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

Security of Wireless Sensor Networks in the Era of Artificial Intelligence and IoT: A Systematic Literature Review

Prince Kumar[1], Dr. Neeraj Kumar Kamal[2]

[1]Research Scholar, Department of Computer Science and I.T, Magadh University, Bodh-Gaya, India
[2]Assistant Professor ,Dept of Physics, A.M.College,Gaya,India

Abstract

The Wireless Sensor Networks (WSN) and the Internet of Things (IoT) have revolutionized various application areas such as smart cities, health, industrial automation, environment, agriculture, and intelligent transportation systems. Despite the successful widespread use of WSNs-IoT, they still have several security issues including resource constrained sensor nodes, decentralized design, and the combination of heterogeneous communication protocols and insecure wireless communication channels. Most traditional security solutions including cryptographic methods, intrusion detection systems are rule-based, which is not enough to protect against the advanced, evolving and zero-day attacks. Therefore, the paradigm of artificial intelligence (AI) has become an exciting approach to creating intelligent, adaptive and autonomous cyber security solutions. This paper is a systematic literature review of the security solutions based on artificial intelligence (AI) applied to WSNs (WSNs) in the context of IoT. Structured review methodology is followed in the study, which critically analyzes recent machine learning, deep learning, reinforcement learning, federated learning, blockchain and edge intelligence advancements in the field of intrusion detection, anomaly detection, threat prediction, authentication, privacy preservation, and secure communication. These approaches are compared on the basis of their accuracy to detect the target, computational complexity, energy efficiency, scalability, and privacy and feasibility for deployment in resource constrained environments. Moreover, it classifies the already known security threats, examines layer-wise defense measures and analyzes upcoming hybrid AI frameworks, which combine several intelligent technologies. The review reveals several gaps in the research, such as the lack of explainability of models, use of benchmark datasets, susceptibility to adversarial and model-poisoning attacks, blockchain scalability issues, and the absence of standardized, secure system architectures that can offer reliable, privacy-preserving, and energy-efficient protection. The paper then proposes future research directions that highlight the need of combining Explainable Artificial Intelligence (XAI), Federated Learning, Blockchain, and Edge AI for the construction of strong and adaptive cybersecurity frameworks. This review is a comprehensive reference for researchers and practitioners who are interested in designing secure, intelligent and sustainable WSN-IoT systems for next-generation cyber-physical ecosystems.

Keywords: Wireless Sensor Networks (WSNs); Internet of Things (IoT); Artificial Intelligence; Intrusion Detection Systems; Federated Learning; Blockchain Security.

1. Introduction

1.1 Evolution of Wireless Sensor Networks (WSNs)

Wireless Sensor Networks (WSNs) have become a basic technology in distributed sensing, data acquisition and intelligent monitoring. A WSN is a collection of such sensor nodes that are interconnected, which can sense, process and wirelessly transmit data. Due to the ever-evolving embedded systems, microelectronics, low power communication and networking methods, WSNs have found a wide range of applications like environmental monitoring, healthcare, industrial automation, military surveillance, precision agriculture, smart infrastructure etc., [1] [2]. Initially, WSN was intended to be primarily for simple sensing and data communication. Over time, technology developed to make hardware energy efficient and protocols sophisticated enough for deployments to scale and to gather data in real-time. Despite the advancements, the limitations of computation power, memory, bandwidth and energy resources still presented formidable obstacles and limitations in the field of secure and reliable communications [3]-[5].

1.2 Emergence of IoT-Based Ecosystems

Internet of Things (IoT) is an example of the applications where the WSNs have been playing a significant role, in which physical objects, sensors, machines and digital services communicate on interconnected networks [6]. WSNs are now rapidly evolving to become intelligent cyber physical systems with the recent development of cloud computing, edge computing, AI, and advanced communication technologies. The modern IoT environments consist of billions of devices generating and communicating enormous amounts of data in different fields such as smart cities, industrial IoT, healthcare systems, transportation systems, and smart energy infrastructures [7, 8]. As this explosive growth has come, the necessity for secure, scalable, interoperable, and real-time protection mechanisms to protect sensitive data and system reliability has increased by a huge order of magnitude [9].

1.3 Security Challenges in Resource-Constrained WSN-IoT Environments

Some of the major problems in WSN and IoT systems are low computing power, low storage capacity and low energy at sensor nodes coupled with security concerns. The traditional security measures can be problematic in resource constrained systems [10]. There are a number of attacks that can be launched on wireless communication channels: Eavesdropping, Spoofing, Replay, Denial-of-service, and Unauthorized access attacks. Furthermore, the distributed sensors can be easily captured, targeted with physical attack, and attacked with Sybil, blackhole, selective forwarding, and sinkhole attack [11] [12]. Furthermore, IoT devices exist in many different forms, each with varying hardware platforms, communication protocols and operating systems, making security management much more complex. Various traditional cryptographic and rule-based security solutions are often unable to safeguard against dynamic, complex and evolving cyber threats and intelligent and adaptive security solutions are needed [13, 14].

1.4 Role of Artificial Intelligence in WSN-IoT Cybersecurity

In artificial intelligence (AI) era, AI is a promising solution to address the complex cyber security problem in the WSN-IoT based system. AI-based security systems can learn from network data and detect anomalies, predict trends in attack, and provide adaptive security [15]. Decision Trees, Support Vector Machines (SVM), Random Forest and K-Nearest Neighbour (KNN) are some of the machine learning techniques that have shown to be effective in intrusion detection and anomaly classification [16]. In addition, deep learning techniques such as Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs) have demonstrated great potential in the detection of intricate

cyberattack patterns in large-scale network traffic sources [17] [18]. AI cybersecurity offers several advantages, such as real-time threat detection, automated incident response, predictive analysis, and scalability. Some of the advanced techniques that can enhance security of distributed IoT networks are recent developments such as federated learning, explainable AI, reinforcement learning, and edge intelligence [19]–[21]. But there are still several challenges to be addressed, such as model transparency, computational cost, privacy protection, adversarial attack and data quality [22].

1.5 Research Motivation

The new opportunities for intelligent and adaptive security frameworks have been brought about by the advent of WSNs, IoT and AI. The research state of the art is however, fragmented and includes topics from networking, Cyber security, Machine learning and Embedded systems. Some studies have introduced an AI-based intrusion detection system, blockchain-based security model, anomaly detection and federated learning approaches, but further research is necessary. The existing surveys, in general, are only concerned with specific technologies or specific attack categories and do not offer a comprehensive view of AI-based security solutions for WSN-based IoT environments [23]. To this end, a comprehensive analysis is needed to assess the current security solutions, uncover research gaps, and propose potential future research directions on secure, intelligent and resilient IoT infrastructures.

1.6 Objectives and Contributions of the Review

This systematic literature review (SLR) presents a comprehensive analysis of AI-driven security mechanisms for WSN-based IoT environments. The study examines traditional security approaches, machine learning-based intrusion detection, deep learning techniques, federated learning frameworks, and blockchain-supported security solutions.

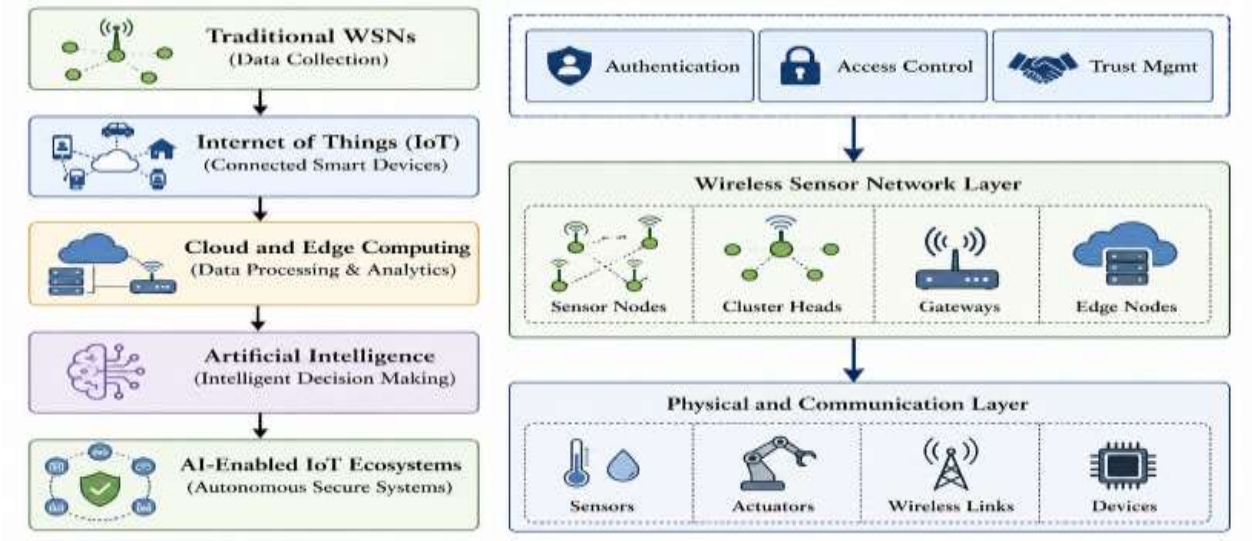

Figure 1.Conceptual Architecture of an AI-Driven Secure Wireless Sensor Network (WSN)–IoT Ecosystem.

2. Literature Review

2.1 Conventional Security Approaches for WSNs and IoT

Wireless Sensor Networks (WSNs) have become an important and essential component of the Internet of Things (IoT) and are used to deliver intelligent sensing, monitoring and communication in a vast range of application areas. Although WSNs are ubiquitous, limited processing power, memory and battery capacity of sensor nodes make them susceptible to many kinds of possible threats to security. Initial

research revealed that eavesdropping, node capture, replay attacks, spoofing, Sybil attacks, sinkhole attacks, wormhole attacks, and denial-of-service (DoS) attacks are among the primary attacks that threaten the network's security and impact its confidentiality, integrity and availability [6]. A common approach to the solution of these challenges was the use of cryptographic techniques, such as symmetric and asymmetric encryption, authentication protocols, digital signatures and key management schemes, etc., [7]. While these techniques have greatly improved secure communications and data integrity, in many scenarios they have demanded more resources than have been at the disposal of low-power sensor nodes. The integration of WSNs with IoT made the security concerns related to heterogeneous devices, vast number of connections, scattered communication and increasingly sophisticated cyber threats, such as malware, botnets, ransomware, and advanced persistent threats [12] even worse. Therefore, the rule-based security systems are no longer suitable for securing modern IoT based WSN environments, and adaptive and intelligent security systems are needed.

2.2 AI-Based Security Techniques

AI is a game-changing technology for bolstering cybersecurity with smart threat detection, foreseeing potential threats, and adapting defensive strategies. The technology of Artificial Intelligence (AI) is a gamechanger in the field of cybersecurity, enhancing threat detection, predicting potential threats, and creating a more robust security strategy. Many machines learning (ML) algorithms have been employed for intrusion detection systems (IDSs), malware classification and anomaly detection and have been shown to be superior to signature-based methods for known and unknown attacks [17]. Moreover, Deep Learning (DL) has improved cyber security based on AI by providing automatic feature extraction and high dimensional complex representation learning from network traffic. The Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM) network, and Autoencoders have been proven to be excellent algorithms for intrusion detection, malware detection, and abnormal communications detection in the WSN and IoT environment [33, 36, 37]. The evolution of the Intrusion Detection Systems (IDS) from signature-based to anomaly-based detection systems and hybrid systems that can detect zero-day attacks and adapt dynamically to the continuously changing threat-landscape have also been seen [18, 19, 31, 34]. But the limitations of edge devices, complexity of training, interpretability of the models, and computational burden of AI-driven security solutions remain.

2.3. Introduction of Federated Learning and Blockchain Technologies to IoT.

In response to privacy, trust and decentralization issues of centralized AI models, the recent research has shifted much weight towards Federated Learning (FL) and Blockchain technologies. The Federated Learning (FL) approach allows distributed model training without uploading the raw data to centralized servers, thus maintaining data privacy and promoting collaborative learning for multiple IoT devices [25,27]. While these benefits exist, FL is still prone to model poisoning, gradient leakage, backdoor attack, communication overhead, and such, and needs enhanced aggregation and defense.

Blockchain technology plays a complementary role to the use of AI-powered security systems, enabling decentralized trust management, secure data storage, authentication and verification of transactions that are difficult to tamper with [28, 29]. By combining Blockchain with Federated Learning, the partnership promises to create more secure, privacy-conscious, and trustworthy IoT systems, providing data integrity and improving collaborative intelligence. Additionally, the adoption of Edge Computing and Edge AI has made real-time security analysis possible by allowing intelligent processing of data as it comes in, minimizing latency, bandwidth usage, and privacy concerns [30]. Yet scalability, consensus delays,

transaction fees, energy usage, model synchronization and secure update procedures are all major challenges to scaling into the large scale.

2.4. Critical Literature Review

Table 1.Critical Literature Review of Security Mechanisms for WSN-IoT Environments

Ref.	Methodology/Technique	Contribution	Key Limitation
[1]	WSN Architecture Survey	Established foundational WSN architecture, communication model, and challenges	Limited focus on security intelligence
[5]	WSN Security Framework	Defined core security requirements for sensor networks	Resource constraints remained unresolved
[17]	SVELTE IDS	Introduced real-time intrusion detection for IoT environments	Scalability limitations
[20]	Deep Learning (DL)	Demonstrated the effectiveness of DL for automated feature learning	Cybersecurity applications not fully explored
[25]	Federated Learning (FL)	Introduced privacy-preserving distributed learning paradigm	Vulnerable to poisoning attacks
[27]	Federated Learning Survey	Identified major FL challenges and research directions	Trust and security mechanisms lacking
[28]	Blockchain-Based IoT Security	Proposed decentralized trust management for IoT systems	High computational overhead
[33]	Deep Learning IDS for IoT	Achieved high intrusion detection accuracy using DL	Lack of model explainability
[34]	ML-Based IoT Security Survey	Comprehensive taxonomy of AI-driven IoT security solutions	Explainable AI not addressed
[40]	DL Cybersecurity Survey	Compared DL techniques for IoT cybersecurity applications	Energy efficiency concerns ignored
[49]	Edge Intelligence for IoT Security	Enabled low-latency and distributed threat detection	Resource-constrained deployment challenges
[50]	Explainable AI (XAI) for Cybersecurity	Improved transparency and interpretability of AI decisions	Limited implementation in WSN/IoT systems

2.5 Research Gaps Identified from the Literature

Although there has been significant advancement in the application of Artificial Intelligence (AI), Deep Learning (DL), Federated Learning (FL), Blockchain (BC) and Edge Intelligence (EI) to secure Wireless Sensor Networks (WSNs) and Internet of Things (IoT) ecosystems, there are still numerous challenges to be overcome. Current AI-based intrusion detection systems and cybersecurity models are mostly black-box systems with poor explainability, transparency, and user trust, as well as high computational complexity, memory usage, and high energy consumption, which makes them difficult to implement in WSN-IoT settings with limited resources. In addition, most of current research is based on benchmark datasets with limited complexity and limited heterogeneity and dynamics in real use. The lack of standardization of datasets, evaluation procedures and benchmarking methods further hinder objective comparison, reproducibility and practical generalization of proposed security solutions.

The challenges of privacy, robustness and scalability remain huge in next generation intelligent security systems. While Federated Learning offers many benefits for data privacy, it can be susceptible to model poisoning, inference attacks, communication overhead, and gradient leakage. Likewise, the Blockchain-based security mechanisms offer more trust and data integrity, but lack scalability, consensus latency, storage space requirements and energy consumption. Moreover, existing AI security solutions suffer from a lack of adversarial attack resistance, zero-day attack protection, advanced persistent threat (APT) resistance, and comprehensive cross-layer protection and autonomous response to threats. One more restriction is that the majority of current security architectures are tested in a static or simulated setting, and the impact of real-time network dynamics, mobility of devices, heterogeneous communication protocols, and streaming data is minimized. Given these challenges, a lack of a comprehensive cybersecurity framework exists in the literature that embeds Explainable Artificial Intelligence (XAI), Edge Intelligence, Federated Learning, Blockchain and continual learning all within a single architecture. Such an integrated framework should offer scalable, energy-efficient, adversarially robust and autonomous security that would enable the provision of real-time security for next-generation intelligent WSN-IoT ecosystems.

3. Future Research Directions

The following are the directions for future research in the field of AI driven security in Wireless Sensor Networks (WSNs) and IoT systems:

1. to build intelligent, adaptive, scalable, and resource-efficient security architectures for new environments to counter ever-changing cyber threats, enhance trust, privacy, explainability and sustainability [10, 14, 15];
2. integration of Explainable Artificial Intelligence (XAI) to improve transparency, interpretability, forensic analysis, trustworthiness of intrusion detection and threat intelligence systems [23, 34, 40];
3. secure aggregation methods and mechanisms to ensure the robustness of Federated Learning (FL) against poisoning, backdoor attack and gradient leakage [25,27], [43], [44]; and
4. lightweight architectures for implementing blockchain-based AI security models for decentralized authentication, secure model sharing and immutable audit trails for IoT constraints [28], [29], [38]; and
5. real-time threat detection systems, which use edge intelligence and TinyML, for low-latency cybersecurity at the device and gateway level [30], [33], [34]; and
6. the use of Green AI techniques like pruning, quantization, and knowledge distillation to develop energy-efficient and environmentally friendly security solutions [20], [21], [40].
7. Adversarial robust machine learning models through adversarial training and robust feature engineering to counter attacks on AI systems [21] and [23] and [34]; and,
8. Cross-layer security mechanisms and Digital Twin technologies for predictive threat analysis, attack simulation and adaptive mitigation in cyber-physical environments [29], [31] and [32];
9. reinforcement learning and cognitive security-based evolution towards autonomous and self-healing cybersecurity systems for automated detection, adaptation and recovery [23], [34], [40];
10. the study of quantum-resistant cryptographic methods, as well as ethical frameworks and governance principles to guide the secure deployment of AI-powered IoT systems, ensuring their fairness, accountability, and transparency [15], [23], [38];

11. standardization of datasets, protocols, and hybrid security architectures incorporating AI, XAI, FL, blockchain and edge computing to provide scalable, repeatable and secure cybersecurity solutions for future IoT ecosystems [17,18].

4. Research Methodology

This study is conducted in the context of a Systematic Literature Review (SLR) following the PRISMA guidelines, to understand the role of Artificial Intelligence (AI) in improving the Wireless Sensor Networks (WSNs) Security in IoT (Internet of Things) applications. The review utilizes a systematic approach to find, evaluate, and synthesize the peer-reviewed literature of the past decade (2015–2025) from top scientific databases, such as IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, Scopus, and Web of Science. The methodology mainly concentrates on studying the WSN-IoT security threats, AI-enabled defence techniques, intrusion detection techniques, federated learning model, blockchain-based security model, and recent studies in the field of WSN-IoT security [10], [12], [14], [15], [34], [40].

4.1 Research Questions

The review covers five research questions related to (i) major security threats in the WSN-IoT and their mitigation, (ii) AI-based security techniques, (iii) effectiveness of machine learning and deep learning for intrusion detection, (iv) challenges in deploying AI in resource constrained WSNs, and (v) future research directions on secure and resilient AI enabled WSN ecosystems [3], [10], [17], [18], [34].

4.2 Literature Search and Selection

A thorough search strategy was used, where several Boolean combinations of keywords were employed related to the WSN, IoT, AI, ML, DL, IDS, FL, Blockchain, Edge, and Cybersecurity. They only included studies written in the English language, in peer-reviewed journals with experimental validation and performance evaluation, and excluded duplicate, non-peer-reviewed, or non-relevant publications to guarantee the quality of the review and reliability of the results [11, 12, 14, 34, 39].

4.3 Quality Assessment

Selected studies were evaluated according to pre-defined quality criteria such as research objectives, methodological rigor, quality of collected data, experimental validation, reproducibility and practical contribution to the security of a WSN. The studies that met the quality standards set were retained for further analysis, [18, 31, 34].

4.4 Completely remove data from various sources and combine them into a coherent synthesis.

Systematic extraction of relevant information like security threat, AI techniques, datasets, evaluation metrics, performance outcomes, limitations, and the future research opportunities. The literature selected was classified into 5 themes: Machine Learning-based Security Solutions, Deep Learning-based Intrusion Detection Systems, Federated Learning Security Frameworks, Blockchain-Assisted Security Architectures, Hybrid AI Security Models. A comparative and thematic analysis was then conducted to highlight the main findings, strengths and weaknesses and research gaps concerning AI-based WSN-IoT security [20, 25, 27, 28, 33, 36, 37, 40].

4.5 Discuss security requirements in WSNs.

The key requirements for WSN security are confidentiality, integrity, availability, authentication, and non-repudiation. Confidentiality, integrity, availability, authentication and non-repudiation are the core requirements for WSN security.

4.6 Threat Models in Wireless Sensor Networks

A WSN can be attacked by a combination of attack types over several layers of the system. Physical attacks like node capture, tampering and jamming affect the integrity of the devices and form insider threats [20]–[24]. The attacks against the network layer are sinkhole, Sybil, wormhole, and selective forwarding attacks that affect the routing and data flow [25]–[28]. The degradation of network reliability and packet delivery caused by routing attacks, including black hole, gray hole, hello flood, and routing table poisoning, are described in [29]–[32]. Application layer attacks include malware injection, data manipulation, false data reporting and AI-driven adversarial attacks on intelligent WSN components [33]–[36].

The distributed structure, resource-limited sensor nodes, and deployment in unsupervised and hostile environments of Wireless Sensor Networks (WSN) make them susceptible to many types of security attacks. These attacks can involve different layers of the network stack, and may affect the confidentiality, integrity, availability and reliability of the sensed data. In general, WSN attacks can be divided into four types: Physical Attacks, Network Layer Attacks, Routing Attacks, and Application Layer Attacks, as shown in Figure X. Physical attacks involve capturing nodes, tampering and jamming, which directly affect sensor hardware or communication paths. At the network layer attacks like sinkhole, Sybil, wormhole, selective forwarding attacks etc, affect packet transmission and topology. The different types of routing attacks such as black hole, gray hole, hello flood, routing table poisoning change the routing information so as to affect the performance of the network and the data delivery. Application-layer attacks include those that involve malware injection, false data injections, data aggregation manipulation, and adversarial AI attacks, which are attacks on the data processing and decision-making mechanisms. Awareness of these attack categories is crucial for developing a powerful approach to AI-based intrusion detection, secure routing protocols, and comprehensive defense system for contemporary WSN-based IoT applications.

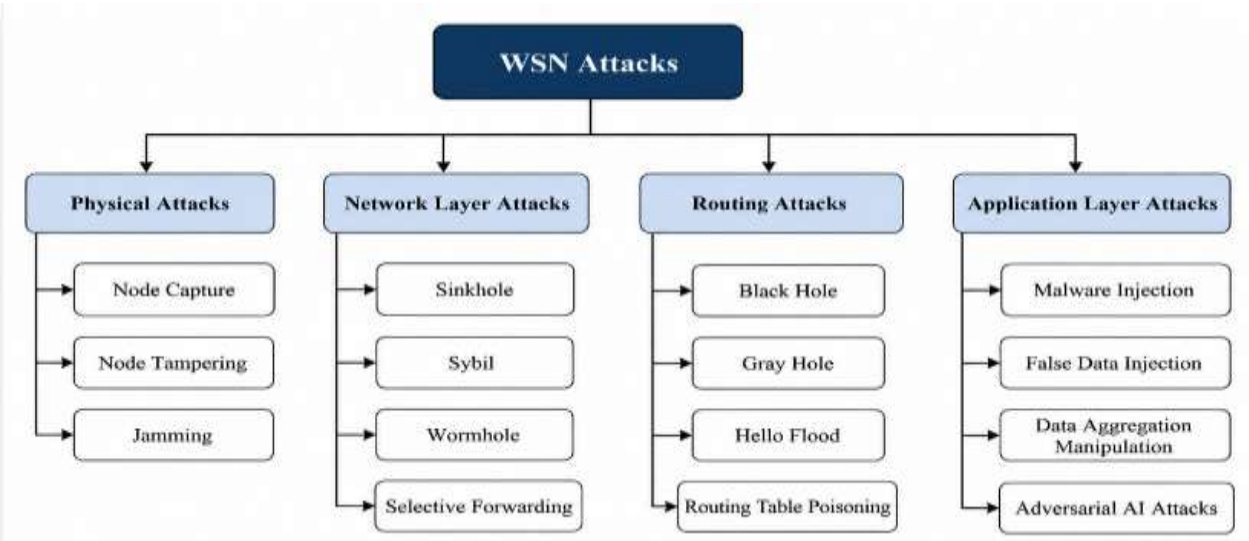

Figure 2.Classification of security attacks in Wireless Sensor Networks (WSNs)

Table 2.Summary of Common Security Attacks in Wireless Sensor Networks and Their Impacts

Attack Category	Representative Attacks	Impact
Physical Layer	Jamming, Node Capture	Service Disruption, Key Exposure

Network Layer	Sinkhole, Sybil, Wormhole	Routing Manipulation
Routing Layer	Black Hole, Gray Hole, Hello Flood	Packet Loss, Traffic Diversion
Application Layer	Malware, False Data Injection	Data Corruption, System Failure

5. Artificial Intelligence for WSN Security

Artificial Intelligence (AI) has become a promising method of protecting Wireless Sensor Networks (WSNs) from emerging malicious attacks in IoT environments. AI models offer a data-driven, adaptive, and autonomous approach to security that goes beyond traditional techniques like cryptographic and rule-based solutions, offering the ability to identify intrusions, anomalies, predict attacks, and respond to threats in real-time. In dynamic deployments of WSNs, Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL), and hybrid approaches enhance detection accuracy, scalability and resilience with low false positive rates [23,24] and [34].

5.1 Security Approaches based on Artificial Intelligence

The use of Artificial Intelligence (AI) has become a gamechanger in securing Wireless Sensor Networks (WSNs) and Internet of Things (IoT) systems, offering intelligent, adaptive, and automated threat detection capabilities that surpass traditional rule-based security measures. Many ML algorithms such as SVM, DT, RF, KNN and ANN have been used to detect attacks, classify them and detect anomalies in the network traffic patterns, leading to better detection of unknown and zero-day attacks [20]–[24], [31], [33] and [34]. In addition, Deep Learning (DL) models like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Autoencoders can be used to automatically learn complex spatial and temporal patterns from high-dimensional network data, which is suitable for recognizing sophisticated cyber threats and anomalous communication behaviours [20, 21, 33, 36, 37, 40]. Reinforcement Learning (RL) can further enhance these functions by enabling autonomous decision-making to ensure secure routing, adaptable intrusion mitigation, and dynamic resource management through ongoing interaction with network environments. Furthermore, by incorporating intelligent threat detection, decentralized learning, privacy protection, trust management, and secure data sharing, hybrid AI frameworks that incorporate ML, DL, Federated Learning (FL), Blockchain, and Edge Intelligence have proven to be more effective [25]–[30] [43] [44]. The use of AI-powered IDSs, such as signature-based, anomaly-based, and hybrid models, has consistently outperformed traditional security methods in terms of detection accuracy, precision, recall, and F1-score, with hybrid IDS models offering the strongest protection against both known and new types of cyber-attacks. However, some challenges such as computational complexity, model interpretability, scalability, and energy consumption are still present which hinder the implementation of AI-based security systems for future WSN-IoT networks, thus necessitating the development of lightweight, explainable and energy-efficient intelligent security systems for next-generation WSN-IoT networks.

Table 3.Comparison of Artificial Intelligence Techniques and Their Applications in Wireless Sensor Network (WSN) Security

AI Technique	Algorithm	Primary Application	Advantages
Machine Learning	SVM	Intrusion Detection	High accuracy
Machine Learning	Decision Tree	Attack Classification	Interpretability
Machine Learning	Random Forest	Threat Detection	Robustness

Deep Learning	CNN	Traffic Analysis	Automatic feature extraction
Deep Learning	RNN	Sequential Attack Detection	Temporal learning
Deep Learning	LSTM	Predictive Security Analytics	Long-term dependency modeling
Deep Learning	Autoencoder	Anomaly Detection	Unsupervised learning
Reinforcement Learning	Q-Learning/DQN	Adaptive Security	Autonomous decision making
Hybrid AI	CNN-LSTM	Complex Threat Detection	Improved performance
Hybrid AI	Federated Learning	Privacy-Preserving Security	Distributed intelligence

Figure 6. AI-Based WSN Security Framework

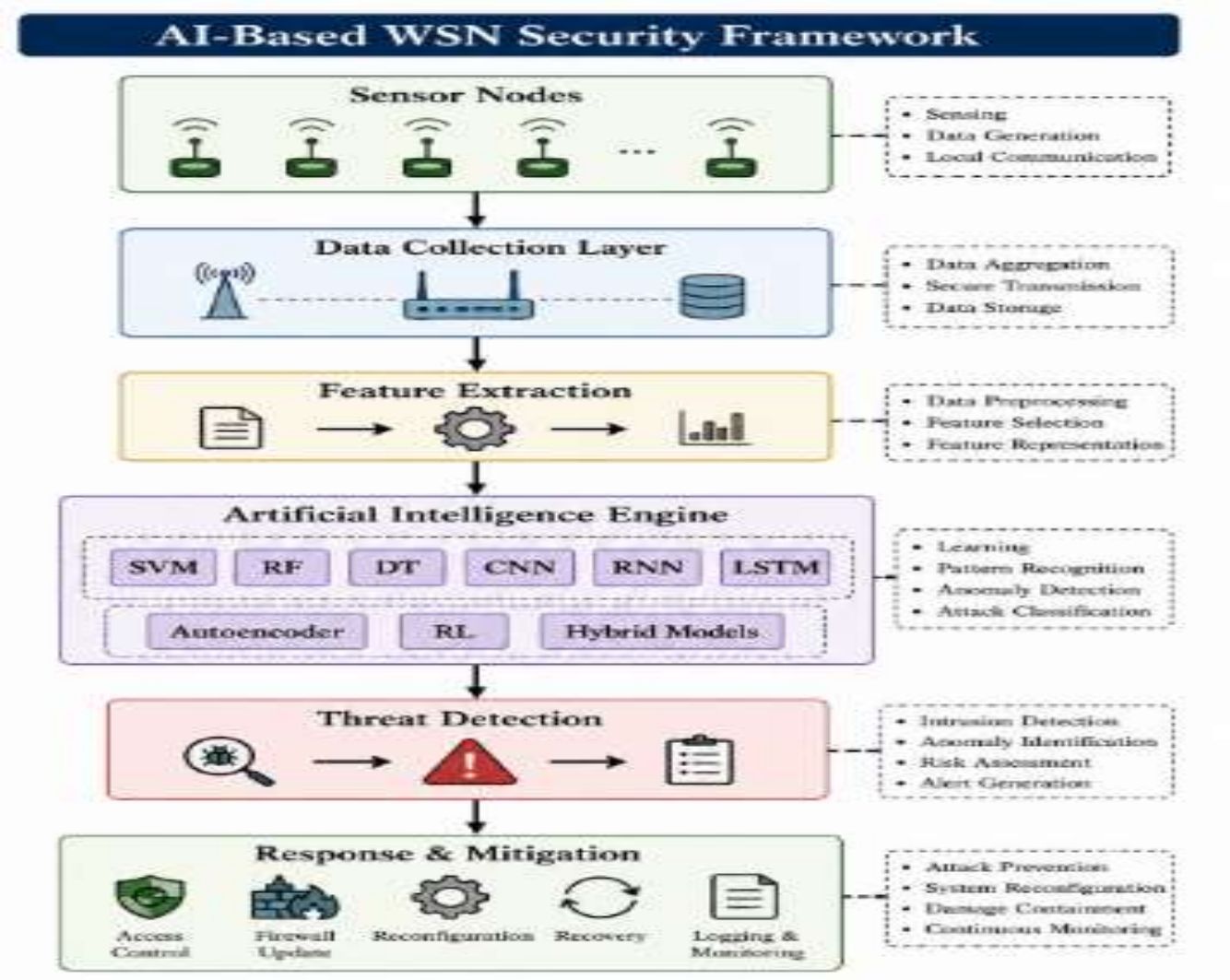

Figure 3.Conceptual Workflow of an AI-Powered Intrusion Detection and Response System for Secure WSN–IoT Networks.

5.2. Deep Learning and Federated Learning for IoT Security

Three technologies have become prominent in protecting IoT and WSN environments from the ever-growing threat of cyber-attacks: Federated Learning (FL), Deep Learning (DL), and Edge AI. DL models like CNNs, RNNs, and LSTMs have the capability to extract features automatically and detect intrusions, malicious activities, DDoS attacks, and abnormal network behavior [20, 21, 33, 36, 37, 40]. In terms of privacy, Federated Learning offers several benefits, such as decentralized collaborative model training without exposing sensitive local data, minimizing centralized vulnerabilities, and fostering regulatory compliance [25]–[27], [43], [44]. Moreover, by processing data at the network edge, Edge AI enables timely threat detection and response, which reduces latency, communication overhead and reliance on the cloud, thereby making it more scalable and efficient [29], [30]. However, issues like model poisoning, gradient leakage and adversarial attacks remain and require reliable distributed learning frameworks, secure aggregation and blockchain-based trust management [27], [28]. The three technologies—DL, FL, and Edge AI—offer an scalable, privacy-preserving and resilient basis for future IoT cybersecurity architectures [34], [38]–[40].

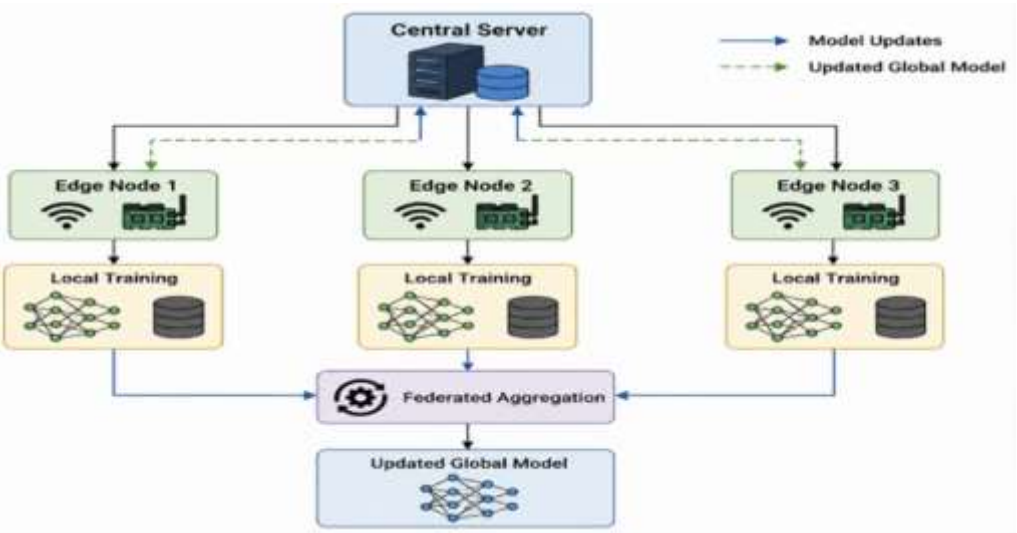

Figure 4.Federated Learning-Based Distributed Security Framework for Wireless Sensor Networks (WSNs)

5.3. Comparative Analysis of AI-Driven Security Mechanisms in WSN–IoT Environments

The synergy of WSNs and IoT has led to increased cyberattack surface, making it necessary to go beyond cryptographic security mechanisms, and rely on AI-based security mechanisms **[10]–[16], [29], [39]**. The quality of datasets and learning algorithms largely determines the security performance **[18], [19], [31], [34]**. Early studies were conducted on KDD Cup 1999 and NSL-KDD datasets, while recent research has turned to new IoT-specific datasets, including Bot-IoT, UNSW-NB15, CICIDS2017 and IoT-23, where there is still a need to have a standard IoT-WSN-specific benchmark **[31], [34], [40]**. While traditional machine learning approaches like SVM, Decision Trees, Random Forest, and KNN offer computational efficiency and moderate detection accuracy **[18], [23], [24], [31]**, deep learning methods like CNNs, RNNs, and LSTMs excel in feature extraction and attack detection performance **[20], [21], [33], [36], [37], [40], [45]–[47]**. The concept of Federated Learning (FL) further extends privacy by allowing model training through decentralization instead of sharing raw sensor data **[25]–**

[27], [43], [44], and hybrid AI solutions aim to strike a balance between accuracy, privacy, and resource allocation **[34], [40], [44]**. In terms of accuracy, the rule-based system would typically yield 80–90% detection accuracy, while machine learning would yield 90–97% and deep learning would exceed 98% and high accuracy is usually coupled with a high number of operations and false positives **[17]–[19], [31], [33], [34], [36], [37], [40]**. While energy efficiency is still a key issue, with resource-limited nodes, lightweight ML, TinyML, edge computing, and fog computing being potential solutions for low-power deployments **[1], [2], [13], [14], [30], [34]**. Another scalability related challenge in a large-scale IoT deployment is the limited communication and processing capabilities of centralized security approaches, while FL and blockchain-based approaches enhance distributed trust and scalability, but with increased latency and complexity **[25]–[30], [43], [44]**. Future research needs to emphasize hybrid, lightweight, privacy-protecting, and scalable architectures for AI-driven security that can maintain a high detection accuracy while having a low energy and computational cost **[27], [28], [30], [34], [40], [44]**.

Table 4.Comparative Performance Analysis of AI-Based Security Techniques for Wireless Sensor Networks (WSNs) Based on Detection Rate and Energy Efficiency

Study	AI Technique	Detection Rate (%)	Energy Efficiency
[17]	SVELTE IDS	85–90	High
[18]	ML-Based IDS	90–94	High
[36]	Deep Neural Network	95–97	Medium
[37]	Deep Autoencoder	97–98	Medium
[33]	CNN-Based IDS	98–99	Medium-Low
[34]	Hybrid ML/DL	96–99	Medium
[25]	Federated Learning	95–98	High
[26]	Federated Learning	96–99	High
[28]	Blockchain Security	90–95	Medium
[27]	Federated AI Framework	97–99	High

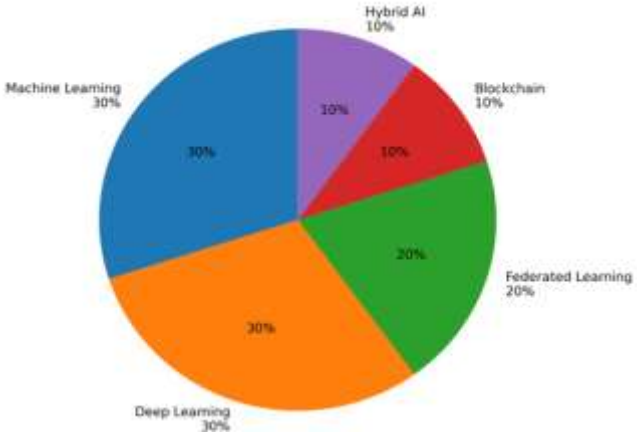

Figure 5. Distribution of Artificial Intelligence Techniques Used in Wireless Sensor Network Security Research.

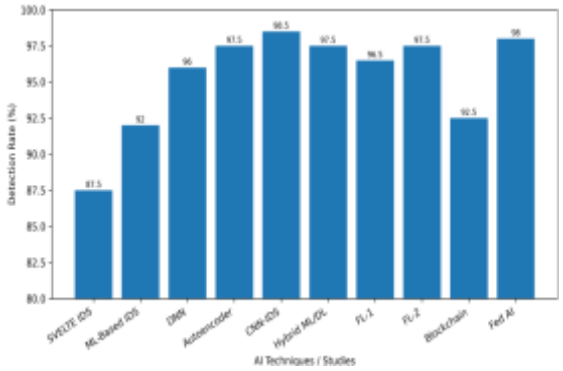

Figure 6. Comparative Detection Performance of AI-Based Intrusion Detection Techniques in Wireless Sensor Networks.

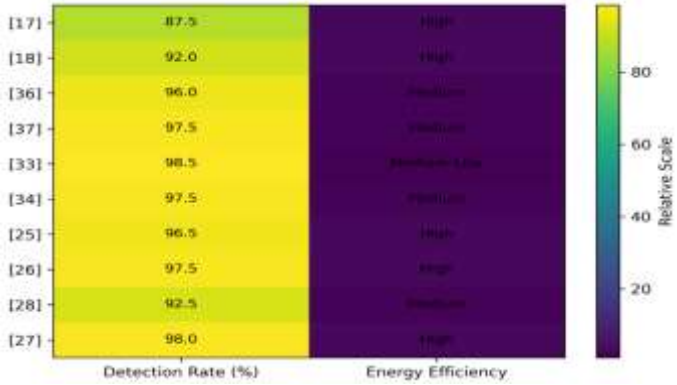

Figure 7.Heat Map Comparing Detection Accuracy and Energy Efficiency of AI-Based WSN Security Techniques.

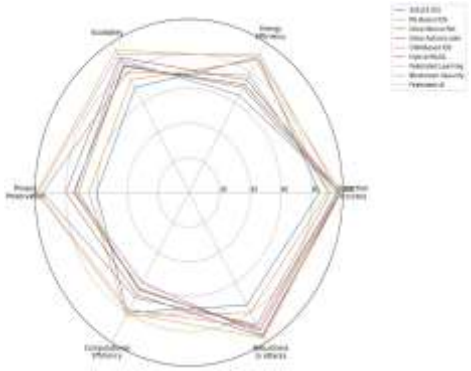

Figure 8. Multi-Criteria Performance Comparison of AI-Based Security Techniques for Wireless Sensor Networks.

6. Open Challenges and Research Gaps

Although significant progress has been made in the field, there are still several challenges that need to be addressed to create secure, reliable, and intelligent security systems for WSNs and IoT [10]–[16], [29], [39]. While great strides have been made in the area of AI-backed security for WSNs and IoT, there are still some challenges that remain to be tackled to ensure the creation of scalable, reliable, and intelligent, security systems for WSNs and IoT [34], [40]. Some of the key areas of research are the absence of realistic, standardized and balanced datasets, which makes it difficult to generalize and compare models across various IoT scenarios [34], [40]. Confidentiality and trust concerns also persist, as data leakage is

a concern in centralized learning, and federated learning architectures can be vulnerable to potential leaks [25]–[27], [44]. Privacy-preserving techniques, such as differential privacy, secure aggregation and blockchain-based validation, address those concerns [25]–[28], [44]. In addition, most of the deep learning-based security models are black-box models, which lack interpretability and trust; and are vulnerable against adversarial attacks, which has raised concerns about robustness and reliability [20], [21], [33], [36], [37], [40], [46]. The scarcity of computing resources, memory, and energy also poses limitations for implementing complex AI models in sensor nodes, underscoring the importance of lightweight and energy-efficient approaches like TinyML and edge AI [30], [34], [40]. Further, current security approaches are largely tested in a static or synthetic environment and may not be able to deal with dynamic attacks, evolving attack patterns, mobility of devices, continuous data streams and network topologies [17]–[19], [31], [32], [34], [40]. Hence, further research is needed on trustworthy and explainable AI, adversarial robust learning, privacy-centric security approaches, standardized datasets, scalable edge-intelligence designs, online and continuous learning approaches, distributed intrusion detection systems, and autonomous security orchestration approaches that will provide adaptable, real-time security across large, dynamic IoT environments [25]–[34], [40], [44].

7. Conclusion

With the rapid development of IoT, WSNs are becoming an essential technology for smart cities, healthcare, industrial automation, environmental monitoring and precision agriculture. Their decentralized structure, limited resources, and open communication systems make them vulnerable to a variety of cybersecurity threats, nonetheless. The review points out that in large scale IoT ecosystems traditional security methods such as cryptography, authentication, key management and secure routing are indispensable for securing the confidentiality, integrity and availability of the data, but they are limited in terms of scalability, flexibility and computational complexity. Machine learning, deep learning, federated learning, edge intelligence, explainable AI, and blockchain integration are all areas that can be leveraged with AI to improve intrusion detection, anomaly detection, and intelligent threat mitigation. The study also highlights key research opportunities for lightweight security models, explainability, adversarial robust, privacy preservation, and energy efficiency approaches for resource-limited WSN environments. Leveraging AI in conjunction with traditional security approaches and building adaptive, hybrid, and trustworthy security frameworks that harness edge computing, federated learning, and blockchain technologies will be a promising area for future research. In summary, the fusion of AI and IoT holds immense potential for developing smart, scalable, robust, and sustainable future cybersecurity solutions for WSN-enabled IoT deployments.

8. Future Research Directions

Future security research for WSN-IoT should be directed towards the creation of Adaptive, Scalable, Energy efficient, Explainable and Resilient Security frameworks to meet the changes in cyber threats in resource limited environments. Combining Explainable AI (XAI), TinyML, and edge intelligence can improve transparency, trustworthiness, and threat detection in real-time while minimizing computational and communication load. Federated learning and distributed analytics can take privacy protection, scalability and collaborative security in decentralized IoT networks one step further.

The future of quantum-enabled attacks is looming, and emerging infrastructures will need post-quantum cryptographic mechanisms to protect against those future attacks. They will also need lightweight

security solutions for constrained devices. Moreover, 6G, powered by IoT, will also require privacy-preserving communication architectures, decentralized authentication, and intelligent threat detection and analysis for IoT ecosystems. By combining Digital Twin technology with AI powered analytics, real-time attack simulation, vulnerability assessment, predictive defense and proactive mitigation of advanced attacks can enable secure, autonomous and next generation WSN-IoT systems for development.

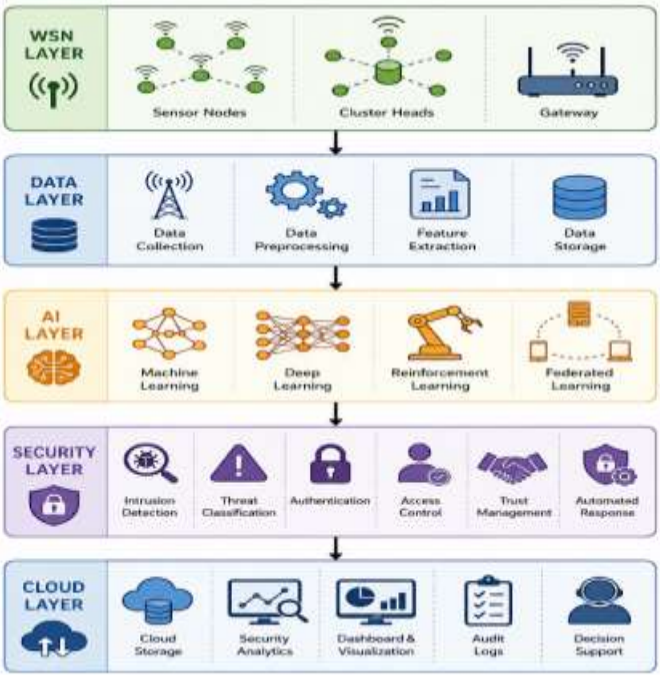

Figure 8.Layered Architecture of an AI-Enabled Secure Wireless Sensor Network Ecosystem

References

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, Mar. 2002, doi: 10.1016/s1389-1286(01)00302-4
2. J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008, doi: 10.1016/j.comnet.2008.04.002. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128608001254. [Accessed: July 11, 2026]
3. Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008, doi: 10.1109/comst.2008.4625802
4. Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006, doi: 10.1109/comst.2006.315852
5. A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, p. 53, June 2004, doi: 10.1145/990680.990707
6. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 293–315, Sept. 2003, doi: 10.1016/s1570-

8705(03)00008-8
7. L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” *Proceedings of the 9th ACM conference on Computer and communications security*, pp. 41–47, Nov. 2002, doi: 10.1145/586110.586117
8. Haowen Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” *Proceedings 19th International Conference on Data Engineering (Cat. No.03CH37405)*, pp. 197–213, doi: 10.1109/secpri.2003.1199337
9. R. Irani, S. Khatibi, and S. Eivazzadeh, “Security by Light in Sensor Networks: A Structured Review of Optical and Photonic Security Mechanisms,” *Journal of Cybersecurity and Privacy*, vol. 6, no. 4, p. 115, July 2026, doi: 10.3390/jcp6040115
10. I. Tomic and J. A. McCann, “A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, Dec. 2017, doi: 10.1109/jiot.2017.2749883
11. Q. Yang, X. Zhu, H. Fu, and X. Che, “Survey of Security Technologies on Wireless Sensor Networks,” *Journal of Sensors*, vol. 2015, p. e842392, Aug. 2015, doi: 10.1155/2015/842392. Available: https://www.hindawi.com/journals/js/2015/842392/. [Accessed: July 11, 2026]
12. M. N. Bhuiyan, Dr. Md. M. Rahman, M. M. Billah, and D. Saha, “Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security and market opportunities,” *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 1–1, 2021, doi: 10.1109/jiot.2021.3062630
13. R. S. Mohammed, A. H. Mohammed, and F. N. Abbas, “Security and Privacy in the Internet of Things (IoT): Survey,” Feb. 2019, doi: 10.1109/iceccpce46549.2019.203774
14. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/jiot.2017.2683200
15. N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/comst.2019.2910750
16. S. Bansal and V. K. Tomar, “Challenges amp; Security Threats in IoT with Solution Architectures,” *IEEE Xplore*, Jan. 01, 2022. doi: 10.1109/PARC52418.2022.9726660. Available: https://ieeexplore.ieee.org/document/9726660. [Accessed: July 11, 2026]
17. H. H. Sulimani, “Real-Time Intrusion Detection in Fog Computing Environments Using Machine Learning Approaches,” *2026 IEEE 5th International Conference on Computing and Machine Intelligence (ICMI)*, pp. 1–6, Apr. 2026, doi: 10.1109/icmi68585.2026.11539796
18. P. C, T. B. B. R, K. K, K. M, M. S, and S. C. C, “A Comprehensive Survey on Intrusion Detection Systems in IoT-Enabled Wireless Sensor Networks: Techniques, Challenges and future directions,” *2024 International Conference on Smart Technologies for Sustainable Development Goals (ICSTSDG)*, pp. 1–7, Nov. 2024, doi: 10.1109/icstsdg61998.2024.11026314
19. M. M. Rahman and H. J. Kim, “The Performance Evaluation of Intrusion Detection Models: The Boosting Model and the Graph-Based Model,” *2025 International Conference on Smart Applications, Communications and Networking (SmartNets)*, pp. 1–5, July 2025, doi: 10.1109/smartnets65254.2025.11106787

20. R. Darwish and K. Roy, "Comparative Analysis of Federated Learning, Deep Learning, and Traditional Machine Learning Techniques for IoT Malware Detection," *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, pp. 1–10, Feb. 2025, doi: 10.1109/icaic63015.2025.10849203. Available: https://ieeexplore.ieee.org/abstract/document/10849203. [Accessed: July 11, 2026]
21. N. V. Rajeesh Kumar and M. Arun, "Deep Learning Model to Improve Security in IOT Systems," *2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, pp. 1–5, Mar. 2022, doi: 10.1109/icstsn53084.2022.9761347
22. M. Moucharraf, M. Ridouani, F. Salahdine, and N. Kaabouch, "Hybrid Deep Learning and Boosting Approach for Iot Intrusion Detection Using Autoencoder and Xgboost," *2025 International Conference on Circuit, Systems and Communication (ICCSC)*, pp. 1–6, June 2025, doi: 10.1109/iccsc66714.2025.11135052
23. Pragya Bajpayi, S. Sharma, and M. S. Gaur, "AI Driven IoT Healthcare Devices Security Vulnerability Management," Mar. 2024, doi: 10.1109/icdt61202.2024.10488939. Available: https://ieeexplore.ieee.org/document/10488939. [Accessed: July 11, 2026]
24. A. Srivastava, A. Jindal, A. Shrivastava, and V. Sawan, "A Review on IoT Attack Detection Using Machine Learning Algorithms," *2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, pp. 1098–1103, July 2025, doi: 10.1109/icdici66477.2025.11135398
25. Y. Liu *et al.*, "Deep Anomaly Detection for Time-series Data in Industrial IoT: A Communication-Efficient On-device Federated Learning Approach," *IEEE Internet of Things Journal*, pp. 1–1, 2020, doi: 10.1109/jiot.2020.3011726
26. D. B. Srinivas, R. H C, S. P. H R, and R. Jadhav, "A Hybrid Privacy-Preserving Framework for Machine Learning in Edge Computing," *2026 Fourth International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, pp. 179–185, Apr. 2026, doi: 10.1109/icaiss68683.2026.11525873
27. [W. Toussaint and A. Y. Ding, "Machine Learning Systems in the IoT: Trustworthiness Trade-offs for Edge Intelligence," *2020 IEEE Second International Conference on Cognitive Machine Intelligence (CogMI)*, pp. 177–184, Oct. 2020, doi: 10.1109/cogmi50398.2020.00030
28. "IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management," doi: 10.1109/ieeestd.2021.9329260
29. N. Nelufule, T. Z. Singano, D. Shadung, and K. Masemola, "Privacy-Preservation and Containment in IoT Forensics Investigations: A Comparative Study," *2023 11th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC)*, pp. 121–125, Dec. 2023, doi: 10.1109/jac-ecc61002.2023.10479652
30. Y. Zhang, X. Yang, and N. Wang, "Fog Computing-Based Privacy-Preserving Multi-Dimensional and Multi-Directional Data Aggregation for the Internet of Things," *2026 7th International Conference on Computing, Networks and Internet of Things (CNIOT)*, pp. 1–5, May 2026, doi: 10.1109/cniot69547.2026.11582482
31. S. Pathania, M. Singh, and A. Singh, "Machine Learning-Driven Approaches for Intrusion Detection in Wireless Sensor Networks," *2025 7th International Conference on Intelligent Sustainable Systems (ICISS)*, pp. 471–476, Mar. 2025, doi: 10.1109/iciss63372.2025.11076389

32. K. Talal and R. Hadi, "Federated Learning-Based Secure Intrusion Detection Framework for Edge-IoT Communication Systems," *International Journal of Computers and Informatics*, vol. 5, no. 6, pp. 19–51, June 2026, doi: 10.59992/ijci.2026.v5n6p2
33. N. W. Meegammana and H. Fernando, "Detection of Network Attacks on Application Servers Using Deep Learning in IoT Environments," Dec. 2023, doi: 10.1109/icac60630.2023.10417159
34. K. Kamalakannan and V. Parthipan, "Survey of Data-Centric Machine Learning Approaches in IoT-Enabled Self-Evolving Smart Environments," *2025 2nd International Conference on Electronic Circuits and Signaling Technologies (ICECST)*, pp. 1151–1156, Oct. 2025, doi: 10.1109/icecst66106.2025.11307637
35. L. Astakhova and I. Medvedev, "Scanning the Resilience of an Organization Employees to Social Engineering Attacks Using Machine Learning Technologies," *2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, May 2020, doi: 10.1109/usbereit48449.2020.9117746
36. S. M. Nour and S. A. Said, "Deep Learning Performance Evaluation Model for Enhancing Network Intrusion Detection Systems," pp. 61–65, Oct. 2024, doi: 10.1109/niles63360.2024.10753184. Available: https://ieeexplore.ieee.org/document/10753184. [Accessed: July 11, 2026]
37. V. Kurnala, S. A. Naik, D. C. Surapaneni, and Ch. B. Reddy, "Hybrid Detection: Enhancing Network & Server Intrusion Detection Using Deep Learning," *2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, pp. 248–251, Oct. 2023, doi: 10.1109/icccmla58983.2023.10346699
38. M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 269–282, Feb. 2018, doi: 10.1109/jiot.2017.2780232
39. S. K. Jagatheesaperumal, Q.-V. Pham, R. Ruby, Z. Yang, C. Xu, and Z. Zhang, "Explainable AI Over the Internet of Things (IoT): Overview, State-of-the-Art and Future Directions," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 2106–2136, 2022, doi: 10.1109/OJCOMS.2022.3215676. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9930971. [Accessed: July 11, 2026]
40. E. Rodriguez, B. Otero, N. Gutierrez, and R. Canal, "A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1920–1955, 2021, doi: 10.1109/comst.2021.3086296
41. V. S, J. Anand, and R. K. Verma, "IoT-Enabled Sign Language to Speech Converter for Enhanced Communication," *2024 4th International Conference on Advancement in Electronics & Communication Engineering (AECE)*, pp. 1230–1234, Nov. 2024, doi: 10.1109/aece62803.2024.10911559
42. R. P, K. Suresh, B. M, M. Gokul, G. D. Kumar, and A. R, "IoT Based Voice Assistant using Raspberry Pi and Natural Language Processing," *2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS)*, pp. 1–4, Dec. 2022, doi: 10.1109/icpects56089.2022.10046890
43. U. Pandey, V. Kumar, S. Kaushik, and M. Kumari, "IoT-Assisted Gesture-to-Audio Conversion System for Enhancing Accessibility in Speech-Impaired Users," pp. 1–5, Aug. 2024, doi: 10.1109/indiscon62179.2024.10744281
44. Y. Goldberg, "Neural Network Methods for Natural Language Processing," *Synthesis Lectures on*

Human Language Technologies, vol. 10, no. 1, pp. 1–309, Apr. 2017, doi: 10.2200/s00762ed1v01y201703hlt037

45. A. Asheralieva, D. Niyato, and X. Wei, "Dynamic Distributed Model Compression for Efficient Decentralized Federated Learning and Incentive Provisioning in Edge Computing Networks," *IEEE Transactions on Mobile Computing*, vol. 24, no. 7, pp. 6293–6314, July 2025, doi: 10.1109/tmc.2025.3543295
46. I. Jaggi and H. Wadhwa, "Comparative Study of Machine Learning Algorithms for IoT Security," *2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM)*, pp. 1–5, Aug. 2023, doi: 10.1109/elexcom58812.2023.10370131
47. S. Srinivasan *et al.*, "Deep Convolutional Neural Network Based Image Spam Classification," *IEEE Xplore*, Mar. 01, 2020. doi: 10.1109/CDMA47397.2020.00025. Available: https://ieeexplore.ieee.org/abstract/document/9044249. [Accessed: July 11, 2026]
48. Z. He *et al.*, "Edge Device Identification Based on Federated Learning and Network Traffic Feature Engineering," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 4, pp. 1898–1909, Dec. 2022, doi: 10.1109/tccn.2021.3101239