Scientific Journal of Computer Science

futuristech
PT. Teknologi Futuristik Indonesia

Date of publication December 31, 2025, date of current version December 31, 2025.
Digital Object Identifier 10.64539/sjcs.v1i2.2025.328

Article

An Ensemble-based Adaptable and Privacy-aware Threat Detection Mechanism for Wireless Sensor Network in Healthcare Systems

Emmanuel Iheanacho Afonne[1,*], Patrick Ejeh[1], Linda Chioma Aworonye[1]

[1] Department of Computer Science, Novena University, Ogume, Delta State 322107, Nigeria; achokemma@gmail.com
* Correspondence

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Abstract: Recently, wireless sensor networks (WSNs) have been widely integrated in critical applications such as environmental monitoring, smart cities, and modern healthcare for remote patient monitoring and data collection. This makes WSNs increasingly susceptible to security threats, including eavesdropping, jamming, sybil, data injection, routing, senor node capture, malicious intrusion attacks etc., therefore maintaining integrity, confidentiality, and availability of sensitive data and preserving privacy become a challenge. Existing mechanisms do not integrate threat detection, privacy preservation, and adaptability to evolving threats leading to security breaches in the left-out security requirements. This paper proposes an ensemble-based threat detection mechanism (FAL-ELeM-IDS) with privacy-awareness and adaptability to evolving threats for WSNs-based healthcare systems. The ensemble consists of Online Random Forest, Online AdaBoost, Support Vector Machine, Neural Network, and XGBoost to ensure detection high accuracy and low false-positives. Federated Learning combined with ensemble technique to provide confidentiality and a combined Online Adaptive Boosting and Online Random Forests algorithms to provide adaptability. The proposed model trained on a real-world healthcare sensor dataset demonstrates its superiority in performance compared to conventional models. An accuracy of 97.8%, a recall of 97%, precision of 98%, and F1-score of 97.5%, was achieved outperforming individual models by significant margins, showing that the model is accurate and reliable in detecting threats. This mechanism implies enhanced system security and privacy, timely threat mitigation ensuring patient safety, and boost in public acceptance for sensor-based healthcare services. Overall, this work contributes a scalable, privacy-aware, and adaptive threat detection mechanism suitable for integration in the sensitive healthcare applications.

Keywords: Wireless Sensor Networks; Threat Detection; Federated Learning; Adaptive Learning; Dynamic Threats; Ensemble Learning; Online AdaBoost; Online Random Forest.

1. Introduction

Wireless sensor networks (WSNs) have been widely integrated in critical applications such as environmental monitoring [1], smart cities [2], and modern healthcare for remote patient monitoring and data collection [3]. This makes WSNs increasingly susceptible to security threats, including eavesdropping, jamming, sybil, data injection, routing, senor node capture, malicious intrusion attacks [4] etc., therefore maintaining integrity, confidentiality, and availability of sensitive data and preserving privacy become a challenge. Existing mechanisms do not integrate threat detection, privacy preservation, and adaptability to evolving threats leading to security breaches in the left-out security requirements. To solve this problem, this work is aimed at developing an ensemble-based threat detection mechanism with privacy-awareness and adaptability to evolving threats for WSNs-based healthcare systems.

A key contribution of this work is its focus on preserving patient privacy. Data anonymization techniques are integrated to ensure that sensitive patient information is not exposed during analysis. The system employs federated learning with differential privacy mechanisms to protect individual patient data while still enabling effective threat detection [5]. Furthermore, the system employs secure communication protocols to safeguard data

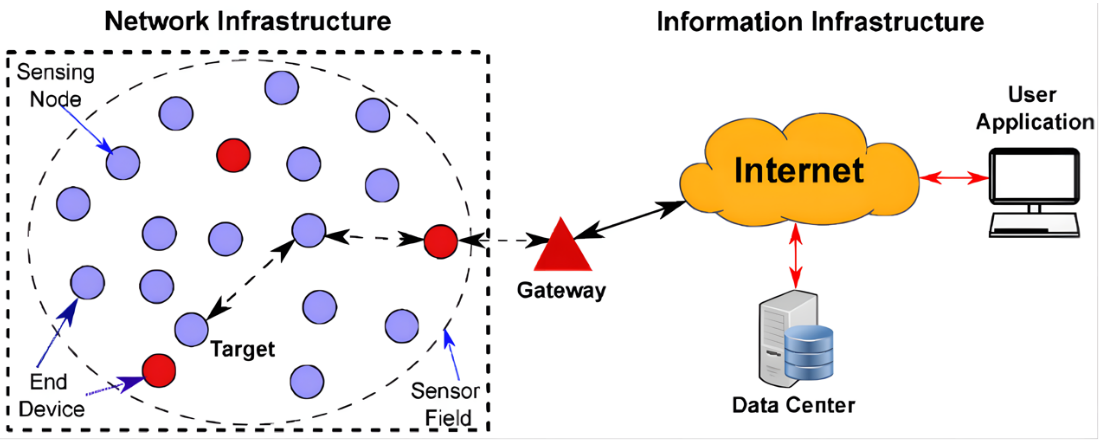

Figure 1. A Simple Architecture of WSN.

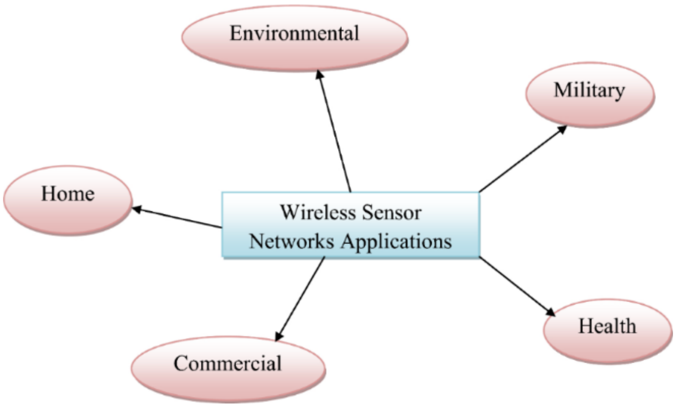

Figure 2. Basic Application Areas for WSNs.

transmission between sensors and the central monitoring station. This layered approach ensures that patient privacy is prioritized without compromising the system's ability to detect and respond to security threats.

The deployment of federated learning framework proposed in this paper encourage collaborations among healthcare organizations in training the intrusion detection model without worrying about patient privacy compromise. Also, health providers will be able to align themselves with the stringent data privacy regulations to ensure compliance. Through federated learning, the thesis will promote a collaborative and secure methodology ensures integrity and confidentiality of patient data. Existing IDS models for intrusion detection in WSNs are grappling with limited dataset leading to poor detection performance. This is because of the significant limitation intrinsic in traditional machine learning techniques. Deploying FL promotes the amalgamation of local health datasets for improved model efficiency and performance [6]. This methodological innovation is important in harnessing the voluminous health data generated in a real-time environment while not jeopardizing the accuracy of detection novel types of cyber threats.

The work in this paper will safeguard healthcare infrastructure against cyber threats, potential intrusions and data breaches. It will foster trust among patients and other stakeholders. The work will ensure privacy and security in health data and health monitoring systems leading to seamless healthcare service delivery. The proactive nature of the methodologies selected for the proposed model enhance the security and privacy of WSNs in healthcare, making this work very significant. The aim is to address current inadequacies, promote collaborative data-sharing.

The rest of this paper has been arranged in the following order: Section 2 provides an explanation of Wireless Sensor Networks as a concept, focusing on its adoption in healthcare systems and privacy risks and threats common in the network under study. Section 3 is concerned with the review of literature. Section 4 presents the research methodology adopted in design, development, and evaluation of the system being discussed. Section 5 states the findings and their implications, while Section 6 highlights the limitations and directions for future studies. Finally, Section 7 concludes the paper.

2. Wireless Sensor Network

2.1. WSN Adoption in Healthcare Systems

The adoption of Wireless Sensor Networks (WSNs) in healthcare has been on the increase. Sequel to this, there is also a corresponding increase in the vulnerability of WSNs-based healthcare systems to cyberattacks. WSNs is critical in monitoring patients' health conditions and facilitates health data transmission to healthcare servers in real-time ensuring prompt medical intervention in emergency situations [7]. WSNs is one of the transformative technologies that have revolutionized healthcare systems, by helping in real-time monitoring and collection of critical data health data including heart rate, blood pressure, body temperature, respiratory rate, blood glucose levels, etc., thereby improving patient-care delivery and management. As shown in Figure 1, WSNs are simply a network of small, intelligent, and energy-efficient sensor nodes interconnected using wireless communication [8] that monitor and transmit data over short distances to centralized systems.

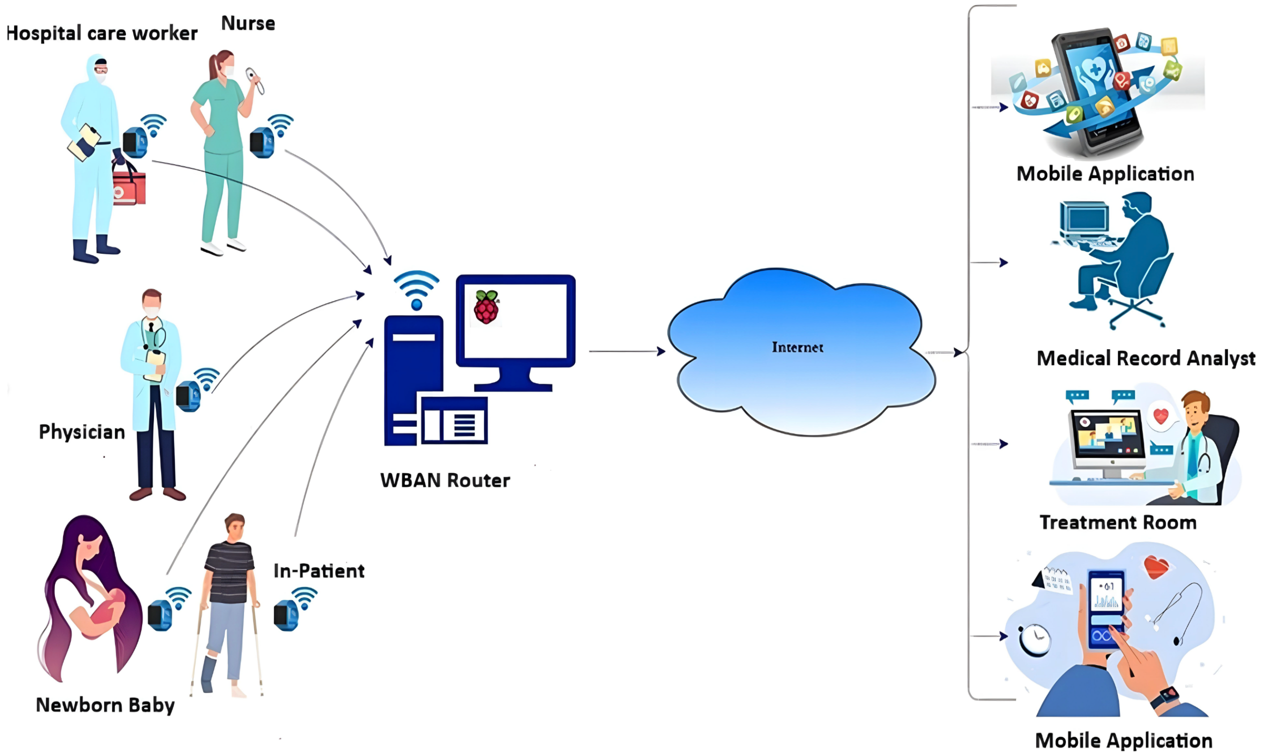

Figure 3. A Typical Architecture of WSN-based Patient Monitoring System. Source: Abubeker and S. Baskar [9].

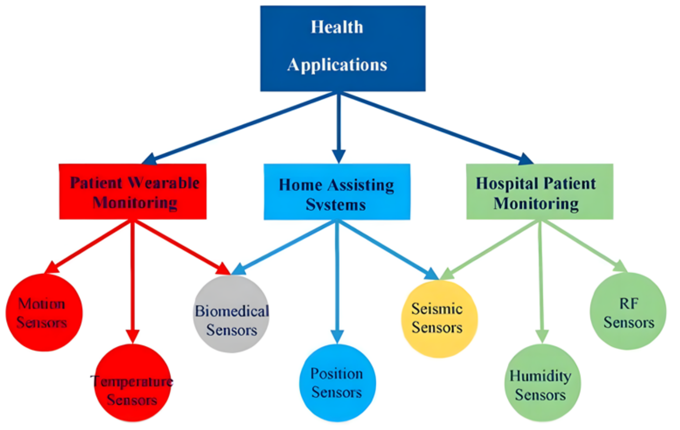

Figure 4. Health Applications of WSNs.

WSN consists of spatially autonomous devices which cooperatively monitor real-life physical or environmental conditions [10]. These networks collect and process data from tiny nodes and then transfer it to the operators. WSNs are compact nodes which are usually low-powered, multifunctional and cheap [11]. WSNs have many applications, as shown in Figure 2, including environmental monitoring [12], smart agriculture [13], home and industrial automation [14], smart cities [15], surveillance [16], wild life tracking [17], [18], underground mines [19] and healthcare [20].

WSNs are extensively deployed in smart healthcare applications for continuous monitoring of patients remotely to acquire real-time health data for the improvement of the patients' quality of life [21]. A WSN-based patient monitoring system consists of sensor, relay and actor nodes with managements from cluster heads, gateways, and base stations as depicted in Figure 3.

The deployment is necessitated by the need to collect patients' health data about their physical, physiological, psychological, cognitive, and behavioral processes. In healthcare and other applications, WSNs combines wireless communications and embedded systems [22], [23], which is used in different medical scenarios like monitoring vital signs, monitoring patients during normal daily lives, in-hospital monitoring, monitoring children and the elderly, monitoring diseases such as Alzheimer's disease and other mental illnesses. Figure 4 shows the different health application areas where WSNs is applied.

2.2. Privacy Risks and Threats in WSNs

WSN is the bedrock of IoTs technology and powers smart systems [24] including healthcare systems. Based on WSNs, IoTs sensors helps in monitoring patients' vital signs, activity levels, and other medical metrics in real time and allow healthcare professionals to identify potential risks and intervene promptly [25]. These sensors have the capability of collecting patients' data in real-time and forward same to software algorithms for analysis. The output of the analysis is transmitted to a central system, which detect potential issues and remotely alert health professionals about any deviations from normal observable conditions. This real-time transmission of vital patients' health parameters provides healthcare professionals with access to important information anytime ensuring efficient diseases management, personalized medicine and timely interventions and decisions in cases of deteriorating situations leading improved patient outcomes.

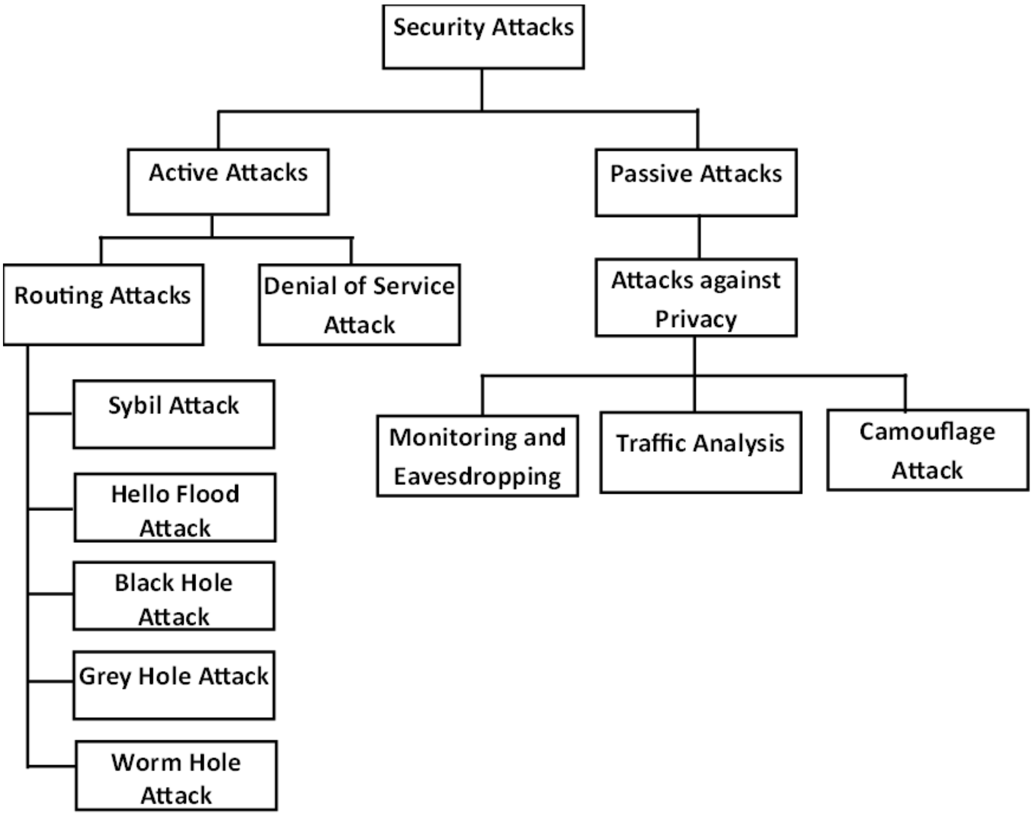

Figure 5. A Taxonomy of Security Threats in WSNs.

Nonetheless, the sensitivity of patient data navigating through WSNs, and the ever-evolving and changing cyber threats landscape, are a major risk to patient privacy, data integrity, and system availability. WSNs are susceptible to multiple cyber threats due to their wireless and distributed nature [26]. Given this scenario, data privacy can be compromised, which may give rise to data breaches due to the sensitive nature of healthcare data. Unattended data breaches have drastic negative effects necessitating the need for efficient and effective security mechanisms to address security and privacy issues of WSNs in healthcare. Due to the dynamic and decentralized nature of WSNs, threat detection is nontrivial as conventional IDS cannot evolve with the dynamic cyber threat landscape. One requirement in WSNs is centralized data collection which can lead to patient privacy and breach in regulatory requirements [27]. Though cybersecurity technologies have developed over the year, traditional IDS models have not been able to address the dynamic landscape of cyber threats [28] because most of the existing IDS models only often rely on the detection of known vulnerabilities and are not enabled or properly equipped to evolve with novel and continuously evolving attacks. Apart from the non-adaptability of existing systems to evolving threats there is also challenges with regards to privacy of patients' health data [29]. Hence cybersecurity in WSNs with particular emphasis on healthcare is of paramount importance in this paper because WSNs is the technological backbone of IoTs present in most modern applications and systems architecture therefore attracting the attention of threat actors and malicious agents [30]. Since the technology is deployed for many areas of applications, it is vulnerable to wide range of cyberattacks, hence securing WSNs is akin to securing IoTs [31]. Cyber-attacks against WSNs can be classified into active and passive attacks as shown in Figure 5.

Active attacks are those cyber-attacks which are based on the OSI stack layer and threaten network integrity and availability. At the physical layer, there are threats such as jamming, tampering, and node cloning [32]. Attacks at the data link layer include denial of sleep, collision, exhaustion and unfairness [33]. At the network layer, we have sinkhole, wormhole, blackhole, selective forwarding (grayhole), 'Hello' flooding, sybil, spoofing, homing and replay attack [34]. These attacks actually hinder proper packet delivery to the destination by exploiting the multi-hop routing protocol used in WSNs. The transport layer is bedeviled by threats such as session hijacking, flooding, and de-synchronization attacks while the application layer is threatened by selective forwarding, deluge, and clock skewing. Other forms of attack such as DoS and Man-in-the-middle (MITM) attacks are orchestrated across multiple layers of WSN stack. Irrespective of the type or form of cyberattacks (passive or active) against WSNs, they both impact negatively on security and privacy of patients' health data. In passive attacks, the attackers have unauthorized access to the data with no intention to alter or damage it but simply capture the data through eavesdropping and traffic analysis. This can have a far-reaching negative impact on privacy of patients' data as attackers or malicious entities can capture sensitive medical history or diagnoses [35] which can be used to build patients' profiles, compromising confidentiality. Also, the patients' health conditions can be inferred from healthcare metadata such as appointment times and health providers leading to discrimination or stigmatization and consequently suicide.

Active attacks interfere with the communication channel altering or mutilating the data in some manner [36]. This form of attack comes with more direct consequences including data modification where attackers, for instance, modify medication lists leading to decisions which can result in unsafe treatment and delays in health-care provision. Attackers could also carry our log-in credentials thefts to gain unauthorized access to systems allowing them view or manipulate sensitive health data, thereby causing patients' trust and consent to be be undermined through identity theft and other fraudulent activities. Active attack may also be in form of Denial-of-Service (DoS) where systems are overwhelmed with unnecessary traffic to compromise availability, obstructing access to critical patient information. Unauthorized access to healthcare records can lead to changes in data, misinform health providers, and subsequently, compromise patients' safety.

Apart from the effects that these cyberattacks have on the patients, they also impact negatively on the organizations i.e. the healthcare providers. Violations of privacy regulations (e.g., NDPR in Nigeria and HIPAA in the U.S.) can result in legal and regulatory penalties leading to financial loss due to fines and lawsuits by patients. The healthcare providers may also suffer reputational damage when the patients lose trust in the health organization as a result of a data breach. Data breaches can cause emotional distress for patients due to exposure or misuse of their personal health information.

Based on the aforementioned, it is the focus of this paper to implement a rigorous security measure to mitigate the risks associated with these cyberattacks and protect sensitive patient information to ensure security and privacy through safeguarding confidentiality, integrity and availability. To achieve the objective of protecting the privacy of patients' health data and respond, in real-time, to the ever-evolving cyber threats, we propose to develop an Ensemble Learning Model based on Federated Learning (FL) for enhanced data privacy and Adaptive Learning (AL) techniques to enable the system respond to the evolving, new and emerging cyber threats.

Huge and large volumes of health datasets is required for training healthcare system models to detect intrusion and cyber threats for improved performance and increased detection rate. Federated machine learning is a technique which allows models to be trained on multiple local datasets without unauthorized data exposure [37]. With FL, models can be trained while preserving and protecting patient data privacy.

With the changing and evolving cyber threats landscape, threat or intrusion detection systems must be capable of dynamically responding to new cyber threats. Traditional intrusion detection systems are trained on static dataset and cannot respond to new threats. With the dynamic threats landscape, intrusion-detection systems must adapt to evolving data distributions and carry out processing in real-time by learning continuously to update the model based on new data [38]. This is called adaptive machine learning, one of the technologies adopted for this paper.

3. Literature Review

3.1. Machine Learning and Deep Learning-based Intrusion Detection in WSNs

The field of intrusion detection in wireless sensor networks (WSNs) has garnered significant attention in recent years, particularly since machine learning (ML) and deep learning (DL) techniques came on the scene. Initial studies on the subject of intrusion detection for WSNs primarily relied on traditional statistical and rule-based techniques. However, these methods often struggled with adaptability and scalability, particularly in dynamic environments. Also, the arrival of deep learning has brought about a revolution on how intrusions are detected in WSNs, particularly supporting the analysis of complex, high-dimensional data. Models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been effectively applied in feature extraction as well as classification tasks in WSN settings. To address these limitations, researchers began to explore ML and DL algorithms in detecting intrusions and cyber threats in WSNs.

Vinolia et al., [39] focused their study on how deep learning (DL) and machine learning (ML) networks are applied in a number of methodologies at various stages of the intrusion detection process to get improved outcomes. Their work aimed at discussing the available technology for detecting intrusions with the use of various techniques, including soft computing, data mining, and other approaches. The authors systematically analyzed some research papers on the subject in order to identify the advantages and disadvantages of a number of methodologies, including supervised and unsupervised learning techniques. A special focus was on the experimental outcomes, which demonstrated the effectiveness of unsupervised, DL-based techniques in achieving superior accuracy rates. They conducted a comprehensive analysis of the research outcomes, which emphasized the efficacy of unsupervised, DL-based techniques with a remarkable accuracy.

Alruhaily & Ibrahim [40] proposed an innovative intrusion detection framework that is multi-layered for Wireless Sensor Networks (WSNs) designed to enhance security against the increasing spectrum of cyberattacks. By implementing a two-layer system utilizing a Naive Bayes classifier within the sensor level, and a Random Forest classifier on the cloud level, the authors aimed to optimize attack detection and analysis while improving performance metrics significantly. Their work set the stage for a multi-layer framework, which promises to mitigate these concerns while enhancing detection accuracy.

Gowdhaman &. Dhanapal [41] proposed a novel intrusion detection system (IDS) utilizing deep neural networks (DNNs) to improve detection rates, particularly in dealing with imbalanced attack data; to identify the challenges in WSNs including the resource-constrained nature of sensor nodes and the unique challenges posed by deployment strategies and communication channels, making WSNs susceptible to unauthorized access and security breaches. The authors employed cross-correlation for optimal feature selection and demonstrated through experiments that their DNN outperforms conventional machine learning algorithms.

With the proliferation of IoT devices, the associated vulnerabilities and potential for exploitation by cybercriminals have grown exponentially. To address this, Awajan [42] originated an intrusion detection system that is based on Deep Learning (DL) for IoT devices. He proposed a four-layer neural network architecture, deep and Fully Connected (FC), that was designed to detect various types of attacks, including Opportunistic Service, Blackhole, Distributed Denial of Service (DDoS), Sinkhole, and Workhole. The communication protocol-independent design is a notable strength, as it potentially allows for easier deployment across diverse IoT environments. However, further elaboration on the specific training data used, the rationale behind the choice of hyperparameters, and the mechanisms involved in training the model would enhance understanding of the model's effectiveness. Additionally, a comparison with existing methodologies or frameworks in terms of their architectures, training processes, and performance metrics could have bolstered the validity of the proposed systems.

Kagade & Jayagopalan [43] proposed a novel IDS that utilizes deep learning and an optimization technique known as self-improved sea lion optimization (SI-SLnO). The study focused on optimal cluster head (CH) selection based on energy, delay, and distance, while also integrating a multi-dimensional trust model. The final approach was influenced by a deep learning model for intrusion detection, with optimized training using SI-SLnO.

Sharma et al., [44] introduced an intrusion detection method tailored for wireless sensor networks (WSN), influencing both developmental and operational frameworks. The authors focused on integrating deep learning techniques with feature extraction and classification is both timely and pertinent. They aimed at developing a distinctive intrusion detection approach which would not only prioritize security in the wireless environment but would also improve the accuracy and efficiency of attack-detection methods. The major contribution of this paper is the integration of a deep convolutional neural network (DCNN) model.

3.2. Federated Learning in Cybersecurity

Federated learning has been utilized in various cybersecurity applications to enhance anomaly detection while preserving user privacy. Alazab et al., [45] presented a comprehensive study of the application of federated learning (FL) in enhancing cybersecurity measures against the backdrop of increasing cyberattacks. It explores the foundational concepts of FL, particularly within the framework of decentralized data management, and addresses the hesitance observed among industries in adopting emerging technologies like the Internet of Everything. The authors conduct a thorough survey of existing FL models aimed at improving authentication, privacy, trust management, and attack detection. Moreover, the paper showcases real-time use cases that illustrate the successful integration of FL into cybersecurity protocols. The conclusion outlines key challenges and future research directions that could enhance the implementation of FL in practical scenarios.

Dash et al., [46] presented an extensive, up-to-date and relevant exploration of federated learning within the artificial intelligence (AI) and machine learning (ML) environments and their application in the FinTech industry. The abstract portrays the rapidity in the advancement in AI and ML, respectively, and their intersection with cyber security, particularly emphasizing the importance of data privacy—a critical concern in today's digital landscape.

Friha et al., [47] proposed a Federated Learning-based Intrusion Detection System (FELIDS) that is used for securing agricultural Internet of Things (IoT). The infrastructure offers a timely and innovative approach to a pressing issue in the realm of IoT security. The significance of ensuring data privacy while safeguarding against potential cyber threats is underscored in this research, which effectively addresses the unique challenges faced by agricultural IoT systems. A very interesting feature of FELIDS is its commitment to data privacy through local learning. By enabling devices to learn from the knowledge of their peers without sharing sensitive data directly, the system strikes a commendable balance between collaboration and confidentiality.

At a time when cyber threats are becoming increasingly sophisticated and pervasive, Idrissi et al., [48] addressed a critical issue that organizations of all sizes grapple with: the integration of effective cybersecurity measures capable of maintaining data privacy by presenting a compelling case for the adoption of Federated Learning (FL) in the area of Network Intrusion Detection Systems (NIDS), offering innovative solutions to the privacy concerns associated with centralized machine learning models. This sets the stage for the introduction of Fed-ANIDS, a novel framework that seeks to address these concerns through collaborative model training among distributed clients.

de Oliveira et al., [49] proposed the F-NIDS. This is an intrusion detector that makes use of federated artificial intelligence and asynchronous communication techniques between system entities, to provide horizontal scalability, along with differential privacy techniques to deal with the issues of data confidentiality. The authors presented an innovative approach to addressing significant challenges related to Network Intrusion Detection Systems (NIDS) within a rapidly evolving Internet of Things (IoT) landscape. The authors introduce F-NIDS, a federated learning-based architecture that leverages asynchronous communication and differential privacy techniques to enhance scalability and security.

Alazab et al., [50] proposed federated learning, which is a distributed machine learning approach, aimed at surmounting these challenges. Federated learning involves multiple clients which collaborate to train a shared model without sharing sensitive data, which is then aggregated at a centralized server. The results of this study revealed that federated learning achieves higher accuracy and lower losses compared to traditional deep learning models, especially when the emphasis is on data privacy and security. The authors utilized a federated learning framework, where multiple clients learn local models on different datasets and communicate with an aggregation server to produce a global model.

dos Santos et al., [51] proposed a new Federated Learning model for a dependable network-based intrusion detection with a high level of confidence, and can update over time. The authors compared their framework against traditional Federated Learning techniques, which showed superiority across various scenarios. The authors rightly highlight the pressing need for adaptive systems in a landscape where cyber threats continuously evolve.

Lazzarini et al., [52] addressed the escalating threat of cyber-attacks targeted on IoT infrastructure due to the proliferation of IoT devices. The authors emphasized the importance of Intrusion Detection Systems (IDSs) within a multi-layered cybersecurity defense strategy, spotlighting the predominant reliance on centralized machine learning (ML) approaches which pose data privacy risks. The paper details an implementation using a shallow artificial neural network (ANN) and explores different aggregation algorithms within the Flower FL framework, finding that federated averaging (FedAvg) and its modified version, FedAvgM, outperform other adaptive algorithms in this context.

3.3. Adaptive Learning Model in Threats Detection

The adoption of Adaptive Learning for intrusion and cyber threat detection have garnered significant attention in recent research. Given the growing sophistication of cyber-attacks, traditional static detection methods often fall short, leading researchers to explore adaptive approaches that can evolve in response to changing threat landscapes.

In dealing with the complex and evolving cybersecurity threats, and to do so in a situation where conventional methodologies have an uphill task of catching up with the dynamic nature of modern threats, Fenjan et al., [53] proposed a Deep Learning-Based, Adaptive Intrusion Detection System (IDS) infrastructure, that leverages the capabilities of various neural network architectures to improve accuracy and scalability. The proposed framework utilized a combination of Convolutional Neural Networks (CNNs), Artificial Neural Networks (ANNs), and Multilayer Perceptrons (MLPs), in order to classify network traffic scenarios as either normal or anomalous. The proposed framework was evaluated on a dataset with various network traffic scenarios, achieving a promising 96% accuracy in classifying scenarios as normal or anomalous.

Villegas-Ch et al., [54] anticipated an adaptive intrusion detection system (AIDS) that leverages deep learning algorithms that are able to detect and respond to threats in real-time, by adapting to emerging threats as well as familiar attacks. The system's capabilities were enhanced by simultaneously combining machine learning and deep learning techniques, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs). The research concentrated on the assessment of the system’s ability to identify and counteract cyber threats more efficiently and accurately than traditional methods.

Motivated by the growing complexities in cyber threats and the dynamic nature of data streams, Shyaa et al., [55] contemplated a superior Intrusion Detection System (IDS) with the capability of adapting to Concept and Feature Drift. In view of this, the authors came up with a framework that includes all the necessary components for a drift-aware Intrusion Detection System (IDS). The framework is a combination of dynamic feature selection, adaptive learning algorithms, and continuous monitoring techniques to handle Concept Drift and Feature Drift effectively.

Traditional methods cannot easily keep pace with the high rate of metamorphosis of cyber threats. As a result, adaptive and deep learning techniques have been introduced as critical components in combating cyber threats. Rizqullah et al., [56] recommended a technique involving ARF for intrusion detection systems. This was based on the hypothesis that adaptive models significantly outperform traditional static approaches. The proposed mechanism is characterized by continuous learning, enabling ARF to incrementally learn from new instances of data, maintaining its relevance. Secondly, ARF is designed to process and learn from these data streams efficiently, adapting to changes as they occur. Thirdly, ARF can train on a comprehensive dataset that mirrors real-world conditions, leading to better generalization across different attack scenarios.

Li & Sun [57] recommended an adaptive deep learning algorithm that has a data pre-processing module, a neural network pre-training module and a classifier module, all working together in classifying intrusion data types, aided by their high-dimensional data features. The recommended Adaptive Deep Learning (ADL) algorithm arrives at the number of layers and the number of neurons in each layer by ascertaining the characteristic dimension of the network traffic. Transfer learning was utilized by the authors' recommended model for obtaining the original data dimensions and to find new abstract features. A combination of deep learning models and traditional machine learning-based classification models brought about a significant improvement in the performance of the classification of network traffic data.

Nie et al., [58] proposed an adaptive network intrusion detection technique that identifies anomalies in industrial cyber-power grids and is capable of detecting unknown attacks with significant accuracy. The proposed intrusion detector incorporated an adaptive incremental learning when exposed to a new vulnerability. This proposed solution can be deployed at the device level in the phasor measurement network systems and evolves with the latest knowledge-base of cyber threats. Results revealed that the incremental method made brute-force attacks and penetration-test attacks more accurate. They validated their model on two publicly available datasets where incremental learning improved DDoS attack detection accuracy, UDP attacks, DoS attacks and Scan attacks.

3.4. Ensemble-based Machine Learning

Ensemble-based machine learning approaches have gained significant traction in cybersecurity due to their effectiveness in improving classification performance, robustness, and overall reliability of predictions. By joining the forces of multiple models together will cause ensemble methods to get over the limitations of individual learners, making them well-suited for the dynamic and adversarial nature of cybersecurity threats.

With rapid increase in the manufacture and use of IoT devices, there has been an unprecedented increase in the volume of data being accessed in real-time, thereby giving rise to security situations where traditional detection systems are finding it difficult to cope with the issues effectively. To bridge this gap, Tanveer et al., [59] developed Ensemble-Guard IoT, which is an innovative method that utilizes an ensemble model with a combination of three machine learning algorithms: Gaussian Naive Bayes (GNB), Logistic Regression (LR), and Random Forest (RF) through soft voting classifiers. This model's advantage is that it reduces computational costs. This makes it a perfect solution for real-time IoT attack detection applications. Inspite of all the advantages of Ensemble-Guard IoT, there are possible limitations to be considered, some of which are computational overheads in high volume scenarios and lack of robustness against adversarial attacks.

Alhashmi et al., [60] proposed a fraud-detection model that is very innovative. It was designed for bank payment transactions using advanced ensemble techniques. This study presented an all-embracing assessment of an ensemble model conducted on the Bank Account Fraud (BAF) dataset. The authors reviewed the performance of various base models and ensemble methods. They compared the model's performance with current tech models by using critical metrics such as accuracy, precision, recall, and F1-score. The performance of the proposed ensemble model was quite remarkable because it attained a high accuracy score. The study underscored the importance of precision-recall trade-offs in fraud detection and highlighted the potential of ensemble methods, especially the "Stacking" model, to reinforce the ruggedness and effectiveness of existing security systems.

To take harness the potentials of machine learning; to develop and execute intrusion detection systems (IDSs) for resisting unfortunate cyber threats, Jaw & Wang [61] recommended a potentially capable hybrid feature selection (HFS) with an ensemble classifier, that is efficient in selecting useful features and can provide consistent attack classification. Adopting a voting method and average of probabilities, the authors presented an ensemble classifier that utilizes K-means, One-Class SVM, DBSCAN, and Expectation-Maximization (KODE) to consistently classify the asymmetric probability distributions between malicious and normal instances. Their ensemble model had an excellent performance accuracy, thereby outperforming all the other classification methods, cutting-edge feature selection, and some current IDSs techniques that were selected.

Hossain & Islam [62] proposed a solution to botnet detection problem using an Ensemble-based Hybrid Feature Selection method which blends Categorical Analysis,

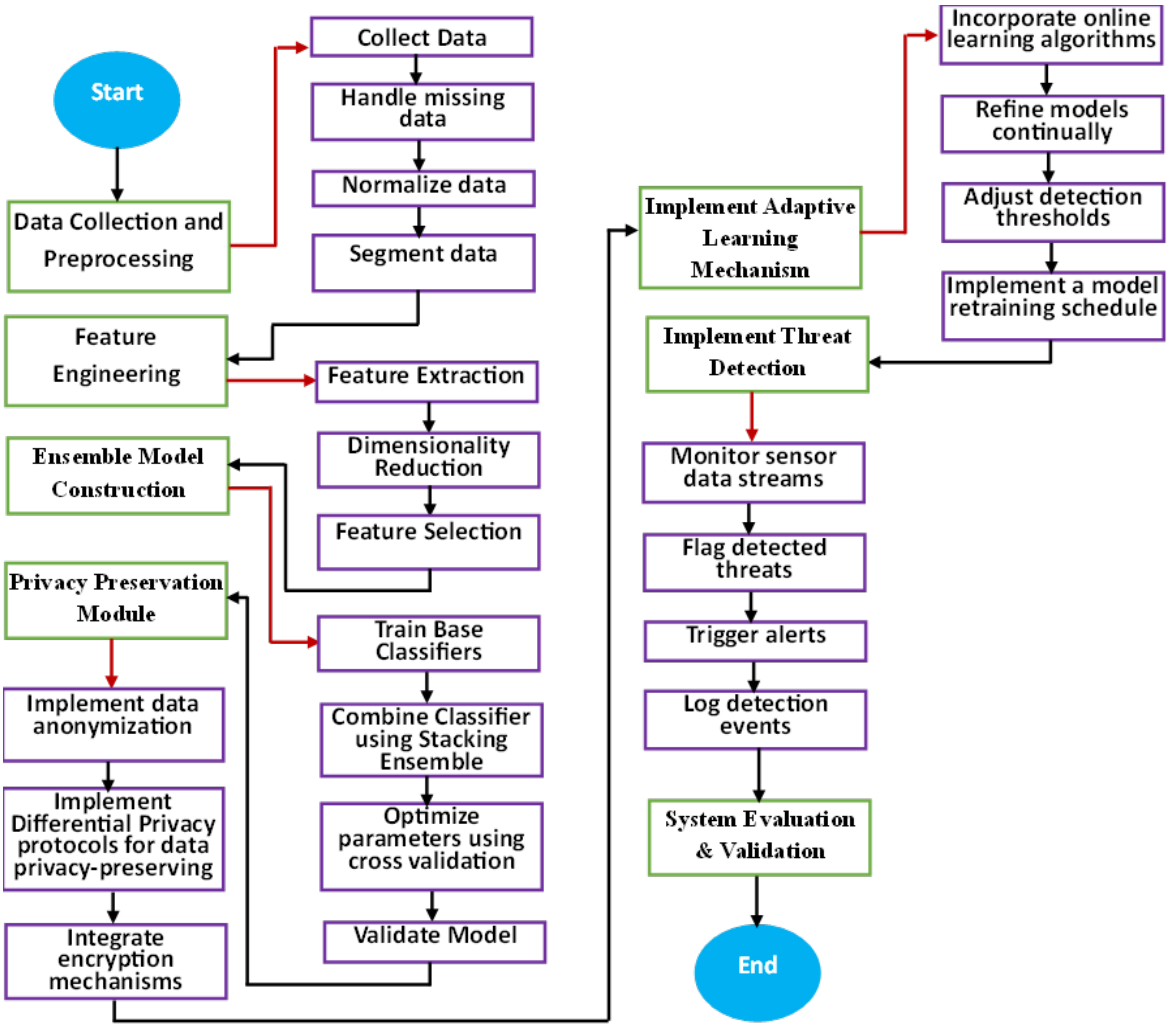
Start
Data Collection and Preprocessing
Collect Data
Handle missing data
Normalize data
Segment data
Feature Engineering
Feature Extraction
Dimensionality Reduction
Feature Selection
Ensemble Model Construction
Train Base Classifiers
Combine Classifier using Stacking Ensemble
Optimize parameters using cross validation
Validate Model
Privacy Preservation Module
Implement data anonymization
Implement Differential Privacy protocols for data privacy-preserving
Integrate encryption mechanisms
Implement Adaptive Learning Mechanism
Incorporate online learning algorithms
Refine models continually
Adjust detection thresholds
Implement a model retraining schedule
Implement Threat Detection
Monitor sensor data streams
Flag detected threats
Trigger alerts
Log detection events
System Evaluation & Validation
End

Figure 6. Block Diagram of the Proposed System.

Mutual Information, and Principal Component Analysis to effectively refine the dataset, and extract meaningful patterns and features that contribute to more accurate detection mechanisms. They used Extra Trees algorithm as the ensemble technique which enables robust classification performance. Their results showed accuracy rate of 99.99% in classifying botnets across various datasets. This level of accuracy outperforms existing benchmarks and also indicates a significant leap in the ability to adapt to novel botnet threats no matter how adversaries' tactics evolve.

Torabi et al., [63] reviewed feature selection and ensemble techniques used in anomaly-based IDS research. The authors evaluated various dimensionality reduction methods and classified feature selection techniques to show their effectiveness on training phase and detection. The study examined and discussed various IDS-based machine learning techniques with several detection models (single classifier-based or ensemble-based), to illustrate their significance and success in the intrusion detection area. The authors concentrated particularly on ensemble techniques that are used in anomaly-based IDS models, and illustrated how their use improves the performance of the anomaly-based IDS models.

Hossain & Islam [64] proposed a novel ensemble-based machine-learning technique for intrusion detection. They utilized several public datasets and a number of ensemble strategies, including Random Forest, Gradient Boosting, Adaboost, Gradient XGBoost, Bagging, and Simple Stacking to evaluate the performance of their proposed method. The result revealed that the proposed method using the Random Forest technique recorded higher accuracy than the existing methods.

Hossain & Islam [65] recommended an enhanced approach for detecting DDoS attacks implementing a hybrid feature selection technique in combination with ensemble-based classifiers. They employed the ensemble-based method by combining many decision trees to increase classification accuracy and reduce overfitting and model robustness. The feature selection technique employed for their study made use of correlation analysis, mutual information, and principal component analysis to identify the most useful characteristics for attack detection. As a result, the ensemble-based Random Forest classifier from the various ensemble-based approaches with the specified relevant features produced the best detection rates.

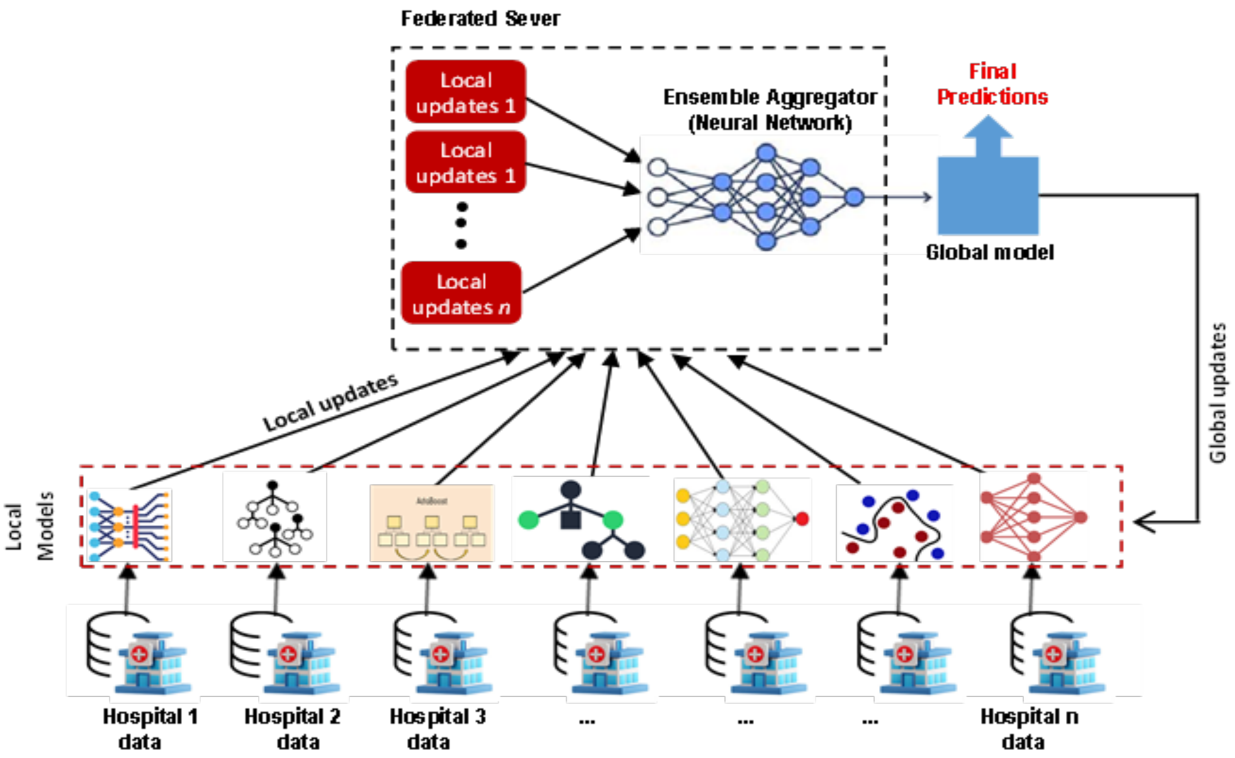

Figure 7. Architecture of Proposed Ensemble-based Threat Detection Model.

Das & Sunitha [66] designed an Intrusion Detection System based on Machine Learning classifiers trained and evaluated on the UNSW- NB15 dataset. In the design, the ensemble model consisted of Balanced Bagging, XGBoost, and RF-HDDT to address imbalance in the dataset. The work recommended two new algorithms to address the class overlap issue in the dataset and applied during training to help improve the performance on the testing dataset by affecting the final classification decision made by the ensemble classifier with a majority vote combiner. The results of their experiments revealed that their model performed better than those reported in the literature by a significant margin for both binary and multi-category classification cases.

4. Research Methodology

The methodology involves designing, developing, and evaluating the system through a series of structured phases, ensuring robustness, adaptability, and privacy preservation. This study proposes an ensemble-based threat detection framework for Wireless Sensor Networks (WSNs) in hospital systems dedicated to remote patient monitoring. The framework integrates federated learning with differential privacy, adaptive learning mechanisms, and a neural network-based ensemble classifier to ensure robust, privacy-preserving, and adaptive threat detection across multiple hospital sites. Figure 6 depicts the flow of the process design for the proposed model showing different main activities and sub-activities involved the implementation process. The major activities are shown in green boxes while the sub activities are shown in purple-colored boxes. Black arrows in the flowchart shows entries into main activities and exits from main activity's components while a red arrow shows beginning of a main activity's components. This approach aims to provide healthcare systems with reliable, privacy-aware security, resilient against evolving threats in wireless sensor networks.

4.1. Architecture of Proposed Threat Detection Model

The model proposed in this paper combines several technologies and techniques including federated learning with dissimilar local models, SSL socket enabled secure communication, differential privacy for data privacy, and an adaptive ensemble neural network for robust and efficient threat detection in hospital WSNs. Figure 7 depicts the integrated architecture followed in this paper to deliver an efficient, effective and privacy-conscious threat detection that supports the monitoring of patients remotely. Under this section, we illustrate the core of the architectural framework that make up the proposed an ensemble-based threat detection framework tailored for WSNs. This framework is composed of federated learning, a secure communication protocol, an ensemble and model aggregation strategy, differential privacy, and adaptive learning techniques.

4.2. Proposed Threat Detection Model Development

4.2.1. Data Collection and Preprocessing

The different datasets consisting of patient health data collected from hospital WSN deployments monitoring patient health parameters, network traffic, and device activity were loaded into the Python program where data normalization was applied to ensure all features are on a comparable scale, using min-max normalization:

$$x' = \frac{x - \min(X)}{\max(X) - \min(X)} \tag{1}$$

where x is the local clients' original feature values, $\min(X)$ and $\max(X)$ represent the minimum and maximum values of the feature X, and x' is the normalized value. The normalization is to reduce the variance in feature values, enabling the individual models to be and effectively and independently trained on respective host data and the CNN-based ensemble to be more effectively trained on the local models' updates.

4.2.2. The Ensemble-based Threat Detection Model

We proposed an Ensemble-based architecture consisting of local models at each hospital (clients) site including XGBoost, online AdaBoost, online Random Forest, multilayer perceptron, and SVM ML models. Each hospital (client) system trained a local model f_i independently on client-specific dataset D_i in order to capture domain-specific threat patterns with hyperparameters optimized using cross-validation within each local domain to enhance robustness of the local models. Each local model upgrade was transferred to federated (central) sever using Secure Sockets Layer (SSL) sockets communication. This offers encrypted channels for the communication, preventing interception or tampering of sensitive model updates while in transit. By so doing, the proposed model maintains integrity and confidentiality of patient data. The federated sever aggregates the local models into an ensemble representation:

$$\bar{f} = \frac{1}{N}\sum_{i}^{N} f_i \tag{2}$$

where $\bar{f}$ is the aggregated feature tensor and N is the number of local models trained on individual hospital datasets, D_i. CNN neural network was utilized as an ensemble classifier. To capture spatial patterns in local model upgrades, the federated server applies convolution filters $K \in \mathbb{R}^{k_h k_w}$ to the aggregated feature tensor, $\bar{f}$ to extract higher-level features. Hence for each filter $K^{(m)}$, the convolution output at position (i, j) specified as:

$$S_{i,j}^{(m)} = \sigma\left(\sum_{u=1}^{k_h}\sum_{v=1}^{k_w}\sum_{c=1}^{C} K_{u,v,c}^{(m)} \cdot \bar{f}_{i+u,j+v,c} + b^{(m)}\right) \tag{3}$$

where $\bar{f}_{i+u,j+v,c}$ represents the aggregate features at position $(i+u, j+v)$ in the spatial dimension and channel c, $K^{(m)}$ represents the m^{th} filter, $b^{(m)}$is the bias term and σ is the activation function. The CNN model receives the feature representations as outputs from the local models and adopts a stack-based ensemble technique to generate a global model and subsequently, a final threat detection decision at the end of the required iterations. The global model is then distributed to all the local clients to perform an update of their individual local models. Apart from the existential privacy contribution of the federated learning scheme employed in the proposed model, differential privacy mechanism is also employed in the local model training stage to further enhance privacy of patient data. Each local model applies a local differential privacy mechanism such that for local dataset D_i, the mechanism can be modelled as:

$$\bar{D_\iota} = \mathcal{M}_i(D_i) \tag{4}$$

where $\bar{D_\iota}$ is the anonymized data shared with federated server. This helps to hide the identity of an individual patient ensuring a patient's data cannot be inferred from shared model parameters, provides the requisite privacy guarantees in line with healthcare data protection regulation (NDPR, GDPR, etc.) requirements. Since the hospital data is mainly numeric health measurement value, the differential privacy mechanism was design using Laplace Mechanism as:

$$\mathcal{M}_i(D_i) = D_i + \eta_i, \quad \eta_i \sim \text{Laplace}\left(0, \frac{\Delta f}{\epsilon}\right) \tag{5}$$

where Δf is the sensitivity of the function (maximum change in f when one data record changes), η_i is the noise introduced into the data for data anonymization and ε controls the privacy level.

4.3. System Evaluation

The proposed ensemble-based adaptable and privacy-aware threat detection mechanism for Wireless Sensor Network in healthcare systems was extensively tested to evaluate it performance in the detection of cyber threats in hospitals' WSNs used to collect patients' vital health data for real-time monitoring. In this study, the evaluation was performed in terms of robustness to threat detection and privacy-preserving requirement for ensuring privacy assurance in remote patient monitoring. This section presents experimental setup, dataset, performance evaluation, and analysis of results.

4.3.1. Experimental Setup

The proposed model was implemented on a laptop computer with an Intel(R) Core (TM) i7-6820HQ CPU @ 2.70GHz, 2701 Mhz, 4 Core(s), with 8 Logical Processor(s) and Microsoft Windows 11 Pro as the operating system. All code to simulate the proposed system were written in Python 3.13.7 using PyCharm in Anaconda Navigator IDE

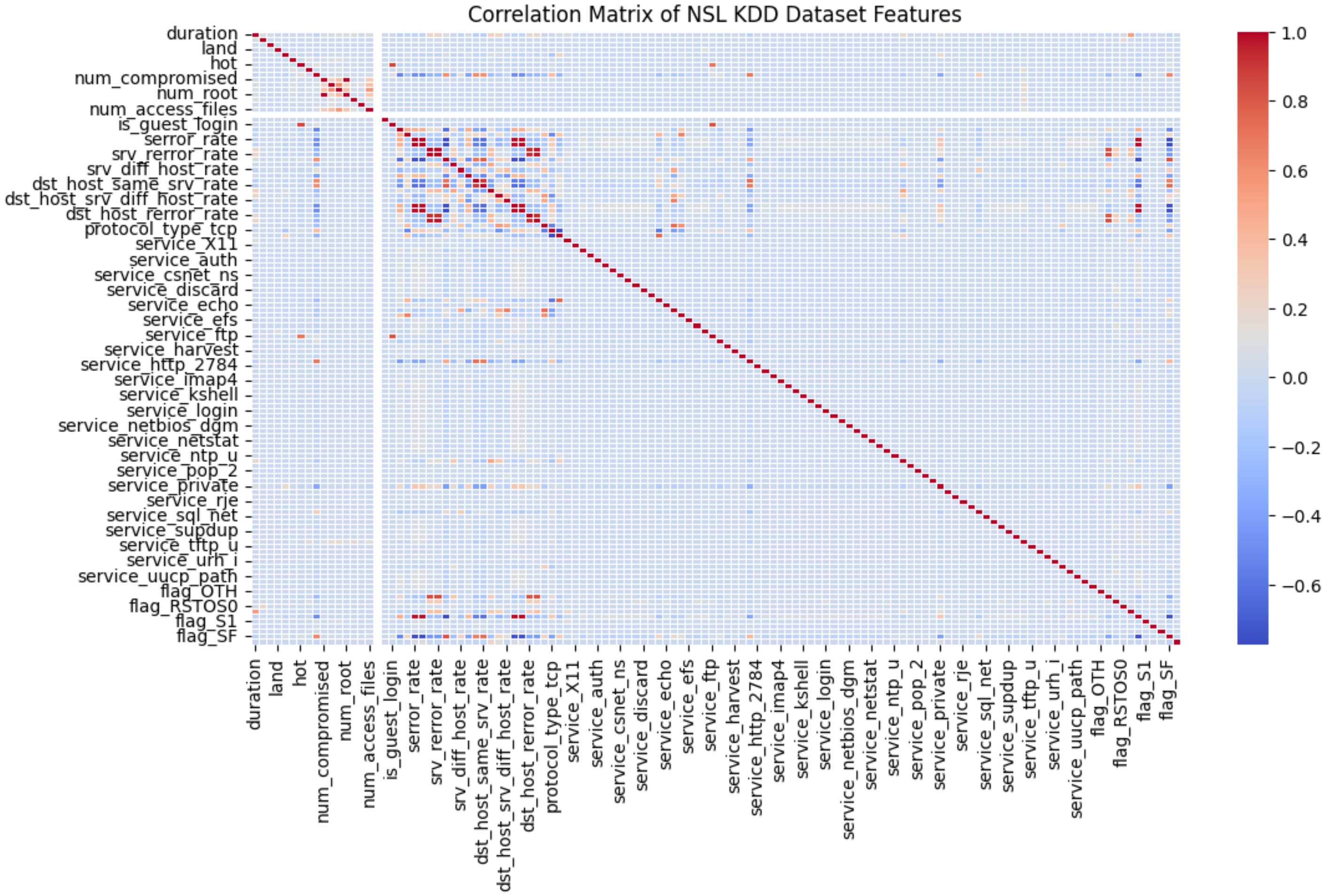

Figure 8. Correlation Matrix of NSLKDD Dataset.

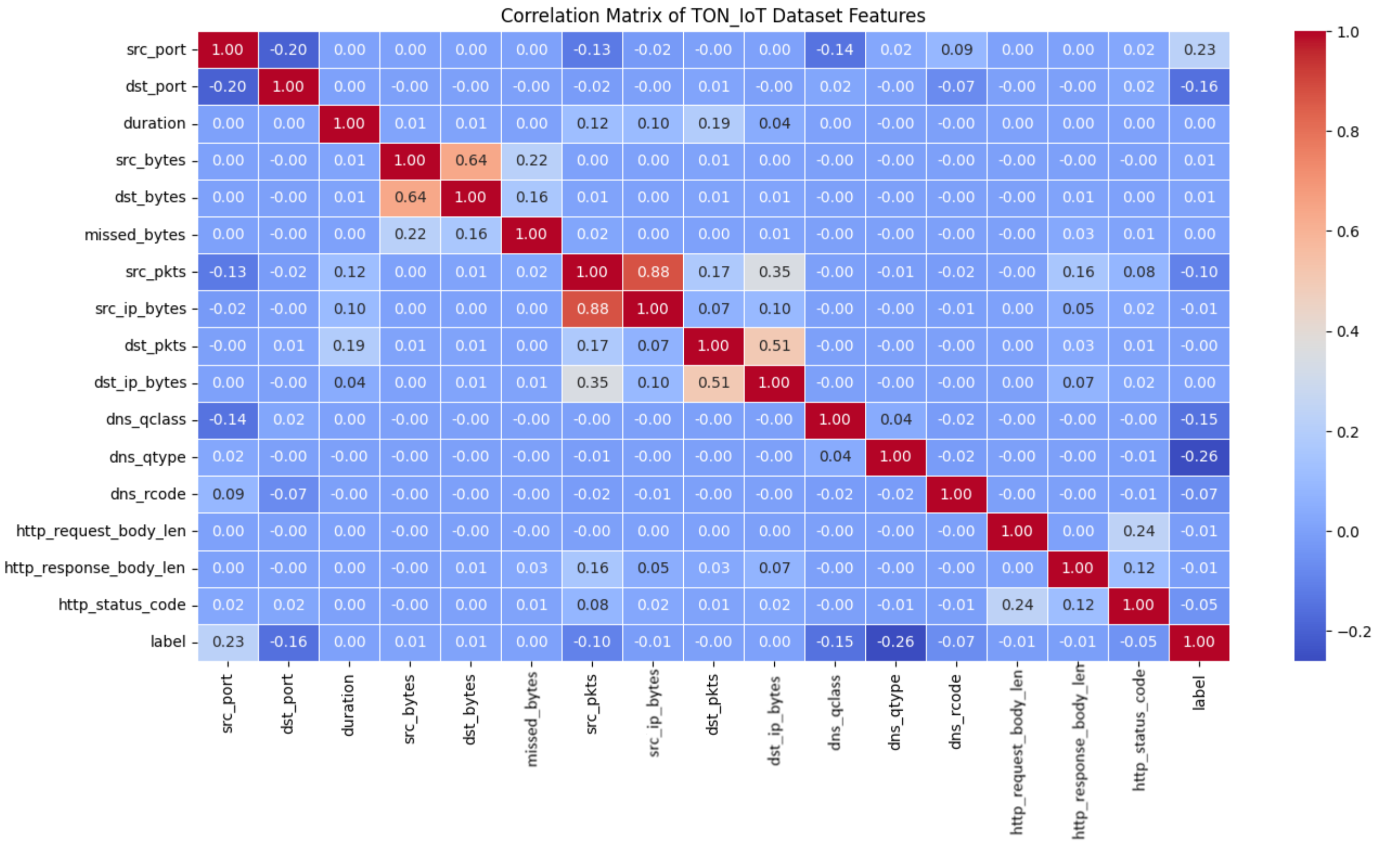

Figure 9. Correlation Matrix of TON_IoT Dataset.

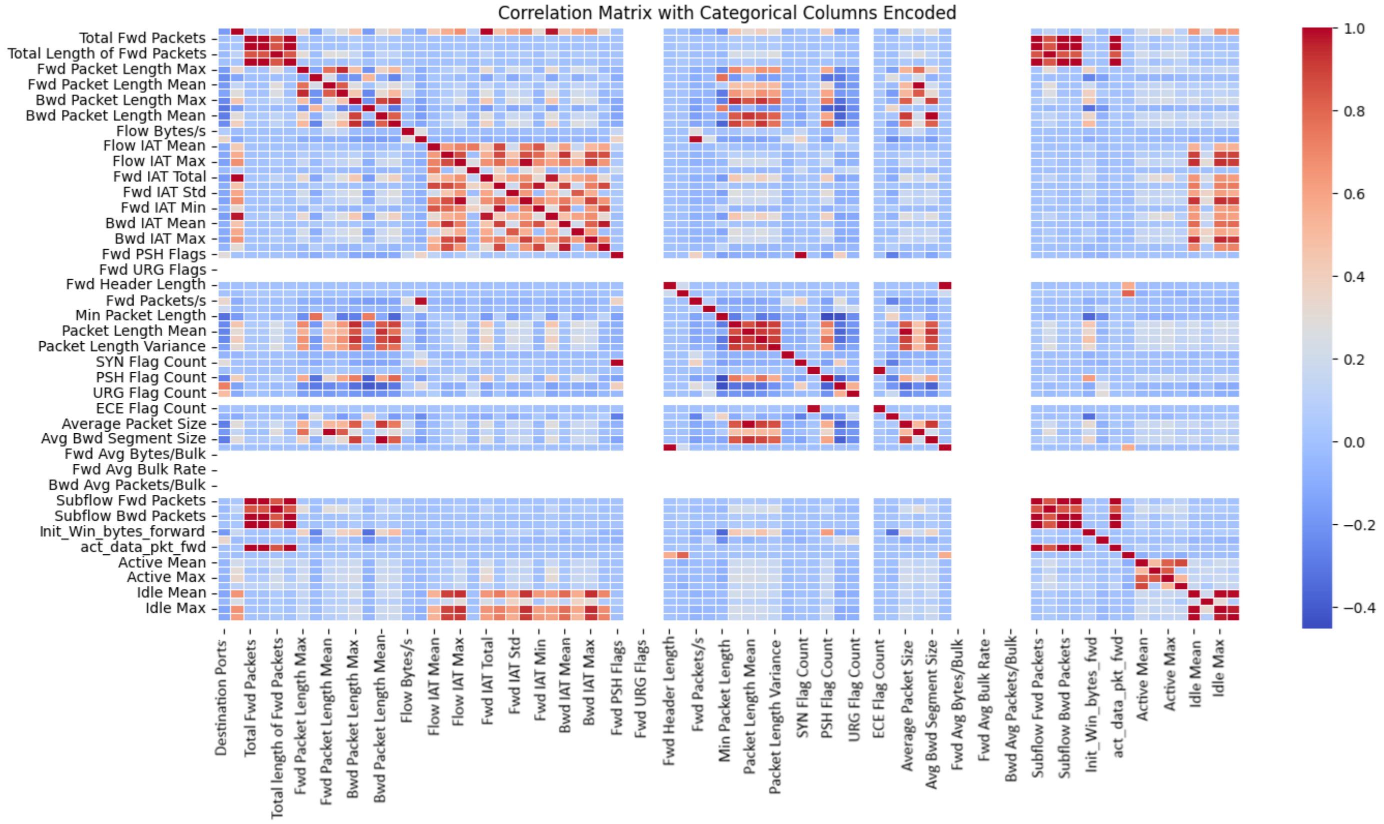

Figure 10. Correlation Matrix of CICIDS2017 Dataset.

for its implementation. In the experiment, 10 hospitals were selected and a series of machine learning and neural networks models were trained on each local hospital data. Using a grid search to achieve the best performance, the hyper-parameters which were optimized include learning rate, batch size, and dropout rates.

4.3.2. Datasets

The datasets used in this experiment included the NSL-KDD, TON_IoT Network, and CICIDS2017 datasets. These datasets were distributed among the ten (10) hospitals used in this experiment. Data preprocessing was performed locally at each hospital site, where the preprocessed data were partitioned into two, namely, training sets and and testing sets for both the training and testing of each local model.

a) NSL-KDD Dataset
The NSL-KDD dataset is one of the datasets analyzed in this paper. It is an improved version of the KDD Cup 1999 dataset used for anomaly detection researches. This dataset is used to evaluate the effectiveness of the ensemble model in detecting the threats in the WSN traffic patterns and the relationship of the protocols available in the widely used network protocol stack with the attacks used by attackers to generate undesired network conditions. It is made up 148,517 records with 15.18% as the test data and 84.92% as the training data. Figure 8 shows the correlation matrix to help in understanding then context of the data.

b) TON_IoT Network Dataset
This dataset is a component of the TON_IoT dataset collection created by the Cyber Range Lab of UNSW Canberra. The dataset consists of network traffic data captured from simulated IoT and IIoT environments for intrusion detection and machine learning models training and testing. Visualization of the statistical properties of this dataset is shown in a correlation matrix in Figure 9. It includes malicious and benign network flows captured in a realistic smart environment using tools like Argus and Bro. This dataset can be accessed at: https://research.unsw.edu.au/projects/toniot-datasets.

c) CICIDS2017 Dataset
The is a complete and publicly available dataset commonly used benchmark dataset for network intrusion detection related research created by the Canadian Institute for Cybersecurity to facilitate the development and evaluation of intrusion detection systems, especially in modern network environments, including cloud and IoT. It consists or normal traffic plus a wide variety of attack types, including DoS, DDoS, infiltration, brute-force, botnet, web attacks, and more. Figure 10 shows the correlation matrix for the dataset.

4.3.3. Performance Metrics Calculation

The functioning of the threat detection system was evaluated using standard metrics: accuracy, precision, recall (sensitivity), F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC). These metrics were calculated as follows:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \quad (6)$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (7)$$

$$\text{Recall (sensitivity)} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (8)$$

$$\text{F1} - \text{Score} = 2 \times \frac{\text{Precision} \ \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (9)$$

where:

True Positives (TP) is the number of instances correctly identified, False Positives (FP) is the normal instances incorrectly classified as threats, True Negatives (TN) instances where a system correctly predicts the absence of a threat, and False Negatives (FN) is the threat instances missed by the system.

5. Results and Discussion

This section presents the performance of the proposed ensemble model developed in this paper and compares its performance against the baseline models. These performances are presented in Table 1. The results presented show that the proposed model outperformed the baseline models with accuracy of 97.8%, precision of 98%, Recall of 97% and a calculated F1-score of 97.5%. These results demonstrate the proposed model's superior performance across multiple evaluation metrics compared to the baseline models offering substantial improvements in the evaluated aspects of the system. This improved performance can be attributed to first, the robustness of the proposed model occasion by the combined strength of the ensemble of the baseline model. Secondly, the incorporation of adaptive learning and privacy preserving techniques allow the model be effective in healthcare systems while protecting privacy. Lastly, the high metrics values indicate better generalization to unseen data and the model's response to unknown and evolving threats.

Figure 11 shows a comparison of the accuracies of the baseline models and the model proposed in this work. As a meta-classifier, the CNN provides effective feature learning, captures complex relationships, and offer robustness against noise. This leads to more accurate, reliable, and adaptive threat detection in wireless sensor networks for healthcare.

Figure 12 shows a comparison of the precision of the various models in this research, with the ensemble model proposed in this paper achieving the highest precision at 98%, significantly outperforming XGBoost, online AdaBoost, online Random Forest, MLP, and SVM models. This high precision indicates the proposed model's effectiveness in correctly identifying actual intrusions.

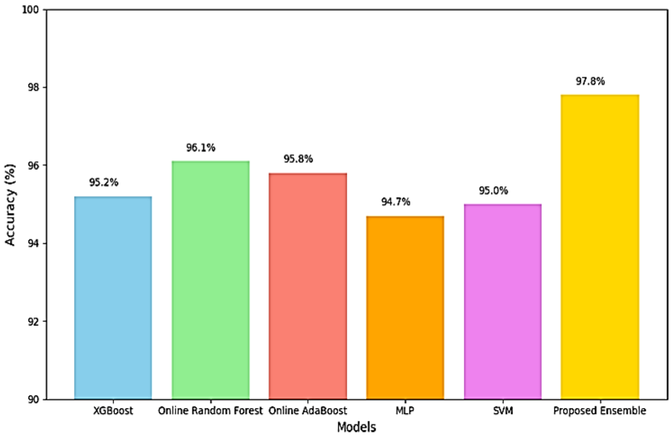

Figure 11. Comparison of Accuracies of Baseline Models and the Proposed Ensemble-Based Detection Mechanism.

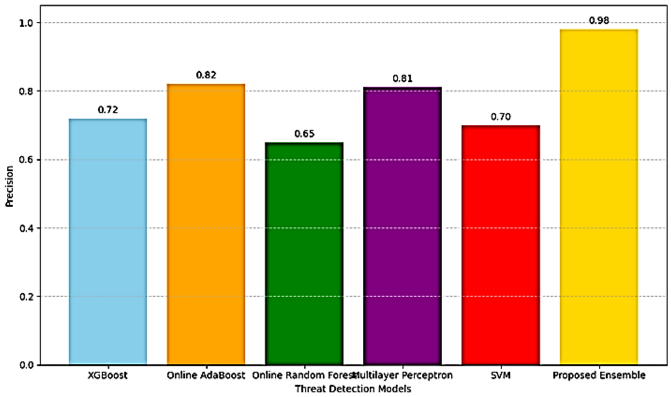

Figure 12. Precision Comparison of Threat Detection Models.

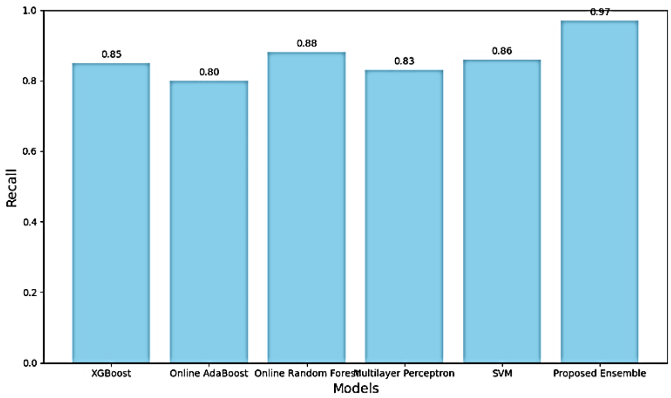

Figure 13. Comparison of Accuracies of Baseline Models and the Proposed Ensemble-Based Detection Mechanism.

Figure 13 shows recall metric values for the experiments in this paper. The proposed model recorded a recall of 97%, leading its baseline counterparts. This demonstrates our model's sensitivity to detecting intrusions. Compared to the other models, the recall result reflects high percentage of actual attacks, reducing missed intrusions.

F1-score of 97.5% in Table 1 indicates that our model is both accurate in its positive predictions and effective at capturing most positive instances. This is especially

Table 1. Performance Comparison of Threat Detection Models.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Latency Reduction (%)
XGB	95.2	72 .0	85.0	78.0	120ms
OAB	95.8	82.0	80.0	81.0	130ms
ORF	96.1	65.0	88.0	74.8	150ms
MLP	94.7	81.0	83.0	81.9	180ms
SVM	95.0	70.0	86.0	77.2	160ms
Proposed Model	97.8	98.0	97.0	97.5	80ms

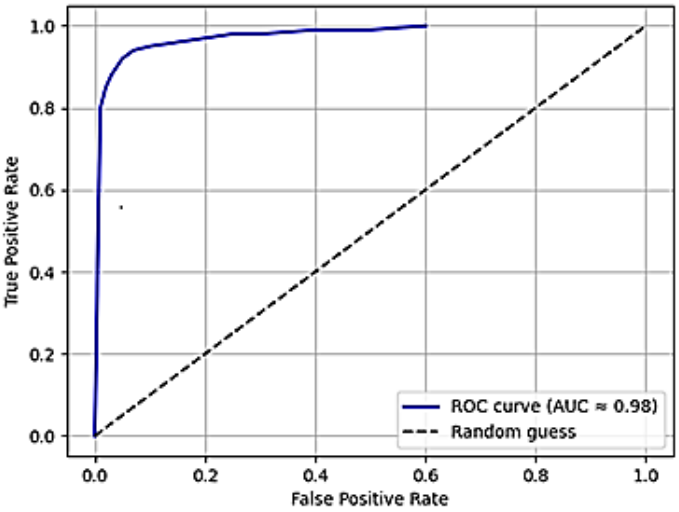

Figure 14. AUC-ROC Curve for Threat Detection in WSN-based Patient Data.

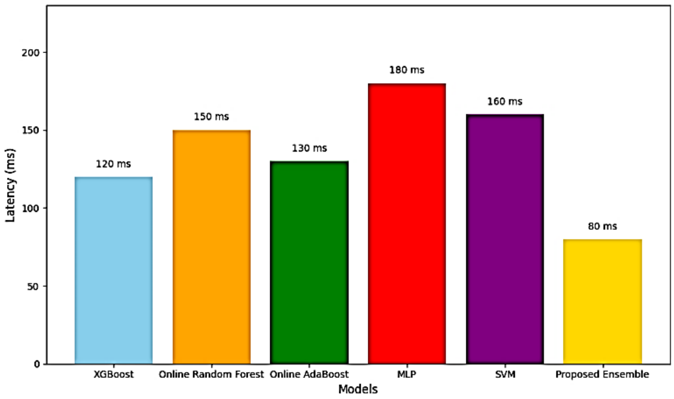

Figure 15. Latency Reduction Achieved by the Ensemble-Based Threat Detection Mechanism Compared to Baseline Models in Wireless Healthcare Sensor Networks.

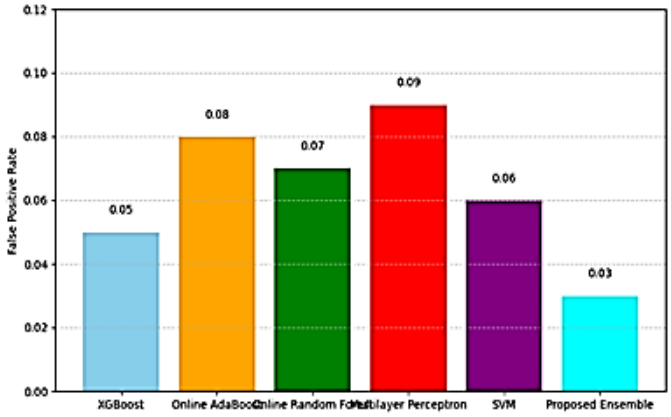

Figure 16. False Positive Rates (FPR) of Different Threat Detection Models.

useful to balance false positives and false negatives in the proposed model for effective threat detection, patient health monitoring, and medical diagnosis. Figure 14 illustrates a representative ROC curve demonstrating the detection performance of the proposed ensemble-based threat detection mechanism. AUCROC was computed by plotting the true positive rate against the false positive rate at various thresholds and calculating the area under the curve. This indicates a high true positive rate across various false positive rates, with an area under the curve (AUC) of approximately 0.98, which slightly below 1 reflecting a strong discriminative capability. This is critical in hospital environments where timely and accurate threat detection can directly impact patient safety and privacy.

Figure 15 shows that the proposed model has the lowest latency of 80ms indicating that the system can recognize and adapt to new or emerging threats within a relatively short period. In a hospital environment where sensitive patient data and critical systems are involved, a low latency window allows the system to remain effective against evolving threats without significant delay. The brisk response ensures continuous security posture and reduces the risk of attacks leveraging unknown vulnerabilities. Our system demonstrated scalability across multiple hospital nodes, with minimal overhead introduced by privacy mechanisms and secure communication protocols. The stack-based ensemble approach effectively combined heterogeneous local models, enhancing robustness against diverse attack vectors. Additionally, the neural network aggregator provided a flexible and powerful ensemble mechanism capable of handling varying data distributions.

Figure 16 shows the FPR exhibited by the proposed model. The false positive rate was maintained below 3%, demonstrating reliable threat identification with minimal disruption to normal operations.

The evaluation was performed over 50 rounds of federated training with each local model trained for 10 epochs. In terms of privacy, the integration of differential privacy resulted in an epsilon value of 1.0, indicating strong

Table 2. Comparison of Key Findings.

Aspect	Our Work	Related Works	Comparison/Insights
Main Focus	Development of an ensemble learning-based, adaptable, and privacy-preserving threat detection mechanism tailored for WSNs in healthcare systems.	Various techniques, including rule-based, anomaly-based, or single ML models for intrusion detection in WSNs or IoT healthcare setups.	The paper emphasizes ensemble learning for improved accuracy and robustness, contrasting with single-model approaches in other works.
Threat Detection Approach	Combines multiple classifiers (e.g., Decision Trees, Random Forests, SVMs) into an ensemble to enhance detection performance and adaptability.	Many studies use individual classifiers (e.g., SVM, KNN, Decision Trees) with limited ensemble integration.	Ensemble methods generally outperform single classifiers in accuracy, false positive rate, and adaptability.
Privacy Preservation	Incorporates privacy-aware mechanisms, ensuring sensitive health data remain protected during analysis.	Other works may focus solely on detection accuracy without explicit privacy considerations.	Highlighting privacy adds a novel dimension, aligning with healthcare data confidentiality requirements.
Adaptability	The system dynamically updates models based on new data, handling evolving threats effectively.	Some works use static models, leading to decreased effectiveness over time.	The adaptability feature is a significant advancement, addressing concept drift and evolving attack patterns.
Performance Metrics	Achieved high detection accuracy (>95%), low false positive rates, and robustness against various attack types.	Performance varies; many achieve 80-90% accuracy with higher false positives.	Demonstrates superior performance, emphasizing the benefits of ensemble and privacy-aware designs.
Data Used	.Use of public datasets like NSL-KDD, UNSW-NB15, or custom datasets without privacy focus.	Simulated or real healthcare sensor data with attack scenarios, emphasizing privacy constraints	The focus on healthcare-specific data and privacy is more aligned with real-world healthcare system requirements.
Novelty and Contributions	Integrates ensemble learning with privacy preservation and adaptability tailored for healthcare WSNs.	Many studies focus on detection accuracy but lack integrated privacy or adaptability features.	The holistic approach is more suited for sensitive healthcare environments, providing practical benefits.

privacy guarantees while maintaining high detection performance. The secure SSL communication effectively prevented interception or tampering of model updates. The adaptive learning component enabled the model to respond swiftly to new threat patterns, with an average adaptation latency of 80ms, and subsequent accuracy improvements of up to 3% in detecting novel threats.

Table 2 shows a summarized comparison of proposed work and with other related works in the sphere of threat detection in wireless sensor networks (WSNs), with emphasis on healthcare systems.

6. Limitations and Future Work

Though the results obtained by the proposed system are promising, there are some factors seemingly limiting the performance of this system. These imitations include the computational overhead arising from the deployment of differential privacy noise addition and the need for real-world deployment to validate performance given the resource-constrained nature of WSN and other operational constraints. Future work will focus on extending the adaptive learning component for more rapid responses to the evolving threats than is obtained in this work. Also, the privacy-utility trade-offs can be further enhanced by exploring more efficient privacy preserving techniques to ensure more data confidentiality, and deploying the system in live hospital environments for comprehensive validation. Overall, the evaluation demonstrates that our ensemble-based federated learning system effectively balances high threat detection accuracy, patient privacy, and adaptability to evolving threats in hospital WSNs for remote patient monitoring. Its robust architecture and privacy-preserving features make it a viable solution for secure healthcare WSNs environments.

7. Conclusions

This study presented a novel adaptive and privacy-aware ensemble-based threat detection scheme to make sure that evolving threats are held in check on a real-time basis and to guarantee that patients' data confidentiality is not compromised in wireless sensor networks deployed within healthcare systems. Using diverse classifiers, federated learning with differential privacy mechanism and adaptive learning strategies, the proposed model effectively detects security threats in patient data collected from the WSNs and also efficiently provides confidentiality and integrity of sensitive patient data. Experimental results showed that our model outperforms traditional single-model detection methodologies in terms of detection accuracy, robustness, and computational efficiency, making it well-suited for real-time healthcare environments. Furthermore, the incorporation of privacy-preserving capability through federated learning and differential privacy ensures confidentiality of patient information in line with the stringent privacy requirements inherent in medical applications. Future work will focus on extending the framework to incorporate federated learning paradigms for distributed threat detection and exploring its scalability in large-scale healthcare deployments. Overall, this research contributes a practical and resilient solution to bolster the internal security and privacy of Wireless healthcare Sensor Networks (WSNs), thereby fostering trust and reliability in digital health infrastructures. The performance metrics confirm that the proposed ensemble-based federated threat detection system effectively balances accuracy, privacy, and adaptability, making it a viable solution for secure remote patient monitoring in hospital wireless sensor networks.

8. Declarations

8.1. Author Contributions

Emmanuel Iheanacho Afonne: Review & Editing, Project Administration and Supervision. The author approved the final version of the manuscript; **Patrick 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, Funding acquisition.

8.2. Institutional Review Board Statement

Not applicable.

8.3. Informed Consent Statement

Not applicable.

8.4. Data Availability Statement

The data is available from the corresponding author upon reasonable request.

8.5. Acknowledgment

Not applicable.

8.6. Conflicts of Interest

The authors declare no conflicts of interest.

9. References

[1] A. Lanzolla and M. Spadavecchia, "Wireless Sensor Networks for Environmental Monitoring," *Sensors*, vol. 21, no. 4, p. 1172, Feb. 2021, doi: https://doi.org/10.3390/s21041172.

[2] Q. S. Zhang, "Environment Pollution Analysis on Smart Cities Using Wireless Sensor Networks," *Strategic Planning for Energy and the Environment*, Dec. 2022, doi: https://doi.org/10.13052/spee1048-5236.42112.

[3] T. Jabeen, I. Jabeen, H. Ashraf, N. Z. Jhanjhi, A. Yassine, and M. S. Hossain, "An Intelligent Healthcare System Using IoT in Wireless Sensor Network," *Sensors*, vol. 23, no. 11, p. 5055, Jan. 2023, doi: https://doi.org/10.3390/s23115055.

[4] A. Sayari and S. Rekhis, "Cyber Deception Across Domains: A Comprehensive Survey of Techniques, Challenges, and Perspectives," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 7, 2025, doi: https://doi.org/10.14569/ijacsa.2025.0160792.

[5] S. Akhilendranath and P. Senthilkumar, “The HALF framework: a privacy-preserving federated learning approach for scalable and secure AI applications,” *International Journal on Smart Sensing and Intelligent Systems*, vol. 18, no. 1, Jan. 2025, doi: https://doi.org/10.2478/ijssis-2025-0058.

[6] A. Chaddad, Y. Wu, and C. Desrosiers, “Federated Learning for Healthcare Applications,” *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7339–7358, Oct. 2023, doi: https://doi.org/10.1109/jiot.2023.3325822.

[7] R. Uddin and I. Koo, "Real-time remote patient mon-itoring: A review of biosensors integrated with multi-hop IoT systems via cloud connectivity," *Applied Sciences,* vol. 14, no. 5, pp. , 14(5), 1876., 2024, https://doi.org/10.3390/app14051876.

[8] D. Kandris, C. Nakas, D. Vomvas and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," *Applied system innovation,* vol. 3, no. 1, p. 14, 25 Feb 2020, https://doi.org/10.3390/asi3010014.

[9] K. M. Abubeker and S. Baskar, “Wireless sensor and wireless body area network assisted biosensor network for effective monitoring and prevention of non-ventilator hospital-acquired pneumonia,” *Frontiers in Sustainable Cities*, vol. 4, Nov. 2022, doi: https://doi.org/10.3389/frsc.2022.1063067

[10] R. Kashyap, "Applications of wireless sensor networks in healthcare. In IoT and WSN applications for modern agricultural advancements," *Emerging research and opportunities,* pp. 8-40, 2020, https://doi.org/10.4018/978-1-5225-9004-0.ch002.

[11] G. Ijemaru, "Large-Scale Internet of Things and Wireless Rechargeable Sensor Networks for Deployment in Smart Cities.," 2023, https://doi.org/10.25907/00821.

[12] S. L. Ullo and G. R. Sinha, "Advances in smart environment monitoring systems using IoT and sensors," *Sensors,* vol. 20, no. 11, p. 3113, 2020, https://doi.org/10.3390/s20113113.

[13] M. N. Mowla, N. Mowla, A. S. Shah, K. M. Rabie and T. Shongwe, "Internet of Things and wireless sensor networks for smart agriculture applications: A survey," *IEEE Access,* vol. 11, pp. 145813-145852, 2023, https://doi.org/10.1109/ACCESS.2023.3346299.

[14] B. Bhushan and G. Sahoo, Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective.: Handbook of computer networks and cyber security: principles and paradigms, pp. 683-713, 2020, https://doi.org/10.1007/978-3-030-22277-2_27.

[15] H. Sharma, A. Haque and F. Blaabjerg, "Machine learning in wireless sensor networks for smart cities: a survey," *Electronics,* vol. 10, no. 9, p. 1012., 2021, https://doi.org/10.3390/electronics10091012.

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

[17] K. Karunanithy and B. Velusamy, "An efficient data collection using wireless sensor networks and internet of things to monitor the wild animals in the reserved area," *Peer-to-Peer Networking and Applications,* vol. 15, no. 2, pp. 1105-1125, 2022, https://doi.org/10.1007/s12083-021-01289-x.

[18] R. Vera-Amaro, M. E. R. Angeles and A. Luviano-Juarez, "Design and analysis of wireless sensor networks for animal tracking in large monitoring polar regions using phase-type distributions and single sensor model," *IEEE Access,* vol. 7, pp. 45911-45929., 2019, https://doi.org/10.1109/ACCESS.2019.2908308.

[19] S. Sadeghi, N. Soltanmohammadlou and F. Nasirzadeh, “Applications of wireless sensor networks to improve occupational safety and health in underground mines,” *Journal of safety research,* vol. 83, pp. 8-25, 2022, https://doi.org/10.1016/j.jsr.2022.07.016.

[20] R. Alekya, N. D. Boddeti, K. S. Monica, R. Prabha and V. Venkatesh, "IoT based smart healthcare monitoring systems: A literature review," *European Journal of Molecular & Clinical Medicine,* vol. 7, no. 11, 2020, https://www.researchgate.net/profile/Venkatesh-Ramani/publication/348930509_IoT_based_Smart_Healthcare_Monitoring_Systems_A_Literature_Review/links/6017d531299bf1b33e3d5fee/IoT-based-Smart-Healthcare-Monitoring-Systems-A-Literature-Review.pdf.

[21] M. Yuvaraja, R. Ramesh, R. Priya and J. Dhanasekar, "Wireless Body Sensor Networks for Real-Time Healthcare Monitoring: A Cost-Effective and Energy-Efficient Approach," *Integrative Biomedical Research,* vol. 8, no. 7, pp. 1-13, 2024, https://doi.org/10.25163/angiotherapy.879796.

[22] H. M. A. Fahmy, "WSNs applications. In Concepts, applications, experimentation and analysis of wireless sensor networks," *Cham: Springer Nature, Switzerland,* pp. 67-242, 2023, https://doi.org/10.1007/978-3-031-20709-9_3.

[23] H. M. Kaidi, M. A. M. Izhar, R. A. Dziyauddin, N. E. Shaiful and R. Ahmad, " A comprehensive review on wireless healthcare monitoring: System components," *IEEE Access,* vol. 12, pp. 35008-35032, 2024, https://doi.org/10.1109/ACCESS.2024.3349547.

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

[25] A. Ahmed, M. M. Khan, P. Singh, R. S. Batth and M. Masud, "IoT-based real-time patients vital physiological parameters monitoring system using smart wearable sensors," *Neural Comput Appl,* , vol. 34, no. 22, pp. 19397-19673, 2023, https://doi.org/10.1007/s00521-022-07090-y.

[26] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics,* vol. 12, no. 6, p. 1333, 2023, https://doi.org/10.3390/electronics12061333.

[27] A. Akinsola, T. K. Njoku, O. Ejiofor and A. Akinde, "Enhancing data privacy in wireless sensor networks: investigating techniques and protocols to protect privacy of data transmitted over wireless sensor networks in critical applications of healthcare and national security," *International Journal of Network Security Its Applications (IJNSA),* vol. 16, no. 2, 2024, https://doi.org/10.5121/ijnsa.2024.16204.

[28] M. A. I. Mallick and R. Nath, "Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments," *World Scientific News,* vol. 190, no. 1, pp. 1-69, 2024, https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf.

[29] S. Benoy, "Wireless Sensor Networks for Healthcare Monitoring Challenges and Opportunities," *Journal of Biomedical Systems for Emerging Technology,* vol. 10, p. 163, 2023, https://www.hilarispublisher.com/open-access/wireless-sensor-networks-for-healthcare-monitoring-challenges-and-opportunities-98539.html.

[30] A. John, I. F. Isnin and S. H. H. Madni, "Current security threats in applications of wireless sensor network," *International Journal on Engineering, Science and Technology,* vol. 5, no. 3, pp. 255-272, 2023, https://doi.org/10.46328/ijonest.174.

[31] S. Ismail, D. W. Dawoud and H. Reza, "Securing wireless sensor networks using machine learning and blockchain: A review," *Future Internet,* vol. 15, no. 6, p. 200, 2023, https://doi.org/10.3390/fi15060200.

[32] L. Cai, J. Wang, R. Zhang, Y. Zhang, T. Jiang, D. Niyato and X. Shen, "Secure physical layer communications for low-altitude economy networking: A survey," *IEEE Communications Surveys & Tutorials*. (Early Access), 2025, https://doi.org/10.1109/COMST.2025.3634768.

[33] S. Jeyalakshmi, S. Sekar, S. Ravikumar and D. Kavitha, "Random forest-based oppositional henry gas solubility optimization model for service attack improvement in WSN," *Journal of The Institution of Engineers (India): Series B,* vol. 103, no. 3, pp. 939-950, 2022, https://doi.org/10.1007/s40031-021-00702-6.

[34] P. R. Grammatikis and P. Sarigiannidis, "Network Threats," in *Cyber-Security Threats, Actors, and Dynamic Mitigation* , CRC Press, pp. 159-198, 2022, http://doi.org/10.1201/9781003006145-5.

[35] R. U. Z. Wani, F. Thabit and O. Can, "Security and privacy challenges, issues, and enhancing techniques for Internet of Medical Things: A systematic review," *Security and Privacy,* vol. 7, no. 5, p. e409, 2024, https://doi.org/10.1002/spy2.409.

[36] E. Illi, M. Qaraqe, S. Althunibat, A. Alhasanat, M. Alsafasfeh, M. De Ree and S. Al-Kuwari, "Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks," *IEEE Communications Surveys & Tutorials*, vol. 6, no. 1, 2024, https://doi.org/10.1109/COMST.2023.3327327.

[37] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai and W. Zhang, "A survey on federated learning: challenges and applications," *International journal of machine learning and cybernetics,* vol. 14, no. 2, pp. 513-535, 2023, https://doi.org/10.1007/s13042-022-01647-y.

[38] F. Sharif, "The role of ensemble learning in strengthening intrusion detection systems: A machine learning perspective," *Int. J. Comput. Eng. Technol,* pp. 1-14, 2024, http://doi.org/10.13140/RG.2.2.10798.93766.

[39] A. Vinolia, N. Kanya and V. N. Rajavarman, "Machine learning and deep learning based intrusion detection in cloud environment: a review.," in *5th International Conference on Smart Systems and Inventive Technology (ICSSIT),* January, 2023, https://doi.org/10.1109/ICSSIT55814.2023.10060868.

[40] N. M. Alruhaily and D. M. Ibrahim, "A multi-layer machine learning-based intrusion detection system for wireless sensor networks," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 4, pp. 281-288, 2021, https://doi.org/10.14569/IJACSA.2021.0120437.

[41] V. Gowdhaman and R. Dhanapal, "An intrusion detection system for wireless sensor networks using deep neural network," *Soft Computing,* vol. 26, no. 23, pp. 13059-13067, 2022, https://doi.org/10.1007/s00500-021-06473-y.

[42] A. Awajan, "A Novel Deep Learning-Based Intrusion Detection System for IoT Networks," *Computers,* vol. 12, no. 2, p. 34, 2023, https://doi.org/10.3390/computers12020034.

[43] R. B. Kagade, S. Jayagopalan, "Optimization assisted deep learning based intrusion detection system in wireless sensor network with two-tier trust evaluation," *International Journal of Network Management,* vol. 32, no. 4, p. e2196, 2022, https://doi.org/10.1002/nem.2196.

[44] H. S. Sharma, A. Sarkar and M. M. Singh, "An efficient deep learning-based solution for network intrusion detection in wireless sensor network," *International Journal of System Assurance Engineering and Management,* vol. 14, no. 6, pp. 2423-2446, 2023, https://doi.org/10.1007/s13198-023-02090-0.

[45] M. Alazab, S. P. RM, M. Parimala, P. K. R. Maddikunta, T. R. Gadekallu and Q. V. Pham, "Federated learning for cybersecurity: Concepts, challenges, and future directions," *IEEE Transactions on Industrial Informatics,* vol. 18, no. 5, pp. 3501-3509, 2021, https://doi.org/10.1109/TII.2021.3119038.

[46] B. Dash, P. Sharma and A. Ali, " Federated learning for privacy-preserving: A review of PII data analysis in Fintech," *International Journal of Software Engineering Applications (IJSEA),* vol. 13, no. 4, 2022, Available at SSRN: https://ssrn.com/abstract=4323967.

[47] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, K. K. R. Choo and M. Nafaa, "FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things," *Journal of Parallel and Distributed Computing,* vol. 165, pp. 17-31, 2022, https://doi.org/10.1016/j.jpdc.2022.03.003.

[48] M. J. Idrissi, H. Alami, A. El Mahdaouy, A. El Mekki, S. Oualil, Z. Yartaoui and I. Berrada, "Fed-anids: Federated learning for anomaly-based network intrusion detection systems," *Expert Systems with Applications,* vol. 234, p. 121000, 2023, https://doi.org/10.1016/j.eswa.2023.121000.

[49] J. A. de Oliveira, V. P. Gonçalves, R. I. Meneguette, R. T. de Sousa Jr, D. L. Guidoni, J. C. Oliveira and G. P. Rocha Filho, "F-NIDS—A Network Intrusion Detection System based on federated learning.," *Computer Networks,* vol. 236, p. 110010., 2023, https://doi.org/10.1016/j.comnet.2023.110010.

[50] A. Alazab, A. Khraisat, S. Singh and T. Jan, "Enhancing privacy-preserving intrusion detection through federated learning," *Electronics,* vol. 12, no. 16, p. 3382, 2023, https://doi.org/10.3390/electronics12163382.

[51] R. R. dos Santos, E. K. Viegas, A. O. Santin and P. Tedeschi, "Federated learning for reliable model updates in network-based intrusion detection," *Computers Security,* vol. 133, p. 103413, 2023, https://doi.org/10.1016/j.cose.2023.103413.

[52] R. Lazzarini, H. Tianfield and V. Charissis, "Federated learning for IoT intrusion detection.," *AI,* vol. 4, no. 3, pp. 509-530, 2023, https://doi.org/10.3390/ai4030028.

[53] A. Fenjan, M. T. M. Almashhadany, S. R. Ahmed, H. A. Fadel, R. Sekhar, P. Shah and B. S. Veena, "Adaptive Intrusion Detection System Using Deep Learning for Network Security," in *Cognitive Models and Artificial Intelligence Conference*, pp. 279 – 284, 2024, https://doi.org/10.1145/3660853.3660928.

[54] W. Villegas-Ch, J. R. Govea, A. Gutierrez, M. Navarro and A. Mera-Navarrete, "Effectiveness of an Adaptive Deep Learning-Based Intrusion Detection System," *IEEE Access,* vol. 12, pp. 184010-184027, 2024, http://doi.org/10.1109/ACCESS.2024.3512363.

[55] M. A. Shyaa, N. F. Ibrahim, Z. Zainol, R. Abdullah, M. Anbar and L. Alzubaidi, "Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems," *Engineering Applications*

of Artificial Intelligence, vol. 137, p. 109143, 2024, https://doi.org/10.1016/j.engappai.2024.109143.

[56] N. Z. Rizqullah, J. Alekhine, D. L. Yonia, R. M. R. Purnomo and A. M. Shiddiqi, " Enhancing Intrusion Detection Systems with Adaptive Learning Techniques," in *IEEE International Conference on Artificial Intelligence and Mechatronics*, 2024, https://doi.org/10.1109/AIMS61812.2024.10513076.

[57] X. J. Li, M. Ma and Y. Sun, "An adaptive deep learning neural network model to enhance machine-learning-based classifiers for intrusion detection in smart grids," *Algorithms,* vol. 16, no. 6, p. 288, 2023, https://doi.org/10.3390/a16060288.

[58] Z. Nie, S. Basumallik, P. Banerjee and A. K. Srivastava, "Intrusion Detection in Cyber-Physical Grid using Incremental ML with Adaptive Moment Estimation," *IEEE Transactions on Industrial Cyber-Physical Systems,* vol. 2, pp. 206-219, 2024, https://doi.org/10.1109/TICPS.2024.3413607.

[59] M. U. Tanveer, K. Munir, M. Amjad, S. A. J. Zaidi, A. Bermak and A. U. Rehman, "Ensemble-Guard IoT: A Lightweight Ensemble Model for Real-Time Attack Detection on Imbalanced Dataset," *IEEE Access,* vol. 12, no. 6, pp. 168938-168952, 2024, https://doi.org/10.1109/ACCESS.2024.3495708.

[60] A. A. Alhashmi, A. M. Alashjaee, A. A. Darem, A. F. Alanazi and R. Effghi, "An ensemble-based fraud detection model for financial transaction cyber threat classification and countermeasures," *Engineering, Technology Applied Science Research,* vol. 13, no. 6, pp. 12433-12439, 2023, https://doi.org/10.48084/etasr.6401.

[61] E. Jaw and X. Wang, "Feature selection and ensemble-based intrusion detection system: an efficient and comprehensive approach," *Symmetry,* vol. 13, no. 10, p. 1764, 2021, https://doi.org/10.3390/sym13101764.

[62] M. A. Hossain and M. S. Islam, "A novel hybrid feature selection and ensemble-based machine learning approach for botnet detection," *Scientific Reports,* vol. 13, no. 1, p. 21207, 2023, https://doi.org/10.1038/s41598-023-48230-1.

[63] M. Torabi, N. Udzir, M. Abdullah and R. Yaakob, "A Review on Feature Selection and Ensemble Techniques for Intrusion Detection System," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 5, pp. 538-553, 2021, https://doi.org/10.14569/IJACSA.2021.0120566.

[64] M. A. Hossain and M. S. Islam, "Ensuring network security with a robust intrusion detection system using ensemble-based machine learning," *Array,* vol. 19, p. 100306, 2023, https://doi.org/10.1016/j.array.2023.100306.

[65] M. A. Hossain and M. S. Islam, "Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity," *Measurement Sensors,* vol. 32, p. 101037, 2024, https://doi.org/10.1016/j.measen.2024.101037.

[66] A. Das and B. S. Sunitha, "Anomaly-based network intrusion detection using ensemble machine learning approach.," *International Journal of Advanced Computer Science and Applications,* vol. 13, no. 2, 2022, https://doi.org/10.14569/IJACSA.2022.0130275.