Ripon. "Data mining approach to analyzing intrusion detection of wireless sensor network." Indonesian Journal of Electrical Engineering and Computer Science 21, no. 1 (2021): 516-523. http://doi.org/10.11591/ijeecs.v21.i1.pp516-523
85. Alruhaily, Nada M., and Dina M. Ibrahim. "A multilayer machine learning-based intrusion detection system for wireless sensor networks." International Journal of Advanced Computer Science and Applications 12, no. 4 (2021): 281-288. https://doi.org/10.54216/FPA.200109
86. Anwar, Raja Waseem, Mohammad Abrar, Abdu Salam, and Faizan Ullah. "Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: a multi-dataset analysis." PeerJ Computer Science 11 (2025): e2751. https://doi.org/10.7717/peerj-cs.2751
87. Dener, Murat, Celil Okur, Samed Al, and Abdullah Orman. "Wsn-bfsf: a new data set for attacks detection in wireless sensor networks." IEEE Internet of Things Journal 11, no. 2 (2023): 2109-2125. https://doi.org/10.1109/JIOT.2023.3292209
88. Abdullah, Hazem Salim Abdullah. "A comparison of several intrusion detection methods using the NSL-KDD dataset." Wasit Journal of Computer and Mathematics Science 3, no. 2 (2024): 32-41. https://doi.org/10.31185/wjcms.251
89. Ngueajio, Mikel K., Gloria Washington, Danda B. Rawat, and Yolande Ngueabou. "Intrusion detection systems using support vector machines on the KDD Cup'99 and nsl-kdd datasets: A comprehensive survey." In Proceedings of SAI Intelligent Systems Conference, pp. 609-629. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-031-16078-3_42
90. Hakke, Dasganu Govindrao. "PERFORMANCE EVALUATION OF MACHINE LEARNING-BASED INTRUSION DETECTION USING NSL-KDD, UNSW-NB15 AND CICIDS2017 DATASETS." International Journal of Applied Mathematics 38, no. 3s (2025): 447-469. https://doi.org/10.12732/ijam.v38i3s.160
91. Gade, Lourdu Mary. "Advanced ML Approaches for Intrusion Detection: A Comprehensive Analysis Using UNSW-NB15 and NSL-KDD Datasets." PhD., Dublin, National College of Ireland, 2025. https://norma.ncirl.ie/id/eprint/8204
92. Al-Shabi, Mohammed, Anmar Abuhamdah, and Malek Alzaqebah. "Improving network security using deep learning for intrusion detection." International Journal of Electrical & Computer Engineering (2088-8708) 15, no. 6 (2025). https://doi.org/10.11591/ijece.v15i6.pp5570-5583
93. Khan, Zafar Iqbal, Mohammad Mazhar Afzal, and Khurram Naim Shamsi. "A comprehensive study on CIC-IDS2017 dataset for intrusion detection systems." Int Res J Adv Eng Hub 2, no. 02 (2024): 254-260. https://doi.org/10.47392/IRJAEH.2024.0041
94. Maseer, Ziadoon Kamil, Robiah Yusof, Nazrulazhar Bahaman, Salama A. Mostafa, and Cik Feresa Mohd Foozy. "Benchmarking of machine learning for anomaly-based intrusion detection systems in the CICIDS2017 dataset." IEEE Access 9 (2021): 22351-22370. https://doi.org/10.1109/ACCESS.2021.3056614
95. OYELAKIN, Akinyemi Moruff. "Overview and exploratory analyses of CICIDS2017 intrusion detection dataset." Indonesian Journal of Data and Science (2023). https://doi.org/10.56705/ijodas.v4i3.80

96. KVK, Chithanya, and V. Lokeswara Reddy. "Deep learning-based intrusion detection for cloud environments using Modified Stacked Bidirectional Gated Recurrent Unit." Discover Computing 29, no. 1 (2026): 159. https://doi.org/10.1007/s10791-026-10020-4
97. Ileri, Kadir. "Comparative analysis of CatBoost, LightGBM, XGBoost, RF, and DT methods optimized with PSO to estimate the number of k-barriers for intrusion detection in wireless sensor networks." International Journal of Machine Learning and Cybernetics 16, no. 9 (2025): 6937-6956. https://doi.org/10.1007/s13042-025-02654-5
98. Saleh, Hadeel M., Hend Marouane, and Ahmed Fakhfakh. "Stochastic gradient descent intrusion detection for wireless sensor network attack detection system using machine learning." IEEe Access 12 (2024): 3825-3836. https://doi.org/10.1109/ACCESS.2023.3349248
99. Dharini, N., Jeevaa Katiravan, Sruthi Priya DM, and Sakthi Sneghaa VA. "Intrusion detection in novel WSN-leach dos attack dataset using machine learning-based boosting algorithms." Procedia Computer Science 230 (2023): 90-99. https://doi.org/10.1016/j.procs.2023.12.064
100. Ismail, Shereen, Diana Dawoud, and Hassan Reza. "A lightweight multilayer machine learning detection system for cyber-attacks in WSN." In 2022, IEEE 12th Annual Computing and Communication Workshop and conference (CCWC), pp. 0481-0486. IEEE, 2022. https://doi.org/10.1109/CCWC54503.2022.9720891
101. Mittal, Mohit, Rocío Pérez De Prado, Yukiko Kawai, Shinsuke Nakajima, and José E. Muñoz-Expósito. "Machine learning techniques for energy efficiency and anomaly detection in hybrid wireless sensor networks." Energies 14, no. 11 (2021): 3125. https://doi.org/10.3390/en14113125
102. Mahbooba, Basim, Radhya Sahal, Wael Alosaimi, and Martin Serrano. "Trust in intrusion detection systems: an investigation of performance analysis for machine learning and deep learning models." Complexity 2021, no. 1 (2021): 5538896. https://doi.org/10.1155/2021/5538896
103. Yao, Ruizhe, Ning Wang, Zhihui Liu, Peng Chen, Di Ma, and Xianjun Sheng. "Intrusion detection system in the Smart Distribution Network: A feature engineering-based AE-LightGBM approach." Energy Reports 7 (2021): 353-361. https://doi.org/10.1016/j.egyr.2021.10.024
104. Ismail, Shereen, Tala Talaei Khoei, Ronald Marsh, and Naima Kaabouch. "A comparative study of machine learning models for cyber-attacks detection in wireless sensor networks." In 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0313-0318. IEEE, 2021. https://doi.org/10.1109/UEMCON53757.2021.9666581
105. Pan, Jeng-Shyang, Fang Fan, Shu-Chuan Chu, Hui-Qi Zhao, and Gao-Yuan Liu. "A lightweight intelligent intrusion detection model for wireless sensor networks." Security and communication Networks 2021, no. 1 (2021): 5540895. https://doi.org/10.1155/2021/5540895