International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Wireless Sensor Networks Under Cyber Attacks: Trends, Defences, and Review Insights

Priya[1], Prof. Raghu Knojia[2]

[1]MCA Student, Department of Computer Science, Global Group of Institutes
[2]Assistant Professor, Department of Computer Science, Global Group of institutes

ABSTRACT
Wireless Sensor Networks (WSNs) have become an essential part of modern intelligent systems such as smart healthcare, home automation, traffic monitoring, and environmental sensing. Since sensor nodes operate with limited battery power, storage, and processing capability, they are highly vulnerable to different security attacks. Although several methods including encryption, secure routing, authentication, and key management have been proposed ,none of them alone can fully safeguard of the network. This paper reviews the major security challenges in WSNs and examines commonly reported attacks such as Sybil and Sinkhole attacks. It also provides an overview of intrusion detection techniques used in recent research and compares their performance in terms of accuracy, energy consumption, and real-time capability. Finally, the study highlights open issues in existing approaches and suggests future research directions for designing lightweight and more efficient security solutions for WSNs.

Keyword: wireless sensor network (WSN), security problems, intrusion detection, Attacks in WSN, Cyberattacks.

Introduction

Wireless Sensor Networks (WSNs) are formed by a large number of lightweight sensor nodes that work together to gather information from their surroundings. These networks support various modern applications, including healthcare monitoring, smart homes, traffic control, environmental observation, and industrial automation. Because sensor nodes have limited battery power, small memory, and low processing capability, they are more vulnerable to security threats and operational failures.

WSNs are exposed to multiple cyber-attacks such as Sybil, Sinkhole, Wormhole, and Blackhole attacks. Although several security measures—such as authentication, encryption, secure routing, and key management—have been introduced, these methods still do not provide complete protection. Most existing approaches struggle with constraints like high energy usage, low detection accuracy, and poor real-time performance, especially in dynamic and resource-limited environments.

With the rapid growth of technologies like IoT, cloud computing, artificial intelligence, and 5G, WSNs have become more widely used, but their risk of attack has also increased. Sensitive information, such as health records, industrial data, and traffic updates, is transmitted continuously, so any security breach can lead to data manipulation, system disruption, or unauthorized access. Additionally, harsh environmental conditions, node failures, and routing manipulation make securing WSNs even more challenging.

For these reasons, a detailed review of existing attacks, intrusion detection approaches, and defence techniques is essential. Such a study can help identify the limitations of current solutions and highlight future research needs for building more reliable, energy-efficient, and secure WSN frameworks.

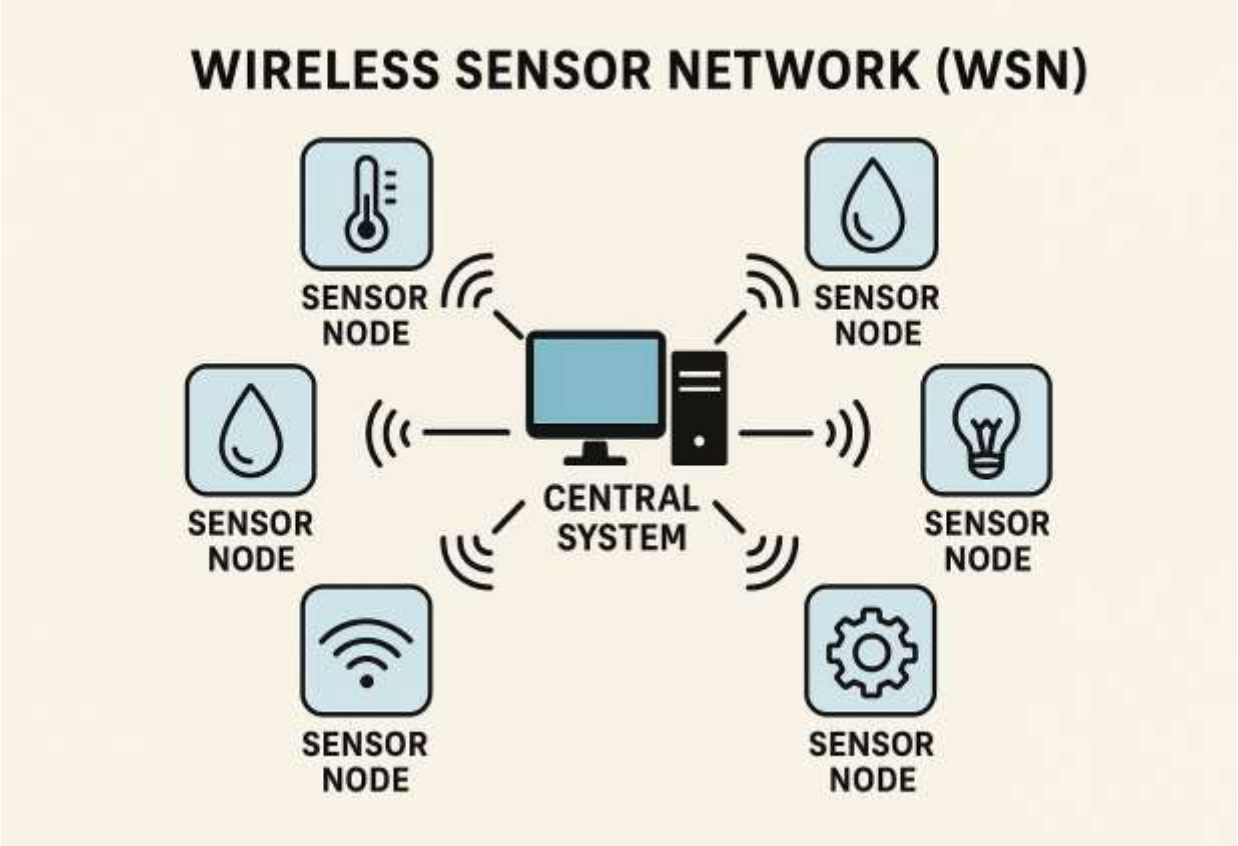


Figure1. wireless sensors network

Background of Wireless sensors networks(WSNs)

Wireless Sensor Networks (WSNs) consist of many small sensor nodes that sense environmental data, perform simple processing, all the data gathered by the sensor nodes is sent to a central point, which is known as the base station or sink. Because these nodes operate on limited battery power and use wireless communication, they are designed to be lightweight and resource-constrained. Today, WSNs play a major role in smart healthcare, environmental monitoring, industrial automation, smart cities, home automation, and traffic management.

Although WSNs have become widely used in recent years, their origin dates back several decades. Early sensing systems were developed for military applications; for instance, underwater sensor networks in the 1950s were used to detect submarine movement. These early systems were bulky and expensive compared to modern wireless sensors. A significant development occurred in the 1980s when DARPA launched the Distributed Sensor Network (DSN) program, which promoted research on small, interconnected sensing devices.

Literature Review

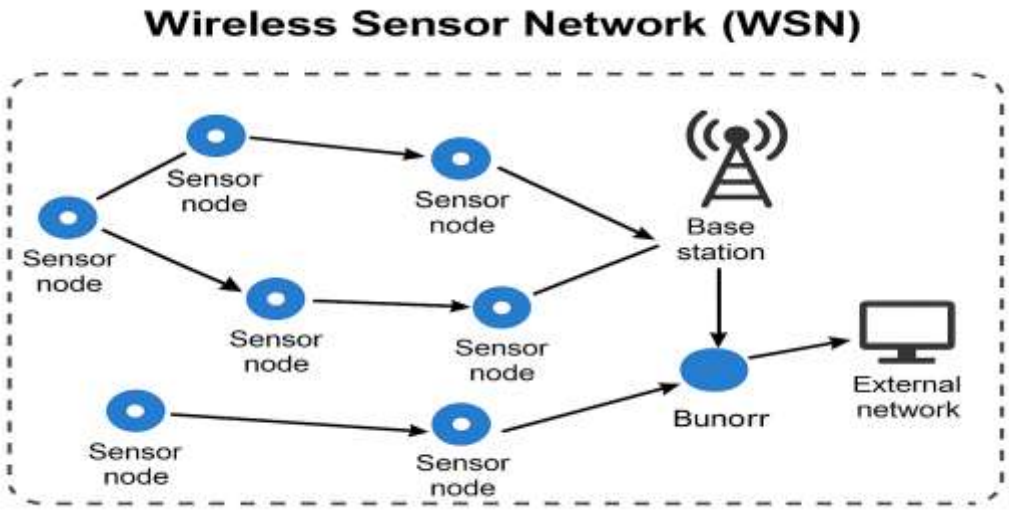
Recent studies on Wireless Sensor Networks (WSNs) show that these networks are becoming more exposed to cyber attacks as they are used in sensitive environments like health monitoring, defence, and

industrial systems .Earlier research mostly explained the basic functioning of sensor nodes and how data moves within the network. But with time, many researchers started pointing out that the small battery size, limited processing ability, and open wireless medium make WSNs much easier for attackers to target compared to traditional networks.

More recent investigations have shifted toward understanding how attackers exploit routing protocols and how intrusion detection can be improved for such lightweight devices. Some studies propose machine-learning-based defence mechanisms, but many note that these approaches require higher computation, which is difficult for sensor nodes. Other researchers suggest trust-based and anomaly-detection frameworks; however, they often face issues like slow detection or high false alarms. Overall, literature indicates a clear trend.

Architecture of WSNs

several sensor nodes are spread across a monitoring area. Each node collects information from its nearby environment and then forwards it to other nodes in sequence, forming a multi-hop path. The arrows in the figure simply show how the sensed data moves from one node to another until it finally reaches the base station. The base station works as the central point where all data is gathered. In this diagram, the received information is further sent to a sink or aggregator node , which then transfers the processed data to an external network such as a server or user system. Overall, the architecture captures the essential components of a WSN sensor nodes, "The figure shows a simple Wireless Sensor Network setup. several sensor nodes collect data and pass it forward until it reaches a central unit called the Base Station, which then connects the network to outside systems."



Application of WSNs

a) Healthcare

- Remote patient monitoring via wearable sensors.
- Tracking vital signs and generating alerts for emergencies.
- Sensitive to attacks because privacy and data integrity are critical.

b) Military

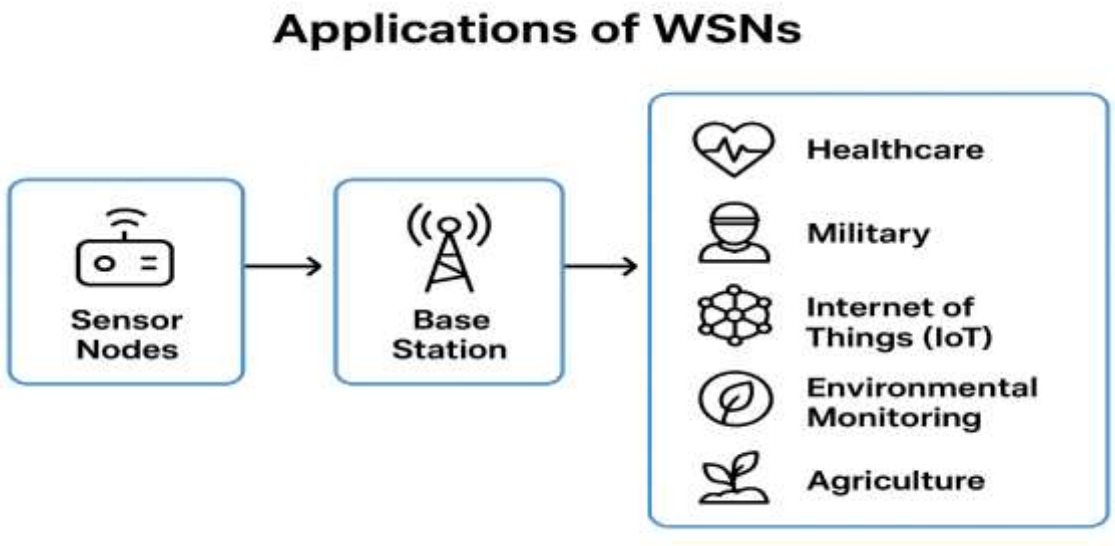
- Battlefield surveillance, target tracking, coordination of drones or robots.
- Security is crucial because data tampering or node compromise can cause severe damage.

c) Internet of Things (IoT)

- Smart homes (energy, security, temperature control).
- Smart cities (traffic, pollution, environment monitoring).
- Industrial IoT (machine monitoring, predictive maintenance).
- Attacks can disrupt services or leak sensitive data.

d) Environmental Monitoring

- Detecting floods, forest fires, soil conditions.
- Attacks can prevent timely alerts, causing losses.



Security threats in WSN'

1. Sybil Attack

- What happens: A bad node pretends to be many nodes at the same time.
- How IDS finds it: It checks if the same node ID is appearing in multiple places, or if the signal/location doesn't match the identity.

2. Sinkhole Attack

- What happens: A malicious node tells everyone it has the best path to the base station, so all data goes through it. Then it can drop or misuse the data.
- How IDS finds it: IDS notices if one node is suddenly getting too much traffic or acting suspicious in routing.

3. Blackhole Attack

- What happens: A node says it has the shortest path to the base station, but instead of sending the data, it keeps or drops it.
- How IDS finds it: IDS monitors nodes to see if packets are being delivered properly. If a node keeps losing packets, it's suspicious.

4. Wormhole Attack

- What happens: Two bad nodes create a "tunnel" to send data far away quickly, confusing the network.
- How IDS finds it: IDS checks if some routes are too short or too fast compared to normal paths.

5. Hello Flood Attack

- What happens: An attacker floods nodes with "Hello" messages to trick them into thinking it's a neighbour.
- How IDS finds it: IDS checks if nodes are really reachable in two-way communication. Too many hellos from one node is a red flag.

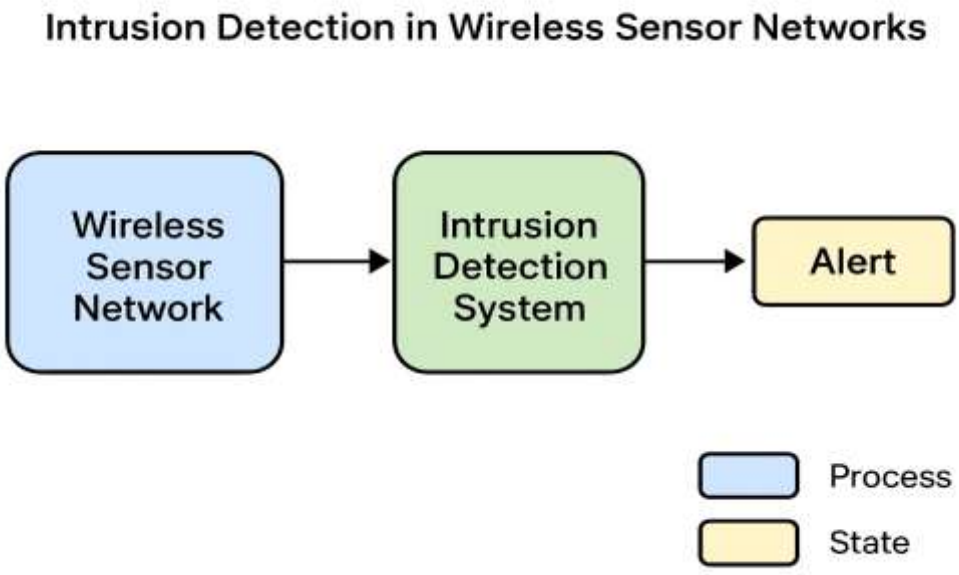
6. Denial of Service (DoS) Attack

- What happens: The attacker tries to drain the network's energy or resources, making it unusable.
- How IDS finds it: IDS watches for high traffic or unusual energy/battery use to spot problem nodes.

Intrusion detection system (IDS) in WSN

Intrusion Detection simply means watching a network to catch anything suspicious or harmful**.** In a wireless sensor network (WSNs), many small sensor node communicate with each other. Because these nodes are weak and work in an open wireless environment, attackers can easily target them. An Intrusion Detection System (IDS) works like a security guard for the network. It keeps an eye on all the activities happening inside the network.

An Intrusion Detection System (IDS) helps the network stay secure by constantly observing how nodes behave, how data moves, and whether any activity looks suspicious. Whenever the IDS notices something that does not match normal behaviour—such as a node sending strange messages, dropping data, or pretending to be another node—it raises an alert.



Why IDS Is Required in WSN

Wireless Sensor Networks face many security challenges because they operate in open environments and contain resource-limited nodes. Traditional security methods alone are not enough, so an IDS becomes necessary to detect abnormal behaviour and identify attacks early. It works as an additional protection layer to keep the network reliable and safe.

Key Reasons Why IDS is Important in WSN

- Open wireless medium makes WSN easy to attack.

- Nodes are physically unprotected, so attackers can capture or damage them.
- Limited resources (battery, memory) prevent strong cryptographic security.
- IDS detects attacks like blackhole, wormhole, Sybil, DoS, etc.
- Ensures data accuracy by identifying malicious changes.
- Prevents network failure or false data injection.
- Improves trust and reliability in sensitive applications (healthcare, military, IoT).
- Provides real-time monitoring and quick response to suspicious behaviour.

Acts as a second line of defence when basic security fails.

Types of intrusion detection (IDS)

In Wireless Sensor Networks, different intrusion detection approaches are used depending on how the network observes and analyse unwanted activities. The main types are described below:

Signature based IDS: This type of IDS detects attacks by comparing network behaviour with a database of previously known attack signatures. If an action matches a stored signature, it is classified as malicious. Signature-based IDS is fast and highly accurate for identifying known threats; however, it cannot detect new, unknown, or modified attacks that are not already in its signature database.

Anomaly-Based IDS: An anomaly-based IDS learns the normal behaviour of sensor nodes, including their traffic rates, energy consumption, and communication patterns. Whenever a node behaves differently from these learned patterns, the system marks it as suspicious. This approach can detect new or previously unknown attacks, but it may also generate false alarms because unusual behaviour is not always malicious.

Distributed IDS

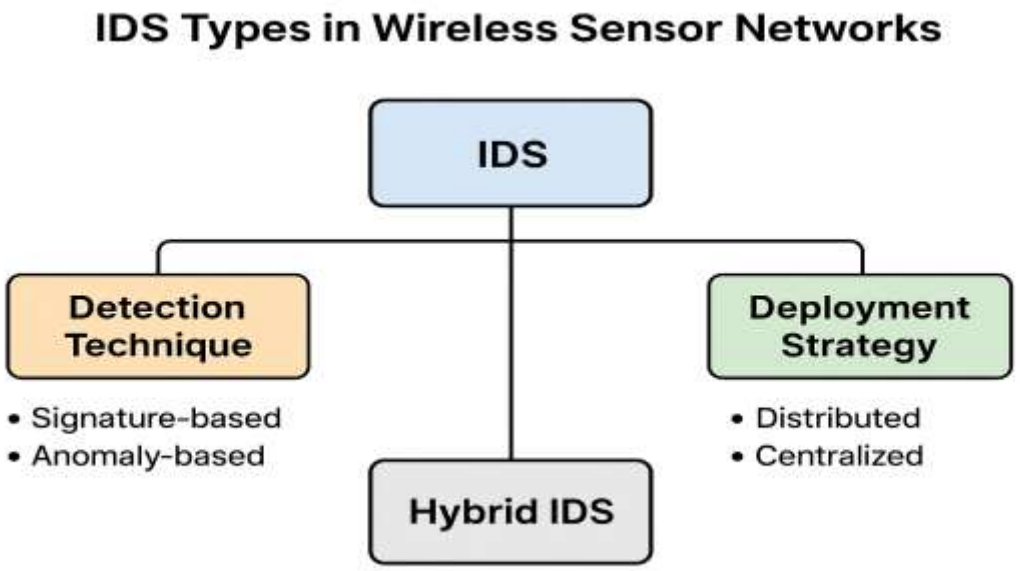
In a distributed IDS, many sensor nodes participate in monitoring and detection. Each node observes its neighbourhood, which increases coverage and makes the system more scalable and fault-tolerant.

Centralized IDS

A centralized IDS collects data from the entire network and performs detection at a single point, usually the base station.it offers good analysis accuracy but creates a single point of failure.

Hybrid IDS

A hybrid IDS combines both signature-based and anomaly-based detection methods. This improves detection accuracy and allows the system to handle both known and unknown types of attacks



Future Scope of IDS in Wireless Sensor Networks

The security needs of Wireless Sensor Networks continue to grow as they are used in critical areas like healthcare, smart cities, and defence. Several promising research directions are emerging for improving intrusion detection in WSNs.

1.AI-Based IDS

Future IDS solutions are likely to use more advanced and adaptive AI techniques. Instead of relying on fixed rules, these systems will continuously learn from the network's behaviour and automatically recognize new attack patterns. Lightweight deep learning models that require less computation will be an important research area for making AI possible even on small sensor nodes.

2. Lightweight IDS

Sensor nodes have very limited battery, memory, and processing power. Future IDS solutions need to be lightweight so they consume less energy and can still run efficiently on small sensor devices.

3. Blockchain-Based IDS

Blockchain can provide secure and tamper-proof communication between nodes. Using blockchain, the network can verify data integrity and prevent attackers from modifying routing or sensor information.

4. Cloud and Edge-Based IDS Support

Instead of performing all calculations inside the sensor network, future solutions may shift heavy processing tasks to cloud or edge servers. This allows the IDS to analyse large amounts of data quickly while keeping the sensor nodes free from extra burden. Cloud-assisted IDS can improve detection speed and accuracy in real time.

Conclusion

Intrusion Detection Systems play an essential role in protecting Wireless Sensor Networks from various cyberattacks. Although many IDS techniques have been developed, no single approach can address all security challenges due to the limited resources and open nature of WSNs. Each method has strengths and weaknesses, which makes the design of an ideal IDS still an open research problem. Future developments

must focus on improving detection accuracy while reducing energy consumption, so that WSNs remain secure, reliable, and efficient in real-world applications.

REFERENCES

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.
2. J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.
3. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2, pp. 293–315, 2003.
4. A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54–62, 2002.
5. H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks, Wiley, 2005.
6. R. Roman, P. Najera, and J. Lopez, "Securing wireless sensor networks," IEEE Internet Computing, vol. 16, no. 2, pp. 54–62, 2012.
7. Z. Jingjing, "Intrusion detection model for wireless sensor networks based on CNN-GRU," International Journal, 2022
8. S. Narasimha Prasad, "Intrusion Detection System in Wireless Sensor Networks," Wireless Communications Journal, 2022
9. M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly detection in wireless sensor networks: a survey," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1302–1325, 2011.
10. N. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," International Journal of Distributed Sensor Networks, 2013.
11. W. Yao, L. Hu, Y. Hou, and X. Li, "A Lightweight Intelligent Network Intrusion Detection System Using One-Class Autoencoder and Ensemble Learning," MDPI (journal name missing), 2023.
12. S. Alsharifi, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," AI Conference/Survey (2023).
13. T. M. Nguyen, "Enhancing intrusion detection in wireless sensor networks using optimization techniques," Sensors (MDPI), 2024.
14. R. Mitchell and I.-R. Chen, "A survey of intrusion detection in wireless network applications," Computer Communications, vol. 42, pp. 1–23, 2014.
15. M. Wazid, "Hybrid Anomaly Detection using K-Means Clustering in Wireless Sensor Networks," Journal Article, year varies
16. S. Sedjelmaci and M. Feham, "Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network," IJACSA / IJNSA, 2015
17. "A Study on Intrusion Detection System in Wireless Sensor Networks," International Journal of Computer Networks & Information Security (IJCNIS), 2020
18. A. Kathirvel and M. Maheswaran, "Enhanced AI-based intrusion detection and response system for WSN," book chapter / conference, 2023.
19. M. Devi, "Federated learning-enabled lightweight intrusion detection for WSN," Elsevier/ScienceDirect, 2025.
20. S. Wilson Neelankavil & M. K. S., "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," conference/journal, 2020.