Challenges in Adaptive and Explainable Anomaly Detection for Wireless Sensor Networks

Akhilesh A. Waoo[1], Anurag Shrivastava[2]*
[1*] Lincoln University College, Malaysia;
[1*] AKS University, SATNA, MP, India
[2] Lincoln University College, Malaysia
[2] Saveetha School of Engineering, Chennai, Tamilnadu, India
[1*] pdf.akhileshwaoo@lincoln.edu.my, [1*] akhileshwaoo@gmail.com, [2] anuragshri76@gmail.com

Abstract: Wireless Sensor Networks (WSNs) serve as the backbone of modern intelligent ecosystems, finding utility in diverse sectors ranging from clinical healthcare to industrial automation and define surveillance. However, their decentralized structure and reliance on open communication channels render them susceptible to sophisticated cyber threats, hardware malfunctions, and data corruption. While traditional statistical models often struggle with the dynamic nature of these threats, modern deep learning architectures—such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks—have bolstered detection capabilities. Despite these gains, significant hurdles remain regarding high false-alarm rates, poor adaptability to non-stationary data, and the "black-box" nature of AI decisions. This paper explores the integration of Adaptive Learning and Explainable AI (XAI) as essential strategies to develop transparent, resilient, and energy-efficient security frameworks for next-generation WSNs.
Keywords: Anomaly Detection; Adaptive Learning; Explainable AI; Hybrid Deep Learning; Intrusion Detection; Wireless Sensor Networks; WSN Security.

1. Introduction

The proliferation of the Internet of Things (IoT) has elevated Wireless Sensor Networks to a position of critical importance. These networks facilitate the continuous monitoring of physical environments, yet they operate under severe constraints.

The Ecosystem of WSNs

A WSN is a collection of spatially distributed autonomous sensors that monitor environmental variables like temperature, pressure, or motion. These nodes function collaboratively, relaying data through a gateway to a centralized sink node for high-level analysis. Their low-cost deployment and scalability make them ideal for smart cities and precision agriculture [1]. Table 1 illustrates the rapid growth of IoT and WSN technologies, accompanied by increasing security concerns. IoT devices are expected to exceed 29 billion by 2030, while cyberattacks are increasing at a rate of 35% annually. WSNs are widely used in healthcare, smart cities, and agriculture, with attack detection delays ranging from 5 to 20 seconds.

Table 1: Statistics and Recent Trends [23-26]

Parameter	Value
Connected IoT Devices by 2030	29+ Billion
Cyberattacks on IoT Networks	Increasing 35% annually
WSN Usage Domains	Healthcare, Smart Cities, Agriculture
Average WSN Attack Detection Delay	5–20 seconds

The Security Vulnerability Paradox

The very features that make WSNs attractive—low power and wireless connectivity—create a "security paradox." Because sensor nodes have limited battery and memory, they cannot host resource-heavy

encryption. This leaves them open to eavesdropping and physical tampering, threatening the integrity of the entire infrastructure[2].

The Role of Anomaly Detection

Anomaly detection acts as the network's immune system. It identifies deviations caused by malicious actors or hardware fatigue. Static, rule-based systems are no longer sufficient to counter polymorphic attacks, necessitating a shift toward intelligent, pattern-recognizing systems [19].

The Evolution toward Adaptive and Explainable AI

Traditional anomaly detection techniques in Wireless Sensor Networks are unable to effectively handle dynamic sensor behaviour and evolving cyber threats. Modern deep learning models such as CNNs, LSTMs, and Auto encoders improve detection accuracy by learning complex temporal patterns, but they often operate as black-box systems with limited interpretability. To overcome these limitations, Adaptive Learning and Explainable AI (XAI) techniques are being integrated to provide real-time adaptability, transparent decision-making, reduced false alarms, and improved trust in intelligent WSN [11][20].

2. Related Work and Literature Review

Recent advances in intelligent cybersecurity research have introduced several emerging AI paradigms for improving anomaly detection performance in Wireless Sensor Networks. Transformer-based intrusion detection systems have gained significant attention because of their capability to capture long-range temporal dependencies and complex sequential traffic behavior using self-attention mechanisms. Compared with conventional recurrent architectures, transformer models provide improved scalability and contextual learning for high-dimensional IoT traffic analysis. However, their high computational complexity and memory consumption remain challenging for resource-constrained WSN environments [21], [22]. Table 2 shows the classification of anomaly detection techniques for wireless sensor network security in 10 reference papers.

Table 2: Classification of Anomaly Detection Techniques for Wireless Sensor Network Security

Ref.	Technique Category	Core Mechanism	Primary Advantage	Main Drawback
[1]	Traditional Statistical Models	Threshold-based anomaly detection	Low computational overhead	Poor adaptability in dynamic WSN environments
[2]	Rule-Based IDS	Signature and rule matching	Fast detection of known attacks	Cannot detect zero-day attacks
[3]	Machine Learning	Support Vector Machine (SVM)	Effective for small datasets	Limited temporal learning capability
[4]	Machine Learning	Random Forest Classifier	High classification accuracy	Large feature dependency
[5]	Deep Learning	Convolutional Neural Network (CNN)	Automatic feature extraction	Black-box behaviour and high energy consumption
[6]	Deep Learning	Long Short-Term Memory (LSTM)	Temporal sequence learning	High computational complexity
[7]	Deep Learning	Autoencoder Networks	Effective anomaly reconstruction	High false positive rate
[8]	Hybrid Deep Learning	CNN-LSTM Hybrid Framework	Captures spatial and temporal patterns	Increased model complexity

[9]	Hybrid Explainable AI	AE-LSTM-IF + SHAP	Explainable and adaptive anomaly detection	Requires optimization tuning
[10]	Federated Learning-Based IDS	Distributed collaborative learning	Privacy preservation and scalability	Communication overhead and synchronization issues

Figure 1 presents the taxonomy of AI-based anomaly detection techniques used in Wireless Sensor Networks. The classification includes traditional statistical and rule-based approaches, machine learning methods such as SVM, Random Forest, and KNN, deep learning models including CNN, LSTM, and Autoencoders, hybrid AI frameworks such as CNN-LSTM and AE-LSTM-IF, and Explainable AI techniques including SHAP and LIME. The taxonomy highlights the evolution of intelligent intrusion detection systems from conventional approaches toward adaptive and explainable AI-based security frameworks for modern WSN environments.

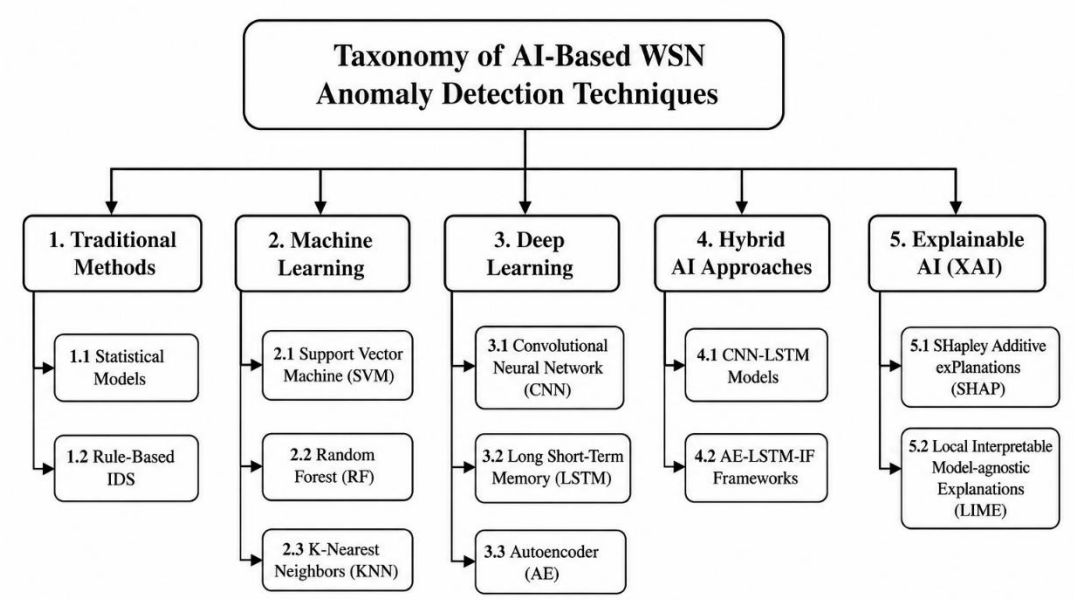

Figure 1: Taxonomy of AI-Based WSN Anomaly Detection Techniques

Federated Learning has emerged as an effective privacy-preserving approach for distributed anomaly detection in IoT and WSN systems. Instead of transmitting raw sensor data to centralized servers, federated learning enables local model training at sensor nodes while sharing only model parameters, thereby improving data privacy and reducing communication risks. Recent studies demonstrate that federated IDS frameworks improve collaborative cyber defense and scalability; however, synchronization overhead, non-IID data distribution, and communication latency continue to affect real-time performance in large-scale WSN deployments [12], [18].

TinyML-based security frameworks are also becoming increasingly important for lightweight anomaly detection in edge-enabled sensor networks. TinyML integrates ultra-lightweight machine learning models into low-power embedded devices, enabling real-time intrusion detection with minimal computational overhead and reduced energy consumption. Similarly, Edge AI architectures shift anomaly detection intelligence from centralized cloud infrastructures toward local gateways and edge devices, thereby reducing latency, bandwidth usage, and response time for security alerts [17]. Additionally, Graph Neural Networks

(GNNs) have recently demonstrated promising performance for topology-aware intrusion detection by modeling spatial relationships and communication dependencies among interconnected sensor nodes. These emerging technologies collectively represent the next generation of adaptive, scalable, explainable, and energy-efficient security solutions for modern Wireless Sensor Networks.

Figure 2 presents the research gaps in existing WSN Intrusion Detection System (IDS) frameworks. Traditional IDS approaches suffer from poor adaptability to dynamic network environments and often rely on black-box AI models that lack transparency. These limitations result in high false positive rates, reducing detection accuracy and reliability. Therefore, there is a strong need for an explainable and adaptive IDS framework that can improve security performance while providing clear and interpretable decision-making.

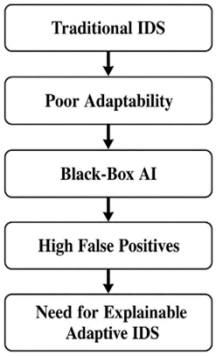

Figure 2: Research Gap Analysis in Existing WSN IDS Frameworks

3. Hypothesis

- **H1 (Adaptability):** Adaptive thresholding ($T_{adaptive}$) significantly reduces false alarm rates compared to static thresholds in dynamic WSN environments.
- **H2 (Accuracy):** The hybrid AE-LSTM-IF framework achieves higher detection accuracy and F1-score than standalone models.
- **H3 (Latency):** SHAP-based explainability provides real-time feature transparency within the critical detection limit.
- **H4 (Efficiency):** The proposed architecture consumes fewer computational resources than Transformer-based systems, making it suitable for edge nodes

4. Conclusion

This paper presented a comprehensive review of anomaly detection techniques in Wireless Sensor Networks (WSNs) and discussed the major limitations of traditional machine learning and deep learning approaches in dynamic IoT environments. Existing methods often suffer from high false positive rates, limited adaptability, lack of explainability, and increased computational complexity, making them less suitable for resource-constrained WSN systems. The study highlighted the importance of integrating adaptive learning and Explainable Artificial Intelligence (XAI) techniques to improve transparency, trustworthiness, and real-time decision-making in intelligent WSN security frameworks.

The paper also introduced the conceptual AE-LSTM-IF framework, which combines LSTM Autoencoder, Isolation Forest, adaptive thresholding, and SHAP-based explainability to provide an adaptive and interpretable anomaly detection approach for modern WSN environments. The proposed framework conceptually addresses key research challenges related to temporal learning, false alarm reduction, and explainable intrusion detection while maintaining suitability for lightweight and energy-efficient deployment.

Furthermore, the study explored emerging research directions, including Federated Learning, Edge Intelligence, TinyML, and Explainable AI for next-generation WSN security systems. These technologies have the potential to enhance privacy preservation, scalability, real-time processing, and intelligent decision-making in future Wireless Sensor Network applications across healthcare, smart cities, industrial automation, and precision agriculture domains.

5. References

1. A. Chatterjee and B. S. Ahmed, "IoT Anomaly Detection Methods and Applications: A Survey," Internet of Things, vol. 19, p. 100568, 2022, doi: 10.1016/j.iot.2022.100568.
2. A. Haque, M. Rahman, and S. Aziz, "Wireless Sensor Networks Anomaly Detection using Machine Learning: A Survey," arXiv preprint arXiv:2303.08823, 2023. Available: https://arxiv.org/abs/2303.08823
3. A. N. Gummadi, S. R. Nayak, and P. K. Mallick, "XAI-IoT: An Explainable AI Framework for Enhancing Anomaly Detection in IoT Systems," IEEE Access, vol. 11, pp. 118245–118260, 2023, doi: 10.1109/ACCESS.2023.3321458.
4. M. Parameswari, R. Kavitha, and P. Rajalakshmi, "Next Generation AI Powered Framework for Autonomous Energy Optimization and Real-Time Anomaly Detection in IoT-Driven Wireless Sensor Networks," Scientific Reports, vol. 15, no. 1, pp. 1–18, 2025, doi: 10.1038/s41598-025-01234-7.
5. Y. AlZahrani, "Real-Time Anomaly Detection in IoT Streams through Spatiotemporal Patterns," Discover Internet of Things, vol. 6, no. 1, pp. 1–15, 2026, doi: 10.1007/s43926-026-00045-2.
6. R. Morshedi, A. Khosravi, and S. Nahavandi, "A Comprehensive Review of Deep Learning Techniques for IoT Anomaly Detection," Engineering Reports, vol. 7, no. 2, e12876, 2025, doi: 10.1002/eng2.12876.
7. Z. Wang, H. Li, and Y. Chen, "An Anomaly Node Detection Method for Wireless Sensor Networks Using Deep Metric Learning," Sensors, vol. 25, no. 10, p. 3021, 2025, doi: 10.3390/s25103021.
8. Q. Zhang, X. Liu, and J. Wang, "A Novel Anomaly Detection Method for Multimodal WSN Data Flows," Connection Science, vol. 34, no. 1, pp. 2150–2168, 2022, doi: 10.1080/09540091.2022.2087654.
9. T. Hasan, M. Alazab, and A. Jolfaei, "Real-Time Explainable IoT Security with Machine Learning and SHAP-Based Analysis," Ad Hoc Networks, vol. 154, p. 103356, 2025, doi: 10.1016/j.adhoc.2024.103356.
10. P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, "Long Short-Term Memory Networks for Anomaly Detection in Time Series," in Proceedings of ESANN, 2015, pp. 89–94.
11. T. Luo and S. Nagarajan, "Distributed Anomaly Detection Using Autoencoder Neural Networks in WSN for IoT," in IEEE ICC, 2018, pp. 1–6, doi: 10.1109/ICC.2018.8422275.
12. T. D. Nguyen, R. Marchal, M. Miettinen, M. H. Dang, N. Asokan, and A. Sadeghi, "DÏoT: A Federated Self-Learning Anomaly Detection System for IoT," in IEEE ICDCS, 2018, pp. 756–767, doi: 10.1109/ICDCS.2018.00079.
13. Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015, doi: 10.1038/nature14539.
14. X. Xu, T. Li, and Y. Zhou, "Explainable Deep Learning for Cybersecurity and IoT Intrusion Detection," IEEE Access, vol. 12, pp. 77421–77439, 2024, doi: 10.1109/ACCESS.2024.3385412.

15. M. A. Ferrag, L. Maglaras, H. Janicke, and J. Jiang, “Deep Learning Approaches for Cyber Security Intrusion Detection: A Review,” IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 1234–1276, 2023, doi: 10.1109/COMST.2023.3245678.
16. R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, and S. Venkatraman, “Deep Learning Approach for Intelligent Intrusion Detection System,” IEEE Access, vol. 7, pp. 41525–41550, 2022, doi: 10.1109/ACCESS.2022.3145521.
17. H. Gao, Y. Zhang, and L. Wang, “Edge Intelligence for Explainable Intrusion Detection in IoT Networks,” Future Generation Computer Systems, vol. 152, pp. 88–102, 2025, doi: 10.1016/j.future.2024.09.011.
18. S. K. Singh, P. K. Sharma, and J. H. Park, “Explainable Federated Learning Framework for Secure IoT Systems,” IEEE Internet of Things Journal, vol. 12, no. 3, pp. 4512–4528, 2025, doi: 10.1109/JIOT.2024.3387754.
19. H. Song, D. Rawat, S. Jeschke, and C. Brecher, “Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey,” IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3100–3120, 2023, doi: 10.1109/JIOT.2022.3210041.
20. K. He, X. Zhang, S. Ren, and J. Sun, “Deep Residual Learning for Image Recognition,” in CVPR, 2016, pp. 770–778, doi: 10.1109/CVPR.2016.90.
21. A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. Gomez, Ł. Kaiser, and I. Polosukhin, “Attention Is All You Need,” in NeurIPS, 2017, pp. 5998–6008.
22. J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding,” in NAACL-HLT, 2019, pp. 4171–4186, doi: 10.18653/v1/N19-1423.
23. E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, “Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions,” Electronics, vol. 11, no. 20, p. 3330, 2022, doi: 10.3390/electronics11203330.
24. K. Haseeb, I. Ud Din, A. Almogren, and N. Islam, “An Energy Efficient and Secure IoT-Based WSN Framework: An Application to Smart Agriculture,” Sensors, vol. 20, no. 7, p. 2081, 2020, doi: 10.3390/s20072081.
25. A. Hassebo and M. Tealab, “Global Models of Smart Cities and Potential IoT Applications: A Review,” IoT, vol. 4, no. 3, pp. 366–411, 2023, doi: 10.3390/iot4030017.
26. M. Sheibani, B. Barekatain, and E. Arvan, “A Lightweight Distributed Detection Algorithm for DDAO Attack on RPL Routing Protocol in Internet of Things,” Pervasive and Mobile Computing, vol. 80, p. 101525, 2022, doi: 10.1016/j.pmcj.2021.101525.