American Journal of Computer Science and Technology
2025, Vol. 8, No. 3, pp. 151-163
https://doi.org/10.11648/j.ajcst.20250803.13

Review Article

Cybersecurity Vulnerabilities and Intrusion Detection Mechanisms in Wireless Sensor Networks: A Review

Emmanuel Iheanacho Afonne*, Patrick Ejeh, Linda Chioma Aworonye

Department of Computer Science, Novena University, Ogume, Nigeria

Abstract

Wireless Sensor Networks (WSNs) have become integral to various sensitive and life-critical areas and applications, including environmental monitoring, healthcare, and smart cities. However, their widespread adoption raises significant cybersecurity concerns due to inherent vulnerabilities in their architecture, communication protocols, and resource constraints. This paper comprehensively analyzes security vulnerabilities specific to WSNs. Physical vulnerabilities arise from the unattended deployment of sensor nodes, making them susceptible to tampering and theft. Network-layer vulnerabilities include issues such as eavesdropping, replay attacks, and denial of service, which can severely disrupt the functionality of WSNs. Application-layer vulnerabilities often involve inadequate security measures in software, leading to data breaches and manipulation. In the face of these threats, traditional threat detection mechanisms are deficient in addressing the problem due to the inherent properties of the sensor nodes, such as limited energy, processing power, and memory. This led to the development of custom Intrusion Detection Systems (IDS) for WSNs. IDS can be classified into various types based on detection method, architecture, and deployment strategy. Additionally, this paper evaluates existing intrusion detection mechanisms designed to mitigate these vulnerabilities. We categorize these mechanisms into anomaly-based and signature-based approaches, analyzing their strengths and limitations concerning WSNs' unique characteristics. Anomaly-based systems are adept at detecting novel attacks but may suffer from high false-positive rates, while signature-based systems offer faster detection for known threats but struggle with the emergence of new vulnerabilities. We also highlight recent advancements in machine learning and artificial intelligence as innovative approaches for enhancing intrusion detection capabilities in WSNs. These strategies promise to improve the accuracy and efficiency of intrusion detection systems by leveraging large datasets to recognize complex attack patterns. Based on our findings, this article underscores the urgent need for robust security frameworks tailored to WSN environments. This review work is aimed at providing researchers and practitioners with foundational information to aid their understanding of the security posture of wireless sensor networks.

Keywords

Wireless Sensor Networks, Intrusion Detection, Security Vulnerability, Sensor Nodes, Detection Techniques

1. Introduction

Wireless Sensor Networks (WSNs) are infrastructureless networks made up of several spatially distributed sensor nodes connected in an ad-hoc manner that communicate wirelessly to gather and transmit data for real time monitoring

*Corresponding author: achokemma@gmail.com (Emmanuel Iheanacho Afonne)

Received: 8 August 2025; **Accepted:** 21 August 2025; **Published:** 19 September 2025

and decision making [1]. WSNs are indispensable technology recently deployed in various application areas e.g. Internet of Things (IoTs), security surveillance and monitoring, surroundings monitoring, monitoring patients' health conditions, and detection and proactive response to landslide, etc. [2]. The limitation of WSNs is that they are vulnerable to diverse cyber threats [3] due to their existential characteristics including their distributed and scalable nature, low computational power, energy constraints, dynamic topologies, and self-organizing capability [4]. The vulnerabilities orchestrated by cyber threats such as eavesdropping, jamming, and spoofing, etc. can lead to serious consequences such as unauthorized access, disruption of access to critical services, and data theft [5]. Each sensor node in the WSN is hence designed to be power efficient, fault tolerant to handle node failures and able to operate in a harsh environment [6, 7]. As the WSNs are unavoidably utilized in life-critical applications, there are a myriad of security threats occasioned by the popular use of the technology [8]. This makes the security of WSNs very important and a challenging nightmare, which has to be to addressed as the security of the network and the data it collects is a major priority. For instance, a compromised WSN can cause inaccurate data collection [9], which negatively affect the reliability of applications that depend on information from such data when processed. Recent studies indicate an alarming increase in cyber-attacks targeting to compromise WSNs calling for development of robust intrusion detection mechanisms to help in identifying malicious activities in WSNs, thereby safeguarding the confidentiality, integrity and availability of networked data. In this paper, we conduct a systematic review of the current state of IDS for WSNs with respect to various detection techniques, algorithms, and architectures to understand the nature of WSNs vulnerabilities and the efficacy of existing IDS solutions. Specifically, it is our aim to Identify and categorize the various types of cybersecurity vulnerabilities in WSNs, including physical, network, and application layer vulnerabilities. The work also evaluates the effectiveness of current intrusion detection mechanisms deployed in WSNs, highlighting their strengths, weaknesses, and applicability in different scenarios and propose areas for future research and development to secure WSNs through development of novel approaches to detecting intrusion that are emerging threats-proof.

In this review, specific research gaps were identified that needs to be addressed. In the current literature, no exhaustive analysis of all known vulnerabilities in WSNs is provided. Therefore, we explore areas where certain types of vulnerabilities, such as physical, communication, or software-related vulnerabilities, have not been thoroughly investigated. With widespread implementation of WSNs in many sensitive applications, new types of attacks and cyber threats emerge with no adequate information on how the emerging threats target WSNs [9] and how the threats are different from already known threats. Many IDSs are designed to detect specific types of threats without paying attention to their ability to detect emerging threats in real-world scenario. There is no doubt that machine learning and AI is increasingly deployed in cybersecurity but there is a lack of an all-inclusive review on their efficacy and limitations when deployed in WSNs. Apart from cybersecurity vulnerabilities, privacy issues in WSNs are often not given due consideration. Existing literatures on intrusion detection fail to provide adequate discussion of the intersection of cybersecurity and privacy in WSNs.

The main aim of this paper is to analyze the state-of-the-arts in intrusion detection in WSNs research designers and implementers requisite insights into intrusion detection mechanisms in different scenarios. Specifically, this paper identifies the types of vulnerabilities in WSNs, evaluates the degree of effectiveness of existing detection systems in WSNs in terms of their strengths, weaknesses, and applicability in different instances, and also proposes future research directions for innovative approaches to intrusion detection in WSNs.

During the conduct of this systematic literature review it was found that there is limited literature in the area of intrusion detection in WSNs. Those available do not provide extensive and thorough analysis of vulnerabilities in WSNs. To fill this gap, we investigate physical, communication, and software-related vulnerabilities. The development in technology has brought new types of attacks e.g. those that exploit IoT, cloud computing, and Machine Learning technologies. There is also inadequate information on the modus operandi of these emerging threats against WSNs and how they are different from traditional threats.

It is no longer news that machine learning (ML) and artificial intelligence (AI) algorithms and techniques are deployed in cybersecurity with impacting gains [10, 11] but there is little or no comprehensive reviews on effectiveness and limitations of these technologies with regards to WSNs. To fill this gap, we discuss the potential and challenges of utilizing ML and AI in vulnerabilities detection and mitigation.

Another research gap identified is the lack of standardized protocols for WSNs vulnerabilities assessment and IDS effectiveness. Based on this, we highlight the need for such standards, which is capable of motivating future research on developing metrics with global acceptance.

The contribution of this paper is the analysis of cybersecurity vulnerabilities and cyber threat intrusion detection mechanisms for wireless sensor networks (WSNs). We classify cybersecurity vulnerabilities fundamental peculiar to WSNs by analyzing existing literature to combine the different sources of risk in different layers of WSNs into a cohesive framework. This is to provide researchers with an educative insight into the intricate nature of threats to WSNs. This paper also contributes to the existing body of knowledge with of review of current intrusion detection mechanisms specifically designed for WSNs focusing on intrusion detection methodologies, effectiveness, and their limitations. Various intrusion detection approaches such as anomaly-based, signature-based, and hybrid methods are compared and contrasted to bring forth the strengths and weaknesses of each

intrusion detection mechanism.

This paper provides a methodical classification of security vulnerabilities peculiar in wireless sensor networks. By critically analyzing existing literature, we consolidate varied sources of risk—including physical, network, and application-layer vulnerabilities—into a unified framework. This synthesized understanding equips researchers and practitioners with a deeper insight into the multifaceted nature of threats posed to WSNs. We carefully examine existing intrusion detection mechanisms particularly designed for WSNs, with emphasis on their methodologies, effectiveness, and limitations.

We also contribute to the existing knowledge in intrusion detection systems by making practical recommendations for sensor manufacturers, network designers, and system integrators as it concerns strategies for enhancing the security posture of WSN deployments narrowing the gap between academic research and practical application.

2. Literature Review

In this section, we present a summarized review of research works based on machine learning methodology, WSNs architecture, and intrusion detection techniques for threat detection in WSNs. The section also provides an overview of vulnerabilities in WSNs. This is aimed at providing a deeper understanding of existing research works on this area in order to proffer strengthened recommendation of innovative and adaptive security mechanisms for WSNs.

2.1. WSNs Architecture

WSN architecture comprises the design structure, the topology in which the sensor nodes are arranged, protocols for communication, and components to handle data processing [12]. WSNs structure can be categorized into hierarchical (cluster-based) or flat architectures [13].

2.1.1. Flat-based Architecture

In this architecture, all sensor nodes (SN) are configured as peers performing similar operations [14, 15]. The nodes sense and process the sensed information and transmit to the base station (BS) using a multi-hop routing protocol, a flooding technique deployed to sustain the quality of the communication path from individual SN to the BS. In this architecture, intrusion detection may be affected at either the SN or at the BS [16]. Figure 1 depicts a flat WSN architecture.

2.1.2. Hierarchical-based Architecture

A typical Hierarchical (Cluster)-based architecture is made up of three components namely, a cluster head (CH), a base station (BS) and sensor nodes [17]. In this network structure, sensor nodes are grouped into clusters with a CH for each cluster elected for the cluster based on energy levels of the sensors in that cluster. Unlike the flat architecture, sensor nodes transmit the sensed and processed sensor data to the CH for onward transmission of accumulated data to the BS as depicted in Figure 2. Notable routing algorithms used in this topology include Low-energy adaptive clustering hierarchy (LEACH), Base station Controlled Dynamic Clustering Protocol (BCDCP), Energy-Efficient Unequal Clustering (EEUC), HEED (Hybrid Energy-Efficient Distributed Clustering) etc. In this topology intrusion detection can be performed any of the three points in the network or in a distributed manner.

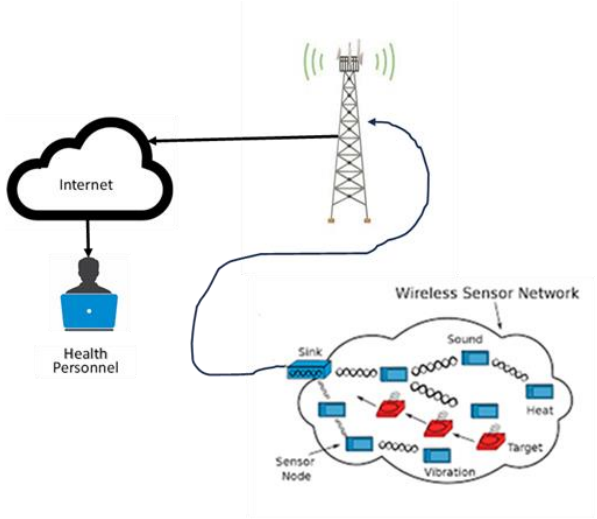

Figure 1. *Flat based WSN Architecture.*

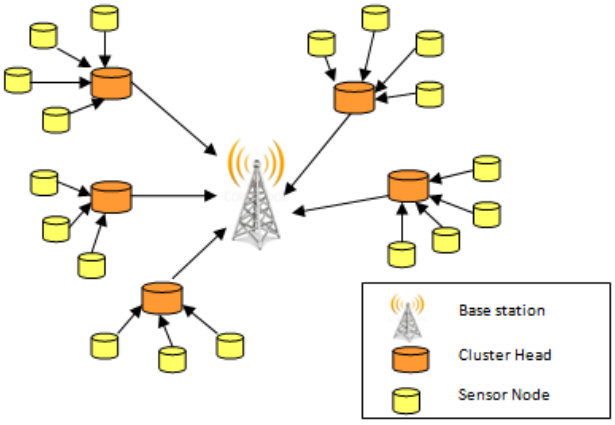

Figure 2. *Hierarchical (Cluster) based WSN Architecture.*

2.2. Vulnerabilities and Attacks in WSN

Attacks launched against WSNs leverage the open wireless communication channels used, the network's resources constraints in terms of processing capacity, power consumption, etc., and the ad hoc nature of the network. These attacks are different from attacks against wired networks, hence requiring

a different approach toward attacks mitigation. WSNs-based Attacks can be classified into passive attacks and active attacks [2]. In the former, the adversary tries to gain unauthorized access to the data packets by observing the communication link. However, the attacker is not interested in modifying or mutilating the data. Few examples of passive attacks are node tampering, traffic analysis and eavesdropping. In the later type of attack, the attacker listens to the communication link at different layers of WSN and modifies the data packet or drop the packets in middle of the communication. This attack type is of more consequence compared to passive attacks. The types of active attacks in WSNs are categorized according to the different layers of OSI model for WSNs [18]. We give a summarized layer-wise classification of active attacks in WSN in Figure 3.

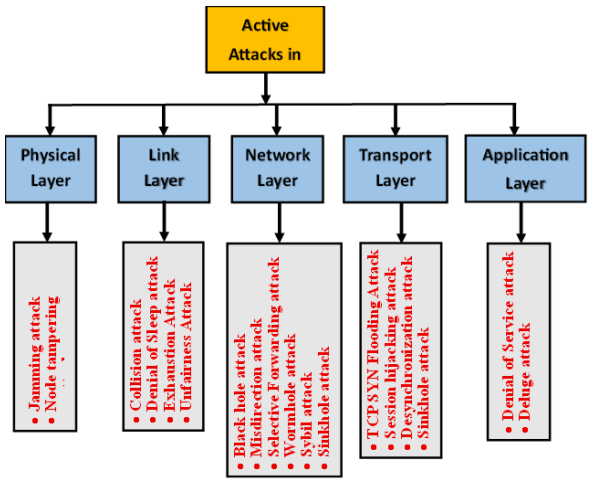

Figure 3. *A Taxonomy of WSN Attack Types.*

2.3. Intrusion Detection Techniques in WSNs

Intrusion detection is a method of monitoring networks for malicious activity and violation of security policies [19]. An intrusion detection system (IDS) conducts analysis on system events log, user behavior, and network traffic to identify harmful patterns that can expose any malicious intrusion attempt or attack in progress ranging from simple port scans to exploits using high-tech malware deployments [20]. Several techniques and methods are often deployed in IDS design including Signature-based detection [21], Anomaly-based intrusion detection [22], Heuristic-based intrusion detection [23], Behavioral analysis-based intrusion detection [24] and Network traffic analysis-based IDS [25]. The significance of the deployment of intrusion detection systems in WSNs threat landscape is not optional due to the proliferation and sophistication [26] in attacks development and availability of exploits for the majority of cyber threats. Reasons necessitating a serious consideration in IDS deployment include but not limited to prevalence of Zero-day attacks, Advanced persistent threats (APTs), attacks exploiting Cloud and IoT environments, emerging and evolving malwares, increased attack sophistication, more targeted and sophisticated modern attacks with capability to bypass traditional security controls using techniques like social engineering, polymorphic malware, and obfuscation [27]. IDS systems need to correlate various data sources and employ advanced analytics to detect these sophisticated threats.

2.4. Related Works

Many novel proposals have been made in researches on IDSs to provide protection for WSNs. In this section, we make reviews of studies conducted using each of the aforementioned IDS techniques. For instance, [28] developed a lightweight, signature-based, and centralized online passive intrusion detection system. The proposed system can easily be integrated into Wi-Fi-based IoT environments without modifying any network settings or existing devices. [29] proposed a signature-based and behavior-based system for preventing IoT device attacks on home wi-fi router. The signature-based component deploys snort software while the behavior-based component utilized machine learning algorithm to optimize performance. [22] proposed a model based on anomaly detection method for IDS in WSNs. The proposed model used mutual information for feature selection and the synthetic minority oversampling technique (SMOTE) for solving the imbalanced dataset problem. The model used different machine learning (ML) algorithms including random forest (RF), decision tree (DT), support vector machine (SVM), and K-nearest neighbors (KNNs) to analyze network traffic. [30] proposed a hierarchical anomaly detection-based IDS using support vector machines (SVM) and a statistical-based deep learning technique for gateway intrusion detection. This detection protocol dynamically and hierarchically executes on-demand SVM classifier on detecting an intrusion. Their approach balances efficiency of intrusion detection with complexity for WSN and gateway security. [31] proposed an efficient and effective anomaly-based intrusion detection system for Internet of Medical Things networks. Their proposed system deployed machine learning (ML) techniques to detect anomalies and identify malicious incidents in the IoMT network. They tested and evaluated a set of six commonly implemented ML algorithms for anomaly detection in their proposal to ascertain which algorithms are the most suitable.

ElDahshan et al [32] proposed a meta-heuristic optimization algorithm-based hierarchical IDS. Their objective is to identify several types of attack and to secure the network. The meta-heuristic optimization algorithms are introduced to optimize the hyperparameters of the extreme learning machine during the construction of multiple binary models to detect different attack types. [23] introduced a hybrid heuristic technique that uses AI to enhance intrusion detection systems (IDS) in IoT environments. Machine learning models used in the proposed work are logistic regression, KNN, na-

ive Bayes, SVM, decision trees, random forests, and neural networks to train, tune, and validate a sequential neural network to predict intrusion occurrences based on extensive data analysis. The effectiveness of the proposed architecture is the system's learning ability of the patterns associated with malicious activities while emphasizing the avoiding of overfitting.

Huang et al [33] developed a WSN Security Protocol Simulation Platform based on OMNeT++, a discrete-event simulation framework. Through this work, the author presented a broad and new method for conducting security analysis in WSNs by combining cognitive computing with advanced simulation techniques. The strength of Huang's work is in the analysis of the behaviors of malicious node by monitoring the communication pattern and incorporating a mechanism to mutually assess trust among sensor nodes.

Machine Learning and Artificial Intelligence in IDS

Many authors have deployed machine learning approach to security against threats in WSNs. For instance, [34] proposed a predictive framework for intrusion detection in wireless sensor networks-based Industry 4.0 using machine-learning and deep-learning algorithms. The authors used a multi-criteria approach by implementing Decision Tree, MLP, and Autoencoder, as proposed algorithms in the framework. The developed framework showed enhanced threat detection performance. [35] described a machine learning (ML) based comprehensive security solution for network intrusion detection using ensemble supervised ML framework and ensemble feature selection methods after providing provide a comparative analysis of several ML models and feature selection methods. The goal of their research was to design a generic detection mechanism and achieve higher accuracy with minimal false positive rates (FPR). [36] presented an intrusion detection system based on the ensemble of prediction and learning mechanisms aimed at improving anomaly detection accuracy in a network environment. The authors used automated machine learning as the learning mechanism, and deployed the Kalman filter as the prediction model. [37] proposed an XGBoost-based IDS for WSNs cyberattacks including blackhole, grayhole, flooding, and scheduling attacks. They used decision trees and naive Bayes to benchmark the performance of the proposed method. [38] presented a lightweight and multi-layered threat detection system using a Naive Bayes algorithm as First-layer detection for binary classification, and a LightGBM algorithm as Second-layer detection for multi-class classification to mitigate WSNs targeted attacks. The proposed system can detect four network-layer internal Denial-of-Service (DoS) attacks. [39] developed a novel and intelligent IDS framework for protecting WSN from cyber-attacks using an Intensive Binary Pigeon Optimization (IBiPO) and Bi-directional Long Short-Term Memory (Bi-LSTM) mechanisms for accurate intrusion detection and classification. [40] proposed a deep learning-based IDS framework with adaptability to emerging attacks. Their solution consists of different phases including a phase to identify new attacks using deep learning-based open set recognition methods and a phase to cluster the data samples by combining the deep model and clustering algorithms making the labeling procedure more practical in terms of reduced the time and effort of expert team.

Other researches have been aligned along WSNs architecture in the design of an IDS for threat detection in WSNs. [41] aimed at detecting malicious nodes and discarding their sensed data. To achieve this, the authors proposed a centralized architecture-based hybrid Intrusion Detection System (IDS) for clustered WSNs. The proposed system is based on functional reputation and misuse detection rules. In this system, each sensor node computes functional reputation values for its neighbors by observing their activities. Base Station (BS) detects malicious nodes by combining functional reputation values and misuse detection rules. Their proposed idea increases the network longevity and freshens sensed data by detecting malicious nodes in a centralized way with reduced energy consumption.

3. Research Methodology

This review followed the process described in [42]. Figure 4 shows the visual description and breakdown of the systematic review methodology used to identify existing research works on vulnerabilities and intrusion detection mechanisms in WSNs.

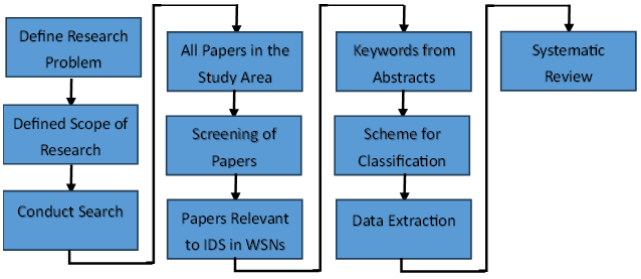

Figure 4. *Systematic Review Process Diagram.*

3.1. Research Questions

The main aim of this review paper is to analyze the state-of-the-arts in intrusion detection in WSNs research designers and implementers requisite insights into intrusion detection mechanisms in different scenarios. Based on this, we formulated five fundamental research questions to help in a methodical analysis of existing cybersecurity vulnerabilities terrain and intrusion detection mechanisms in WSNs. The questions we seek answers to include the following:

RQ1: What are the universally identified cybersecurity vulnerabilities in wireless sensor networks? This research question is to foster understanding of the different WSNs-based vulnerabilities like Sybil attacks, sinkhole attacks, routing attacks,

and physical tampering.

RQ2: What are the dominant intrusion detection mechanisms proposed for WSNs by authors of research papers? This question is aimed at reviewing the different intrusion detection techniques used to detect cyber threats in WSNs. This includes signature-based, anomaly-based, and hybrid detection methods.

RQ3: What is the effectiveness of the current intrusion detection methods in mitigating the identified cybersecurity vulnerabilities and threats in WSNs? Here, we seek to evaluate the performance metrics used in current detection methods in terms of scalability, detection accuracy, energy efficiency, and false positive rates.

RQ4: What limitations and challenges do existing intrusion detection systems deployed in WSNs face? Here, we seek to identify gaps with respect to scalability issues, detection latency, resource constraints, and robustness against sophisticated attacks.

RQ5: What emerging and innovative technologies can be deployed in future researches to threats detection in WSNs? This question is aimed at investigating how machine learning, lightweight algorithms, and hybridized detection techniques can be deployed to address the limitations and challenges identified in RQ4.

3.2. Search Strategy

In the study, we conducted a comprehensive search for existing research output (published papers, books, conferences, etc.) across different academic repositories, including, Google Scholar, ScienceDirect, ACM Digital Library, Springer, Wiley Online Library, and IEEE Xplore. The choice of these databases was based on their popularity in the computing discipline. The keywords and phrases used in the search include Wireless sensor networks, Cybersecurity vulnerabilities, Intrusion detection systems, Security mechanisms, Threat models, Secure communication protocols, Sensor node attacks, Network security, and Anomaly detection. We also made used of Boolean operators and truncation techniques to maximize the search results. Table 1 presents the distributions of the research papers retrieved from the above-mentioned repositories.

Table 1. *Distribution of Retrieved Research Papers.*

Digital Library	Initial Results	Most Relevant Papers
Google Scholar	112	15
ScienceDirect	35	6
ACM Digital Library	18	5
Springer	61	10
IEEE Xplore	26	6
Wiley Online Library	17	4
Total	279	92

3.3. Paper Selection Criteria

In order to guarantee that only qualitative papers and those relevant to vulnerabilities and intrusion detection in WSNs are selected and included in the review study, we formulated a set of inclusion and exclusion criteria as follows:

Inclusion Criteria:

1) Publications from peer-reviewed journals and conferences published between 2015 and 2025.
2) Studies focusing explicitly on vulnerabilities, attack types, and intrusion detection mechanisms in WSNs.
3) Papers or articles of empirical, theoretical frameworks, or comprehensive surveys type or nature.

Exclusion Criteria:

1) Articles in which the publication language is not English.
2) Studies with exclusive focus on hardware design with no mention any security considerations.
3) Papers that are not peer-reviewed
4) Papers whose abstracts explicitly show that their contributions lie outside the subject of vulnerabilities and intrusion detection in WSNs
5) Papers with contents showing sparse use of the phrase "intrusion detection in WSNs"
6) Papers published before 2015.

3.4. Selection Process and Paper Classification

A total of 279 research papers were sourced from the six academic repositories mentioned in the search strategy section (see Table 1). For a start, we used keywords to read the titles and abstracts of each paper to filter out irrelevant and out-of-scope papers. Where the quality of the abstracts are not good enough to determine a paper's suitability, we went further

to read the introduction and conclusion sections in order to form meaningful keywords. After the initial screening, we reviewed the full text for each shortlisted papers to determine their relevance and contribution to our objectives. Based on this, 92 papers were found to be relevant to our study objectives and were therefore selected as the ones on which our review study is based. With further filtering, 46 were the most relevant selected finally.

We analyzed three main aspects in our study including intrusion detection architecture, detection techniques, and vulnerabilities and attack types in WSNs. These three aspects then formed the categories into which we classify the selected papers. The methodological quality of the included studies was evaluated using criteria such as research rigor, clarity of proposed mechanisms, and validation approaches. Studies meeting high-quality standards were prioritized in the analysis.

3.5. Methodological Quality of Selected Research Papers

In this section, we evaluated the quality and effectiveness of methods adopted in the selected research papers based on some key criteria including the thoroughness of the research work, clear presentation of proposed mechanisms, and approaches used in result validations.

Research Thoroughness:

Most of the studies under review exhibited convincing research details and a rigorous approach as evident in the distinctive definition of exact problems the research is seeking solutions, all-inclusive review of literature, in-depth theoretical frameworks, and explicit and well-defined methodologies. A good number of research papers reviewed used formal models to back their findings. These approaches ensure that security vulnerabilities and intrusion detection techniques in WSNs are examined in detail. However, the authors in other papers either failed to provide extensive experimental details or address potential perplexing issues that might contribute to the limitations of their research outputs.

Presentation of Proposed Mechanisms:

Majority of research papers reviewed in this work effectually communicated their proposed intrusion detection mechanisms by way of proposing well-articulated algorithms and system architecture which help in understanding the working of their proposed system and easy implementation. However, we identified a handful of research works whose proposed mechanisms either lacked adequate technical specifics or bereft with confusing descriptions. These can hamper smooth implementation of the proposed mechanisms and make comparative analysis with existing solutions difficult.

Validation Approaches:

Different validation methods were deployed throughout the reviewed works. Some of the works were interested on quantitative results and as such they utilized environments like NS-2/NS-3 or MATLAB for their simulation. This helped to demonstrate the effectiveness of proposed systems. A few other papers employed real-world experiments to determine their proposed mechanisms' effectiveness, which promotes the practical applicability of their findings. While these two groups utilized controlled simulation environments and real-world experiments respectively, a third category of research works exclusively depended either on theoretical evaluation or limited simulation scenarios. This invariably limits the generalizability of their solutions and raised real-world applicability and implementation of these proposed security mechanisms.

4. Discussion of Findings

4.1. Implication of Findings

This review paper scrutinizes existing research on security vulnerabilities and intrusion detection mechanisms in WSNs. In the scrutiny, key findings, challenges dominant in IDS in WSNs, and new and emerging trends WNSs security are highlighted. It was found that a typical WSNs is vulnerable to a multitude of security threats because of its intrinsic characteristics, which includes resource constraints, deployment environments, and wireless nature. Across the proposed mechanisms in different reviewed research papers, the prevalent and most common vulnerabilities mentioned are identified to include node capture attacks, Sybil attacks, sinkhole and wormhole attacks, and false data injection [43]. The most potent solution against these threats undoubtedly remains a cryptographic approach to securing sensor nodes sensed data. But the application of robust cryptographic algorithms is hampered by the limited computational power and energy resources of sensor nodes. In the light of this limitation, WSNs are vulnerable to both passive eavesdropping and active exploitation.

Proposed mechanisms for detecting intrusions in WSNs is mainly classified into signature-based, anomaly-based, and hybrid techniques. Other techniques include behavior-based, specification-based and machine learning-based. We found that Signature-based methods can detect known attacks with high accuracy and precision but is not adaptable to fighting emerging threats. Anomaly-based detection provides flexibility in such a way that the resulting mechanisms are adaptable to detection of novel and new attacks. However, this approach may bring about higher false positive rates. Hybrid IDS mechanisms leverage the strengths of both Signature-based and Anomaly-based detection methods [44] but unfortunately, schemes which are based on this technique are bereft with challenges ranging from high computational overhead to high energy consumption.

In our findings, various experimental evaluations in different proposed IDS mechanisms showed that for resource-constrained environments such as WSNs where sensor nodes have limited processing power, small memory, and short battery lifetime, a lightweight and distributed detection architecture are suitable. The distributed architecture promotes collaborative detection instead of overloading a single

sensor node with detection responsibility. Cluster-based architectures promise high detection accuracy while minimizing energy consumption. Again, evaluation results in most proposed IDS mechanisms for WSNs based on machine learning [45, 46] show promising potentials for improved threats detection but with optimized learning algorithms for deployment in WSNs.

Despite the efforts made by existing research outputs in providing solutions to secure WSNs, there abounds a myriad of challenges that frustrate the deployment of these solutions in WSNs. First, the problem of balancing detection accuracy with resources consumption constitutes a nightmare. Second is the issue of scalability in large WSNs, and third is the difficulty in security maintenance given the dynamic and complex network topologies utilized in WSNs. Lastly, majority of existing IDS security mechanisms in WSNs are made to combat specific attack types and therefore are not adequate for the dynamic, ever evolving, and rapidly changing cybersecurity landscape.

Interpretation of Findings:

The findings in this paper indicate that there are trade-offs between detection accuracy, energy efficiency, and scalability in existing intrusion detection techniques. Particularly, the review reveals that though signature-based detection techniques show great accuracies for known attacks, they are effective in detecting evolving threats and also require substantial computational resources, in agreement with the findings [47]. On the other hand, anomaly-based detection methods tend to be more responsive to unknown threats but may generate higher false-positive rates as posited in [48]. Also, this review Furthermore, the review highlights that most current works in detection of threats in WSNs are designed specifically for a kind of attack types hence lacking resilience and robustness against sophisticated and advanced attacks prompting [49] to advocate for hybrid detection frameworks that combine multiple techniques to improve overall resilience.

Comparison with Previous Works:

The findings in this paper validate previous works in their conclusions that security in WSNs remains a significant challenge due to resource constraints and susceptibility to adversarial threats. For instance, [50] laid a foundation to understanding of WSN vulnerabilities, which is confirmed in this review. Similarly, based on the need for energy efficient threat detection in WSNs, the effectiveness of lightweight anomaly detection mechanisms proposed by [51] supports the findings in this paper. Furthermore, the review in this paper also uncovers gaps previously identified in previous researches especially in the area of limited adoption of machine learning methods in detection of threats in WSNs.

4.2. Comparative Analysis of IDS Methods

The review conducted in this paper shows that there are different methodologies in which Intrusion Detection Systems are based to identify threats against computer systems and networks by flagging malicious activities and possible violations of security policies. In this section, we present a comparative analysis of the methodologies popularly adopted in Intrusion Detection Systems for security of WSNs in Table 2.

Table 2. *Comparisons of Intrusion Detection Methods used in WSNs.*

Criteria	Signature-Based Detection	Anomaly-Based Detection	Specification-Based Detection	Hybrid Approaches	Data Mining & Machine Learning
Overview	Characterized by use of predefined attack signatures of already known attacks.	Systems proposed with this as the detection method detects deviations from normal network or system behavior.	This method can also be called Rule-based. It utilizes predefined rules that describe valid behavior.	This method aggregates multiple schemes	Deploys data analysis and Artificial intelligence and machine learning techniques for threats identification.
Detection approach	Pattern matching against maintained known attack signature database.	Creates desired patterns of normal behavior outside of which the IDS flags deviations.	IDSs under this category monitor WSN behavior against set specifications.	Leverages individual IDS method's strengths to improve detection.	Classifies and predicts attacks and threat by learning attacks pattern in threats datasets.
Advantages	High accuracy in detecting static and non-evolving threats; low false positives.	Useful in detecting unknown attacks; can be deployed to combat evolving threats.	Lower false positives if high quality specifications are assured; effective for attacks and threats with known footprints and deterministic behaviors.	There are improved rates of threat detection; there is reduced false positives and negatives.	It is scalable and good at adapting to new and evolving threats and attack patterns; scalable.

Criteria	Signature-Based Detection	Anomaly-Based Detection	Specification-Based Detection	Hybrid Approaches	Data Mining & Machine Learning
Disadvantages	Inability to respond to emerging threats or unknown attacks (zero-day).	Has higher false positive rate; secondly, it requires a lot of training and parameter tuning.	It is not flexible since it requires accurate static specifications.	Implementation cost is high and not suitable for WSNs environment due to resource constraints.	Require huge and extensive datasets; uses rigorous model training which increases the complexity of the model.
Resource suitability	Suitable for detecting attacks in which attack signatures are known.	Suitable for detecting attack in a changing attack landscape	Suitable given well-defined specifications describing desired system behavior	adaptable to resource constraints	Suitable for implementation in various scenarios
Implementation Complexity	Computational complexity is moderate (only requires signature database maintenance	High; involves training models and establishing normal behavior profiles	Moderate depending on size of specifications to be updated	High complexity due to combining multiple detection techniques	High complexity due to the processes involved: collecting data, model training, and updating
Response to Attacks	Prompt response to attacks detection especially for known threats but unproductive against emerging threats	Good at detecting new and unknown attacks; may have higher false positives	Effective for detecting deviations from defined specifications	fast; can detect of known and unknown attacks	Efficiently identifies complex attack patterns depending on accuracy of the model
Energy Consumption	Moderate except in the resource-intensive signature matching operations.	Higher; continuous monitoring and complex computations consume more energy	Moderate; less energy-intensive than anomaly-based but needs specifications updates	Higher due to implementation of multiple techniques	Energy-intensive due to model training and real-time analysis
Examples in Literature	Visoottiviseth et al., Thankappan et al	Yahyaoui et. al., Zachos et. al. Fuhaidi et al.	Ozcelik et al	Aldeen et al.,	Al-Quayed et al., Das et al, Ismail et al

4.3. Future Research Directions

Based on the foregoing, future researches on designing and implementing IDS in environments such as WNSs calls for integrating various technologies due to peculiarities and importance of WSNs. In the light of this, this review emphasizes the need for incorporating lightweight machine learning algorithms to take cognizance of the resource-constraint limitation of WSNs, blockchain technology for data security, and context-aware detection mechanisms for reduced false positives, enhanced detection of attacks and adaptive response based on specific situation. Due to the rapid change in the security landscape by reason of emerging nature of threats, there is need to adopt a cross-layer and adaptive approach to security. This is necessitated by the need to dynamically adjust to network conditions for better detection of threats. We recommend that future researches on IDS mechanisms especially those meant for WSNs should emphasize on energy efficiency, scalability, and robust detection frameworks with thorough real-world validation for applicability and implementation.

5. Conclusions

This review has provided a comprehensive analysis of the prevalent cybersecurity vulnerabilities and the diverse range of intrusion detection mechanisms within Wireless Sensor Networks (WSNs). As WSNs continue to evolve and integrate into critical applications such as healthcare, environmental monitoring, and military operations, ensuring their security becomes increasingly vital. The examined vulnerabilities—ranging from resource constraints and insecure communication channels to physical tampering—highlight the multifaceted nature of threats faced by these networks.

Concurrently, the various intrusion detection approaches, including signature-based, anomaly-based, and hybrid techniques, demonstrate significant strides in detecting and mitigating attacks, although challenges such as energy efficiency, scalability, and real-time responsiveness persist. In this paper, we recommend that research efforts should be focused on developing lightweight, adaptive, and context-aware detection mechanisms that can operate effectively within the limited resources of sensor nodes while maintaining high accuracy. Additionally, fostering integrated security frameworks that combine intrusion detection with prevention strategies will be crucial in fortifying WSNs against evolving threats. Ultimately, a holistic and proactive security paradigm is essential to safeguard the integrity, confidentiality, and availability of wireless sensor networks in their expanding array of applications.

Abbreviations

IDS	Intrusion Detection System
WSN	Wireless Sensor Network
DoS	Denial of Service
AI	Artificial Intelligence
ML	Machine Learning
KNN	k-Nearest Neighbors
SMOTE	the Synthetic Minority Oversampling Technique
APT	Advanced Persistent Threat

Author Contributions

Emmanuel Afonne: Review & Editing, Project Administration and Supervision. The author approved the final version of the manuscript

Patrict Ejeh: Project Administration and Supervision. Also approved the final version of the manuscript

Linda Chioma Aworonye: Conceptualization, Data Curation, Literature Review, initial Manuscript Drafting, Investigation and Methodology

All the authors agree to be accountable for all aspects of the work.

Funding

This work is entirely funded by the Authors but most especially Linda Chioma Aworonye, the PhD student.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Förster A, Dede J, Könsgen A, Kuladinithi K, Kuppusamy V, Timm‐Giel A, Udugama A, Willig A. A beginner's guide to infrastructure‐less networking concepts. IET Networks. 2024 Jan; 13(1): 66-110. https://doi.org/10.1049/ntw2.12094

[2] Fahmy H, M. WSNs applications: In Concepts, applications, experimentation and analysis of wireless sensor networks 2023 Feb 14 (pp. 67-242). Cham: Springer Nature Switzerland.

[3] Yu, J. Y., Lee, E., Oh, S. R., Seo, Y. D., Kim, Y. G. A survey on security requirements for WSNs: focusing on the characteristics related to security. IEEE Access. 2020 Mar 2; 8: 45304-24. https://doi.org/10.1109/ACCESS.2020.2977778

[4] Trigka M, Dritsas E. Wireless Sensor Networks: From Fundamentals and Applications to Innovations and Future Trends. IEEE Access. 2025 May 21. https://doi.org/10.1109/ACCESS.2025.3572328

[5] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 12(6), 1333. https://doi.org/10.3390/electronics12061333

[6] Adday, G. H., Subramaniam, S. K., Zukarnain, Z. A., & Samian, N. Fault tolerance structures in wireless sensor networks (WSNs): survey, classification, and future directions. Sensors, 2022, 22(16), 6041. https://doi.org/10.3390/s22166041

[7] Mohapatra, H., & Rath, A. K. Fault‐tolerant mechanism for wireless sensor network. IET wireless sensor systems. 2020, 10(1), 23-30. https://doi.org/10.1049/iet-wss.2019.0106

[8] Gardašević G, Katzis K, Bajić D, Berbakov L. Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare. Sensors. 2020 Jun 27; 20(13): 3619. https://doi.org/10.3390/s20133619

[9] Lata, S., Mehfuz, S., & Urooj, S. Secure and reliable WSN for Internet of Things: Challenges and enabling technologies. IEEE Access. 2021, 9, 161103-161128.

[10] Basu, A. The Impact of Artificial Intelligence on Cybersecurity. In Abu Dhabi International Petroleum Exhibition and Conference. 2024, November (p. D021S077R001). SPE. https://doi.org/10.2118/222493-MS

[11] Mohamed, N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems. 2025, 1-87. https://doi.org/10.1007/s10115-025-02429-y

[12] Bukar, U. A., & Othman, M. (2022). Architectural design, improvement, and challenges of distributed software-defined wireless sensor networks. Wireless Personal Communications, 122(3), 2395-2439. https://doi.org/10.1007/s11277-021-09000-2

[13] Jan, B., Farman, H., Javed, H., Montrucchio, B., Khan, M., & Ali, S. (2017). Energy efficient hierarchical clustering approaches in wireless sensor networks: A survey. Wireless Communications and Mobile Computing, 2017(1), 6457942. https://doi.org/10.1155/2017/6457942

[14] Kawa, J., Pyciński, B., Smoliński, M., Bożek, P., Kwasecki, M., Pietrzyk, B., & Szymański, D. Design and implementation of a cloud PACS architecture. Sensors. 2022, 22(21), 8569. https://doi.org/10.3390/s22218569

[15] Dalal, B., & Kukarni, S. Wireless Sensor Networks. Wireless Sensor Networks: Design, Deployment and Applications, 2021, 3.

[16] Godala, S., & Vaddella, R. P. V. A study on intrusion detection system in wireless sensor networks. International Journal of Comm. Networks and Information Security, 2020, 12(1), 127-141. https://doi.org/10.17762/ijcnis.v12i1.4429

[17] Singh, S., Garg, D., & Malik, A. A novel cluster head selection algorithm based IoT enabled heterogeneous WSNs distributed architecture for smart city. Microprocessors and Microsystems, 2023, 101, 104892. https://doi.org/10.1016/j.micpro.2023.104892

[18] Sharma, S., Yadav, A., Panchal, M., & Vyavahare, P. D. December). Classification of security attacks in WSNs and possible countermeasures: a survey. In 2019 IEEE Int'l conference on advanced networks and telecom. systems (ANTS). 2019, (pp. 1-6). IEEE. https://doi.org/10.1109/ANTS47819.2019.9118119

[19] Jose, S., Malathi, D., Reddy, B., & Jayaseeli, D. A survey on anomaly-based host intrusion detection system. In Journal of Physics: Conference Series. 2018, (Vol. 1000, p. 012049). IOP Publishing. https://doi.org/10.1088/1742-6596/1000/1/012049

[20] Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. Host-based IDS: A review and open issues of an anomaly detection system in IoT. Future Generation Computer Systems. 2022, 133, 95-113. https://doi.org/10.1016/j.future.2022.03.001

[21] Díaz-Verdejo J, Muñoz-Calle J, Estepa Alonso A, Estepa Alonso R, Madinabeitia G. On the detection capabilities of signature-based intrusion detection systems in the context of web attacks. Applied Sciences. 2022 Jan 14; 12(2): 852. https://doi.org/10.3390/app12020852

[22] Al-Fuhaidi, B., Farae, Z., Al-Fahaidy, F., Nagi, G., Ghallab, A., & Alameri, A. 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

[23] Aldeen Y. A, Jabor F. K, Omran G. A, Kassem M. H, Kassem R. H, Abood A. N. A Hybrid Heuristic AI Technique for Enhancing Intrusion Detection Systems in IoT Environments. Journal of Intelligent Systems & Internet of Things. 2025 Jan 1; 14(1). https://doi.org/10.54216/JISIoT.140101

[24] Amirthayogam, G., Kumaran, N., Gopalakrishnan, S., Brito, K. A., RaviChand, S., & Choubey, S. B. Integrating behavioral analytics and intrusion detection systems to protect critical infrastructure and smart cities. Babylonian Journal of Networking, 2024, 88-97. https://doi.org/10.58496/bjn/2024/010

[25] S. Kumar, S. Gupta and S. Arora, "Research Trends in Network-Based Intrusion Detection Systems: A Review," in IEEE Access, vol. 9, pp. 157761-157779, 2021, https://doi.org/10.1109/ACCESS.2021.3129775

[26] Collier, B., & Clayton, R. A "sophisticated attack"? innovation technical sophistication and creativity in the cybercrime ecosystem. In 21st Workshop on the Economics of Information. 2022. https://doi.org/10.1088/1742-6596/1339/1/012098

[27] Birthriya, S. K., Ahlawat, P., & Jain, A. K. A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. Journal of Applied Security Research, 2025, 20(2), 244-292. https://doi.org/10.1080/19361610.2024.2372986

[28] Thankappan, M., Rifà-Pous, H., & Garrigues, C. A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. IEEE Access, 12, 23096-23121, 2024. https://doi.org/10.1109/ACCESS.2024.3362803

[29] Visoottiviseth, V., Sakarin, P., Thongwilai, J., & Choobanjong, T. Signature-based and behavior-based attack detection with machine learning for home IoT devices. In 2020 IEEE REGION 10 CONFERENCE. 2020, November (pp. 829-834). IEEE. https://doi.org/10.1109/TENCON50793.2020.9293811

[30] Yahyaoui A, Abdellatif T, Attia R. Hierarchical anomaly based intrusion detection and localization in IoT. In2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) 2019 Jun 24 (pp. 108-113). IEEE. https://doi.org/10.1109/IWCMC.2019.8766574

[31] Zachos G, Essop I, Mantas G, Porfyrakis K, Ribeiro JC, Rodriguez J. An anomaly-based intrusion detection system for internet of medical things networks. Electronics. 2021 Oct 20; 10(21): 2562. https://doi.org/10.3390/electronics10212562

[32] ElDahshan KA, AlHabshy AA, Hameed BI. Meta-heuristic optimization algorithm-based hierarchical intrusion detection system. Computers. 2022 Nov 28; 11(12): 170. https://doi.org/10.3390/computers11120170

[33] Huang X. A Data‐Driven WSN Security Threat Analysis Model Based on Cognitive Computing. Journal of Sensors. 2022; 2022(1): 5013905. https://doi.org/10.1155/2022/5013905

[34] 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. https://doi.org/10.1109/ACCESS.2024.3372187

[35] Das, S., Saha, S., Priyoti, A. T., Roy, E. K., Sheldon, F. T., Haque, A., & Shiva, S. Network intrusion detection and comparative analysis using ensemble machine learning and feature selection. IEEE trans. on network and service management, 2021, 19(4), 4821-4833. https://doi.org/10.1109/TNSM.2021.3138457

[36] Imran, Jamil, F., & Kim, D. An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments. Sustainability. 2021, 13(18), 10057. https://doi.org/10.3390/su131810057

[37] Putrada, A. G., Alamsyah, N., Pane, S. F., & Fauzan, M. N. Xgboost for ids on WSN cyber attacks with imbalanced data. In 2022 International Symposium on Electronics and Smart Devices (ISESD). 2022, November (pp. 1-7). IEEE. https://doi.org/10.1109/ISESD56103.2022.9980630

[38] Ismail, S., Dawoud, D., & Reza, H. A. lightweight multilayer machine learning detection system for cyber-attacks in WSN. In 2022 IEEE 12th annual computing and communication workshop and conference (CCWC). 2022 (pp. 0481-0486). IEEE. https://doi.org/10.1109/CCWC54503.2022.9720891

[39] Nabi, F. Cyber-Attacks in WSN & Security Optimization by a Novel Technique based Intensive Binary Pigeon Optimization (IBiPO) & Bi-LSTM-based IDS Framework, 05 September, PREPRINT (Version 1) available at Research Square 2023 https://doi.org/10.21203/rs.3.rs-3308713/v1

[40] Soltani, M., Ousat, B., Siavoshani, M. J., & Jahangir, A. H. An adaptable deep learning-based intrusion detection system to zero-day attacks. Journal of Info. Security and Applications. 2023, 76, 103516. https://doi.org/10.1016/j.jisa.2023.103516

[41] Ozcelik, M. M., Irmak, E., & Ozdemir, S. A hybrid trust based intrusion detection system for wireless sensor networks. In 2017 International symposium on networks, computers and communications (ISNCC). 2017, May (pp. 1-6). IEEE. https://doi.org/10.1109/ISNCC.2017.8071998

[42] Petersen, K., Vakkalanka, S., & Kuzniarz, L. Guidelines for conducting systematic mapping studies in software engineering: An update. Information and software technology. 2015, 64, 1-18. https://doi.org/10.1016/j.infsof.2015.03.007

[43] Savoudsou B, Tchakount éF, Yenke BO, Y á émou T, Atemkeng M. An enhanced dissection of attacks in wireless sensor networks. International Journal of Computing and Digital Systems. 2023 Aug 1; 14(1): 1-. https://doi.org/10.12785/ijcds/140146

[44] Rehman F, Mushtaq F, Zaman H. A Host-based Intrusion Detection: Using Signature-based and AI-driven Anomaly Detection for Enhanced Cybersecurity. In2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2) 2024 Oct 22 (pp. 1-7). IEEE.

[45] Sadia H, Farhan S, Haq YU, Sana R, Mahmood T, Bahaj SA, Khan AR. Intrusion detection system for wireless sensor networks: A machine learning based approach. IEEE Access. 2024 Mar 21; 12: 52565-82. https://doi.org/10.1109/ACCESS.2024.3380014

[46] Karthikeyan M, Manimegalai D, RajaGopal K. Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection. Scientific Reports. 2024 Jan 2; 14(1): 231. https://doi.org/10.1038/s41598-023-50554-x

[47] Karn R. R, Kudva P, Huang H, Suneja S, Elfadel I. M. Cryptomining detection in container clouds using system calls and explainable machine learning. IEEE transactions on parallel and distributed systems. 2020 Oct 6; 32(3): 674-91. https://doi.org/10.1109/TPDS.2020.3029088

[48] Mahdi Z, Abdalhussien N, Mahmood N, Zaki R. Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on Internet of Things (IoT) Networks Using Machine Learning Algorithms. Computers, Materials & Continua. 2024 Aug 1; 80(2). https://doi.org/10.32604/cmc.2024.053542

[49] Elzaghmouri BM, Jbara YH, Elaiwat S, Innab N, Osman AA, Ataelfadiel MA, Zawaideh FH, Alawneh MF, Al-Khateeb A, Abu-Zanona M. A Novel Hybrid Architecture for Superior IoT Threat Detection through Real IoT Environments. Computers, Materials & Continua. 2024 Nov 1; 81(2). https://doi.org/10.32604/cmc.2024.054836

[50] Jondhale SR, Maheswar R, Lloret J. Fundamentals of wireless sensor networks. InReceived Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks 2021 Jul 29 (pp. 1-19). Cham: Springer International Publishing.

[51] Abdelhamid A, Elsayed M. S, Jurcut A. D, Azer M. A. A lightweight anomaly detection system for black hole attack. Electronics. 2023 Mar 8; 12(6): 1294. https://doi.org/10.3390/electronics12061294

Biography

Emmanuel Iheanacho Afonne received Higher National Diploma (HND), Electrical/Electronics Engineering from The Polytechnic Nekede, Owerri in 1988: MSc Computer Science in 2009 from Universite des Sciences Appliquee et Management, Porto Novo, Benin Republic: and Ph.D. Computer Science, specializing in Networking and Telecommunication in 2018 from Babcock University, Ilisan – Remo, Ogun State, Nigeria. He is a Senior Lecturer at Department of Computer Science, Novena University, Ogume, Nigeria. His research interests include: Data Communication and Computer Networks, Wireless Networks, Intelligent Systems, Information and Cybersecurity, and Ubiquitous Computing. He is a member of the prestigious: Nigerian Computer Society (NCS), and Council for Registration of Computer Professionals of Nigeria (CPN).

Patrick Ejeh is currently a Senior Lecturer in the Department of Computer Science, College of Computing and Telecommunications Technology, Novena University, Ogume, Delta State. He is an accomplished academic and researcher with a strong foundation in Computer Science. He received his PhD degree from the University of Sunderland, Sunderland, United Kingdom (2017), MSc in Computer Science from Northumbria University, Newcastle Upon Tyne, UK (2010). His research interests span several core areas of Computing, including Knowledge Management, Machine Learning, Computer Networks, and Database Management Systems. He is a Member of Nigeria Computer Society and Higher Education Academic, United Kingdom.

Linda Chioma Aworonye is a lecturer and a PhD candidate in the Department of Computer Science at Novena University Ogume, Delta State. She obtained her B. Tech. Degree (2006) in Computer Science and Mathematics from the Federal University of Technology, Minna and M. Sc. (2018) in Computer Science at the Federal University of Petroleum Resources, Effurun, Delta State, Nigeria, respectively. She has a Master's in Business Administration (MBA) 2010 from Delta State University, Abraka, and PGD (2016) in Health Environmental Safety and Security from Federal University of Petroleum Resources, Effurun, Delta State, Nigeria. She has participated in multiple international research collaboration projects in recent years. Her research interests include Cyber Security, Cloud Computing, Information and Data Security, Networking, Deep Learning and Data Science.

Research Field

Emmanuel Iheanacho Afonne: Data Communication and Computer Networks, Wireless Networks, Ubiquitous Computing, Information and Cyber Security, and Intelligent Systems.

Patrick Ejeh: Knowledge Management, Machine Learning, Computer Networks, and Database Management Systems.

Linda Chioma Aworonye: Cloud Computing, Information and Cyber Security, Networking, Deep Learning and Data Science.