International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 5, Sep-Oct 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Wireless Sensor Network Intrusion Detection: A Review of Statistical, Machine Learning, and Federated Methods

[1]Jennifer Kyari-Ayele, [2]Joseph Mom M, [3]Iorkyase Ephraim T.

[1]Electrical and Electronics Engineering Technology, College of Agriculture, Science and Technology Lafia, Nasarawa State.
[2,3]Department of Electrical and Electronics Engineering, Joseph Sarwuan Tarka University, Makurdi, Nigeria

Abstract

Wireless Sensor Networks have become essential infrastructure across environmental monitoring, healthcare, smart agriculture, industrial automation, and smart city applications. However, their distributed, resource-constrained, and physically accessible design creates serious security risks. This paper surveys cybersecurity challenges and intrusion detection in WSNs, tracing the field from statistical methods to machine learning, deep learning, explainable AI, and federated learning. Our analysis shows that while signature-based and anomaly-based detection provide foundational security, they face significant limitations in dynamic, resource-limited WSN environments. Machine learning and deep learning achieve strong results, Random Forest reaching 98–99.5% accuracy and deep learning architectures exceeding 99% in some studies, but these figures depend heavily on dataset, preprocessing, and evaluation choices. Explainable AI techniques such as SHAP and LIME address the "black-box" problem by enabling transparent security decisions, while federated learning enables privacy-preserving, communication-efficient collaborative detection. Significant gaps remain: integrated frameworks that detect both data theft and eavesdropping are lacking, passive attacks receive limited attention, developing-region contexts are under-addressed, and energy-aware adaptive security remains aspirational. We identify future directions including lightweight deep models, energy-aware adaptive security, hybrid architectures, and robust, poisoning-resilient federated mechanisms.

Keywords: **Wireless Sensor Networks, Intrusion Detection, Anomaly Detection, Machine Learning, Deep Learning, Explainable AI, Cybersecurity, Federated Learning, Eavesdropping, Energy-Aware Security**

1. Introduction

Wireless Sensor Networks (WSNs) bring compact, energy-efficient sensors together with wireless communication to monitor environments and collect data (Akyildiz et al., 2002). These networks consist of spatially distributed, resource-constrained sensor nodes that collaboratively monitor physical phenomena such as temperature, humidity, pressure, light, and motion and transmit data wirelessly to central processing units (Yick et al., 2008). The fundamental architecture of WSNs is characterised by distributed, self-organising nodes that create ad hoc networks, where data is relayed through multiple intermediate nodes until it reaches a sink node acting as a gateway to external systems (Karl & Willig, 2005). This multi-hop design helps WSNs cover large areas, including remote and difficult environments (Al-Karaki & Kamal, 2004).

WSNs have spread with the growth of the Internet of Things (IoT) (Ali et al., 2021a). WSNs serve as the sensory infrastructure for IoT applications across environmental monitoring, healthcare, industrial automation, smart agriculture, and smart cities (Ali et al., 2021a). In developing regions such as Nigeria, WSNs are gaining ground in universities and industry, with applications ranging from real-time water quality monitoring. In (Ogundero et al., 2025), the author built a decentralized IoT plus wireless sensor network framework (off-the-shelf water quality sensors, TUYA cloud platform) for real-time remote water quality monitoring in Nigerian communities, measuring temperature, pH, salinity, electrical conductivity, total dissolved solids, and specific gravity with local high-school students trained as citizen scientists.

(Olayinka et al., 2026) undertook a systematic review of smart IoT-driven *domestic* water quality monitoring systems that uses Nigeria as its case study noting that 68–70% of water in Nigeria is contaminated and that ML-based predictive contamination detection and edge computing are the emerging trends for resource-constrained settings. (Mensah et al., 2026) designed an IoT-enabled handheld tester for sachet water quality at point-of-sale locations in Minna, Nigeria at low-cost physicochemical sensors with wireless data transfer to a cloud platform. Despite these localized successes, the inherent vulnerability of these nodes to malicious interference persists, necessitating robust security protocols to protect sensitive environmental data (Hassan et al., 2023; Khashan et al., 2024). (Emmanuel et al., 2018) developed a farm monitoring and security system using WSNs for Nigerian agriculture large-scale farms, intrusion detection at the perimeter, real-time alerts to the owner.

Furthermore, the deployment of such networks in resource-constrained environments like those found in developing regions facilitates the acquisition of critical environmental data over extensive periods, despite

persistent infrastructural challenges (López-Ramírez & Aragón-Zavala, 2023). These challenges faced by WSNs are categorised into three basic constraints, namely:

i. Resource Limitations: Sensor nodes have little processing power, memory, and bandwidth, so traditional security measures are hard to use (Padmavathi & Shanmugapriya, 2009). Most sensor nodes are battery-powered, and replacing batteries in large-scale deployments can be impractical, so security measures must use little energy (Diop et al., 2013).
ii. Wireless Communication Vulnerability: Because wireless signals travel openly, attackers can intercept, listen to, or disrupt communications (Zou et al., 2016). Unlike wired networks, WSNs work in open environments, so attackers can intercept or alter data and inject false information (Ahmed et al., 2024).
iii. Physical Accessibility: These physical vulnerabilities often lead to node capture attacks, enabling adversaries to extract cryptographic keys or inject malicious code to compromise the entire network's integrity (King Faisal University et al., 2025; Oztoprak et al., 2025).

Among the security threats facing WSNs, data theft and eavesdropping are of particular concern (Ahmed et al., 2024). Data theft includes unauthorised access, improper information modification, and destruction. Its companion volume (NIST SP 800-60, quoting FIPS 199) states the flip side being "A loss of integrity is the unauthorized modification or destruction of information" (Kissel, 2013).

Furthermore, the inherent broadcast nature of wireless transmission increases these risks, as it facilitates eavesdropping, replay attacks, and denial-of-service maneuvers that can paralyze network operations (Tan, 2010). Conversely, eavesdropping involves the passive interception of transmissions, which allows adversaries to capture sensitive data without alerting the network's communication protocols (Butun et al., 2020).

Consequently, these passive interceptions create long-term privacy risks for data, as malicious actors may exploit captured information to gain competitive advantages or inflict financial losses on owner (Han et al., 2025). This survey reviews cybersecurity challenges and intrusion detection methods in WSNs. It asks five questions:

- Which security threats and intrusion detection system (IDS) designs matter most in WSNs?
- Which statistical, machine-learning, deep-learning, and hybrid methods are used to detect intrusions?
- How do explainable AI and federated learning address security and deployment challenges?
- What weaknesses affect current evaluations?
- What research gaps and future directions emerge from the literature?

The paper surveys research on WSN cybersecurity. It examines peer-reviewed journal articles, conference proceedings, and reputable technical reports published in the field. Studies use different datasets, attack distributions, preprocessing steps, train-test splits, hardware, and metrics, so reported accuracy values are not directly comparable and must be interpreted within their experimental context (Conti et al., 2021; Layeghy & Portmann, 2023; Le Jeune et al., 2021). This distinction is essential because a model can report high accuracy while performing poorly on minority attack classes or under deployment constraints. Consequently, the implementation of robust authentication mechanisms and privacy-preserving protocols remains paramount to mitigating the risks of node capture and unauthorized data exploitation (Saleh et al., 2024). Beyond these authentication measures, advanced intrusion detection systems are increasingly leveraging deep learning architectures to identify complex, non-linear attack patterns that traditional statistical methods often overlook (Behiry & Aly, 2024).

2. WSN Architecture, Security Requirements, and Threat Taxonomy

2.1 WSN Architecture and Vulnerabilities

A typical WSN has sensor nodes with five main parts: sensing units, processing units, communication units, power units, and memory. Sensing units use transducers and analogue-to-digital converters (ADCs); processing units use microcontrollers; communication units use transceivers (transmitters and receivers); power units use batteries or energy-harvesting systems and the Memory stores code and data (Akyildiz et al., 2002). The network topology can be organised as star, mesh, or cluster configurations, each with distinct security implications (Baviskar et al., 2025).

A WSN normally comprises sensor nodes, sink or cluster-head nodes, gateways, and application or cloud services. Nodes acquire measurements and may perform local processing before forwarding information (Ali et al., 2021b). Cluster heads or gateways can aggregate traffic and provide more capable processing. This setup helps security because demanding analysis can run on gateways rather than on the most limited devices (Mache et al., 2008).

Table 1: WSN Resource Constraints and Security Implications

Security risk	What can happen	Common safeguards
Limited power and computing capacity (Oztoprak et al., 2025)	Security checks use power and shorten network life	Low-power encryption, adaptive sampling, and edge screening
Open wireless connection (Oztoprak et al., 2025)	Interception, jamming, and traffic analysis	Encryption, frequency/channel diversity, anti-jamming mechanisms
Multi-hop routing (Butun et al., 2020)	Sinkholes (fake routes), Sybil attacks (fake identities), and selective forwarding (dropped messages)	Authentication, trust management, secure routing, multipath checks
Easy physical access (Oztoprak et al., 2025)	Stolen keys and compromised devices	Tamper resistance, key renewal, node attestation
Different kinds of devices (Tomic & McCann, 2017)	Uneven security capabilities	Capability-aware security policies and hierarchical IDS
Data collected in one place (Nguyen et al., 2021)	Privacy loss and one point of failure	Federated learning, local processing, secure aggregation

2.2 Threat Classification

We can group WSN security threats into two types: active and passive attacks (Oztoprak et al., 2025; Rajawat et al., 2024). Active attacks directly disrupt network operations by changing data, injecting false data, blocking service, or using routing attacks such as sinkhole and Sybil (Al-Fuhaidi et al., 2024; Moslehi, 2025). Passive attacks quietly monitor the network without changing it, including eavesdropping, traffic analysis, and side-channel information leakage (Abedini & Al-Anbagi, 2024; Bilal et al., 2025). While active attacks threaten integrity and availability, passive attacks primarily compromise confidentiality (Butun et al., 2020). Emerging threats such as advanced persistent threats and ML-based poisoning attacks make network security harder to manage (Hussain et al., 2025; Oztoprak et al., 2025).

2.2.1 Active Attacks

Active attacks involve direct interference with network operations. These attacks can take several forms:

i. Data Tampering and Theft: This includes unauthorised access, changing, or destruction of packets during transmission, often facilitated by the broadcast nature of wireless communication to bypass security perimeters (Osamah Ahmed Mahmood, 2024).

ii. False Data Injection: Attackers inject fabricated data into the network to corrupt decision-making or waste resources. This is especially dangerous in healthcare monitoring, where false patient data can lead to incorrect diagnoses, and in smart grids, where manipulated energy data can destabilise power distribution networks (Hussain et al., 2025; Oztoprak et al., 2025).

iii. Denial of Service (DoS): Attackers overwhelm the network with excessive traffic or exploit protocol vulnerabilities to disrupt legitimate communication. DoS attacks target different layers of the communication protocol stack, for example, jamming occurs at the physical layer, collision occurs at the MAC layer, and route disruption occurs at the network layer (Mirkovic & Reiher, 2004; Wood & Stankovic, 2002).

iv. Routing Attacks: These attacks manipulate forwarding behaviour or network topology. Sinkhole attacks attract traffic through a malicious node, selective forwarding drops selected packets, and Sybil attacks allow one adversary to appear under multiple identities (Karlof & Wagner, 2003). In practice, several controls help: authentication and key management limit unauthorised participation; secure routing protocols such as SPINS and TinySec protect communication; trust mechanisms identify unusual forwarding; multipath routing reduces reliance on one node; and intrusion detection systems spot unusual traffic and forwarding patterns (Jing Deng et al., 2004). No single control is sufficient because an adversary may combine several attack vectors.

v. Node Compromise: WSN nodes are typically deployed in unattended, physically accessible environments, which makes them vulnerable to physical intrusion and tampering attacks (Khashan et al., 2024; Oztoprak et al., 2025). An adversary who captures a node through direct physical access can extract the security material stored on it — including cryptographic keys — with relative ease; node compromise has been demonstrated on commodity motes in about one minute, and the obtained information can be used

to disrupt operations, falsify sensed data, or eavesdrop on the network (Hartung et al., 2005; Özdemir, 2008). Physical attacks may also destroy nodes permanently, and captured nodes can be reprogrammed, replaced with malicious clones, or have their cryptographic assets extorted, so the network cannot simply rely on cryptographic protection once physical security fails (Özdemir, 2008)). A compromised node therefore becomes an insider: it participates in the network with legitimate credentials while eavesdropping on, intercepting, or altering communications, and such compromised devices pose significant risks to data privacy through their privileged access (Ahmed et al., 2024; Osamah Ahmed Mahmood, 2024). To reduce this risk, use tamper-resistant hardware, renew keys, run remote attestation, and use intrusion detection to find compromised nodes (Ho et al., 2012). Furthermore, implementing mechanisms such as disabling JTAG interfaces or protecting bootstrap loaders can significantly elevate the threshold for physical memory extraction (Butun et al., 2020). Additionally, adopting self-destruct mechanisms for volatile memory upon detection of tampering ensures that critical cryptographic material remains inaccessible even if the physical device is captured (Jing Deng et al., 2005).

2.2.2 Passive Attacks

Passive attacks collect information without changing network activity:

i. Eavesdropping: this occurs when adversaries intercept wireless transmissions without actively interfering with communications (Bilal et al., 2025). This puts people's data at risk, especially in applications that handle private information. Eavesdroppers can exploit traffic analysis techniques to extract sensitive contextual information, including source and sink locations, routing paths, and event occurrence times(Jing Deng et al., 2005). Encryption techniques such as advanced encryption standard (AES)-based link encryption, elliptic curve cryptography (ECC), and lightweight cryptography protocols designed for resource-constrained devices can protect payload confidentiality, but metadata may remain observable (Goswami et al., 2025; Pathan et al., 2006). So protecting privacy may also require hiding traffic patterns, changing transmission schedules, using anonymity tools, and adding physical- or link-layer protections in addition to encryption.

ii. Traffic Analysis: Even when communications are encrypted, attackers can analyse traffic patterns such as timing, frequency, and packet size to infer sensitive information (Shokri et al., 2011). For example, in a healthcare monitoring application, an adversary might infer a patient's location or condition from traffic patterns (Vergutz et al., 2019). You can reduce this risk by sending dummy traffic, padding packets, randomising transmission times, and using onion routing.

iii. Information Leakage: Attackers can study side channels—such as power use, timing, and electromagnetic emissions—to extract sensitive information (Quisquater & Samyde, 2001). This is particularly common in wireless communication systems such as ZigBee, Bluetooth Low Energy (BLE), and LoRaWAN devices, where physical characteristics of transmissions can inadvertently reveal cryptographic keys or sensitive data (Sefati et al., 2025). To reduce this risk, systems can use constant-time code, balance power use, add electromagnetic shielding, and use cryptography designed to resist side-channel attacks.

Passive attacks are hard to detect because they do not change packets, so standard integrity checks may not raise an alarm (Fawaz, 2012). The transmitter also sees the information it sent as correct, so it does not notice the attack. This creates a clear opening for behavioural and statistical detection methods. They can flag unusual changes in what the channel shows, how packets arrive, timing, or node behaviour (Mitchell & Chen, 2014).

2.2.3 Emerging Threats

Modern WSN security must also guard against attacks on the learning infrastructure:

i. Advanced Persistent Threats (APTs): APTs represent sophisticated, targeted campaigns that persist over extended periods, using several ways to attack critical WSN infrastructure (J. L. Liu et al., n.d.). APTs differ from conventional attacks. They stay hidden, last a long time, and change tactics, so traditional signature-based tools often miss them. Detecting APTs with ML is difficult because they are rare in normal traffic, and public datasets rarely include every APT variant. Recent research has introduced datasets like SCVIC-APT-2021 to benchmark ML-based APT detection, demonstrating that attack-centric methods represent significant improvements over baseline approaches (J. L. Liu et al., n.d.).

ii. Machine Learning Poisoning Attacks: As ML-based Intrusion Detection Systems become increasingly prevalent in WSNs, adversaries can manipulate training data to degrade model

performance or induce specific misclassifications (Bout et al., 2022). Gradient poisoning can lower IDS classification accuracy by about 20% on benchmark WSN datasets (Gardiner & Nagaraja, 2017). Label-flipping attacks, a common poisoning variant, can significantly impact deep learning-based profiling in IoT environments. Defensive strategies include input validation, robust learning techniques, adversarial training, and ensemble methods that enhance model resilience against contaminated training data (Huma et al., 2026).

iii. Federated Learning Attacks: FL attacks pose unique threats to privacy-preserving distributed IDS architectures, encompassing both poisoning and inference attacks that compromise model integrity and client privacy (Alsaleh et al., 2024). Poisoning attacks in FL can take multiple forms, including Byzantine behaviour where compromised clients send malicious updates, Sybil attacks where adversaries forge multiple identities to amplify influence, and backdoor attacks that embed hidden triggers into global models (Yeng & Gebrie, 2026a). Defensive mechanisms such as trust-aware aggregation, homomorphic encryption, and differential privacy have been proposed to mitigate these threats while balancing privacy and utility (Yeng & Gebrie, 2026a). Recent frameworks like TrustFed-IDS integrate multi-criteria trust scoring into FL aggregation to detect and reject poisoned updates from adversarial clients, and performs as well as leading systems while resisting Byzantine clients (Yeng & Gebrie, 2026a).

3. Intrusion Detection Systems for WSNs

Classification of Intrusion Detection Systems

Intrusion Detection Systems (IDS) for Wireless Sensor Networks (WSNs) fall into three main groups: detection method, deployment, and operation (García-Teodoro et al., 2009; Hosseini Shirvani & Akbarifar, 2024; Patcha & Park, 2007). Because WSNs have limited resources, choosing the right IDS type helps balance security, battery life, and computing costs (Oztoprak et al., 2025; Rajawat et al., 2024).

A. Classification by Detection Methodology

Detection methodology is how an IDS spots malicious activity. It uses three approaches: signature-based methods (matching known attacks), anomaly-based methods (spotting unusual behavior), and hybrid methods (Gajewski et al., 2019).

i. Signature-Based Detection finds intrusions by comparing network activity with a database of known attack patterns, or "signatures" (Kumar, 1994a). This approach operates on the premise that malicious behaviours leave identifiable traces in network traffic or system logs (Roesch, 1999). Its main benefits are very few false positives and fast detection of known threats because it is well established and efficient (Hussain et al., 2025). However, these systems cannot detect zero-day or new attacks, require continuous updates to signature databases, are ineffective against polymorphic or obfuscated attacks, and can become resource-intensive for large signature sets—a critical concern for memory-constrained sensor nodes (Moslehi, 2025; Rajawat et al., 2024)

ii. Anomaly-Based Detection sets a baseline—what normal network behaviour looks like—and flags major changes as possible intrusions (Denning, 1987). Its main strength is that it can detect new attacks and adapt as networks change (Chandola et al., 2009; Patcha & Park, 2007). Anomaly-based systems can also identify insider threats that may not exhibit known attack signatures (Bhoi et al., 2026). Nevertheless, these systems suffer from higher false positive rates compared to signature-based approaches, can be gradually "trained" to accept malicious activity, require comprehensive and representative training data, and impose computational overhead that may be prohibitive for resource-constrained sensor devices (García-Teodoro et al., 2009; Hosseini Shirvani & Akbarifar, 2024).

iii. Hybrid Detection systems combine signature-based and anomaly-based methods to use the strengths of both approaches (Cahyo et al., 2020). In theory, this layered approach can catch both known and new attacks without too many false positives (Haque et al., 2024). They reduce false positives through signature checks, adapt through anomaly detection, work across resource levels, and add layers of security (Nisioti et al., 2018). However, limitations include increased system complexity, potential for conflicting detection results, and higher overall resource requirements (Mary et al., 2025).

B. Classification by Architectural Deployment

Architectural deployment describes where IDS components sit and how they connect, grouping them into network-based, host-based, and distributed architectures (Hosseini Shirvani & Akbarifar, 2024).

i. Network-based IDS (NIDS) capture and analyze live network packets, looking for patterns, counting traffic, and tracking behavior across the network (García-Teodoro et al., 2009). NIDS usually sit at key points, such as gateways or cluster heads, to watch whole network segments and show traffic patterns across the network (Patcha & Park, 2007).

ii. Host-based IDS (HIDS) track activity on individual sensor nodes or host systems and detect local problems without relying on network traffic (Patcha & Park, 2007). HIDS can catch node-level compromises and insider threats that may not appear in network traffic, but they use computing power on resource-constrained sensor nodes (Hosseini Shirvani & Akbarifar, 2024).

iii. Distributed IDS combine NIDS and HIDS by sharing data across sensor nodes, cluster heads, and base stations (Hosseini Shirvani & Akbarifar, 2024; H. Zhang et al., 2025). This architecture suits WSNs because their components are spread across many nodes. It also broadens coverage by comparing data from several sources, continuing to work when some nodes fail, and growing with the network (Anwer et al., 2025; Hosseini Shirvani & Akbarifar, 2024; Mishra et al., 2025).

Table 2: IDS Architecture Classifications

Architecture	Where It Runs	Strength	Main Drawback
Network-based IDS	Gateway/cluster head	Broad traffic visibility	Limited visibility into local node compromise
Host-based IDS	Individual node	Local behavioural visibility	Uses extra energy and memory
Distributed IDS	Multiple nodes/gateways	Correlation and resilience	Communication and coordination cost
Hierarchical IDS	Edge + gateway/fog/cloud	Fits the network's resource levels	Complex system design and coordination

C. *Classification by Operational Strategy*

Operational strategy explains how IDS components work together and handle data across the network. It covers standalone, hierarchical, and collaborative models (Hosseini Shirvani & Akbarifar, 2024; Raza et al., 2013).

i. Standalone Strategy: In a standalone operational strategy, each sensor node runs its IDS on its own, making local decisions without coordinating with other nodes (Patcha & Park, 2007). This strategy minimises communication overhead but limits detection accuracy due to the lack of a wider view and shared information (Hosseini Shirvani & Akbarifar, 2024).

ii. Hierarchical Strategy: A hierarchical operational strategy uses several layers: simple checks run at the edge (sensor level), while more advanced checks run at the gateway, fog, or cloud (Hussain et al., 2025; Raza et al., 2013). This strategy enables sensors with limited resources to perform initial filtering, while higher-tier nodes conduct complex analysis using machine learning and deep learning models (Sakthimohan et al., 2024). Hierarchical strategies can be implemented through three ways to arrange these layers:

- Sequential Pattern: Signature-based detection is applied first for quick removal of known threats, followed by anomaly-based analysis for deeper investigation of remaining traffic (Raza et al., 2013).
- Parallel Pattern: Both detection methods run at the same time, with their results combined by voting or fusion to make a final classification (H. Zhang et al., 2025).
- Fusion Pattern: Several detection models or data sources are combined with ensemble or fusion methods to improve detection accuracy (Afnan Birahim et al., 2025a; Mishra et al., 2025).

iii. Collaborative Strategy: A collaborative operational strategy lets distributed nodes share detection information, alerts, and model updates to build a shared view (Anwer et al., 2025). Federated learning represents a prominent collaborative strategy where models are trained across multiple clients without sharing raw data, thereby preserving privacy and reducing communication overhead (McMahan et al., 2016a). Collaborative strategies offer enhanced detection accuracy through multi-source correlation, robustness against individual node failures, and privacy preservation through decentralised processing (Alsaleh et al., 2024; Hussain et al., 2025; Vasilomanolakis et al., 2015).

4. Statistical and Machine-Learning Anomaly Detection

Machine learning (ML) and deep learning (DL) methods can help Wireless Sensor Networks detect known attacks and spot new ones automatically (Al-Quayed et al.,

2024). Unlike statistical methods that use fixed thresholds, ML/DL methods learn useful patterns from data and can adapt as conditions change (Gayathri & Surendran, 2024).

Statistical methods work well on sensor nodes with limited computing power for initial filtering. ML and ensemble methods can run on cluster heads and gateways, while deep learning run on fog or cloud systems mis (Hussain et al., 2025; Mishra et al., 2025). This layered approach uses resources wisely while improving detection accuracy (Yahyaoui et al., 2019; Yang et al., 2018).

4.1 Statistical Approaches

Statistical techniques remain valuable at the sensor or edge tier because they are cheap to run (OReilly et al., 2014). Examples include Z-score or robust deviation tests, moving statistics, autoregressive models (ARIMA), Mahalanobis distance, entropy measures, and change-point detection. Their main problem is that normal WSN behaviour often changes over time. Temperature, humidity, battery voltage, traffic load, and radio conditions can change for legitimate reasons (Chen & Li, 2019). As a result, fixed thresholds can trigger false alarms (Gayathri & Surendran, 2024).

The Z-score for a data point $\boldsymbol{x}$ is computed as:

$$\boldsymbol{Z = \frac{(x - \mu)}{\sigma}}$$

where μ is the mean and $\boldsymbol{\sigma}$ is the standard deviation of the training data. Anomalies are flagged when $\boldsymbol{|Z| > \tau}$, where $\boldsymbol{\tau}$ is a predefined threshold.

Mahalanobis Distance

It extends the Z-score idea to data with several variables:

$$\boldsymbol{D_M(x) = \sqrt{(x - \mu)^T \sum^{-1} (x - \mu)}}$$

Here, $\boldsymbol{x}$ is the feature vector, $\boldsymbol{\mu}$ is the mean vector, and ∑ is the covariance matrix of the training data.

Entropy-Based Detection

Entropy-based detection measures how varied the data are using Shannon entropy:

$$\boldsymbol{H(X) = -\sum_{i=1}^{n} p(x_i) log(p(x_i))}$$

Here, $\boldsymbol{p(x_i)}$ is the chance of observing the value $\boldsymbol{x_i}$. Large changes in entropy can point to unusual patterns in the data (Ibidunmoye et al., 2015).

4.2 Classical Machine Learning Approaches

Classical ML algorithms need modest computing power and are easy to interpret, so they work well on cluster heads and gateways (Hastie et al., 2009; M Bishop, 2006).

i. Random Forest builds a group of decision trees from resampled data and randomly chosen features. This makes it less sensitive to noise and useful for data with many features (Breiman, 2001). Studies report Random Forest accuracy ranging from 92.39% to 99% in WSN intrusion detection and higher accuracy than comparison algorithms in some evaluations (Subbiah et al., 2022; Tan, 2010).

The Random Forest algorithm operates through:

a. Bootstrap Sampling: Drawing N bootstrap samples from the original dataset.

b. Decision Tree Construction: For each bootstrap sample, grow an unpruned decision tree. At each node, choose the best split from a random subset of m features (typically m ≈ √p for classification, where p is the number of features).

c. Voting: For classification, the final prediction is the majority vote across all trees.

ii. Support Vector Machines (SVM) find the best boundaries between classes by leaving as much space as possible between them. A kernel can also separate classes that a straight line cannot (Vapnik, 2000). The optimisation objective is defined as;

$$\boldsymbol{min_{\omega,b,\xi} \frac{1}{2}\|\omega\|^2 + C\sum_{i=1}^{n} \xi_i}$$

Subject to:

$$\boldsymbol{y_i(\omega . x_i + b) \geq 1 - \xi_i, \xi_i \geq 0}$$

Here, $\boldsymbol{\omega}$ is the weight vector, $\boldsymbol{b}$ is the bias, $\boldsymbol{\xi_i}$ represents the allowed error, and $\boldsymbol{C}$ controls the penalty for that error. The RBF kernel is often used in WSN applications, where it classifies data well and generalizes from limited training data (Dora & Swain, 2024).

iii. K-Nearest Neighbours (KNN) classifies each instance by choosing the most common class among its nearest neighbours. It is simple and can learn online (Cover & Hart, 1967). The KNN algorithm uses distance metrics such as Euclidean distance:

$$\boldsymbol{d(x, y) = \sqrt{\sum_{i=1}^{p} (x_i - y_i)^2}}$$

KNN can slow down on large datasets, and distances become less useful when there are many features (W. Liu et al., 2018).

Ensemble Methods combine several classifiers to improve results (Dietterich, 2000). The HEXADWSN framework integrates Autoencoders, Isolation Forests, and One-Class SVMs through stacking and voting, identifying temperature, humidity, and voltage as the most influential features (Mishra et al., 2025). (Afnan Birahim et al., 2025a) developed a PSO-based ensemble approach that optimises classifier weights, achieving improved accuracy with SHAP-based interpretability. Ensemble methods achieve 95.0–99.5% accuracy in WSN intrusion detection (Haque et al., 2024).

4.3 Deep Learning Approaches

Deep learning finds features automatically and builds them into layers, going beyond what traditional ML methods can do (Goodfellow et al., 2016; LeCun et al., 2015).

i. Convolutional neural networks (CNNs) find patterns at different scales by alternating convolution and pooling operations (Zuo et al., 2022). In WSN data, 1D convolutions extract features from network traffic to detect subtle intrusion patterns (Robacky Mbongo et al., 2025). The convolution operation for 1D data is:

$$\boldsymbol{y_i = \sigma(\sum_{j=0}^{k-1} \omega_j \cdot x_{i+j} + b)}$$

where $\boldsymbol{\omega_j}$ are the filter weights, $\boldsymbol{k}$ is the kernel size, $\boldsymbol{x}$ is the input, $\boldsymbol{b}$ is the bias, and $\boldsymbol{\sigma}$ is the activation function (typically ReLU). Attention-enhanced CNNs refine feature tensors through spatial and channel attention for intrusion detection (Gatate & Agarkhed, 2024).

ii. Long Short-Term Memory (LSTM) networks track patterns over time using memory cells with gates (Hussain et al., 2025). The cell uses these equations:

Forget gate: $\boldsymbol{f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)}$

Input gate: $\boldsymbol{i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)}$

Candidate cell state:

$$\tilde{C}_t = tanh((W_C \cdot [h_{t-1}, x_t] + b_C))$$

Cell state update: $C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$

Output gate: $o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)$

Hidden state: $h_t = o_t * tanh((C_t))$

LSTMs analyze local and temporal correlations in WSN patterns to detect cyber threats (Haque et al., 2024; Sakthimohan et al., 2024; Sathishkumar et al., 2024).

iii. Hybrid CNN-LSTM Architectures find local patterns and track changes over time in multivariate sensor data (Nizam et al., 2022). They can detect complex attacks that unfold in several phases (Maaz et al., 2024).

iv. Autoencoders learn a compact version of normal data without labels, then detect anomalies by measuring reconstruction error (Torabi et al., 2023). The encoder turns the input x into a smaller internal representation z:

$$z = f_e(x) = \sigma(W_e x + b_e)$$

The decoder reconstructs x from z:

$$\hat{x} = f_d(z) = \sigma(W_d z + bd)$$

We measure the reconstruction error E for each input x as:

$$E(x) = ||x - x||^2$$

It flags an input as anomalous when $E(x) > \tau$, using τ as the chosen threshold. This works well when labelled attack data is scarce (Chandola et al., 2009). The SDLEER mechanism also works in WSN deployments (Sakthimohan et al., 2024).

4.4 Comparative Performance Analysis

Table 3: Comparative Performance of WSN Anomaly Detection Methods

Approach	Typical Role	Primary Strength	Primary Limitation
Statistical	Early screening at the edge	Low computational cost	Sensitive to changing normal behaviour (Rajapaksha et al., 2023)
Decision Tree/RF	Gateway IDS	Handles complex patterns and is fairly easy to interpret	Model maintenance and feature dependence (Aljanabi et al., 2021)
SVM	Gateway/edge	Works well when the input features fit the task	Scaling and parameter sensitivity (Buczak & Guven, 2016)
KNN	Gateway/offline	Simple and flexible	Inference cost grows with data (Rajapaksha et al., 2023)
CNN/LSTM	Fog/cloud	Learns complex patterns across space and time	High computational and training cost (Rajapaksha et al., 2023)

Autoencoder	Anomaly detection	Can use mostly normal data	Threshold selection and drift (Agrawal et al., 2022).
Ensemble	Gateway/fog	Combines complementary models	Higher complexity (Modi et al., 2013)
Federated ML	Distributed clients	Reduces raw-data sharing	Risks from communication, poisoned updates, and data aggregation (De Carvalho Bertoli et al., 2023)

Table 4: Performance summary and evidence

Method	Accuracy Range	Reported Cost Metrics	Suitability	Evidence
Statistical Methods (Threshold-based, Histogram, ARIMA, Mahalanobis Distance)	70–85%	Not reported in most studies.	Sensor nodes	Threshold-based and histogram-based statistical schemes are computationally cheap and well suited to resource-limited sensor nodes (OReilly et al., 2014; Xie et al., 2012), and incremental histogram anomaly detection has demonstrated "a high detection accuracy ratio and a low false alarm ratio" on real WSN data (Wang & Li, 2013).
Traditional ML (SVM, KNN, DT)	85–98%	Not reported; KNN/IBK recorded the shortest build/test time (0.05 s on the WSN dataset) in a WEKA-based comparison (Alsahli et al., 2021).	Cluster heads/gateways	SVM achieved 94.83% accuracy for malicious traffic detection in WSNs (Bhavya et al., 2023), while Decision Trees achieved near-perfect detection rates on NSL-KDD (Megantara & Ahmad, 2021). KNN has been widely evaluated in WSN intrusion detection contexts (Mitchell & Chen, 2014). Results vary: Naïve Bayes and KNN achieved approximately 82.7% accuracy in one configuration (El Ahmar et al., 2024).
Random Forest	98.0–99.5%	Not reported.	Gateways/edge	Random Forest performs very well in WSN intrusion detection. Ali et al. (2025) reported 99.65% accuracy on WSN datasets, while (Khraisat et al., 2025) achieved 99.67% accuracy using federated Random Forest on WSN-DS. Bhavya et al. (2023) reported 99.68% accuracy in ensemble configurations, and Priyanka et al. (2024) achieved 99.92% accuracy with SMOTE-Tomek-Link balancing.
Ensemble Methods	95.0–99.5%	Improved accuracy at the expense of increased run-time (Tabbaa et al., 2023)	Gateways/cloud	Ensemble approaches outperform individual classifiers (Tabbaa et al., 2023). Bhavya et al. (2023) reported the SVM+RF ensemble achieved 96.33% accuracy. Shamila et al. (2026) reported the EWO-IL-BiLSTM model achieved 97.06% accuracy on WSN-BFSF datasets. Studies confirm that ensemble methods regularly achieve over 99% accuracy in WSN intrusion detection (Ouhmi et al., 2026).
Deep Learning	95.0–99.5%	CNN-LSTM: 0.35 s average detection latency, 1.8% FPR (Balajishanmugam et al., 2025); energy not reported	Cloud/fog (offloading)	Deep learning architectures show dataset-dependent performance. Shamila et al. (2026) reported that CNN-LSTM, CNN, and DNN achieved 83.58%, 83.52%, and

				86.30% accuracy, respectively, on WSN-BFSF datasets. However, (Sakthimohan et al., 2024) achieved 99.76% accuracy with the SDLEER mechanism, while hybrid DL models have reported 98.6% accuracy (Haque et al., 2024). In practice, deep learning performance depends on the model and the dataset (Ian et al., 2016; LeCun et al., 2015).
		IEE-FedAgg: 50% and 24% (non-IID) energy savings accounting for computation and communication (C et al., 2023); FedKD: up to 94.89% communication-cost reduction (Wu et al., 2022)		

5. Energy and Cost Reporting Standards

Qualitative labels such as low-cost, cheap, and efficient cannot support reproducible comparison, and most surveyed primary studies evaluate accuracy-based metrics while leaving energy unquantified; this report recommends that WSN research adopt standardized, quantitative cost reporting. Energy should be reported as millijoules per detection cycle (mJ per evaluated traffic window), computed from node-state time accounting. Using Powertrace-style profiling and the nominal operating conditions of the Tmote Sky platform, energy is:

$$E(mJ) = \frac{(CPU \times 1.8 + LPM \times 0.0545 + Transmit \times 19.5 + Listen \times 21.8) \times 3}{4096 \times 8}$$

where CPU, LPM, Transmit, and Listen are the state durations in profiling ticks, the coefficients are the nominal currents in mA, and 3 V is the nominal supply voltage (Pongle & Chavan, 2015). Equivalent formulations in mWs follow from $P(mW) = E(mWs)/t(s)$ (Arshad et al., 2020). Energy figures are only interpretable when the detection window, dataset, duty-cycling regime, and communication overhead (packets or bytes per detection cycle) are stated; detection latency is a rarely used but critical metric, and power consumption, communications overhead, and processor load are the key secondary measures for resource-limited targets (Mitchell & Chen, 2014), with data transmission typically dominating node energy (Mitchell & Chen, 2014). Memory footprint should also be reported against a concrete platform — the Tmote Sky class offers 48 KB of flash and 10 KB of RAM, so IDS code and per-packet state must fit within comparable budgets (Pongle & Chavan, 2015). Where quantitative evidence exists, it should anchor comparisons: an incentive-based energy-efficient federated aggregation scheme reports energy savings of 50% and 24% for IID and non-IID data respectively while accounting for both computation and communication energy (C et al., 2023); communication-efficient federated distillation reduces communication cost by up to 94.89% (Wu et al., 2022); and a hybrid CNN-LSTM IDPS reports an average detection latency of 0.35 s with a 1.8% false-positive rate and is positioned as suitable for resource-constrained WSN environments (PPG Institute of Technology, India et al., 2025). Where a primary study reports no energy data, we record "not reported" rather than inferring a qualitative cost label.

6. Explainable AI for WSN Security

Deep learning models are commonly called “black boxes”. This is because we cannot easily see how they reach a decision. In security work, that makes trust, accountability, and regulatory compliance (Adadi & Berrada, 2018; Raza et al., 2013). Explainable AI (XAI) techniques address this limitation by providing interpretable insights into model predictions.

6.1 Post-Hoc Explanation Methods

Post-hoc explainability must itself be budgeted like any other security workload, and we propose three complementary policies for reconciling SHAP/LIME overhead with node-level constraints. First, explanations should be generated off-node and on demand. Lightweight models can handle routine traffic, with SHAP or LIME reserved for flagged events and high-risk cases requiring deeper analysis (Mohale & Obagbuwa, 2025); in hierarchical deployments such as the layered architectures described in Section 3.1.3, this places the explanation workload at the cluster head, gateway, or fog tier rather than on individual motes. Second, the choice of explainer should match the deploying tier. Benchmarking on real edge hardware shows that SHAP, while offering high-quality explanations, imposes significant computational overhead and is best suited to moderately powered platforms, whereas LIME achieves a workable balance between transparency and resource efficiency and is the most viable option for real-time inference on

lower-end devices; saliency-style methods are computationally lightest when interpretability needs are modest (AlNusif, 2025). Where explainability is required intrinsically, ante-hoc designs are preferable: X-HIDS couples a lightweight signature-based engine with a machine-learning anomaly detector and SHAP/LIME explanations while reporting improved energy efficiency (G & Meenakshisundaram, 2025), and PSO-optimized explainable ensembles demonstrate that interpretability can be engineered into WSN pipelines, reaching 99.73% accuracy on WSN-DS with SHAP-based explanation (Afnan Birahim et al., 2025b). Third, the cost of explanation should be assumed real until measured: SHAP and LIME require model evaluations proportional to feature dimensionality, which renders real-time inference-time explanation on constrained nodes infeasible (Slaoui, 2026a), and empirical studies of XAI in networking confirm that explanation techniques differ markedly in time and energy cost (Corona et al., 2023).

6.2 Importance for WSN Security

XAI strengthens WSN security in several practical ways such as:

i. Trust Building: XAI provides network administrators with clear reasoning for automated detection decisions, building confidence in the IDS and helping operators adopt it (Mohale & Obagbuwa, 2025). When operators understand why an alert was generated, they are more likely to act on it appropriately.

ii. Fault Diagnosis: Explanations help find faults by showing their root causes, which speeds incident response (Mishra et al., 2025). For example, if an anomaly is explained primarily by a voltage drop, this suggests a physical issue rather than a cyber attack, enabling appropriate response.

iii. Model Debugging and Improvement: Understanding which features matter helps us improve the model and detect threats more accurately. If SHAP analysis reveals that certain features contribute little to predictions, they can be removed to reduce computational cost without sacrificing accuracy (Ergün, 2023).

iv. Regulatory Compliance: Regulatory frameworks such as the Nigeria Data Protection Act (NDPA) 2023 (Shokunbi et al., 2026) stress the need to explain automated decisions, particularly when decisions affect individuals' rights. XAI enables compliance with these requirements.

v. Actionable Insights: Explanations give security teams useful guidance. If an attack is explained by unusual traffic patterns from a specific node, the response can be targeted at that node rather than broadly affecting the network.

For WSNs, explanation should be treated as an operational capability rather than a decorative model output. Explanations can support incident triage, feature reduction, model debugging, and trust assessment. However, we must also test explanation quality: a visually convincing explanation is not necessarily faithful to the underlying model, and recent literature identifies several critical obstacles to using XAI operationally. First, computational overhead: SHAP and LIME are computationally intensive and can hinder real-time detection capabilities in high-speed environments (Mohale & Obagbuwa, 2025). Second, the resource–interpretability gap: computationally intensive explainers are frequently applied on constrained edge and federated platforms without explicitly accounting for latency, memory footprint, or energy consumption (Karras et al., 2026). Third, evaluation itself is immature: quality has multiple dimensions — descriptive accuracy, sparsity, stability, efficiency, robustness, and completeness — yet metrics proliferate with duplication, inefficacy, and confusion, creating a pressing need for standardized evaluation frameworks (Arreche et al., 2024; Pawlicki et al., 2024). Fourth, security and privacy: explanation outputs may expose sensitive patterns or features (Mohale & Obagbuwa, 2025), and the transparency XAI provides can itself be exploited by adversaries (Moss et al., 2025). The cybersecurity literature now catalogues at least 25 open challenges for xAI (Pawlicki et al., 2024), and its integration into the Internet of Things domain remains not fully defined (Kök et al., 2023).

Consequently, future research must prioritize the development of lightweight XAI frameworks that balance predictive performance with the strict energy constraints inherent in IoT deployments (Mohammad et al., 2025).

Recent work shows what this looks like. HEXADWSN proposes an explainable ensemble architecture for robust and energy-efficient anomaly detection in WSNs (Mishra et al., 2025). This supports building explainability into detection from the start, rather than adding XAI later.

7. Federated Learning for Privacy-Preserving IDS

Federated Learning (FL) lets several clients train a shared model without sending their raw data. This protects privacy and reduces communication overhead in WSNs (Konečný et al., 2016; McMahan et al., 2016b). This matters for WSN security because sensor data can reveal details about the environment, people, or infrastructure.

7.1 Federated Averaging

FedAvg coordinates training on each client, then combines the updates at a central server (Zhou et al., 2022). The global model at round $t + 1$ is given by:

$$\omega^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} \omega_k^{t+1}$$

where n_k is the number of samples on client k, and n is the total number of samples across all K clients. Weighted averaging ensures clients with more data contribute proportionally more to the global model (Perifanis et al., 2023).

Here is the FL process:

i. Initialisation: The server initialises the global model parameters ω^0.

ii. Client Selection: A subset of clients is selected for participation in each round.

iii. Local Training: Each selected client trains on its private data and computes a model update.

iv. Update Transmission: Clients transmit model updates to the server.

v. Aggregation: The server combines updates using weighted averaging.

vi. Distribution: The server sends the updated global model to clients.

7.2 Advantages for WSN Security

FL offers several benefits for detecting intrusions in WSNs (Agrawal et al., 2022):-

i. Enhanced Data Privacy: By enabling decentralized training, FL ensures that raw sensitive sensor data never leaves local devices, effectively minimizing the risks associated with data exposure (Sharma et al., 2026).

ii. Privacy Preservation: Sensor data stays on each node, which reduces privacy risks from centralized data collection (McMahan et al., 2016b). This is particularly important for applications involving personal data, such as healthcare monitoring or smart home systems.

iii. Reduced Communication Overhead: We reduce communication overhead by sending model updates instead of raw data (Wu et al., 2022). This matters for energy-constrained wireless sensor networks (WSNs), where communication uses most of the energy.

iv. Scalability: FL naturally scales to large networks by distributing computation across nodes (Nguyen et al., 2021). As networks grow, computational load is distributed rather than concentrated at a central point.

v. Robustness: Aggregation provides tolerance to individual node failures or benign device dropouts (T. Li et al., 2020), but the claim that "as long as the majority of clients are honest, the global model remains reliable" oversimplifies the threat model. Without hardened aggregation, a single Byzantine client can fully control the averaged model (Lyu et al., 2024), and a single attacker in one round can embed a backdoor that defeats the model on attacker-chosen inputs (Bagdasaryan et al., 2018). Honest-majority reliability is therefore achieved only with the Byzantine-robust and trust-aware mechanisms.

Despite these advantages, the integration of FL into WSNs introduces significant security vulnerabilities, as malicious participants may attempt to inject poisoned model updates or execute inference attacks to reconstruct local training data (Ceviz et al., 2025; C. Zhang et al., 2024).

7.3 Security Challenges in Federated Learning

However, FL introduces new security and systems problems that must be addressed:

i. Information Leakage: Model updates can leak information about local training data. Gradient inversion attacks can reconstruct training samples from gradients, while membership inference attacks can determine whether a particular sample was used in training (Jegorova et al., 2022).

ii. Poisoning Attacks: Malicious clients can poison the global model through Byzantine behaviour (sending malicious updates), Sybil attacks (forging multiple identities to amplify influence), or backdoor attacks (embedding hidden triggers into global models) (Jimenez-Gutierrez et al., 2026).

iii. Communication Costs: Repeated communication rounds can consume substantial energy, particularly for large models or networks with limited bandwidth(Cui et al., 2021).

iv. Heterogeneity: Non-IID data distributions across clients can degrade model performance, as local updates may diverge from the global optimum (Lu et al., 2024).

7.4 Defensive Mechanisms

Because FedAvg-style averaging is arbitrarily manipulable by even one malicious client (Hu et al., 2024), aggregation must be hardened in layers. We recommend a three-line defense, benchmarked under the Byzantine, Sybil, and backdoor scenarios identified in Section 6.3 and Table 5.

i. Byzantine-robust aggregation (baseline). The pragmatic first line is coordinate-wise trimmed mean and median aggregation and Krum/Multi-Krum distance-based selection (Cao et al., 2021). A 2025 NDSS study argues that enhancing robustness with well-established rules such as trimmed mean and median is preferable to designing ever more complex aggregation protocols, which fuels a costly and potentially unsustainable arms race (Fang et al., 2025). Two caveats apply: these classical rules were designed for IID assumptions and often degrade under non-IID data (S. Li et al., 2024a), and carefully optimized local-model poisoning can defeat claimed-robust rules such as Krum, Bulyan, and trimmed mean (Lyu et al., 2024).

ii. Rejection and filtering (second line). Where the number of Byzantine clients is bounded, meta-aggregation with Bulyan strengthens guarantees, and contribution-similarity filtering with FoolsGold detects colluding clients that submit near-identical updates (Lyu et al., 2024). For resource-constrained deployments, fast Byzantine aggregation, which iteratively removes the most deviant gradients before aggregating, and Zeno++, which scores each update against a clean validation set, are adaptive alternatives — but both carry practical assumptions: FABA expects gradient similarity, and Zeno++ requires trusted server-side data (Madathil et al., 2025).

iii. Trust-aware weighting (third line, particularly suited to WSN IDS). Instead of raw averaging, each client contributes in proportion to a multi-signal trust score. The TrustFed-Honeypot framework fuses detection accuracy, performance stability, update drift, and predictive uncertainty into a unified score and applies sub-linear trust-weighted aggregation (trust^0.8), outperforming FedAvg by 31.50 percentage points in accuracy on the CTU-13 benchmark while reducing the false-negative rate from 43.11% to 9.92% (Yeng & Gebrie, 2026b). Reputation-based aggregation that weights clients by the historical consistency of their updates similarly sustains an F1 score of 0.743 with 40% adversarial clients, versus 0.62 for FedAvg and median-based aggregation (Parvizi et al., 2026). These mechanisms align with the trust-enhanced detection direction already surveyed in this manuscript (Anwer et al., 2025).

For fully decentralized (server-less) topologies, classical centralized Byzantine-robust rules are not directly applicable; dedicated Byzantine-robust aggregation designs for decentralized federated learning should be used instead (Cajaraville-Aboy et al., 2025). Finally, robust aggregation defends only the aggregation stage: it does not by itself block data- and model-poisoning backdoors injected during local training, nor inference-stage leakage. It should therefore be paired with gradient clipping and norm bounding, differential privacy, and anomaly detection on client behavior (Naseri et al., 2022; Wan et al., 2024), given the breadth of documented Byzantine, Sybil, and backdoor attack strategies (Jimenez-Gutierrez et al., 2026).

8. Research Gaps and Future Directions

8.1 Research Gaps Identified

Our review points to several research gaps that cut across evaluation practice, detection coverage, and the operational constraints of WSN deployments. The first cluster concerns evaluation itself: studies rarely use the same metrics, datasets differ sharply in difficulty, and reported accuracies are strongly conditioned by dataset choice, preprocessing, class balance, and split strategy, so results from different studies cannot be read as a controlled ranking, and apparent improvements may reflect differences in data curation or scoring conventions rather than genuine methodological advances (Conti et al., 2021; Le Jeune et al., 2021; Subhan et al., 2026). Benchmark datasets are often collected in simulated environments rather than real-world networks, and their setups differ substantially from the radio, energy, and traffic conditions of actual deployments, so near-perfect benchmark results have not translated into deployed detection performance (Chou & Jiang, 2022; Layeghy & Portmann, 2023). The second cluster concerns detection coverage: passive attacks such as eavesdropping remain under-addressed relative to the threat they pose to confidentiality, even though traffic- and signal-pattern analysis has been shown to detect interception with high accuracy (Bilal et al., 2025; Mansour & Khedr, 2025). The third cluster concerns the learning-based defenses this survey highlights. In federated learning, privacy preservation does not prevent poisoning — a malicious participant can inject a backdoor by uploading poisoned data or models, a single Byzantine client can control plain averaging, and robust aggregation rules degrade sharply on the non-IID data that characterise real WSNs (S. Li et al., 2024b; Lyu et al., 2024; Wan et al., 2024). In explainable AI, explanation quality, fidelity, stability, and overhead are rarely measured, and computationally intensive explainers such as SHAP and LIME require model evaluations proportional to feature dimensionality, rendering real-time inference-time explanation on constrained nodes infeasible k(Karras et al., 2026; Slaoui, 2026b). Finally, because energy and security work in opposition — as security complexity increases, battery drain increases (Ahmad et al., 2022) — the field still lacks

standardized, quantitative reporting of the energy, latency, and communication costs of detection and explanation. Table 5 summarises these gaps and maps each to concrete future directions.

Table 5: Summary of Research Gaps and Corresponding Future Directions

Gap	Evidence/Issue	Required Research Direction
Realistic datasets	Many studies rely on benchmark network datasets instead of real WSN traffic (Chou & Jiang, 2022).	Create and publish realistic WSN datasets from varied settings
Detecting passive attacks	Eavesdropping leaves limited direct evidence	Use behaviour, radio, and traffic patterns as indicators
Evaluation beyond accuracy	Accuracy can hide failures in smaller classes (Vandana & Verma, 2025).	Report precision, recall, F1, MCC, AUROC/AUPRC, FPR and confusion matrices
Energy-awareness	Deep and federated learning can add processing and communication costs	Measure joules, latency, memory and network lifetime
Concept drift	Normal WSN behaviour changes with environment and topology	Use adaptive thresholds and continual/online learning
Explainability	Few studies measure explanation quality and cost	Evaluate fidelity, stability, latency and energy cost
FL robustness	Privacy does not prevent poisoning (Wan et al., 2024).	Test Byzantine, Sybil, backdoor and inference attacks
Detection-mitigation gap	Many studies stop at classification	Add automatic response and safe recovery
Regional deployment	Constraints in developing regions are underrepresented	Evaluate connectivity, power, affordability, and local regulatory requirements
Reproducibility	Different preprocessing and splits hinder comparison	Publish code, configurations, datasets and evaluation protocols

Lack of Integrated Detection Frameworks: We have tools to detect data theft and eavesdropping, but we still lack one framework that handles both threats (Gawdan et al., n.d.). Existing frameworks typically focus on either data tampering or eavesdropping detection in isolation, leaving networks vulnerable to combined attacks. Bringing active- and passive-attack detection into one architecture remains difficult.

Computational and Energy Constraints: Many ML/DL-based detection approaches use substantial computing power and energy, which shortens network life and makes them unsuitable for WSNs with limited resources (Alcaraz et al., 2012; Hosseini Shirvani & Akbarifar, 2024). Because sensor nodes have limited resources, traditional heavyweight security methods do not work well in practice (Soundararajan et al., 2023). Lightweight deep learning models, model compression, pruning, and quantisation techniques enable on-node detection without offloading.

Limited Eavesdropping Detection Research: Limited Eavesdropping Detection Research. Recent work shows that passive-attack detection from traffic and signal patterns is feasible: a 2025 framework profiles node communication behavior, models synthetic eavesdroppers, and trains a hybrid ResNet-LSTM on fused physical- and network-layer features — including signal fluctuation, unexplained packet bursts, and routing anomalies — scored with Mahalanobis distance and classified by fuzzy threat-level inference, achieving 98.76% detection accuracy, a 3.3% false-positive rate, and 46.5 ms latency in heterogeneous WSNs (Bilal et al., 2025). Related hybrid architectures, such as a 2026 GRU-LSTM model for multi-class network-layer attacks (blackhole, flooding, selective forwarding), extend this pattern-based direction (Sharma et al., 2026). The gap we identify is therefore not the absence of such detectors but three unresolved sub-problems. First, dataset scarcity and generalization: passive-attack corpora remain scarce relative to active-attack benchmarks, and classifiers trained on modeled eavesdropping scenarios have not been shown to generalize to covert, adaptive passive adversaries that deliberately minimize their footprint in

traffic statistics (Mansour & Khedr, 2025). Second, node-level energy accounting: hybrid detectors with millisecond-scale latency are demonstrated in simulated or testbed conditions, but their energy per detection cycle on actual motes is not quantified in standardized units, consistent with the broader scarcity of energy reporting identified in Section 4.4 (Subhan et al., 2026). Third, integration: existing hybrid frameworks operate in a centralized mode, and combining physical-layer eavesdropping indicators with privacy-preserving federated training — as well as co-detecting passive eavesdropping and active data theft in one architecture — remains open. More research is needed on detecting passive interception without active interference. This calls for simple signals from device behaviour, radio channels, and traffic patterns that can reveal covert surveillance without disrupting the network. This calls for simple signals from device behaviour, radio channels, and traffic patterns that can reveal covert surveillance without disrupting the network.

Scalability Challenges: Many WSN security techniques become harder to scale as networks grow (Kouicem et al., 2018). Older detection methods often struggle in dynamic IoT WSNs with limited resources (Kouicem et al., 2018). Scalable solutions must balance detection accuracy with communication overhead, energy consumption, and processing requirements as networks grow from tens to thousands of nodes.

Contextual Research Gap: WSN technology is spreading across many settings, but few security frameworks address the infrastructure limits and application needs of developing regions such as Nigeria (Kunle et al., 2017; Ogundero et al., 2025; Olakanni, 2023). A useful framework must consider power reliability, connectivity, hardware heterogeneity, affordability, data governance, and the operational realities of remote sensor deployments.

Large-Scale Validation: Although large WSN datasets are available, few studies compare several detection methods across different datasets (Haque et al., 2024; Mishra et al., 2025). Testing across datasets helps us assess whether methods generalize across network configurations and attack scenarios.

Explainability Gap: While explainable AI has been applied to general IoT security, few WSN security frameworks use it for both detection and mitigation (Afnan Birahim et al., 2025; Sundararajan et al., 2017). Few studies measure explanation quality, fidelity, stability, latency, and energy use, so it is hard to tell whether XAI is practical for resource-constrained deployments (Slaoui, 2026b).

Limited Mitigation Integration: Most research focuses on detection without adequate attention to mitigation strategies(Tomic & McCann, 2017). Few studies bring detection and mitigation together in one framework. Detection should trigger clear responses—such as node isolation, route changes, key renewal, or alert escalation—but each response must be designed carefully so it does not disrupt the network.

Dataset and Reproducibility Issues: Researchers still struggle to find realistic datasets and reproduce results. Many studies use standard network datasets (e.g., NSL-KDD, UNSW-NB15, WSN-DS) rather than physical WSN traffic. These datasets often miss the physical, energy, radio, and environmental conditions of real WSNs (Subhan et al., 2026). Different preprocessing steps, train-test splits, and evaluation metrics also make studies hard to compare. To move the field forward, researchers should publish their code, configurations, datasets, and evaluation protocols.

8.2 Future Research Directions

These gaps point to several useful research directions:

i. Energy-Aware Adaptive Security: Develop energy-aware security that adjusts its intensity to each node's energy, the environment, or the threat level (Kouicem et al., 2018). Researchers should explore cryptographic protocols that adjust encryption as battery levels change and activate extra security only in high-risk situations.

ii. Hybrid Architectures: Schemes that combine real-time analytics with adaptive defences across network layers (Hussain et al., 2025); these combine lightweight statistical methods with more complex machine learning models through edge-cloud architectures.

iii. Lightweight Deep Learning: Building smaller deep-learning (DL) models for low-power devices so they can detect threats on the device without sending data elsewhere (Sakthimohan et al., 2024). Model compression, pruning, and quantisation techniques are promising approaches.

iv. Federated Learning for Privacy: Expanding federated-learning (FL) approaches, which train models without sharing raw data, for privacy-preserving intrusion detection, particularly in healthcare and other sensitive settings (Tabassum et al., 2022). We also need reliable ways to combine model updates and block attacks that corrupt the training data.

v. Explainable AI Integration: Using explainable AI (XAI) tools such as SHAP and LIME more deeply in WSN security frameworks can make their decisions easier to understand and act on (Samout et al., 2025). Quantification of explanation quality, fidelity, and overhead is needed.

vi. Context-Appropriate Solutions: Building security frameworks that fit local infrastructure limits and application needs in developing regions (Dr. IRUKA CHIJINDU ANUGWO, 2025). These frameworks should also account for power reliability, connectivity, affordability, and data governance.

vii. Real-World Validation: We need to move from simulation to practical implementation and use standard

evaluation metrics (Papadopoulos et al., 2013). Methods that fit each setting, track changing threats, and adjust energy use will help keep WSNs secure in unpredictable environments (Oztoprak et al., 2025).

viii. Emerging Technologies: Using 6G communication and lightweight cryptography can provide low latency, fast connections, and secure authentication on devices with limited resources (Moslehi, 2025).

9. Discussion

Research shows a clear shift from rule-based and statistical IDS to data-driven, explainable, and distributed learning systems. But newer methods do not simply replace older ones. Statistical methods remain useful because they can run near the sensor and screen data quickly. ML models can classify complex patterns at gateways. DL works best when enough data and computing power are available. XAI focuses on interpretability, while FL supports training across separate sites without moving local data. These technologies therefore solve different parts of the WSN security problem and are most useful when their roles are explicitly separated.

High benchmark accuracy does not guarantee that a system is ready for deployment. WSNs are cyber-physical systems (Tomic & McCann, 2017); legitimate environmental changes can resemble anomalies (OReilly et al., 2014), network conditions vary over time, and security actions can consume scarce energy (Ahmad et al., 2022). High-quality research should therefore emphasise the relationship between predictive performance and operational cost. This is particularly important when comparing centralised cloud models with edge or federated alternatives.

9.1 Implications for Developing Regions

In developing regions, including Nigeria, deployment context and infrastructure realities shape the security choices available to WSN designers. Because grid power is unreliable in many deployment areas, security mechanisms must be energy-efficient enough to operate on batteries for extended periods, and the gateways that link sensor fields to the wider network must be designed to function with bounded energy supplies (ZENNARO, 2010). Connectivity is similarly intermittent in many rural and semi-urban settings, so detection systems must continue to operate through occasional gateway or cloud access, buffering and securing data locally until a connection becomes available (ZENNARO, 2010). At the same time, deployments frequently mix devices with different sensing, processing, and security capabilities, which means security policies must be capable-aware rather than assuming uniform hardware. Budget constraints compound these technical limits: lightweight security that works without expensive infrastructure is a precondition for adoption rather than an optional optimisation (ZENNARO, 2010). Regulatory requirements add a further layer, since local data protection legislation — such as the Nigeria Data Protection Act 2023 — mandates that data handling and privacy requirements be designed into systems from the outset (Aloamaka, 2025). Finally, because remote sensor sites often have little on-site technical support, security mechanisms must be robust, self-maintaining, and straightforward to operate over long deployments.

9.2 Emerging Technologies

Several emerging technologies are likely to reshape the practical envelope of WSN security. Sixth-generation (6G) communication promises very low latency and high reliability, which would support new security designs and accelerate detection and response in time-critical applications (Nguyen et al., 2021). Post-quantum and lightweight cryptographic schemes offer a path to protecting resource-constrained devices even in a future quantum era, in which conventional public-key systems may no longer be safe (Kumari et al., 2022). Edge AI brings threat detection closer to the data source: as edge processors grow more capable, lightweight inference can screen traffic locally and reserve cloud analysis for events that genuinely require it (Kumar, 1994b). Digital twins provide a complementary tool for security engineering, allowing configurations and responses to be tested against faithful virtual replicas of the physical network without risking live infrastructure (Alcaraz et al., 2026). Blockchain, for its part, offers tamper-resistant audit trails and distributed trust management, strengthening accountability across multi-owner deployments (Alagha & Özçelik, 2025). Realised together, these technologies — combined with the federated learning and explainable AI discussed earlier in this survey — could support security systems that are resilient, adaptive, and practical for resource-limited WSNs.

10. Limitations of the Survey

This survey is necessarily bounded in four ways, and its conclusions should be read in that light. First, in scope: it is a broad review, but it does not exhaust the literature, and some relevant works will inevitably have been missed. Second, in evaluative power: the performance figures surveyed come from heterogeneous studies that use different datasets, attack patterns, preprocessing steps, train-test splits, hardware, and evaluation measures, so they do not constitute a controlled head-to-head comparison and cannot be ranked directly against one another. Third, in reference currency: foundational references have been retained where they define core concepts, and future revisions should substitute newer primary studies as evidence matures. Fourth, in regional coverage: the survey identifies developing-region contexts but gives limited detail on specific regions, and

future work should expand this analysis with context-specific deployments and evaluations.

11. Conclusions

Wireless sensor network cybersecurity is moving toward adaptive, data-driven, and distributed detection. Yet real-world deployment must still balance limits on energy, computing power, communication, privacy, and explainability. This survey shows that statistical detection, classical machine learning, deep learning, explainable AI, and federated learning work best as a team. A resource-aware design can combine them: lightweight methods screen data near sensors, stronger models examine suspicious events at gateways or fog resources, XAI explains decisions, and FL supports privacy-preserving collaboration when appropriate.

Several findings from the surveyed literature support this view. Traditional signature-based and anomaly-based methods provide a basic layer of security, but they struggle in the dynamic WSN environments where resources are limited (G & Meenakshisundaram, 2025; Kipongo et al., 2023). Machine learning and deep learning techniques have shown strong results, with Random Forest reaching 98%–99.5% accuracy (Alsahli et al., 2021) and deep learning architectures exceeding 99% detection rates in some studies when tested under suitable conditions (Sadia et al., 2024). Explainable AI techniques such as SHAP and LIME help explain why the system made a decision, so teams can review and trust it (G & Meenakshisundaram, 2025; Gaspar et al., 2024). Federated learning offers a way to detect intrusions while protecting privacy: it cuts communication overhead and lets sites learn together without sharing raw data (Khraisat et al., 2025). At the same time, important gaps remain. We still lack integrated frameworks that protect against both data theft and eavesdropping; passive attacks receive little attention; developing regions need solutions that fit their context; and adaptive security still rarely accounts for energy limits.

The literature points, accordingly, to a concrete research agenda. We need realistic WSN security datasets that reflect the physical conditions of deployed sensor networks, and rigorous, reproducible evaluation with standardized measures and test procedures. Better detection of passive eavesdroppers should draw on behavior, radio and channel signals, and traffic patterns, while learning algorithms should adjust detection intensity to the resources available at each tier. The agenda likewise calls for robust federated IDS that are resilient to poisoning, Sybil, backdoor, and inference attacks; measurable XAI with quantified fidelity, stability, and overhead; integrated detection-and-mitigation mechanisms with safe automated responses; and solutions suited to developing regions that account for power, connectivity, cost, and data governance.

Together, 6G communication, lightweight cryptography, federated learning, and explainable AI can build security systems that are resilient, adaptive, and practical for resource-limited WSNs (Ferrag et al., 2023; Nguyen et al., 2021). But we still need careful testing to balance strong security with the limits of real deployments.

Reference

Abedini, M., & Al-Anbagi, I. (2024). Enhanced Active Eavesdroppers Detection System for Multihop WSNs in Tactical IoT Applications. *IEEE Internet of Things Journal*, *11*(4), 6748–6760. https://doi.org/10.1109/JIOT.2023.3313048

Adadi, A., & Berrada, M. (2018). Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*, *6*, 52138–52160. https://doi.org/10.1109/ACCESS.2018.2870052

Afnan Birahim, S., Paul, A., Rahman, F., Islam, Y., Roy, T., Asif Hasan, M., Haque, F., & Chowdhury, M. E. H. (2025a). Intrusion Detection for Wireless Sensor Network Using Particle Swarm Optimization Based Explainable Ensemble Machine Learning Approach. *IEEE Access*, *13*, 13711–13730. https://doi.org/10.1109/ACCESS.2025.3528341

Afnan Birahim, S., Paul, A., Rahman, F., Islam, Y., Roy, T., Asif Hasan, M., Haque, F., & Chowdhury, M. E. H. (2025b). Intrusion Detection for Wireless Sensor Network Using Particle Swarm Optimization Based Explainable Ensemble Machine Learning Approach. *IEEE Access*, *13*, 13711–13730. https://doi.org/10.1109/ACCESS.2025.3528341

Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2022). Federated Learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications*, *195*, 346–361. https://doi.org/10.1016/j.comcom.2022.09.012

Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022). Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. *Sensors*, *22*(13), 4730. https://doi.org/10.3390/s22134730

Ahmed, A., Oluomachi, E., Abdullah, A., & Tochukwu, N. (2024). 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. *International Journal of Network Security & Its Applications*, *16*(2), 47–63. https://doi.org/10.5121/ijnsa.2024.16204

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey.

Computer Networks, *38*(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4

Alagha, B., & Özçelik, İ. (2025). Using Blockchain Technology for Audit Trail. In A. Perdana, S. V. Bharathi, R. Karim, S. Arifin, & A. Srivastava, *Digital Strategy and Governance in Transformative Technologies* (1st edn, pp. 239–259). CRC Press. https://doi.org/10.1201/9781003477808-14

Alcaraz, C., Guzman, H., & Lopez, J. (2026). Adaptive Digital Twin: Protection, deception, and testing. *Future Generation Computer Systems*, *179*, 108357. https://doi.org/10.1016/j.future.2025.108357

Alcaraz, C., Lopez, J., Roman, R., & Chen, H.-H. (2012). Selecting key management schemes for WSN applications. *Computers & Security*, *31*(8), 956–966. https://doi.org/10.1016/j.cose.2012.07.002

Al-Fuhaidi, B., Farae, Z., Al-Fahaidy, F., Nagi, G., Ghallab, A., & Alameri, A. (2024). Anomaly-Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms. *Applied Computational Intelligence and Soft Computing*, *2024*(1), 2625922. https://doi.org/10.1155/2024/2625922

Ali, H., Tariq, U. U., Hussain, M., Lu, L., Panneerselvam, J., & Zhai, X. (2021a). ARSH-FATI: A Novel Metaheuristic for Cluster Head Selection in Wireless Sensor Networks. *IEEE Systems Journal*, *15*(2), 2386–2397. https://doi.org/10.1109/JSYST.2020.2986811

Ali, H., Tariq, U. U., Hussain, M., Lu, L., Panneerselvam, J., & Zhai, X. (2021b). ARSH-FATI: A Novel Metaheuristic for Cluster Head Selection in Wireless Sensor Networks. *IEEE Systems Journal*, *15*(2), 2386–2397. https://doi.org/10.1109/JSYST.2020.2986811

Aljanabi, M., Ismail, M. A., & Ali, A. H. (2021). Intrusion Detection Systems, Issues, Challenges, and Needs: *International Journal of Computational Intelligence Systems*, *14*(1), 560. https://doi.org/10.2991/ijcis.d.210105.001

Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications*, *11*(6), 6–28. https://doi.org/10.1109/MWC.2004.1368893

AlNusif, M. (2025). Explainable AI in Edge Devices: A Lightweight Framework for Real-Time Decision Transparency. *International Journal of Engineering and Computer Science*, *14*(07), 27447–27472. https://doi.org/10.18535/ijecs.v14i07.5181

Aloamaka, P. C. A. (2025). A CRITICAL ANALYSIS OF THE NIGERIA DATA PROTECTION ACT 2023: ELEVATING STANDARDS TO GLOBAL NORMS. *UCC Law Journal*, *4*(2), 242–263. https://doi.org/10.47963/ucclj.v4i2.1724

Al-Quayed, F., Ahmad, Z., & Humayun, M. (2024). 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*, 34800–34819. https://doi.org/10.1109/ACCESS.2024.3372187

Alsahli, M. S., Almasri, M. M., Al-Akhras, M., Al-Issa, A. I., & Alawairdhi, M. (2021). Evaluation of Machine Learning Algorithms for Intrusion Detection System in WSN. *International Journal of Advanced Computer Science and Applications*, *12*(5). https://doi.org/10.14569/IJACSA.2021.0120574

Alsaleh, S. S., El Bachir Menai, M., & Al-Ahmadi, S. (2024). Federated Learning-Based Model to Lightweight IDSs for Heterogeneous IoT Networks: State-of-the-Art, Challenges, and Future Directions. *IEEE Access*, *12*, 134256–134272. https://doi.org/10.1109/ACCESS.2024.3460468

Anwer, R. W., Abrar, M., Salam, A., & Ullah, F. (2025). TEAD: Trust-enhanced anomaly detection framework for intrusion detection in IoT-enabled wireless sensor networks (WSNs). *Wireless Networks*, *31*(6), 4179–4197. https://doi.org/10.1007/s11276-025-03987-3

Arreche, O., Guntur, T. R., Roberts, J. W., & Abdallah, M. (2024). E-XAI: Evaluating Black-Box Explainable AI Frameworks for Network Intrusion Detection. *IEEE Access*, *12*, 23954–23988. https://doi.org/10.1109/ACCESS.2024.3365140

Arshad, J., Azad, M. A., Abdeltaif, M. M., & Salah, K. (2020). An intrusion detection framework for energy constrained IoT devices. *Mechanical Systems and Signal Processing*, *136*, 106436. https://doi.org/10.1016/j.ymssp.2019.106436

Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2018). *How To Backdoor Federated Learning* (Version 3). arXiv. https://doi.org/10.48550/ARXIV.1807.00459

Baviskar, P. V., Balpande, V., Jadhav, T., Naidu, S. M. M., Sharma, A., & Minhas, D. (2025). Analyzing the impact of network topology on cryptographic security and data integrity in IoT applications. *Journal of Discrete Mathematical Sciences and Cryptography*, *28*(5-B), 1813–1824. https://doi.org/10.47974/JDMSC-2181

Behiry, M. H., & Aly, M. (2024). Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. *Journal of Big Data*, *11*(1), 16. https://doi.org/10.1186/s40537-023-00870-w

Bhavya, B., Xiong, J., & Zhai, C. (2023). CAM: A Large Language Model-based Creative Analogy Mining Framework. *Proceedings of the ACM Web Conference 2023*, 3903–3914. https://doi.org/10.1145/3543507.3587431

Bhoi, B., Jethava, G., & Jethava, S. (2026). A Comprehensive Review of Anomaly Detection Techniques for Insider Threat Identification. *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)*, 1050–1056. https://doi.org/10.1109/ICAUC68182.2026.11440999

Bilal, N. M., Sivakumar, R., Alqawasmi, K., Gopila, M., Poojasree, P., & R.Suganthi. (2025). A Robust Interception Behavioral Analysis over Wireless Sensor Network Environment to Identify the Existence of Eavesdropping Attack. *2025 International Conference on Recent Innovation in Science Engineering and Technology (ICRISET)*, 1–10. https://doi.org/10.1109/ICRISET64803.2025.11252019

Bout, E., Loscri, V., & Gallais, A. (2022). How Machine Learning Changes the Nature of Cyberattacks on IoT Networks: A Survey. *IEEE Communications Surveys & Tutorials*, *24*(1), 248–279. https://doi.org/10.1109/COMST.2021.3127267

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

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Butun, I., Osterberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364

C, V., S, J., & B, R. (2023). Incentive-based Energy-efficient Federated Learning Aggregation for Intrusion Detection in IoT Sensor Network. *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–6. https://doi.org/10.1109/ICCCNT56998.2023.10306340

Cahyo, A. N., Kartika Sari, A., & Riasetiawan, M. (2020). Comparison of Hybrid Intrusion Detection System. *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 92–97. https://doi.org/10.1109/ICITEE49829.2020.9271727

Cajaraville-Aboy, D., Fernández-Vilas, A., Díaz-Redondo, R. P., & Fernández-Veiga, M. (2025). Byzantine-Robust Aggregation for Securing Decentralized Federated Learning. *IEEE Access*, *13*, 190947–190963. https://doi.org/10.1109/ACCESS.2025.3629864

Cao, X., Fang, M., Liu, J., & Gong, N. Z. (2021). FLTrust: Byzantine-robust Federated Learning via Trust Bootstrapping. *Proceedings 2021 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2021.24434

Ceviz, O., Sadioglu, P., Sen, S., & Vassilakis, V. G. (2025). A novel federated learning-based IDS for enhancing UAVs privacy and security. *Internet of Things*, *31*, 101592. https://doi.org/10.1016/j.iot.2025.101592

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*(3), 1–58. https://doi.org/10.1145/1541880.1541882

Chen, Y., & Li, S. (2019). A Lightweight Anomaly Detection Method Based on SVDD for Wireless Sensor Networks. *Wireless Personal Communications*, *105*(4), 1235–1256. https://doi.org/10.1007/s11277-019-06143-1

Chou, D., & Jiang, M. (2022). A Survey on Data-driven Network Intrusion Detection. *ACM Computing Surveys*, *54*(9), 1–36. https://doi.org/10.1145/3472753

Conti, M., Donadel, D., & Turrin, F. (2021). A Survey on Industrial Control System Testbeds and Datasets for Security Research. *IEEE Communications Surveys & Tutorials*, *23*(4), 2248–2294. https://doi.org/10.1109/COMST.2021.3094360

Corona, J., Rodrigues, P., Almeida, L., Teixeira, R., Antunes, M., & Aguiar, R. (2023). *From Black Box to Transparency: The hidden costs of XAI in NGN*. In Review. https://doi.org/10.21203/rs.3.rs-3714524/v1

Cover, T., & Hart, P. (1967). Nearest neighbor pattern classification. *IEEE Transactions on Information Theory*, *13*(1), 21–27. https://doi.org/10.1109/TIT.1967.1053964

Cui, L., Su, X., Zhou, Y., & Pan, Y. (2021). Slashing Communication Traffic in Federated Learning by Transmitting Clustered Model Updates. *IEEE Journal on Selected Areas in Communications*, *39*(8), 2572–2589. https://doi.org/10.1109/JSAC.2021.3087262

De Carvalho Bertoli, G., Alves Pereira Junior, L., Saotome, O., & Dos Santos, A. L. (2023). Generalizing intrusion detection for heterogeneous networks: A stacked-unsupervised federated learning approach. *Computers & Security*, *127*, 103106. https://doi.org/10.1016/j.cose.2023.103106

Denning, D. E. (1987). An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*, *SE-13*(2), 222–232. https://doi.org/10.1109/TSE.1987.232894

Department of Computer Science, Virtual University of Pakistan, Lahore, 54000, Noman Riaz, M., Buriro, A., & Mahboob, A. (2018). Classification of Attacks on Wireless Sensor Networks: A Survey. *International Journal of Wireless and Microwave Technologies*, *8*(6), 15–39. https://doi.org/10.5815/ijwmt.2018.06.02

Dietterich, T. G. (2000). Ensemble Methods in Machine Learning. In G. Goos, J. Hartmanis, & J. Van Leeuwen (Eds), *Multiple Classifier Systems* (Vol. 1857, pp. 1–15). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45014-9_1

Diop, A., Qi, Y., Wang, Q., & Hussain, S. (2013). *An Advanced Survey on Secure Energy-Efficient Hierarchical Routing Protocols in Wireless Sensor Networks*. https://doi.org/10.48550/ARXIV.1306.4595

Dora, S. S., & Swain, P. K. (2024). Energy Efficient Wireless Sensor Networks using Support Vector Machine. In S. Sethi, B. Sahoo, D. Tosh, S. Kumar Jayasingh, & S. Kumar Bhoi, *Computing, Communication and Intelligence* (1st edn, pp. 132–135). CRC Press. https://doi.org/10.1201/9781003581215-27

Dr. IRUKA CHIJINDU ANUGWO. (2025). *KEY CYBERSECURITY CHALLENGES FOR DEVELOPING COUNTRIES' SMART INFRASTRUCTURE ASSETS MANAGEMENT: A NARRATIVE REVIEW*. https://doi.org/10.5281/ZENODO.17918975

El Ahmar, E., Rachini, A., & Attar, H. (2024). Cybersecurity Enhancement in IoT Wireless Sensor Networks using Machine Learning. *WSEAS TRANSACTIONS ON INFORMATION SCIENCE AND APPLICATIONS*, *21*, 480–487. https://doi.org/10.37394/23209.2024.21.43

Emmanuel, I., O., M., O., I., & A., I. (2018). Design and Implementation of Farm Monitoring and Security System. *International Journal of Computer Applications*, *181*(9), 10–15. https://doi.org/10.5120/ijca2018917598

Ergün, S. (2023). EXPLAINING XGBOOST PREDICTIONS WITH SHAP VALUE: A COMPREHENSIVE GUIDE TO INTERPRETING DECISION TREE-BASED MODELS. *New Trends in Computer Sciences*, *1*(1), 19–31. https://doi.org/10.3846/ntcs.2023.17901

Fang, M., Nabavirazavi, S., Liu, Z., Sun, W., Iyengar, S., & Yang, H. (2025). Do We Really Need to Design New Byzantine-robust Aggregation Rules? *Proceedings 2025 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2025.241796

Fawaz. (2012). A Survey of Intrusion Detection Schemes in Wireless Sensor Networks. *American Journal of Applied Sciences*, *9*(10), 1636–1652. https://doi.org/10.3844/ajassp.2012.1636.1652

Ferrag, M. A., Friha, O., Kantarci, B., Tihanyi, N., Cordeiro, L., Debbah, M., Hamouda, D., Al-Hawawreh, M., & Choo, K.-K. R. (2023). Edge Learning for 6G-Enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses. *IEEE Communications Surveys & Tutorials*, *25*(4), 2654–2713. https://doi.org/10.1109/COMST.2023.3317242

G, S., & Meenakshisundaram, N. (2025). Explainable Hybrid Intrusion Detection Systems for Transparent and Trustworthy Wireless Sensor Network Security. *2025 International Conference on Sustainable Communication Networks and Application (ICSCN)*, 835–840. https://doi.org/10.1109/ICSCN67106.2025.11308301

Gajewski, M., Batalla, J. M., Mastorakis, G., & Mavromoustakis, C. X. (2019). A distributed IDS architecture model for Smart Home systems. *Cluster Computing*, *22*(S1), 1739–1749. https://doi.org/10.1007/s10586-017-1105-z

García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

Gardiner, J., & Nagaraja, S. (2017). On the Security of Machine Learning in Malware C&C Detection: A Survey. *ACM Computing Surveys*, *49*(3), 1–39. https://doi.org/10.1145/3003816

Gaspar, D., Silva, P., & Silva, C. (2024). Explainable AI for Intrusion Detection Systems: LIME and SHAP Applicability on Multi-Layer Perceptron. *IEEE Access*, *12*, 30164–30175. https://doi.org/10.1109/ACCESS.2024.3368377

Gatate, V., & Agarkhed, J. (2024). Enhancing intrusion detection in wireless sensor networks through deep hybrid network empowered by SC-attention mechanism. *Iran Journal of Computer Science*, *7*(2), 229–240. https://doi.org/10.1007/s42044-024-00171-2

Gawdan, I. S., Chow, C.-O., Zia, T., & Gawdan, Q. I. (n.d.). Cross-layer based security solutions for wireless sensor networks. *International Journal of Physical Sciences*, *6*(17), 4245–4254.

Gayathri, S., & Surendran, D. (2024). Unified ensemble federated learning with cloud computing for online anomaly detection in energy-efficient wireless sensor networks. *Journal of Cloud Computing*, *13*(1), 49. https://doi.org/10.1186/s13677-024-00595-y

Goodfellow, I., Courville, A., & Bengio, Y. (2016). *Deep learning*. The MIT Press.

Goswami, P., Khan, T., Pathak, V., & Alabdultif, A. (2025). Machine learning based dynamic trust estimation framework for Securing wireless sensor networks. *Scientific Reports*, *15*(1), 35821. https://doi.org/10.1038/s41598-025-19768-z

Han, M., Benson, A., & Abon, J. E. (2025). Navigating ethics in wireless sensor networks for sustainable agriculture. *Frontiers in Sustainable Food Systems*, *9*, 1634643. https://doi.org/10.3389/fsufs.2025.1634643

Haque, A., Chowdhury, N.-U.-R., Soliman, H., Hossen, M. S., Fatima, T., & Ahmed, I. (2024). Wireless Sensor Networks Anomaly Detection Using Machine Learning: A Survey. In K. Arai (Ed.), *Intelligent Systems and Applications* (Vol. 824, pp. 491–506). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-47715-7_34

Hartung, C., Balasalle, J., & Han, R. (2005). *Node Compromise in Sensor Networks: The Need for Secure Systems* (Technical Report CU-CS-990-05). https://scholar.colorado.edu/downloads/6395w796s

Hassan, K., Madkour, M., & Nouh, S. (2023). A REVIEW OF SECURITY CHALLENGES AND SOLUTIONS IN WIRELESS SENSOR NETWORKS. *Journal of Al-Azhar University Engineering Sector*, *18*(69), 914–938. https://doi.org/10.21608/auej.2023.217015.1380

Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The Elements of Statistical Learning*. Springer New York. https://doi.org/10.1007/978-0-387-84858-7

Ho, J.-W., Wright, M., & Das, S. K. (2012). ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing. *IEEE Transactions on Dependable and Secure Computing*, *9*(4), 494–511. https://doi.org/10.1109/TDSC.2011.65

Hosseini Shirvani, M., & Akbarifar, A. (2024). A Survey Study on Intrusion Detection System in Wireless Sensor Network: Challenges and Considerations. *Journal of Electrical and Computer Engineering Innovations (JECEI)*, (Online First). https://doi.org/10.22061/jecei.2024.10148.683

Hu, K., Gong, S., Zhang, Q., Seng, C., Xia, M., & Jiang, S. (2024). An overview of implementing security and privacy in federated learning. *Artificial Intelligence Review*, *57*(8), 204. https://doi.org/10.1007/s10462-024-10846-8

Huma, Z. E., Jan, S. U., Ahmad, J., Buchanan, W., & Pitropakis, N. (2026). Adversarial Machine Learning in IoT Security: A Comprehensive Survey. *ACM Computing Surveys*, *58*(8), 1–35. https://doi.org/10.1145/3785665

Hussain, S., He, J., Zhu, N., Mughal, F. R., Ahmad, S., Hussain, M. I., & Zardari, Z. A. (2025). Edge AI-based self-learning technique for mitigating DDoS attacks in WSN. *Computer Networks*, *273*, 111769. https://doi.org/10.1016/j.comnet.2025.111769

Ibidunmoye, O., Hernández-Rodriguez, F., & Elmroth, E. (2015). Performance Anomaly Detection and Bottleneck Identification. *ACM Computing Surveys*, *48*(1), 1–35. https://doi.org/10.1145/2791120

Jegorova, M., Kaul, C., Mayor, C., O'Neil, A. Q., Weir, A., Murray-Smith, R., & Tsaftaris, S. A. (2022). Survey: Leakage and Privacy at Inference Time. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1–20. https://doi.org/10.1109/TPAMI.2022.3229593

Jimenez-Gutierrez, D. M., Falkouskaya, Y., Hernandez-Ramos, J. L., Anagnostopoulos, A., Chatzigiannakis, I., & Vitaletti, A. (2026). On the security and privacy of federated learning: A survey with attacks, defenses, frameworks, applications, and future directions. *Information Fusion*, *131*, 104155. https://doi.org/10.1016/j.inffus.2026.104155

Jing Deng, Han, R., & Mishra, S. (2004). Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks. *International Conference on Dependable Systems and Networks, 2004*, 637–646. https://doi.org/10.1109/DSN.2004.1311934

Jing Deng, Han, R., & Mishra, S. (2005). Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, 113–126. https://doi.org/10.1109/SECURECOMM.2005.16

Karl, H., & Willig, A. (2005). *Protocols and Architectures for Wireless Sensor Networks* (1st edn). Wiley. https://doi.org/10.1002/0470095121

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, *1*(2–3), 293–315. https://doi.org/10.1016/S1570-8705(03)00008-8

Karras, A., Giannaros, A., Amasiadi, N., & Karras, C. (2026). Next-Gen Explainable AI (XAI) for Federated and Distributed Internet of Things Systems: A State-of-the-Art Survey. *Future Internet*, *18*(2), 83. https://doi.org/10.3390/fi18020083

Khashan, O. A., Khafajah, N. M., Alomoush, W., & Alshinwan, M. (2024). Innovative Energy-Efficient Proxy Re-Encryption for Secure Data Exchange in Wireless Sensor Networks. *IEEE Access*, *12*, 23290–23304. https://doi.org/10.1109/ACCESS.2024.3360488

Khraisat, A., Talukder, Md. A., Uddin, Md. A., & Alazab, A. (2025). RF-FedAvg: Federated learning-based random forest model for intrusion detection in wireless sensor networks. *Cluster Computing*, *28*(13), 873. https://doi.org/10.1007/s10586-025-05591-8

King Faisal University, Alotaibi, E., Bin Sulaiman, R., Northumbria University, Almaiah, M., & The University of Jordan. (2025). Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks. *Journal of Cyber Security and Risk Auditing*, *2025*(1), 47–59. https://doi.org/10.63180/jcsra.thestap.2025.1.5

Kipongo, J., Swart, T. G., & Esenogho, E. (2023). Design and Implementation of Intrusion Detection Systems using RPL and AOVD Protocols-based Wireless Sensor Networks. *International Journal of Electronics and Telecommunications*, 309–318. https://doi.org/10.24425/ijet.2023.144366

Kissel, R. (2013). *Glossary of key information security terms* (NIST IR 7298r2; p. NIST IR 7298r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7298r2

Kök, İ., Okay, F. Y., Muyanlı, Ö., & Özdemir, S. (2023). Explainable Artificial Intelligence (XAI) for Internet of Things: A Survey. *IEEE Internet of Things Journal*, *10*(16), 14764–14779. https://doi.org/10.1109/JIOT.2023.3287678

Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). *Federated Learning: Strategies for Improving Communication Efficiency* (Version 2). arXiv. https://doi.org/10.48550/ARXIV.1610.05492

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199–221. https://doi.org/10.1016/j.comnet.2018.03.012

Kumar, S. (1994a). *A Pattern Matching Model for Misuse Intrusion Detection*. https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2169&context=cstech

Kumar, S. (1994b). *A Pattern Matching Model for Misuse Intrusion Detection* [Thesis, Purdue University]. https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2169&context=cstech

Kumari, S., Singh, M., Singh, R., & Tewari, H. (2022). Post-quantum cryptography techniques for secure communication in resource-constrained Internet of Things devices: A comprehensive survey. *Software: Practice and Experience*, *52*(10), 2047–2076. https://doi.org/10.1002/spe.3121

Kunle, O. J., Olubunmi, O. A., & Sani, S. (2017). Internet of things prospect in Nigeria: Challenges and solutions. *2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)*, 736–745. https://doi.org/10.1109/NIGERCON.2017.8281942

Layeghy, S., & Portmann, M. (2023). Explainable Cross-domain Evaluation of ML-based Network Intrusion Detection Systems. *Computers and Electrical Engineering*, *108*, 108692. https://doi.org/10.1016/j.compeleceng.2023.108692

Le Jeune, L., Goedeme, T., & Mentens, N. (2021). Machine Learning for Misuse-Based Network Intrusion Detection: Overview, Unified Evaluation and Feature Choice Comparison Framework. *IEEE Access*, *9*, 63995–64015. https://doi.org/10.1109/ACCESS.2021.3075066

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444. https://doi.org/10.1038/nature14539

Li, S., Ngai, E. C.-H., & Voigt, T. (2024a). An Experimental Study of Byzantine-Robust Aggregation Schemes in Federated Learning. *IEEE Transactions on Big Data*, *10*(6), 975–988. https://doi.org/10.1109/TBDATA.2023.3237397

Li, S., Ngai, E. C.-H., & Voigt, T. (2024b). An Experimental Study of Byzantine-Robust Aggregation Schemes in Federated Learning. *IEEE Transactions on Big Data*, *10*(6), 975–988. https://doi.org/10.1109/TBDATA.2023.3237397

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated Learning: Challenges, Methods, and Future Directions. *IEEE Signal Processing Magazine*, *37*(3), 50–60. https://doi.org/10.1109/MSP.2020.2975749

Liu, J. L., Shen, Y. S., Simsek, M. S., Kantarci, B. K., Mouftah, H. T. M., Bagheri, M. B., & Djukic, P. D. (n.d.). *SCVIC-APT-2021* [Data set]. IEEE DataPort. https://doi.org/10.21227/G2Z5-EP97

Liu, W., Liu, Z., Tsang, I., Zhang, W., & Lin, X. (2018). Doubly Approximate Nearest Neighbor Classification. *Proceedings of the AAAI Conference on Artificial Intelligence*, *32*(1). https://doi.org/10.1609/aaai.v32i1.11690

López-Ramírez, G. A., & Aragón-Zavala, A. (2023). Wireless Sensor Networks for Water Quality Monitoring: A Comprehensive Review. *IEEE Access*, *11*, 95120–95142. https://doi.org/10.1109/ACCESS.2023.3308905

Lu, Z., Pan, H., Dai, Y., Si, X., & Zhang, Y. (2024). Federated Learning With Non-IID Data: A Survey. *IEEE Internet of Things Journal*, *11*(11), 19188–19209. https://doi.org/10.1109/JIOT.2024.3376548

Lyu, L., Yu, H., Ma, X., Chen, C., Sun, L., Zhao, J., Yang, Q., & Yu, P. S. (2024). Privacy and Robustness in Federated Learning: Attacks and Defenses. *IEEE Transactions on Neural Networks and Learning Systems*, *35*(7), 8726–8746. https://doi.org/10.1109/TNNLS.2022.3216981

M Bishop, C. (2006). *Pattern recognition and machine learning*.

Maaz, M., Ahmed, G., Sami Al-Shamayleh, A., Akhunzada, A., Siddiqui, S., & Hussein Al-Ghushami, A. (2024). Empowering IoT Resilience: Hybrid Deep Learning Techniques for Enhanced Security. *IEEE Access*, *12*, 180597–180618. https://doi.org/10.1109/ACCESS.2024.3482005

Mache, J., Wan, C.-Y., & Yarvis, M. (2008). Exploiting Heterogeneity for Sensor Network Security. *2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 591–593. https://doi.org/10.1109/SAHCN.2008.80

Madathil, N. T., Dankar, F. K., Gergely, M., Belkacem, A. N., & Alrabaee, S. (2025). Revolutionizing healthcare data analytics with federated learning: A comprehensive survey of applications, systems, and future directions. *Computational and Structural Biotechnology Journal*, *28*, 217–238. https://doi.org/10.1016/j.csbj.2025.06.009

Mansour, Y., & Khedr, A. M. (2025). Passive Attacks and Their Recent Countermeasures in IoT-Based Wireless Sensor Networks: A Review. *2025 IEEE 22nd International Multi-Conference on Systems, Signals & Devices (SSD)*, 871–878. https://doi.org/10.1109/SSD64182.2025.10989910

Mary, O. O., Kennedy, O., King-David, M. O., Ijeh, A. P., & Okokpujie, I. P. (2025). Development of a Network Intrusion Detection Model using Hybridised Machine Learning Algorithms. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *13*(3), 558–568. https://doi.org/10.52549/ijeei.v13i3.5890

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. y. (2016a). *Communication-Efficient Learning of Deep Networks from Decentralized Data*. https://doi.org/10.48550/ARXIV.1602.05629

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. y. (2016b). *Communication-Efficient Learning of Deep Networks from Decentralized Data*. https://doi.org/10.48550/ARXIV.1602.05629

Megantara, A. A., & Ahmad, T. (2021). A hybrid machine learning method for increasing the performance of network intrusion detection systems. *Journal of Big Data*, *8*(1), 142. https://doi.org/10.1186/s40537-021-00531-w

Mensah, K., Diallo, A., Harouna, A., & Koffi, J.-C. (2026). IoT-enabled handheld tester for sachet water quality at point-of-sale in minna: Device integration and wireless data transfer. *International Journal of Materials Science*, *7*(1), 24–28. https://doi.org/10.22271/27078221.2026.v7.i1a.100

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39–53. https://doi.org/10.1145/997150.997156

Mishra, R., Jha, S. K., Prakash, S., & Rathore, R. S. (2025). HEXADWSN: Explainable Ensemble Framework for Robust and Energy-Efficient Anomaly Detection in WSNs. *Future Internet*, *17*(11), 520. https://doi.org/10.3390/fi17110520

Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, *46*(4), 1–29. https://doi.org/10.1145/2542049

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications*, *36*(1), 42–57. https://doi.org/10.1016/j.jnca.2012.05.003

Mohale, V. Z., & Obagbuwa, I. C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity. *Frontiers in Artificial Intelligence*, *8*, 1526221. https://doi.org/10.3389/frai.2025.1526221

Mohammad, A. A. S., Mohammad, S. I. S., Al Oraini, B., Vasudevan, A., Hindieh, A., Altarawneh, A., Alshurideh, M. T., & Ali, I. (2025). Strategies for applying interpretable and explainable AI in real world IoT applications. *Discover Internet of Things*, *5*(1), 71. https://doi.org/10.1007/s43926-025-00155-z

Moslehi, M. M. (2025). Exploring coverage and security challenges in wireless sensor networks: A survey. *Computer Networks*, *260*, 111096. https://doi.org/10.1016/j.comnet.2025.111096

Moss, J., Gordon, J., Duclos, W., Liu, Y., Wang, Q., & Wang, J. (2025). Explainable AI in IoT: A Survey of Challenges, Advancements, and Pathways to Trustworthy Automation. *Electronics*, *14*(23), 4622. https://doi.org/10.3390/electronics14234622

Naseri, M., Hayes, J., & De Cristofaro, E. (2022). Local and Central Differential Privacy for Robustness and Privacy in Federated Learning. *Proceedings 2022 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2022.23054

Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Vincent Poor, H. (2021). Federated Learning for Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *23*(3), 1622–1658. https://doi.org/10.1109/COMST.2021.3075439

Nisioti, A., Mylonas, A., Yoo, P. D., & Katos, V. (2018). From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods. *IEEE Communications Surveys & Tutorials*, *20*(4), 3369–3388. https://doi.org/10.1109/COMST.2018.2854724

Nizam, H., Zafar, S., Lv, Z., Wang, F., & Hu, X. (2022). Real-Time Deep Anomaly Detection Framework for Multivariate Time-Series Data in Industrial IoT. *IEEE Sensors Journal*, *22*(23), 22836–22849. https://doi.org/10.1109/JSEN.2022.3211874

Ogundero, M. A., Lawanson, T., Yinusa, A. A., Umoren, V., Agunbiade, F. O., Fashanu, T. A., & Amuda, M. O. H. (2025). A smart IoT cum citizen science framework for real-time remote water quality monitoring and assessment. *Discover Water*, *5*(1), 108. https://doi.org/10.1007/s43832-025-00299-7

Olakanni, O. O. (2023). *Development of secure framework for data harvesting and monitoring system for large scale farms*. A Research Sponsored by Nigerian Communications Commission.

Olayinka, T. C., Idebi, O. J., & Olayinka, A. S. (2026). *Smart IoT-Driven Domestic Water Quality Monitoring Systems: Architecture, Machine Learning Integration, and Implementation Challenges*. Computer Science and Mathematics. https://doi.org/10.20944/preprints202603.1804.v1

OReilly, C., Gluhak, A., Imran, M. A., & Rajasegarar, S. (2014). Anomaly Detection in Wireless Sensor Networks in a Non-Stationary Environment. *IEEE Communications Surveys & Tutorials*, *16*(3), 1413–1432. https://doi.org/10.1109/SURV.2013.112813.00168

Osamah Ahmed Mahmood. (2024). Enhancing Intrusion Detection in Wireless Sensor Networks through Machine Learning Techniques and Context Awareness Integration. *International Journal of Mathematics, Statistics, and Computer Science*, *1*, 244–258. https://doi.org/10.59543/ijmscs.v2i.10377

Özdemir, S. (2008). Wireless Sensor Network Security: A Comprehensive Overview. *Https://Dergipark.Org.Tr/En/Download/Article-File/384705*, *11*(3), 207–214.

Oztoprak, A., Hassanpour, R., Ozkan, A., & Oztoprak, K. (2025). Security Challenges, Mitigation Strategies, and Future Trends in Wireless Sensor Networks: A Review. *ACM Computing Surveys*, *57*(4), 1–29. https://doi.org/10.1145/3706583

Padmavathi, Dr. G., & Shanmugapriya, Mrs. D. (2009). *A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks*. https://doi.org/10.48550/ARXIV.0909.0576

Papadopoulos, G. Z., Beaudaux, J., Gallais, A., Noel, T., & Schreiner, G. (2013). Adding value to WSN simulation using the IoT-LAB experimental platform. *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 485–490. https://doi.org/10.1109/WiMOB.2013.6673403

Parvizi, N., Saha, S., & Shahriar, N. (2026). RAID: A Reputation-Based Aggregation for Intrusion Detection in Federated Learning. *2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC)*, 1–6. https://doi.org/10.1109/CCNC65079.2026.11366587

Patcha, A., & Park, J.-M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, *51*(12), 3448–3470. https://doi.org/10.1016/j.comnet.2007.02.001

Pathan, A. S. K., Hyung-Woo Lee, & Choong Seon Hong. (2006). Security in wireless sensor networks: Issues and challenges. *2006 8th International Conference Advanced Communication Technology*, 6 pp. – 1048. https://doi.org/10.1109/ICACT.2006.206151

Pawlicki, M., Pawlicka, A., Kozik, R., & Choraś, M. (2024). The survey on the dual nature of xAI challenges in intrusion detection and their potential for AI innovation. *Artificial Intelligence Review*, *57*(12), 330. https://doi.org/10.1007/s10462-024-10972-3

Perifanis, V., Pavlidis, N., Koutsiamanis, R.-A., & Efraimidis, P. S. (2023). Federated learning for 5G base station traffic forecasting. *Computer Networks*, *235*, 109950. https://doi.org/10.1016/j.comnet.2023.109950

Pongle, P., & Chavan, G. (2015). Real Time Intrusion and Wormhole Attack Detection in Internet of Things. *International Journal of Computer Applications*, *121*(9), 1–9. https://doi.org/10.5120/21565-4589

PPG Institute of Technology, India, V, B., A, C. P., Karpagam Institute of Technology, India, B, T., & Queensland University of Technology, Australia. (2025). ENHANCED INTRUSION DETECTION AND PREVENTION IN WIRELESS SENSOR NETWORKS USING HYBRID DEEP LEARNING. *ICTACT Journal on Communication Technology*, *16*(1), 3454–3458. https://doi.org/10.21917/ijct.2025.0513

Quisquater, J.-J., & Samyde, D. (2001). ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. In I. Attali & T. Jensen (Eds), *Smart Card*

Programming and Security (Vol. 2140, pp. 200–210). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45418-7_17

Rajapaksha, S., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., Madzudzo, G., & Cheah, M. (2023). AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey. *ACM Computing Surveys*, *55*(11), 1–40. https://doi.org/10.1145/3570954

Rajawat, A. S., Goyal, S. B., & Hussein, A. A. (2024). Cybersecurity Challenges and Solutions in Wireless Sensor Networks: A Comprehensive Review. *2024 International Conference on Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA)*, 1–7. https://doi.org/10.1109/ARIIA63345.2024.11051751

Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks*, *11*(8), 2661–2674. https://doi.org/10.1016/j.adhoc.2013.04.014

Robacky Mbongo, K. H., Ahmed, K., Mamyrbayev, O., Wang, G., Zuo, F., Akhmediyarova, A., Mukazhanov, N., & Ayapbergenova, A. (2025). Conv1D-GRU-Self Attention: An Efficient Deep Learning Framework for Detecting Intrusions in Wireless Sensor Networks. *Future Internet*, *17*(7), 301. https://doi.org/10.3390/fi17070301

Roesch, M. (1999, November 7). S N O R T — L I G H T W E I G H T I N T R U S I O N D E T E C T I O N F O R N E T W O R K S. *Proceedings of LISA '99: 13th Systems Administration Conference,*. https://www.usenix.org/legacy/event/lisa99/full_papers/roesch/roesch.pdf?utm_source=chatgpt.com

Sadia, H., Farhan, S., Haq, Y. U., Sana, R., Mahmood, T., Bahaj, S. A. O., & Khan, A. R. (2024). Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach. *IEEE Access*, *12*, 52565–52582. https://doi.org/10.1109/ACCESS.2024.3380014

Sakthimohan, M., Deny, J., & Rani, G. E. (2024). Secure deep learning-based energy efficient routing with intrusion detection system for wireless sensor networks. *Journal of Intelligent & Fuzzy Systems*, *46*(4), 8587–8603. https://doi.org/10.3233/JIFS-235512

Saleh, H. M., Marouane, H., & Fakhfakh, A. (2024). A Comprehensive Analysis of Security Challenges and Countermeasures in Wireless Sensor Networks Enhanced by Machine Learning and Deep Learning Technologies. *International Journal of Safety and Security Engineering*, *14*(2), 373–386. https://doi.org/10.18280/ijsse.140206

Samout, N., Gouasmi, T., & Nasri, N. (2025). Explainable AI-based innovative models for intrusion detection in Big Data WSN. *Procedia Computer Science*, *270*, 5065–5072. https://doi.org/10.1016/j.procs.2025.09.633

Sathishkumar, P., Gnanabaskaran, A., Saradha, M., & Gopinath, R. (2024). Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network. *Ain Shams Engineering Journal*, *15*(12), 103052. https://doi.org/10.1016/j.asej.2024.103052

Sefati, S. S., Arasteh, B., Halunga, S., & Fratu, O. (2025). A comprehensive survey of cybersecurity techniques based on quality of service (QoS) on the Internet of Things (IoT). *Cluster Computing*, *28*(12), 792. https://doi.org/10.1007/s10586-025-05449-z

Sharma, H., Kumar, P., & Sharma, K. (2026). Security Solutions for the Internet of Things Using Machine Learning and Deep Learning: Current Trends and Future Directions. *WIREs Data Mining and Knowledge Discovery*, *16*(1), e70059. https://doi.org/10.1002/widm.70059

Shokri, R., Theodorakopoulos, G., Le Boudec, J.-Y., & Hubaux, J.-P. (2011). Quantifying Location Privacy. *2011 IEEE Symposium on Security and Privacy*, 247–262. https://doi.org/10.1109/SP.2011.18

Shokunbi, O., Agbaje, M., & Ogu, E. (2026). MEASURING NIGERIA DATA PROTECTION ACT (NDPA) 2023 COMPLIANCE IN NIGERIAN UNIVERSITIES: A GENERAL COMPLIANCE INDEX AND EVIDENCE OF INSTITUTIONAL DECOUPLING. *FUDMA JOURNAL OF SCIENCES*, *10*(6), 291–296. https://doi.org/10.33003/fjs-2026-1006-5085

Slaoui, S. (2026a). S-AI-IOT: A SPARSE ARTIFICIAL INTELLIGENCE ARCHITECTURE WITH HORMONAL ORCHESTRATION, PARSIMONIOUS AGENT ACTIVATION, AND SYMBOLIC MEMORY FOR ADAPTIVE, SECURE, AND EXPLAINABLE INTERNET OF THINGS SYSTEMS. *International Journal of Artificial Intelligence & Applications*, *17*(3), 01–25. https://doi.org/10.5121/ijaia.2026.17301

Slaoui, S. (2026b). S-AI-IOT: A SPARSE ARTIFICIAL INTELLIGENCE ARCHITECTURE WITH HORMONAL ORCHESTRATION, PARSIMONIOUS AGENT ACTIVATION, AND SYMBOLIC MEMORY FOR ADAPTIVE, SECURE, AND EXPLAINABLE INTERNET OF THINGS SYSTEMS. *International Journal of Artificial Intelligence & Applications*, *17*(3), 01–25. https://doi.org/10.5121/ijaia.2026.17301

Soundararajan, S., R. Tapas Bapu, B., Kotteeswaran, C., Venkatasubramanian, S., J. Sathish Kumar, P., & Mudassar Ali, A. (2023). Modified Adhoc On-Demand

Distance Vector for Trust Evaluation And Attack Detection. *Intelligent Automation & Soft Computing*, *36*(2), 1227–1240. https://doi.org/10.32604/iasc.2023.025752

Subbiah, S., Anbananthen, K. S. M., Thangaraj, S., Kannan, S., & Chelliah, D. (2022). Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm. *Journal of Communications and Networks*, *24*(2), 264–273. https://doi.org/10.23919/JCN.2022.000002

Subhan, R. M., Lee, Y.-D., & Koo, I. (2026). Autoencoder-Based Self-Supervised Anomaly Detection in Wireless Sensor Networks: A Taxonomy-Driven Meta-Synthesis. *Applied Sciences*, *16*(3), 1448. https://doi.org/10.3390/app16031448

Tabassum, A., Erbad, A., Lebda, W., Mohamed, A., & Guizani, M. (2022). FEDGAN-IDS: Privacy-preserving IDS using GAN and Federated Learning. *Computer Communications*, *192*, 299–310. https://doi.org/10.1016/j.comcom.2022.06.015

Tan, Y. K. (Ed.). (2010). *Sustainable Wireless Sensor Networks*. InTech. https://doi.org/10.5772/663

Tomic, I., & McCann, J. A. (2017). A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. *IEEE Internet of Things Journal*, *4*(6), 1910–1923. https://doi.org/10.1109/JIOT.2017.2749883

Torabi, H., Mirtaheri, S. L., & Greco, S. (2023). Practical autoencoder based anomaly detection by using vector reconstruction error. *Cybersecurity*, *6*(1), 1. https://doi.org/10.1186/s42400-022-00134-9

Vandana, V., & Verma, R. (2025). Evaluating Effectiveness: A Critical Review of Performance Metrics in Intrusion Detection System. *Journal of Engineering Science and Technology Review*, *18*(1), 199–209. https://doi.org/10.25103/jestr.181.20

Vapnik, V. N. (2000). *The Nature of Statistical Learning Theory*. Springer New York. https://doi.org/10.1007/978-1-4757-3264-1

Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M., & Fischer, M. (2015). Taxonomy and Survey of Collaborative Intrusion Detection. *ACM Computing Surveys*, *47*(4), 1–33. https://doi.org/10.1145/2716260

Vergutz, A., Medeiros, I., Rosario, D., Cerqueira, E., Santos, A., & Nogueira, M. (2019). A Method for Identifying eHealth Applications Using Side-Channel Information. *2019 IEEE Global Communications Conference (GLOBECOM)*, 1–6. https://doi.org/10.1109/GLOBECOM38437.2019.9013503

Wan, Y., Qu, Y., Ni, W., Xiang, Y., Gao, L., & Hossain, E. (2024). Data and Model Poisoning Backdoor Attacks on Wireless Federated Learning, and the Defense Mechanisms: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *26*(3), 1861–1897. https://doi.org/10.1109/COMST.2024.3361451

Wang, Y., & Li, G. (2013). Incremental histogram based anomaly detection scheme in wireless sensor networks. *2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013)*, 1–5. https://doi.org/10.1109/ICSPCC.2013.6663899

Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. *Computer*, *35*(10), 54–62. https://doi.org/10.1109/MC.2002.1039518

Wu, C., Wu, F., Lyu, L., Huang, Y., & Xie, X. (2022). Communication-efficient federated learning via knowledge distillation. *Nature Communications*, *13*(1), 2032. https://doi.org/10.1038/s41467-022-29763-x

Xie, M., Hu, J., & Tian, B. (2012). Histogram-Based Online Anomaly Detection in Hierarchical Wireless Sensor Networks. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 751–759. https://doi.org/10.1109/TrustCom.2012.173

Yahyaoui, A., Abdellatif, T., & Attia, R. (2019). Hierarchical anomaly based intrusion detection and localization in IoT. *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 108–113. https://doi.org/10.1109/IWCMC.2019.8766574

Yang, K., Ren, J., Zhu, Y., & Zhang, W. (2018). Active Learning for Wireless IoT Intrusion Detection. *IEEE Wireless Communications*, *25*(6), 19–25. https://doi.org/10.1109/MWC.2017.1800079

Yeng, P. K., & Gebrie, M. (2026a). *Multi-Signal TrustFed-Honeypot: A Trust-Aware Federated Intrusion Detection Framework with Comparative Evaluation*. Zenodo. https://doi.org/10.5281/ZENODO.18786478

Yeng, P. K., & Gebrie, M. (2026b). *Multi-Signal TrustFed-Honeypot: A Trust-Aware Federated Intrusion Detection Framework with Comparative Evaluation*. Zenodo. https://doi.org/10.5281/ZENODO.18786478

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, *52*(12), 2292–2330. https://doi.org/10.1016/j.comnet.2008.04.002

ZENNARO, M. (2010). *Wireless Sensor Networks for Development: Potentials and Open Issues* [Doctoral Thesis, KTH School of Information and Communication

Technology SE-16440 Kista]. https://www.academia.edu/download/37804587/FULLTEXT01_2.pdf

Zhang, C., Yang, S., Mao, L., & Ning, H. (2024). Anomaly detection and defense techniques in federated learning: A comprehensive review. *Artificial Intelligence Review*, *57*(6), 150. https://doi.org/10.1007/s10462-024-10796-1

Zhang, H., Upadhyay, D., Zaman, M., Jain, A., & Sampalli, S. (2025). SC-MLIDS: Fusion-based Machine Learning Framework for Intrusion Detection in Wireless Sensor Networks. *Ad Hoc Networks*, *175*, 103871. https://doi.org/10.1016/j.adhoc.2025.103871

Zhou, Y., Ye, Q., & Lv, J. (2022). Communication-Efficient Federated Learning With Compensated Overlap-FedAvg. *IEEE Transactions on Parallel and Distributed Systems*, *33*(1), 192–205. https://doi.org/10.1109/TPDS.2021.3090331

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, *104*(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521

Zuo, C., Qian, J., Feng, S., Yin, W., Li, Y., Fan, P., Han, J., Qian, K., & Chen, Q. (2022). Deep learning in optical metrology: A review. *Light: Science & Applications*, *11*(1), 39. https://doi.org/10.1038/s41377-022-00714-x

