ISSN: 2583-7354

International Journal of Emerging Knowledge Studies

Publisher's Home Page: https://www.ijeks.com/

Fully Open Access Research Paper

Intrusion Detection Systems in Wireless Sensor Networks Using AI & ML

Prashant Kumar [1*] Dr. Deepak Kumar Gupta[2] Shweta Garg[3]

[1]M.Tech Student, Computer Science & Engineering Department School of Engineering & Technology, IIMT University, Meerut, India.

[2]Assistant Professor, Computer Science & Engineering Department, School of Engineering & Technology, IIMT University, Meerut, India.

[3]Co-Guide, Computer Science & Engineering Department, School of Engineering & Technology, IIMT University, Meerut, India.

DOI: https://doi.org/10.70333/ijeks-05-03-017

*Corresponding Author: Kashyapprashant943@gmail.com

Article Info: - Received : 08 February 2026 **Accepted** : 25 March 2026 **Published** : 30 March 2026

Abstract

Wireless Sensor Networks (WSNs) have found numerous applications in fields like environment monitoring, healthcare systems, smart cities, and industrial automation. However, WSNs are susceptible to many kinds of cyber security attacks such as denial-of-service attacks, sinkhole attacks, wormhole attacks and selective forwarding attack because of their distributed architecture, limited computational resources, and wirelesscommunication channels. But it does not help you identify what is bad for a network, how to protect the integrity of your network! Machine Learning (ML) and Artificial Intelligence (AI) techniques have become one of the efficient tools in detecting complex intrusion patterns, during recent years. This research paper provides an overview of various AI and ML-based intrusion detection approaches in WSN domain. This study provides a comprehensive review of different detection approaches such as supervised learning algorithms, unsupervised learning techniques, deep learning methods, and hybrid detection systems. Also, it discusses widely used datasets, feature extraction methods and popular performance measures which include accuracy, precision, recall, F1 score and false positive rate. Moreover, the review highlights and compares pros and cons of several potential machine learning algorithms employed for intrusion detection in resource constrained sensor networks. In addition, this paper showcases specific research challenges such as energy consumption, dataset imbalance, distributed detection methods and model explainability. Finally, this paper identifies potential future research directions to improve the efficiency and scalability of intrusion detection systems (IDS) for next-generation WSNs, including lightweight deep learning models, federated learning, edge intelligence and explainable artificial intelligence.

Keywords: *Intrusion Detection System, Wireless Sensor Networks, Artificial Intelligence, Machine Learning, Network Security, Deep Learning.*

ISSN: 2583-7354

1. Introduction

Wireless Sensor Networks (WSNs) are composed of spatially distributed sensor nodes that communicate wirelessly to monitor environmental and physical conditions such as temperature, pressure, motion, and health-related data. These networks are widely applied in various domains including environmental monitoring, healthcare systems, smart cities, military surveillance, and industrial automation. However, due to the distributed nature of WSNs, limited computational capability, memory constraints, and battery limitations, these networks are highly vulnerable to various security threats and cyberattacks such as denial-of-service (DoS), sinkhole, wormhole, Sybil, blackhole, and selective forwarding attacks **(Alrajeh et al., 2013)**.

Traditional security techniques such as encryption and authentication mechanisms can protect Wireless Sensor Networks from some external attacks, but they are not sufficient to detect insider attacks or newly emerging threats. Therefore, Intrusion Detection Systems (IDS) are considered an essential security mechanism that monitors network traffic and identifies malicious activities or abnormal behavior within the network **(Albulayhi et al., 2021)**. IDS plays a significant role in maintaining network integrity, confidentiality, and availability by detecting both known and unknown attacks.

In recent years, Artificial Intelligence (AI) and Machine Learning (ML) techniques have been widely used in intrusion detection systems because of their ability to learn patterns from network data and detect previously unseen attacks. Machine learning algorithms can automatically classify network behavior as normal or malicious by analyzing traffic patterns, node behavior, and communication anomalies. Various supervised, unsupervised, and deep learning techniques such as Support Vector Machine (SVM), Random Forest, Decision Tree, K-Nearest Neighbor (KNN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN) have been widely applied for intrusion detection in WSN environments **(Ashraf et al., 2020; Pinto et al., 2023)**.

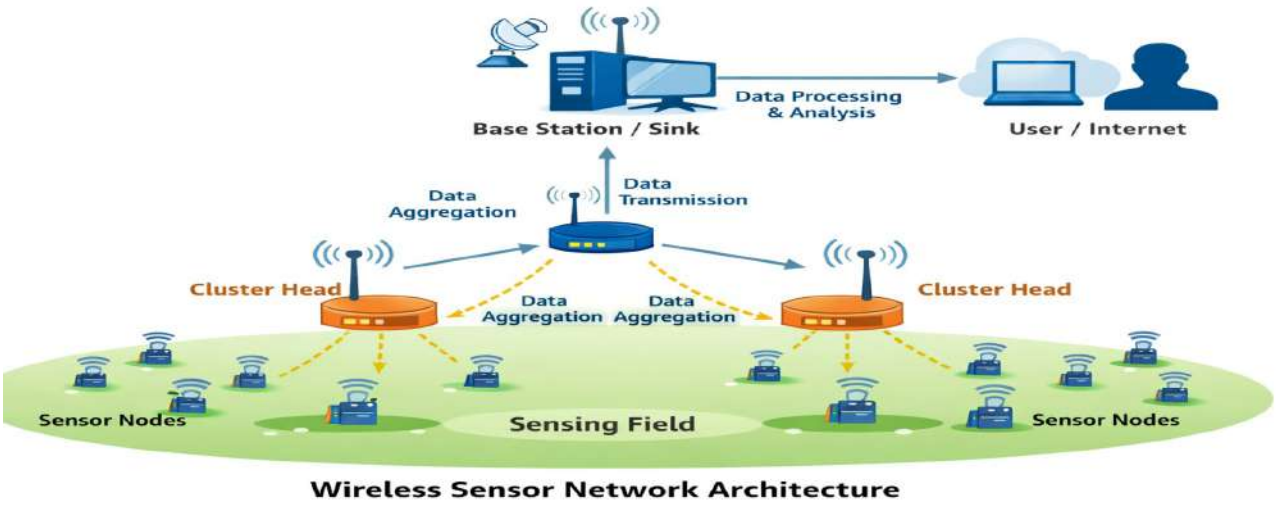

Figure 1: Basic architecture of a wireless sensor network showing sensor nodes, cluster heads, and base station communication.

2. Scope and methodology of the review

This review focuses on Intrusion Detection Systems (IDS) designed specifically for Wireless Sensor Networks (WSNs) using Artificial Intelligence (AI) and Machine Learning (ML) techniques. The review covers various machine learning approaches including supervised learning, unsupervised learning, semi-supervised learning, deep learning, and hybrid models applied to intrusion detection in WSN environments. The study mainly considers research articles published between 2018 and 2025, along with some

foundational and highly cited earlier studies to provide theoretical background and technical context for IDS in WSNs (Ashraf et al., 2020; Pinto et al., 2023).

The literature for this review was collected from major scientific databases and digital libraries, including IEEE Xplore, ScienceDirect, Springer, MDPI, PubMed, and reputable international conferences. The selection of papers was based on specific inclusion criteria to ensure the quality and relevance of the review. The main selection criteria included: (1) studies focusing on Wireless Sensor Networks or resource-constrained IoT networks, (2) studies that clearly describe machine learning or deep learning models used for intrusion detection, and (3) studies that report performance evaluation metrics such as accuracy, precision, recall, F1-score, false positive rate, energy consumption, or latency (Albulayhi et al., 2021).

The methodology of this review involves systematic analysis and classification of selected research papers based on different parameters such as detection techniques, machine learning algorithms, datasets used, feature extraction methods, and performance evaluation metrics. The selected studies were then categorized into different IDS types such as signature-based detection, anomaly-based detection, specification-based detection, and hybrid detection methods. Furthermore, machine learning approaches were classified into supervised, unsupervised, semi-supervised, deep learning, and hybrid learning models to provide a structured taxonomy of IDS techniques for WSNs (Alrajeh et al., 2013).

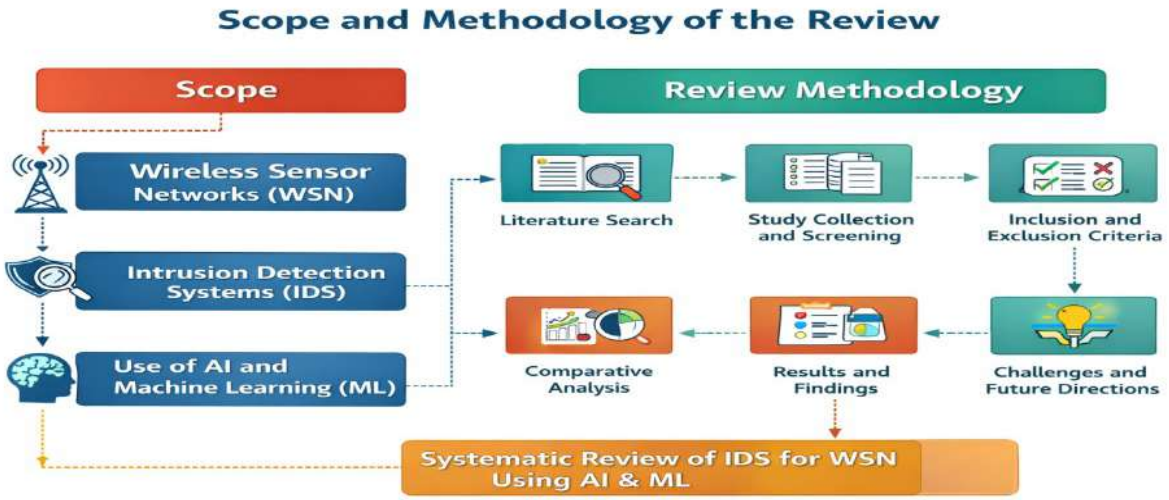

Fig 2:Scope and methodology of IDS review

3. IDS taxonomy for WSNs (AI/ML perspective)

A compact taxonomy helps compare approaches:

- **Detection principle**
  - Signature-based (pattern matching) — low false positives for known attacks, poor at zero-day.
  - Anomaly-based (statistical/ML) — detects novel attacks by modeling normal behavior (Sivagaminathan, V., 2023).
  - Specification-based — application-specific rules.
- **ML learning paradigm**
  - Supervised (SVM, Random Forest, KNN, Decision Trees) — needs labeled data.
  - Unsupervised (k-means, clustering, autoencoders, one-class SVM) — useful for unlabeled traffic.
  - Semi-supervised (positive-unlabeled learning, self-training).
  - Deep learning (CNN, RNN/LSTM, autoencoders, hybrid CNN+RNN) — learns hierarchical or temporal features (Sinha, P., Kumar, R., & Singh, A., 2025).

- Hybrid / ensemble (ML + DL, feature selection + classifier, oversampling + classifier).

❖ **Deployment model**

- Centralized (data aggregated at base station).
- Distributed/collaborative (local detection + cooperative decision).
- Hierarchical/cluster-based (cluster heads perform heavier tasks).

❖ **Resource-aware design**

- Lightweight feature sets, quantized models, edge inference, energy-aware scheduling.

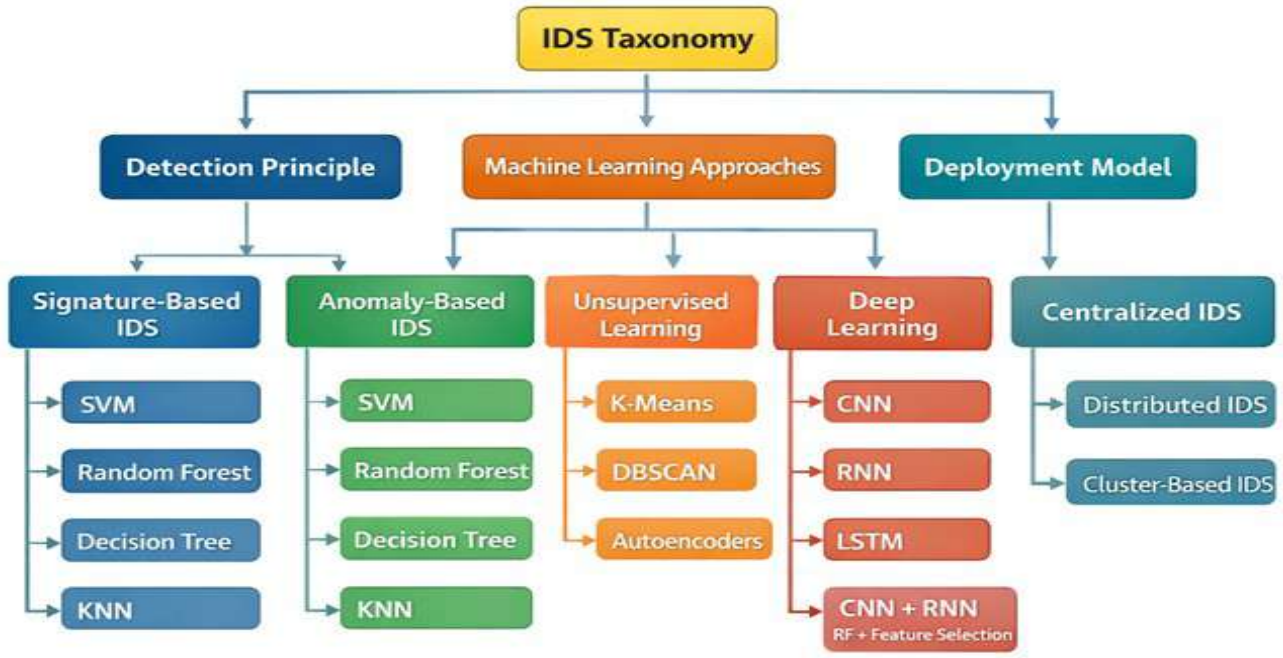

Fig 3: IDS taxonomy for wireless sensor networks

Table2: WSN Attacks vs Detection Techniques

Attack Type	Description	Detection Technique	Algorithms
DoS	Flooding network traffic	Anomaly Detection	SVM, Random Forest
Sinkhole	Fake routing information	Behavior Analysis	Decision Tree
Blackhole	Packet dropping	Traffic Monitoring	Neural Network
Wormhole	Packet tunneling	Time delay analysis	CNN
Sybil	Multiple fake identities	Identity verification	KNN

4. Datasets and benchmarks

Realistic datasets play a crucial role in evaluating the performance of Intrusion Detection Systems (IDS) in Wireless Sensor Networks (WSNs). However, the availability of publicly available WSN-specific datasets is limited, and therefore many researchers use general network intrusion detection datasets and IoT datasets as substitutes for evaluating machine learning and deep learning models in WSN environments (Hindy et al., 2020).

One of the most commonly used benchmark datasets for intrusion detection is the KDD Cup 1999 dataset and its improved version, NSL-KDD. These datasets have been widely used for evaluating traditional machine learning-based intrusion detection systems, although they are not specifically designed for Wireless Sensor

Networks (Tavallaee et al., 2009). In addition, modern intrusion detection datasets such as CIC-IDS2017, CIC-IDS2018, and CICMal2017 contain more realistic and diverse attack scenarios and are widely used in recent machine learning and deep learning-based intrusion detection research (Sharafaldin et al., 2017).

Furthermore, IoT-based datasets such as Bot-IoT, TON-IoT, and IoTID20 are also frequently used as proxy datasets for WSN intrusion detection research because Wireless Sensor Networks share similar characteristics with IoT environments, such as resource constraints, distributed architecture, and wireless communication (Hodo et al., 2016). These datasets include various attack types such as distributed denial-of-service (DDoS), botnet attacks, reconnaissance attacks, and data exfiltration attacks, which are useful for training and evaluating intrusion detection models.

In addition to general network and IoT datasets, some researchers use WSN-specific datasets such as WSN-DS and synthetic datasets that simulate WSN attacks such as blackhole attacks, sinkhole attacks, and selective forwarding attacks. However, the availability of such datasets is limited, and many recent studies generate custom WSN datasets for experimental evaluation. One of the major challenges in intrusion detection research for WSNs is the dataset realism problem and the domain gap between general network traffic datasets and actual WSN traffic patterns. Therefore, developing WSN-specific labeled datasets that include routing features, energy consumption parameters, and temporal network behavior is essential for improving the validity and reliability of intrusion detection systems in Wireless Sensor Networks.

5. Review & comparison of representative works

Several recent studies have explored the application of Machine Learning (ML) and Deep Learning (DL) techniques for Intrusion Detection Systems (IDS) in Wireless Sensor Networks (WSNs). These studies focus on improving detection accuracy, reducing false positive rates, handling class imbalance problems, and developing lightweight models suitable for resource-constrained environments.

Classical machine learning approaches and survey papers provide a comprehensive overview of intrusion detection techniques used in Internet of Things (IoT) and network security environments. These studies highlight commonly used algorithms such as Random Forest, Support Vector Machine (SVM), Decision Tree, and ensemble learning methods for anomaly detection and attack classification. These methods are widely used because of their high accuracy, low computational complexity, and suitability for structured network traffic data (Breiman, 2001; Pinto et al., 2023).

Recent studies have also focused on hybrid approaches and preprocessing techniques to improve intrusion detection performance. For example, Talukder et al. (2024) proposed a machine learning-based intrusion detection model combined with SMOTE and Tomek Link sampling techniques to address the class imbalance problem in intrusion detection datasets. Their study showed that data preprocessing and sampling techniques significantly improve detection accuracy and reduce false positive rates in WSN intrusion detection systems (Talukder et al., 2024).

Deep learning and sequence-based models have also been widely used in recent intrusion detection research. Several studies have combined Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), including Bi-LSTM models with attention mechanisms, to capture both spatial and temporal features of network traffic data. These models have shown high detection accuracy, often achieving more than 90% accuracy on benchmark datasets. However, deep learning models require high computational resources and memory, which makes them more suitable for deployment at cluster heads, gateways, or base stations rather than individual sensor nodes (Sinha et al., 2025).

In addition, cluster-based and distributed intrusion detection systems have been proposed to address the resource constraints of Wireless Sensor Networks. In these systems, lightweight detection algorithms are deployed on sensor nodes, while more complex machine learning models are deployed on cluster heads or base stations. This hierarchical detection approach helps balance detection accuracy and energy efficiency in WSN environments (Alrajeh et al., 2013).

Recent studies published between 2023 and 2025 have focused on practical improvements

such as hybrid machine learning and deep learning pipelines, feature selection techniques, data balancing methods, and hyperparameter optimization techniques such as grid search and tabu search. These approaches aim to improve detection accuracy while reducing computational complexity and improving model robustness against adversarial attacks (Pinto et al., 2023).

Table1: Comparison of AI/ML-based IDS Techniques for WSN

Author / Year	Technique Used	Dataset	Attack Type Detected	Accuracy	Key Contribution
Ashraf et al., 2020	SVM, Random Forest	NSL-KDD	DoS, Probe, U2R	92%	ML algorithms for anomaly detection in network security
Albulayhi et al., 2021	ML-based IDS survey	Multiple datasets	Multiple attacks	—	Comprehensive taxonomy of IDS techniques
Talukder et al., 2024	Random Forest + SMOTE	CIC-IDS2017	DoS, DDoS	96%	Handling class imbalance using hybrid preprocessing
Sinha et al., 2025	CNN + RNN	Bot-IoT	IoT botnet attacks	97%	Deep learning model capturing spatial & temporal features
Sivagaminathan, 2023	Decision Tree	WSN-DS	Sinkhole, Blackhole	94%	Lightweight IDS suitable for resource-constrained WSN
Pinto et al., 2023	Ensemble Learning	CIC-IDS2018	Multiple network attacks	95%	Comparative analysis of ML techniques for IDS

6. Common features and performance metrics used

Feature selection plays an important role in the performance of Intrusion Detection Systems (IDS) in Wireless Sensor Networks (WSNs). Commonly used features in WSN intrusion detection include packet-level features such as packet size and inter-arrival time, flow-level features, routing-related metrics, energy consumption or residual battery power, node-level behavior such as packet forwarding and dropping rates, and timing patterns. Effective intrusion detection systems often combine both network traffic features and node behavior features to improve detection accuracy and reliability (Fawcett, 2006).

The performance of intrusion detection models is evaluated using several standard evaluation metrics. The most commonly used metrics include accuracy, precision, recall (also known as detection rate), F1-score, false positive rate (FPR), and Area Under the ROC Curve (AUC-ROC). In the context of Wireless Sensor Networks, additional performance metrics such as energy consumption, inference latency, and memory usage should also be considered because sensor nodes have limited computational resources and battery power. However, many studies focus primarily on accuracy-based metrics and do not report energy consumption or latency metrics, which creates a gap between experimental research and real-world deployment of IDS in WSN environments (Akkaya & Younis, 2005).

7. Key challenges & open problems

Despite the significant progress in AI and ML-based intrusion detection systems for Wireless Sensor Networks, several research challenges and open problems still exist.

One of the major challenges is resource constraints, as sensor nodes have limited computational power, memory, and battery capacity. These limitations make it difficult to deploy complex machine learning and deep

learning models directly on sensor nodes. Therefore, lightweight models or hierarchical intrusion detection architectures are required to balance detection accuracy and energy efficiency **(Akkaya & Younis, 2005)**.

Another important challenge is dataset realism and labeling. There is a lack of publicly available realistic and labeled WSN datasets, and many studies rely on general network or IoT datasets that do not accurately represent real WSN traffic patterns. This creates a domain gap between training data and real-world deployment environments **(Chawla et al., 2002)**.

Class imbalance and rare attack detection is also a significant issue in intrusion detection datasets because attack traffic is usually much smaller compared to normal traffic. Techniques such as Synthetic Minority Over-sampling Technique (SMOTE), cost-sensitive learning, and one-class classification methods are commonly used to address this issue **(Wang et al., 2006)**.

Distributed detection and collaborative learning is another open research problem in Wireless Sensor Networks. Centralized intrusion detection systems can create communication overhead and single points of failure, while distributed and federated learning approaches are still under development and require efficient communication and energy management strategies.

Explainability and trust in deep learning models is also an important concern, especially in critical applications such as healthcare and military monitoring systems. Many deep learning models act as black-box models and do not provide clear explanations for their decisions, which reduces trust in the system **(Gunning, 2017)**.

Finally, adversarial robustness is an emerging research challenge where attackers can manipulate network traffic patterns to evade machine learning-based intrusion detection systems. Therefore, adversarial training and robustness evaluation methods are necessary to improve the security and reliability of IDS models **(Papernot et al., 2016)**.

8. Recommendations & future directions

Future research on Intrusion Detection Systems (IDS) in Wireless Sensor Networks (WSNs) should focus on developing realistic and efficient solutions that can be deployed in resource-constrained environments. One of the key research directions is the development of WSN-specific datasets and benchmarks. Researchers should create and publish labeled WSN datasets that include routing behavior, energy consumption features, and realistic attack scenarios such as sinkhole, wormhole, blackhole, and selective forwarding attacks. The availability of realistic datasets will significantly improve the reliability and validity of intrusion detection research **(Hodo et al., 2016)**.

Another important research direction is the development of lightweight deep learning models and model compression techniques. Techniques such as pruning, quantization, and knowledge distillation can be used to reduce the computational complexity and memory requirements of deep learning models so that they can be deployed on cluster heads or edge devices in Wireless Sensor Networks **(Han et al., 2016)**.

Federated learning and split learning are also promising research directions for distributed intrusion detection in WSNs. These approaches allow multiple sensor nodes to collaboratively train machine learning models without sharing raw data, which improves privacy and reduces communication overhead. However, more research is needed to evaluate communication cost, energy consumption, and model performance trade-offs in federated learning-based IDS systems **(McMahan et al., 2017)**.

Explainable Artificial Intelligence (XAI) is another important research direction for intrusion detection systems. Many deep learning-based IDS models act as black-box models, making it difficult for network administrators to understand why a particular activity is classified as an attack. Therefore, explainable machine learning techniques should be developed to provide interpretable intrusion detection results and improve user trust in IDS systems **(Gunning, 2017)**.

Furthermore, robustness evaluation is necessary to ensure that intrusion detection models are resistant to adversarial attacks and evasion techniques. Researchers should develop standardized adversarial testing frameworks to evaluate the robustness of IDS models under different attack scenarios **(Papernot et al., 2016)**.

Finally, future research should focus on standard evaluation protocols for IDS in Wireless Sensor Networks. In addition to accuracy,

researchers should report energy consumption, inference latency, memory usage, dataset description, and cross-dataset performance to ensure that IDS models are suitable for real-world deployment environments **(Hodo et al., 2016)**.

9. Minimal reproducible evaluation template

To ensure reproducibility and reliability of machine learning and deep learning-based intrusion detection systems for Wireless Sensor Networks, researchers should follow a standardized evaluation methodology.

First, researchers should clearly describe the dataset used in the study, including data collection methods, feature definitions, and train-test split ratios. If possible, researchers should make their datasets and source code publicly available to support reproducible research **(Ashraf et al., 2020)**.

Second, the preprocessing steps used in the intrusion detection model should be clearly explained. This includes data normalization, handling missing values, feature selection techniques, and data balancing methods such as Synthetic Minority Over-sampling Technique (SMOTE) and Tomek Link sampling **(Albulayhi et al., 2021)**.

Third, researchers should evaluate multiple models, including baseline classical machine learning models such as Random Forest (RF) and Support Vector Machine (SVM), unsupervised learning models such as one-class SVM and autoencoders, and the proposed model such as a lightweight deep learning or hybrid model.

Fourth, multiple evaluation metrics should be reported, including accuracy, precision, recall, F1-score, false positive rate (FPR), and Area Under the ROC Curve (AUC). In addition, WSN-specific performance metrics such as energy consumption, inference latency, memory usage, and confusion matrix should also be included to evaluate the practical applicability of the IDS model.

Finally, ablation studies should be conducted to analyze the effect of feature selection, oversampling techniques, and model complexity on detection performance. Robustness evaluation should also be performed by testing the model on noisy datasets, adversarial datasets, or cross-dataset evaluation scenarios to measure the generalization capability of the intrusion detection system.

10. Conclusion

AI/ML have matured into practical tools for WSN intrusion detection, achieving high detection rates in controlled studies. However, realistic WSN deployment requires balancing detection performance with strict resource constraints, dataset realism, explainability, and adversarial robustness. Future work should prioritize WSN-specific benchmarks, lightweight/federated learning, XAI methods, and standardized energy-aware evaluation.

References

Ashraf, J., Keshk, M., Moustafa, N., Abdel-Basset, M., Khurshid, H., Bakhshi, A. D., & Mostafa, R. R. (2020). A review of intrusion detection systems using machine learning and deep learning in internet of things: Challenges, solutions and future directions. *Electronics, 9*(7), 1177. https://doi.org/10.3390/electronics9071177

Pinto, A., Garcia, S., & Rodrigues, J. J. P. C. (2023). A survey on machine learning-based intrusion detection systems. *Journal of Network and Computer Applications, 214*, 103605. https://doi.org/10.1016/j.jnca.2023.103605

Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: A review. *International Journal of Distributed Sensor Networks, 9*(5). https://doi.org/10.1155/2013/167575

Albulayhi, K., Abu Al-Haija, Q., Alsuhibany, S., Alahmadi, A., & Alharbi, A. (2021). IoT intrusion detection taxonomy, reference architecture, and analyses. *Sensors, 21*(2), 643. https://doi.org/10.3390/s21020643

Talukder, M., Islam, M. S., Rahman, M. M., & Hossain, M. A. (2024). MLSTL-WSN: Machine learning-based intrusion detection in wireless sensor networks. *IEEE Access*.

Sivagaminathan, V. (2023). Intrusion detection system for wireless sensor networks using machine learning. *International Journal of Communication Systems*.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2017). Toward generating a new intrusion detection dataset and intrusion traffic

characterization (CIC-IDS2017). In *Proceedings of the International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0006639801080116

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 dataset (NSL-KDD). In *Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications*. https://doi.org/10.1109/CISDA.2009.5356528

Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32. https://doi.org/10.1023/A:1010933404324

Sinha, P., Kumar, R., & Singh, A. (2025). CNN-RNN based intrusion detection system for cyber security. *IEEE Access*.

Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEE Access, 8*, 104650–104675. https://doi.org/10.1109/ACCESS.2020.2980950

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research, 16*, 321–357. https://doi.org/10.1613/jair.953

Fawcett, T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters, 27*(8), 861–874. https://doi.org/10.1016/j.patrec.2005.10.010

Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks, 3*(3), 325–349. https://doi.org/10.1016/j.adhoc.2003.09.010

Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials, 8*(2), 2–23. https://doi.org/10.1109/COMST.2006.315852

Gunning, D. (2017). Explainable artificial intelligence (XAI). *Defense Advanced Research Projects Agency (DARPA)*. https://doi.org/10.48550/arXiv.1702.08608

Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. (2016). Practical black-box attacks against machine learning. In *Proceedings of the ACM Asia Conference on Computer and Communications Security*. https://doi.org/10.1145/2976749.2978392

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the International Conference on Artificial Intelligence and Statistics (AISTATS)*. https://doi.org/10.48550/arXiv.1602.05629

Han, S., Mao, H., & Dally, W. J. (2016). Deep compression: Compressing deep neural networks with pruning, trained quantization and Huffman coding. In *International Conference on Learning Representations (ICLR)*. https://doi.org/10.48550/arXiv.1510.00149

Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., & Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. In *IEEE International Symposium on Networks, Computers and Communications*. https://doi.org/10.1109/SNCC.2016.7746074

Cite this article as: Prashant Kumar et al., (2026). Intrusion Detection Systems in Wireless Sensor Networks Using AI & ML. International Journal of Emerging Knowledge Studies. 5(3), pp. 454–462. https://doi.org/10.70333/ijeks-05-03-017