Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 8068038, 27 pages
https://doi.org/10.1155/2023/8068038

Research Article

Blockchain-Based Secure Localization against Malicious Nodes in IoT-Based Wireless Sensor Networks Using Federated Learning

Gebrekiros Gebreyesus Gebremariam,[1,2] **J. Panda**,[2] **and S. Indu**[2]

[1]*Department of Electronics and Communication Engineering, Raya University, Maychew, 7020 Tigray, Ethiopia*
[2]*Department of Electronics and Communication Engineering, Delhi Technological University, Shahbad Daulatpur, Main Bwana Road, Delhi 110042, India*

Correspondence should be addressed to Gebrekiros Gebreyesus Gebremariam; kiros2004comp@gmail.com

Received 11 November 2022; Revised 9 January 2023; Accepted 13 January 2023; Published 31 January 2023

Academic Editor: Javier Prieto

Wireless sensor networks are the core of the Internet of Things and are used in healthcare, locations, the military, and security. Threats to the security of wireless sensor networks built on the Internet of Things (IoT-WSNs) can come from a variety of sources. This study proposes secure attack localization and detection in IoT-WSNs to improve security and service delivery. The technique used blockchain-based cascade encryption and trust evaluation in a hierarchical design to generate blockchain trust values before beacon nodes broadcast data to the base station. Simulation results reveal that cascading encryption and feature assessment measure the trust value of nodes by rewarding each other for service provisioning and trust by removing malicious nodes that reduce localization accuracy and quality of service in the network. Federated machine learning improves data security and transmission by merging raw device data and placing malicious threats in the blockchain. Malicious nodes are classified through federated learning. Federated learning combines hybrid random forest, gradient boost, ensemble learning, K-means clustering, and support vector machine approaches to classify harmful nodes via a feature assessment process. Comparing the proposed system to current ones shows an average detection and classification accuracy of 100% for binary and 99.95% for multiclass. This demonstrates that the suggested approach works well for large-scale IoT-WSNs, both in terms of performance and security, when utilizing heterogeneous wireless senor networks for the providing of secure services.

1. Introduction

Technology and network advancements have created a new environment where the Internet of Things (IoT) is flourishing, fostering several positive social and economic changes [1]. The Internet of Things (IoT) are the networked and interconnected systems, devices, applications, and people that process data [2]. The Internet of Things makes it possible for physical objects to communicate with one another and share critical information while also making decisions and completing important tasks. As a result, these objects now have the capacity to see, hear, think, and carry out significant acts [3]. IoT-WSNs are important and popular research areas in recent applications, including military, smart cities, healthcare, and environmental [4]. The rapid growth of the Internet of Things (IoT) is largely due to the contributions of wireless sensor networks (WSNs), which have both practical and academic importance. Ad hoc networks, or WSNs, are made up of a swarm of devices, or "sensor nodes," each of which is equipped with some form of sensing technology. Sensor nodes should be able to self-organize, be deployed at random, be fault-tolerant, and monitor a wide region with high precision. IoT-WSNs are self-organizing networks with different parameters for monitoring and collecting environmental data. The sensor nodes cooperate and evaluate each other for effective data transmission and detection and removal of malicious nodes in the network. The malicious attacks can be internal or external for exploiting information and creating wrong routing information between the sensor node and base station by compromising the beacon node in the cluster region. The malicious node degrades the network performance by

broadcasting wrong information and creating mistrust between the nodes and end users. The trust evaluation process continuously uses threshold and signal strength values between the sensor nodes to detect and analyze the network's malicious nodes.

The integrity of bitcoin networks is ensured by blockchain, a distributed ledger technology [5]. This groundbreaking architecture is now often utilized in a variety of distributed contexts, including healthcare and automotive ad hoc networks (VANET). There are three primary reasons why blockchain technology is well-suited to addressing IoT security concerns, according to a number of studies. As with an IoT network, the data associated with blockchain technology is stored and handled in a decentralized fashion by all of the agents in the network. Distributed blockchain technology offers many advantages over traditional centralized management approaches, including the elimination of a potential single point of failure and a significant reduction in the cost of keeping a large number of Internet of Things devices up and running. Lack of trust between IoT devices is a commonplace because of the energy-limited nature of these devices. As a result, sensitive information stored on these devices is at risk of being exposed or stolen. Due to blockchains unique immutability, it allows parties to exchange information without having to rely on one other's integrity. In the blockchain design, data is saved in blocks, each of which has a hash backup of the data in the preceding block. In many instances, it is also necessary for the devices to be completely untraceable. However, most gadgets have a low setup and are not suited for the complexity of standard encryption methods. With the blockchain architecture of IoT-WSNs, entities connect with one another using transactions as the fundamental unit of information exchange. In the first iteration of the blockchain, every piece of data pertaining to a client's commercial exchange is considered a transaction.

Many fields, including medicine, computer vision, and wireless communication, have benefited from the significant progress made in recent years in machine learning (ML) techniques and especially in deep learning (DL) models. ML also encompasses shallow models [6]. It can provide means for detecting certain forms of attacks without requiring intensive human engagement. Intrusion detection systems (IDS) that employ ML techniques can train themselves by observing and comparing "normal" and "abnormal" flows of traffic. It can be used to detect harmful traffic patterns in a dataset or in an actual environment. Although these approaches have been put to good use for IDS, they often necessitate a centralized organization to process and aggregate data from all users on the network and found that high packet loss rate reduces prediction accuracy at larger network size. In this study, we proposed blockchain-based hybrid federated machine learning techniqe for locating and identifying the origin of assaults in IoT-WSNs, using the immutable and distributed ledger technology blockchain.

1.1. Blockchain Applications in IoT-WSNs. Blockchain is a distributed database for storing transactions' records to provide trust in unknown nodes in the network with the same edge. A blockchain, as its name implies, is a series of linked blocks. The structure for storing bargaining data is a chain of blocks, each of which has its own hash value and contains a specified quantity of transaction data. All the data on the blockchain is secure because each block contains a unique hash value for the one before it [5]. The blockchain is a distributed, unchangeable ledger of all transactions that have been validated by a majority of the network's peers. Distributed ledger is a term for the system of decentralized data storage it describes [7]. Whenever a ledger transaction is performed, it is validated with the approval of the majority of the network users. The most well-known application of blockchain technology in the real world is Bitcoin. Connecting blockchain technology with the Internet of Things has many benefits. For example, a decentralized blockchain storage architecture can synchronize IoT devices and deliver real-time data to each IoT node. However, the data produced by these applications is enormous, leading to problems associated with big data. Therefore, artificial intelligence (AI) functions as an analytical tool and contributes to decision-making, categorization, prediction, and detection in a blockchain-enabled IoT network to solve this problem. Further, the analysis in the current blockchain-based architecture is performed on a cloud server. However, there are limitations associated with using a centralized server, including slow speeds and accuracy, as well as low latency and limited computational storage. Fog computing, a new distributed paradigm that may be able to meet these needs, warrants extensive study. Fog computing, which Cisco first defined in 2012, is a distributed architecture that brings cloud services to the network's periphery. Fog computing's principles offer extensive assistance to blockchain-based applications, including but not limited to location awareness, support for heterogeneity, low latency, mobility, and geodistribution. In addition to these load-balancing and data-gathering benefits, fog computing has found application in other areas. As a result, this research combines fog computing with AI to create a distributed security mechanism that can identify DoS attacks directed at mining pools in a blockchain-enabled IoT network. The integrated secure attack detection model using blockchain, IoT, AI, and fog computing is depicted in Figure 1 for various applications.

Blockchain is an up-and-coming technology that is being implemented in numerous sectors to facilitate security and distributed trust among peer nodes [8]. The following sections cover some literature that has utilized blockchain technology to safeguard IoT applications. For authentication and authorization in IoT-based WSNs, blockchain technology was integrated into IoT. To solve this problem, we propose a blockchain-based decentralized localization technique, a pseudonymous permission management framework that gives users complete authority over their own information while also protecting their privacy. Blockchain models are decentralized access control managers that store access permissions to resources. A new subfield of study is exploring the use of blockchain technology in IoT based-WSNs [9].

Some academics have recently included blockchain in WSNs to solve problems with processing capability, data storage, node failure, and user access management. The mobile edge computing (MEC) server can store encrypted

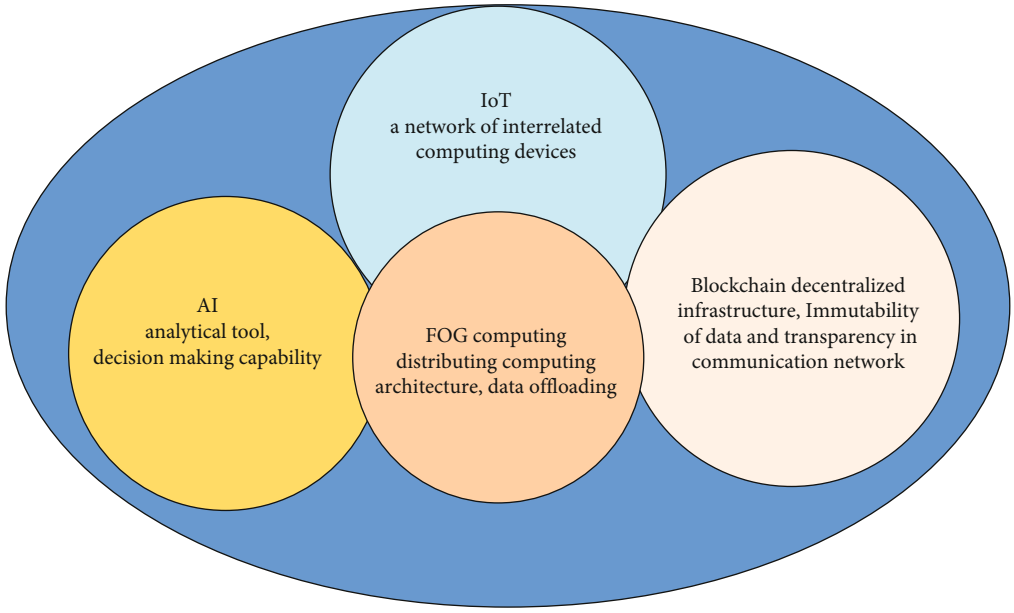


Figure 1: Illustrating of secure IoT-based WSNs showing the use of a detection model incorporating blockchain, IoT, AI, and fog computing [7].

block hashes in memory and delegate computationally difficult mining work to the edge computing nodes. The blockchain uses census algorithms to achieve agreement between unknown nodes using proof-of-work (PoW), proof-of-state, and proof-of-authority (PoA). The blockchain establishes trust in the network by storing the transactions in the block in chronological order consisting of headers and bodies. The headers contain the hash elements, including the transaction root, previous blocks, and timestamp. Blockchain techniques are applied in different domains in IoT-based wireless sensor networks for effective localization of the beacon nodes in the network. Sensor nodes sense and collect data containing precise location and identity to the sink node in the network. However, malicious nodes' presence affects the location and position of sensor nodes by compromising the beacon nodes and sending wrong information to the sink node. The blockchain-based secure localization scheme provides reliable service to the client nodes using the nonrepudiation model.

A sensor node's location can be determined by a global positioning system (GPS) or via other means of precise localization [10]. One approach is to centralize the management of information about the network as a whole, employing mathematical techniques to determine the locations of individual nodes. In WSN, the support vector machine is primarily used for securing nodes and determining their locations. The mobile node localization strategy uses support vector machines and information about network accessibility. It determines the node's position by measuring the strength of the incoming signal or RSSI. Fast and widespread localization is possible with localized SVM, although it is still vulnerable to outliers in the training data. Support vector regression (SVR), a unique data extraction method for localization models, has led to more accurate localization. Without increasing the price of the necessary gear, it enhances localization's precision. Using SVM-based learning with a small number of anchor nodes, we can precisely pinpoint the location of the unknown node. Grid cells of finite size guarantee precision. SVM-based DV-hop works well for large-scale networks. Some AI capabilities are made available to sensor nodes by use of a localization method based on a self-organizing map (SOM). SOM can learn classification on its own without human input. Each sensor node's location is calculated using a self-organizing map. The input layer consists of the spatial coordinates of eight anchor nodes close to the unknown node. After training, the network's output layer provides the unidentified node's unique 2D spatial coordinates. This approach has the drawback that nodes must be uniformly distributed across the monitored area.

This study presents a fog computing-based distributed intrusion detection system (IDS) for mining pools in blockchain-enabled IoT networks, complete with safe planning and simulation, attack detection, and classification. Hybrid federated machine learning algorithms are used to train the suggested IDS. Figure 2 depicts a high-level view of the suggested distributed paradigm. Sensing nodes are the building blocks of the detection system, and it is their job to track and identify any moving objects that come within range. Based on their performance in training and testing, all IoT sensors belong to one of several groups, each with the same capabilities for detection. This cluster sends its data to nearby fog nodes. Since fog nodes act as a gateway or access point for IoT devices, they must incorporate an intrusion detection system as part of their security infrastructure. Incoming traffic is analyzed by IDS, and actions are done based on its results. Assuming a typical influx of data, the transaction is broadcast throughout the mining pool's memory. In a blockchain network hosted in the cloud, miners choose which transactions to mine and create new blocks.

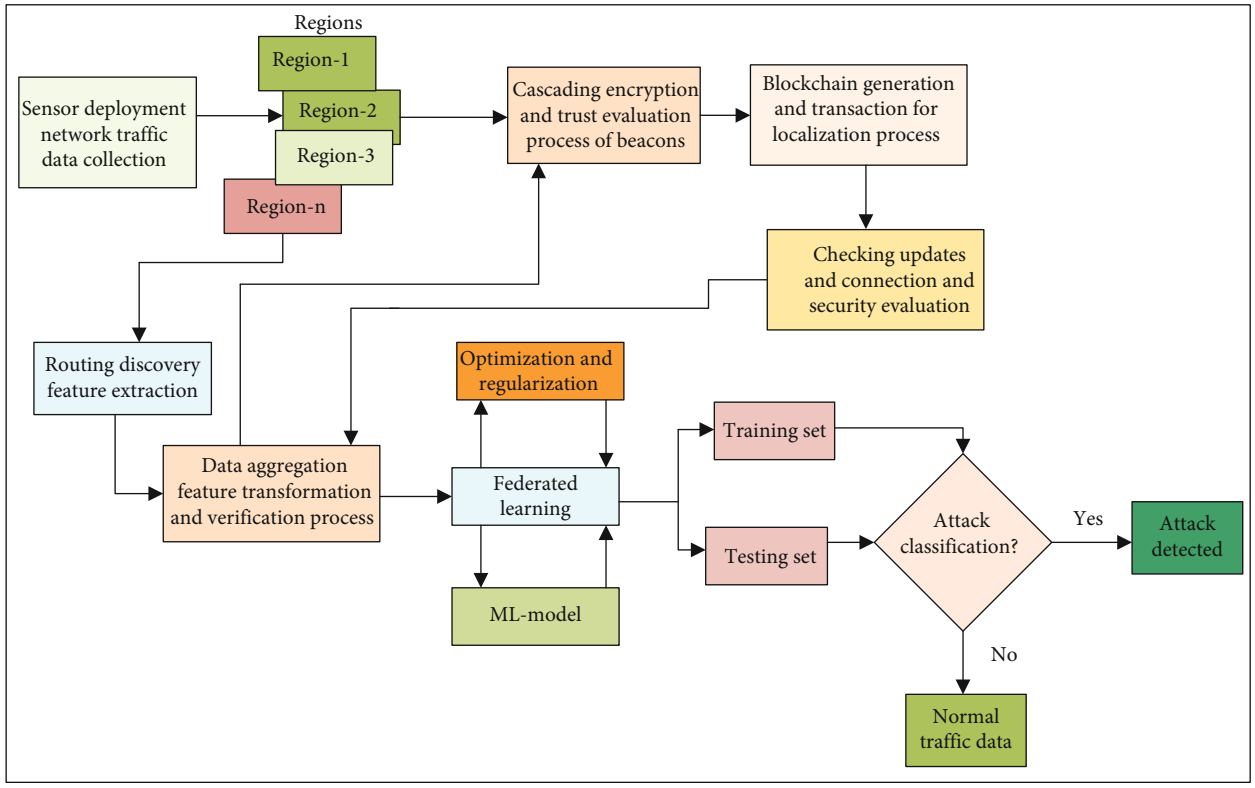


Figure 2: Blockchain-based secure localization detection of attacks for IoT-based wireless sensor networks using federated learning.

To alert the administrator to take corrective action in the event of malicious or invalid transactions, the IDS will sound an alarm. Scalability and detection performances for routing threats in IoT-based WSNs are two advantages of the proposed approach. It functions well in IoT systems that incorporate several wireless sensor networks.

1.2. Motivation and Contribution. The literature reveals a wide variety of security issues and concerns related to the design, development, and implementation of IDS, detection, and classification attacks utilizing blockchain technology in IoT-based wireless sensor networks. As the number of distributed denial of service (DDoS) attacks in the blockchain-IoT ecosystem rises, all IoT networks supported by blockchain will become increasingly at risk. Protecting a blockchain-based Internet of Things network requires a complex distributed security architecture, making sure a security mechanism can deal with the massive amounts of data produced by IoT devices and applies the right analytical tools in a decentralized framework. It is not easy to make an IDS that can tell the difference between safe and dangerous online transactions. Not much is known about how to prevent distributed denial of service (DDoS) attacks against mining pools in blockchain-enabled Internet of Things (IoT) wireless sensor networks once the corresponding model has been implemented. Because of these issues, we presented a hybrid federated machine learning-based technique for detecting and localizing routing attacks in WSNs-IoT by analyzing representative datasets.

In light of these problems, we proposed the use of a secure blockchain enabled by federated learning (FL) in Internet of Things (IoT) wireless sensor networks in order to identify and localize assaults. With FL, devices can work together to learn without transmitting information to a central hub. That is to say, ML/DL can be trained in a distributed fashion, requiring several devices and servers to process data over multiple rounds of training. The two main components of this approach are local learning and model transmission, which together provide for the privacy preservation and cost reduction typical of more traditional centralized machine learning approaches. When using FL, the entire ML/DL model can be refined over time. The FL server picks a subset of clients at the start of each round to take part in the learning process and shares its most recent global model with them. The contributions of the proposed secure localization based on blockchain technique in IoT-based wireless sensor network are bulleted as follows:

(1) Explore blockchain techniques for detecting and localizing malicious nodes in IoT-based wireless senor networks

(2) Enhance detection and localization of malicious nodes in IoT-based wireless sensor networks to improve service quality

(3) Explore the effectiveness of federated learning techniques using performance metrics to evaluate the attack detection performance

(4) Provide secure routing and data transmission in a hierarchical IoT-based wireless sensor network for secure service provisioning

(5) Effective detection and localization of malicious nodes by computing the unknown nodes based on the blockchain technique with the help of beacon node

(6) Secure data aggregation and trust value computation of beacon nodes using a trust management model based on blockchain for malicious node removal and ensuring service provision

(7) Design and plan secure range-free localization processing using blockchain technology-based selection of trust value of the miner beacon nodes

(8) Explore the blockchain secure data aggregation and localization of unknown nodes for malicious node detection and localization using federated learning approaches

The other parts of this paper are organized in the following sections. Section 2 contains previous literature works on secure blockchain-based localization in IoT-based wireless sensor networks. Sections 3 and 4 detail the network models, proposed methods, and simulation techniques of the scheme using blockchain techniques. Sections 5 details simulation results and analysis. Section 6 is about performance evaluation and validation followed by Section 7 containing conclusion and future work.

2. Related Works

Several related works and techniques have been reviewed for detecting and localizing malicious nodes in IoT-based wireless sensor networks. The schemes in the literature include the following:

(i) Secure localization of malicious nodes in low power sensor node networks

(ii) Routing schemes for effective resource consumption and network life time

(iii) Authentication and encryption processes for establishing trust among nodes

(iv) Blockchain-based localization technique for improving quality of services in WSNS

(v) Techniques for achieving optimized and secure data storage in IoT-WSNs

(vi) Secure and optimized models for the next-generation IoT-based WSNs

(vii) Federated machine learning and classification techniques

Kim et al. [1] conducted research on blockchain techniques based on a trust management model for detecting malicious nodes by enhancing relationships among beacon nodes using various evaluation metrics, including closeness, honesty, detection rate, average energy consumption, frequency of interaction, and intimacy. The beacon nodes are selected based on the trust values and broadcast information to the base station, forming a trust evaluation model for detecting and localizing malicious nodes in WSNs. Abubaker et al. [4] presented blockchain-based for detection and localization of malicious nodes in IoT-based wireless sensor networks using federated random forest and support vector machine techniques. They also discussed secure service provisioning using feature evaluation and cascading encryption for detecting and removing malicious nodes in the network. Security and performance metrics, including accuracy, node honesty, and end-to-end delay of the packet transmission, measured the performance of the malicious node detection and secure provisioning approaches. Ming et al. [5] suggested an authenticated group key agreement mechanism using blockchain technology for the Internet of Things. The suggested protocol includes a novel concept called the device manager, whose job is mediating communications between Internet of Things gadgets and blockchain infrastructures. The proposed protocol has been shown to be secure after being subjected to various assaults, as shown by the security analysis. The simulation results demonstrate that the time expenditures of protocol operations are fair and appropriate for IoT settings. Kumar et al. [7] proposed a new distributed intrusion detection system (IDS) leveraging fog computing for detecting DDoS assaults against mining pools in blockchain-enabled IoT networks. Random forest (RF) and a gradient tree boosting system (XGBoost) are trained on fog nodes, and their performances are compared. A real-world IoT dataset is used to evaluate the proposed model's performance, containing the most recent assaults discovered in a blockchain-enabled IoT network. The system for detecting DDoS attacks was connected to a mining pool in a blockchain-enabled IoT network. Three distinct mechanisms power the suggested distributed detection system. First, there is the traffic processing engine, which employs fog nodes to preprocess network data by standardizing its features with the help of the aforementioned Standard Scaler. Goyat et al. [11] examined a secure and novel range-free localization-based blockchain technique in wireless sensor networks against a malicious node in two-dimensional environments. They also discussed the implementation of blockchain technology using beacon nodes' trust value for the mining process of blocks to form a localization process for the unknown nodes with neighbor node list, mobility, residual energy, and repudiation value. The location and precise positions of the unknown nodes are computed using the trusted beacon nodes based on the blockchain-based generated trust values. The malicious nodes broadcast false localization information by compromising the beacon and reporting the false energy information. Awan et al. [12] proposed blockchain-based encryption and trust evaluation model for detection and secure data transmission. The authentication of the sensor nodes and aggregator nodes is in a private and public blockchain, respectively, for detection of the activities of malicious nodes, including transmitting wrong information

of routing and energy by compromising the aggregating node that degrades the network performance by increasing resource consumption and packet loss. The trust values and residual energy of the sensor nodes were computed after authentication based on the detection rate for removing the malicious nodes from the secure routing in the network. Honar Pajooh et al. [13] proposed a multilayer-based distributed and decentralized blockchain security model for a secure IoT model. IoT devices operate under multihop cellular networks using a self-clustering hybrid evolutionary algorithm combining simulated annealing and genetic algorithm approaches by clustering the unknown sensor nodes in the network. The cluster head authenticates and authorizes locally for effective communication between the cluster head and the base station using a private lightweight balanced blockchain with better throughput and network latency. Otoum et al. [14] presented an adaptive framework using integrated blockchain and federated learning using reinforcement support vector federated learning for a secure trust evaluation process in the network. The reinforcement learning occurs at the end devices, and the models were trained for communication with fog and creating a global model. They also evaluated and verified the model through simulation techniques using performance metrics, including trust value, energy consumption, and network lifetime. The model also achieved a detection rate and accuracy of 96% and 93%, respectively, for detecting and localizing malicious nodes using federated learning. She et al. [15] proposed a blockchain trust model framework for detecting malicious nodes in IoT-based wireless sensor networks by constructing blockchain data structure in three-dimensional space using a localization scheme. The detection of malicious nodes is realized using intelligent contact and wireless sensor networks quadrilateral measurement to localize and detect attacks. The sensor nodes are authenticated and recorded in the blockchain network to remove and prevent loss of routing information. Fan et al. [16] proposed a decentralized topology-based blockchain scheme for secure IoT systems during synchronization for detection and analysis attacks using multiple time resources. The scheme solved the problem of time announcement in IoT-based distributed wireless sensor networks using a closed blockchain for recording and broadcasting time for attack detection with adaptive topology for reducing communication overhead. The scheme also avoids centralization using block structure adaptable topology and multiple time sources. Friha et al. [17] presented secure IoT infrastructure using federated learning based on intrusion detection system agricultural applications for data protection producing an improved attack detection model. The scheme utilized a convolutional neural network, recurrent neural network, and deep neural network using benchmark datasets to detect and classify attacks and performance metrics. They also discussed the performance metrics, including recall, precision, F1-score, and accuracy for the multiclass classification federated deep learning model. Javaid [18] examined and designed the Dijkstra algorithm-based routing protocol for secure and efficient communication between the sensor and sink nodes without hole attacks in IoT-based WSNs. The scheme also provided transparency for transaction by the sensor nodes based on the network's blockchain technique for detecting malicious nodes. The transactions were added into blocks using the poof of authority consensus technique to validate the trust model in terms of the energy and detection metrics. Wu and Ansari [19] proposed blockchain-based secure and trust evaluation process for detection of malicious nodes in industrial Internet of Things for information sharing and access control list. The security of access control list is protected and stored by the blockchain. They also designed a voting technique with trust evaluation for access control list for high probability of malicious node detection and authentication in the network. Khan et al. [20] described the implementation of a low-energy, energy-temperature-degree-adaptive, hierarchical routing protocol. One advantage of the protocol is that it reduces the amount of energy used by nodes during data transmission, which in turn increases the lifespan of the network. The cluster heads (CHs) that will be used to carry out routing are chosen by the proposed protocol based on their degree, temperature, and energy. More importantly, the blockchain is used to eliminate the risk of a centralized failure point. Since several nodes are required for a blockchain to function, the CHs and BSs use it to store and record all of the data transactions that take place between them. Blockchain transactions are hashed using the 256-bit secure hashing method (SHA-256). To top it all off, the ETD-LEACH protocol uses a real-time message content validation (RMCV) mechanism to identify rogue nodes before they cause any damage during routing.

Goyat et al. [21] addressed IoT-WSN security issues and trusted architecture of secure localization attacks. In particular, it examines the trust evaluation method and the process of creating a blockchain. Trust values of each beacon node are calculated using several trust metrics, and the weights associated with those values are dynamically changed during the localization process. That is why only the most reliable beacon nodes are chosen during the mining procedure. This two-stage process guarantees an always up-to-date blockchain regarding reliability and the trust values of all beacon nodes. Minoli and Occhiogrosso [22] proposed and implemented a method of protection in the context of a defense-in-depth/castle approach based on blockchain mechanisms (BCMs) playing a role in protecting numerous IoT-oriented applications by becoming part of a security mosaic. A blockchain is an immutable digital ledger that records each completed transaction or piece of data in sequential order in a distributed ledger that outside parties cannot alter. All of the users in the network then have access to these exchanges. Every node in the system keeps the same ledger as all other nodes in the network; the information is saved and published in a public ledger. A full-fledged blockchain-secured network may not always be practical for all IoT applications. The typical limitations of IoT nodes are critical or institutional applications such as smart grids, ITSs, e-health, insurance, and banking that may require nodes with sufficient capabilities to support the necessary peer-to-peer functionality. Ma et al. [23] presented a blockchain-based

secure sharing scheme using ITS as an example for IoV data. It uses smart contracts to enable features like automated registration, speedy authentication, and a reliable sharing mechanism for IoV data. The private information is protected through homomorphic encryption and zero-knowledge proof processing performed by the smart contract and stored as ciphertext on the distributed ledger. We use a tamper-proof Merkle tree-based block to permanently record all IoV data processing and usage procedures and a PBFT consensus mechanism to guarantee the integrity of the entire network's ledger. The IoV chain method maintains the integrity, accessibility, and tamper resistance of the IoV data under the premise of privacy and security, allowing for the data to be traced if and when required.

Yang et al. [24] addressed the issue of centralized anomaly detection in WSNs, and the authors describe a blockchain-based ensemble anomaly detection (BCEAD) system that stores the model of a common anomaly detection method on the distributed ledger. Once a suitable block structure and consensus method have been developed, the scheme changed iteratively to increase detection and classification accuracy. The detection approach is safe from system-level attacks since the blockchain guarantees a trustworthy network environment. In conclusion, the findings demonstrate that BCEAD is superior to competing schemes in terms of performance, cost, and other parameters. Abnormality detection across all network domains is the responsibility of the sink layer. A decentralized ledger stores the isolation forest detection model (tangle). In this study, we also compare and contrast experimental data to show that BCEAD has better detection performance than previous methods. Sarhan et al. [25] presented a federated learning architecture built on a blockchain-based hierarchy to ensure that collaborative IoT intrusion detection is safe and private. The proposed machine learning-based intrusion detection system employs a federated learning architecture with a hierarchical structure to safeguard the confidentiality of the training and company information. There are several potential advantages to using machine learning (ML) skills in the security against IoT cyberattacks. However, the existing framework proposals do not consider data privacy, safe architectures, or scalable deployments of IoT ecosystems. A trusted distributed ledger will manage all business processes and transactions, and the smart contract will ensure that all obligations are met. Hsiao and Sung [26] proposed a method that employed blockchain technology to improve the safety of wireless sensor networks' data transmissions (WSNs). This research combines distributed ledger technology (blockchain) with data transmission to establish a highly reliable WSN infrastructure. Today's wireless network is founded on IoT design principles and uses a blockchain-based approach to ensure the integrity of all transmitted data. The blockchain-based transaction ledger is adapted in this research strategy to store information gathered by sensors. The suggested system collects and analyses sensor data to improve the dependability of the wireless sensing network architecture. To establish a connection between blocks, every blockchain must undergo cryptographic processing and the decryption of public keys. Even more so, before any data can be transmitted in a newly created blockchain, the prior and subsequent sequences of the link must be confirmed. Abbas et al. [27] presented a lightweight blockchain-based authentication solution to store the credentials of standard sensors. Because IoT nodes have a certain amount of time before they die from battery exhaustion, lightweight authentication is achieved by storing only a small number of credentials in the blockchain. Furthermore, a genetic algorithm-enabled software-defined network controller performs the route calculation and is also utilized for on-demand routing to minimize the nodes' energy usage in an IoT network. In addition, we present a route correctness technique to validate the absence of harmful nodes in the suggested path. Abualsauod [28] proposeda peer-reviewed research on UAV IoT frameworks and to analyse it to find answers to problems with the frameworks' overall security and privacy. An optimal solution is provided in the paper for the many security and reliability issues that arise in UAV-enabled IoT applications by integrating different ways based on blockchain technologies. Multiple metrics, including processing speed, latency, accuracy, and overall system usefulness, are used to evaluate and contrast the acquired results.

3. IoT-Based Network Model

The network model comprises various types of wireless sensor nodes operating under different computational processing and clustered into ten regions. Each region is partitioned into clusters, as shown in Figure 3. The nodes are classified into sink nodes, cluster heads, and sensor nodes based on the computational power and data processioning capabilities. The sensor nodes are assumed to be randomly deployed and are unaware of their location and position. At the same time, the beacon nodes and sink nodes are aware of their locations and positions, and they assist the unknown sensor nodes in locating the sensor nodes and identifying the malicious nodes by computing the distance between each node and its position, with each node having its own distinctive identifier [29]. The network model incorporates challenging design requirements and assumptions for efficient performance. The requirements include the following:

(i) Randomly deployed sensor nodes are assumed to be homogeneous, with mobility changing in the topology framework

(ii) Each device in the Internet of Things has its distinct IP address

(iii) The storage and processing power of the cluster's head nodes and base stations, which can be used to implement a smart contract, are described

(iv) The existence of a continuous malicious node in the network makes the framework overconscious

(v) All sink nodes are trustworthy and generate keys to all the nodes in the network

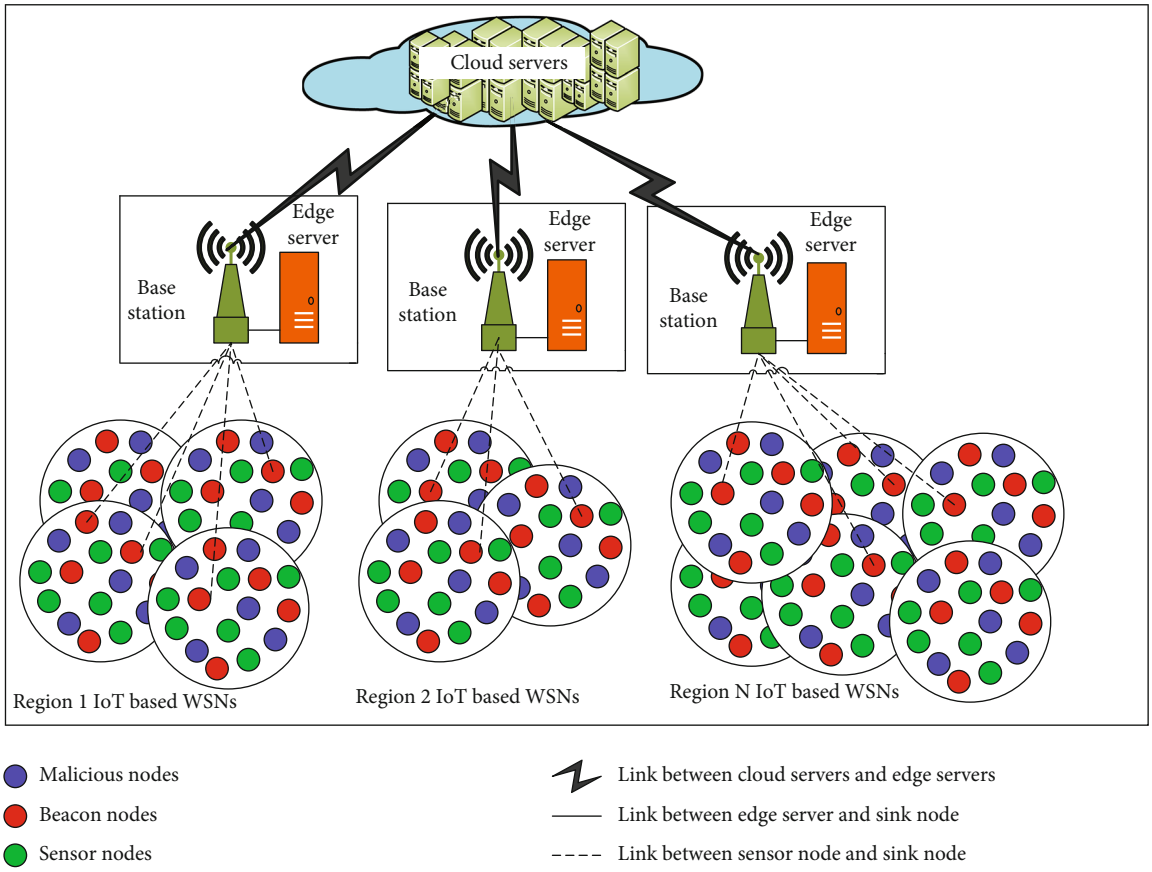


Figure 3: Proposed hierarchical IoT-based wireless sensor network model for secure localization of malicious nodes.

(vi) All sink nodes have high computational and data processing capabilities for data aggregation

(vii) The servers provide reliable and secure storage for the data in the network

The two requirements in IoT-based wireless sensor networks make the sensor nodes broadcast malicious information by gaining control over the other nodes and wrong information about energy and localization that affect the precise localization accuracy. This paper proposed blockchain-based secure localization using a trust evaluation process and cascading encryption for effective network transaction and malicious node detection. The randomly deployed sensor nodes face security threats during the localization process since malicious nodes affect the localization approach's accuracy in IoT-based wireless sensor networks. The blockchain-based technique overcomes this problem through the cascading encryption and effective transaction and trust evaluation process of the beacon nodes. The blockchain receives the trust value list and localizes the malicious nodes using the distributed consensus.

The nodes that send data to the cluster head without knowing their location are unknown and disrupt the normal functioning of the network. To avoid this problem, beacon node having their precise location helps find the accurate location of unknown nodes of their deployment before sending data. The reliable beacon nodes are selected by computing the trust value of beacon nodes without considering the malicious node. The presence of the malicious node is solved by using blockchain-based localization techniques using federated learning without compromising the beacon node and privacy. In this proposed model, each region has its network with multiple clusters for monitoring the environmental conditions. Nodes in the network cooperate to accomplish specified tasks, and the interaction between nodes needs to assure the legitimacy of node identity [30]. One of the crucial ways to safeguard the IoT is through identity authentication. In the network model presented here, two-factor authentication is required to set up encrypted channels between nodes before any communication can occur, or end users can have access to the resources hosted by a node.

4. Proposed System

The proposed system for detecting and localizing malicious nodes, as shown in Figure 2, consists of various phases for identifying and removing attacks in IoT-based wireless sensor networks using hybrid and federated learning-based blockchain technology. The proposed scheme ensures client and service provisioning using hybrid machine federated machine learning models, feature evaluation, and cascading

encryption for effective transaction and localization. The proposed system utilized federated machine learning model for detecting and classifying malicious nodes by training and testing the dataset received from the blockchain trust value lists with suitable data format using preprocessing techniques. In a WSN, the localization process relies on the accuracy of information relayed by beacon nodes; therefore, ensuring their reliability can be difficult [31]. Since IoT-based WSNs' range-free localization method does not rely on any specialized hardware, it is susceptible to mistakes when malicious attacks are present in the network. During the localization procedure, the malicious nodes provide false location data. There is a single point of failure in typical localization strategies for WSNs because they rely on a centralized body. For attack detection and localization, the efficacy of the trust evaluation based on secure blockchain using hybrid federated machine learning, reinforcement learning, and maximum likelihood estimation needs to be put to the test. One application of the blockchain is in the realm of trust administration. Furthermore, just a small set of criteria are employed to determine whether or not to trust a beacon node. For this reason, the trustworthiness of both behaviors and data must be factored into the ultimate trustworthiness assessment. From there, the data is gathered and processed by the blockchain infrastructure that was provided to it by the trusted nodes.

4.1. Sensor Deployment and Routing. The proposed system consists of N number of total sensor nodes deployed with random mobility in two-dimensional environments with B beacon nodes and U unknown nodes. The base stations are located outside the clusters in each region connected to the edge servers. The beacon's network size and communication radius are computed as in the following equations shown below.

$$|N| = |B| + |U|. \tag{1}$$

The transmission range (T_R) of the beacon nodes is computed with the maximum ($T_{\max}$) and minimum ($T_{\min}$) communication ranges as shown below:

$$T_R = (T_{\max} - 1) + \text{random}(0, 1) \times [(T_{\min} - 1) - (T_{\max} - 1)] + 1. \tag{2}$$

Randomly deployed wireless sensor networks face security threats by computing the location estimation and position of unknown nodes in the network. Detecting malicious sensor nodes provides information for calculating the location and enhancing the localization accuracy in WSNs based on beacon nodes. The beacon node is selected from the sensor nodes using the selection three criteria:

(i) The minimum distance of the node from the base station computed using the distance-vector protocol

(ii) The residual energy of the node for activation

(iii) The strength of the received signal from the sensor node

The number of neighbor nodes is close to it. Using the distance vector method, as indicated in equation (3) below, we are able to calculate the distance, denoted by D, that separates any two sensor nodes.

$$D = \sqrt{(u_i - u_j)^2 + (v_i - v_j)^2}. \tag{3}$$

Any node that has a small distance from the base stations (where u and v are the coordinates for nodes i and j, respectively) is probably the cluster head.

Threshold parameters are determined using the multipath model strategy, which is then used to assess the energy expenditure involved in network model communication and activation. In the steady-state phase, each cluster head (CH) communicates with the other nodes to keep their receivers on and respond to its CH [32]. For a data transmission of k bits across a distance D and a threshold distance D_o, we have (4) as the energy required for transmission E_{TX}:

$$E_{\text{TX}} = \begin{cases} k \times E_e + k \times E_f \times D^2, & \text{if } D \le D_o, \\ k \times E_e + k \times E_m \times D^4, & \text{if } D > D_o. \end{cases} \tag{4}$$

For one-bit data transmission, we get where E_{TX} is the energy being sent, E_f is the energy being received, and E_e is the power being lost somewhere along the line [29]. Signal propagation, filtering, modulation, and channel coding all play a role in the amount of energy lost in the process. With a data length of k, we have the following expression for the minimum acceptable transmission distance, d_o:

$$D_o = \sqrt{\frac{E_f}{E_m}}. \tag{5}$$

Energy used by the receiving node for k-bit messages is calculated as

$$E_{\text{RX}(k)} = k \times E_e. \tag{6}$$

4.2. Selection of Miner Node and Localization Process. Methods for computing behavioural trust, data-based trust, and feedback trust, and as well as calculating the overall trust beacon nodes in WSNs, are used. The most trustworthy beacon nodes are picked based on their trust levels when trust is calculated for each node. For mining and trilateration, these beacon nodes are trusted. Our blockchain network's PoA consensus is based on this group of miners. On the sink and beacon nodes, a private blockchain is being used in this network. On the blockchain, the trustworthiness beacon nodes are permanently recorded. In addition, the network's nodes encrypt the trade data and store it on the blockchain. The miner node is the anchor node having its own location with the most significant trusted values for verifying communications and putting the blocks for the next transactions. Figure 1 depicts the architecture of the proposed network model containing block. After this, the translation process begins. Trilateration is used to determine the precise

location of each unknown node. Here, unknown nodes determine their approximate location by calculating the distance between themselves and the three anchor nodes with the highest trust ratings and then utilizing that information to solve for their coordinates using the following equation:

$$D_{\text{tri}} = \begin{cases} \sqrt{(u_a - u_i)^2 + (v_a - v_i)^2} \\ \sqrt{(u_a - u_j)^2 + (v_a - v_j)^2}, \\ \sqrt{(u_a - u_k)^2 + (v_a - v_k)^2} \end{cases} \tag{7}$$

where D_{tri} is the trilateration process for finding the distance of any node a, and (u_a, v_a), (u_i, v_i), (u_j, v_j), and (u_k, v_k) are the positions of the ordinary sensor nodes with respect to i, j, and k beacon nodes.

Finding the nodes' locations and strengths of connections, as well as evaluating their positions, is tasks for which specific algorithms are required. The system is broken down into two types of categories, range-based and range-free localization methods [29]. The second option is more practical financially, but it needs specialized hardware. Accurate positioning and positioning of wireless sensor nodes are evaluated using the received signal strength indicator (RSSI) and the distance vector hop localization techniques. To determine where sensor nodes and cluster leaders are in relation to beacon (base station) nodes, a distance vector localization process is required [33]. Position and separation between the unknown nodes can be calculated and manipulated with the help of the scheme. Beacon nodes in a WSN can be located using the distance vector hop process. The average hop size is used in the distance vector approach to determine the minimal distance. In [34], this algorithm was discovered for the first time. Here are the steps of the range-free distance vector localization scheme [35]:

4.2.1. Routing Initialization. The beacon node transmits a message to all sensor nodes. As soon as it enters the network, the hop count associated with its position data is set to 0 [35]. A node that gets such a message will determine where the beacon node is located, append its own identifier to the message, and then broadcast it to its neighbours while increasing the hop count [36].

4.2.2. Calculating Distance. With the help of the beacon node, we can determine the average hop size and the distance to the unknown node.

4.2.3. Position Estimation. Geometric calculations like triangulation, the polygon technique, and trilateration are frequently employed as the underlying basis for determining the locations of unknown nodes [29]. There are a number of methods that can be used to calculate the separation of two nodes; they include synchronization, radio signal intensity, and the physical features of the carrying wave [37].

4.3. Registration and Authentication Process. Sensor nodes, aggregation nodes, and base stations are the three main categories of WSNs in the proposed network model [12]. Intelligent communications confirm the aggregation, and data processing node exists by using its MAC address and the base station's authentication procedures to verify its identification as in Figure 4. In order to gain access to the model and the public blockchain that is being utilized, the sensor nodes need to be authenticated and given permission [38]. It is essential that the privacy of the nodes be preserved, and in order to do this, our model made use of a layered security architecture. The IoT-WSN framework that has been presented needs to have the capability of establishing trust between different IoT members in order to identify and localize threats. Node placements in wireless sensor networks are shown in Figure 4(a).

In Figures 4(b) and 4(c), we can see that the cluster head (CHs) gathers a large message size, while the sensor nodes (SNs) spend a disproportionate amount of time doing data execution during deployment, registration, and authentication. The cluster heads that are location and position aware are regarded as beacon nodes. The data forwarding, retrieval, processing, and aggregation to the base station are shown in Figure 4(d).

In WSNs, the aggregated node's data and the public blockchain records of certified nodes make it possible to have faith in authentication techniques. After the registration procedure has been finalized, sensor nodes are given permission to join the blockchain, which helps to protect WSNs from outside threats. After being randomly dispersed around the playing field, the sensor nodes eventually form aggregation nodes. As the aggregation nodes communicate with the sensor nodes, they verify and identify sensor nodes via a private blockchain, and the base station verifies the identity of the aggregate node via a public blockchain. Mutual authentication is used for all of the aggregate nodes' internode communications.

4.4. Benchmark Datasets. The evaluation of the proposed system's ability to detect and classify the attack type using machine learning models is conducted against a benchmark consisting of the CICIDS2017 and UNSW-NB15 sample datasets. The dataset was captured and executed using tools for intrusion detection and network attack scenario purposes with seven categories of attacks, as shown in Figure 5(a), with the frequency distribution of the attack samples. The dataset contains normal and common classes of attacks that materialize real-world data, including network traffic analysis. The dataset is also heterogeneous, having diversified attacks with 80 feature sets generated using CICFlowMeter available online.

The UNSW-NB15 is an advanced benchmark dataset for intrusion detection widely used for recent research and many previous works. The raw data traffic packets were generated using the cyber range laboratory IXIA PerfectStorm tool from the Australia Center for cyber security (ACCS) [39], creating hybrid normal and abnormal network traffic packets. The Tool simulates nine classes of attacks and continuously updates the information security vulnerabilities and exposures of captured packets. The dataset consists of 42 attributes, three categorical features, and 39 numerical attributes. The dataset has ten classes of attacks, and the

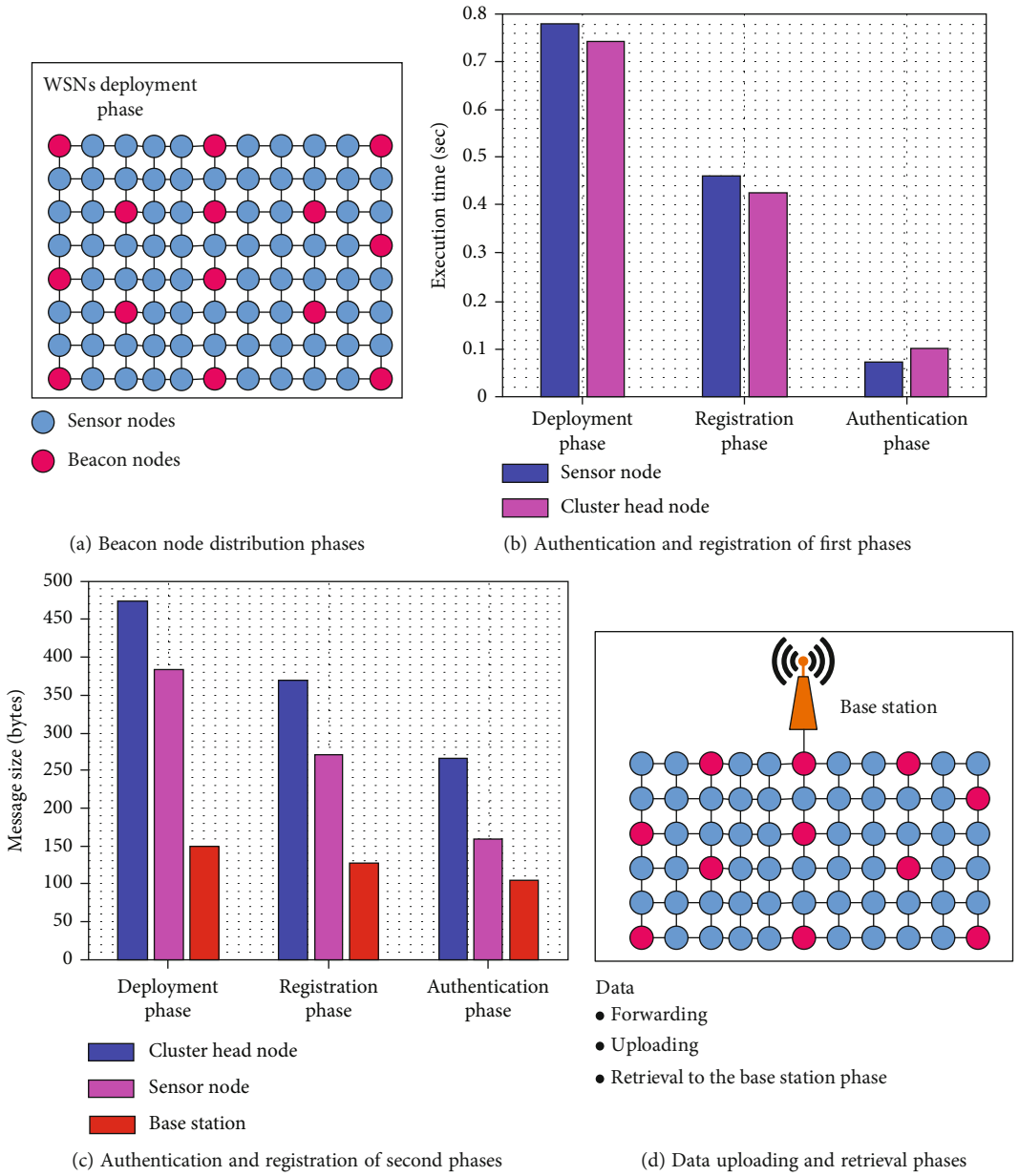
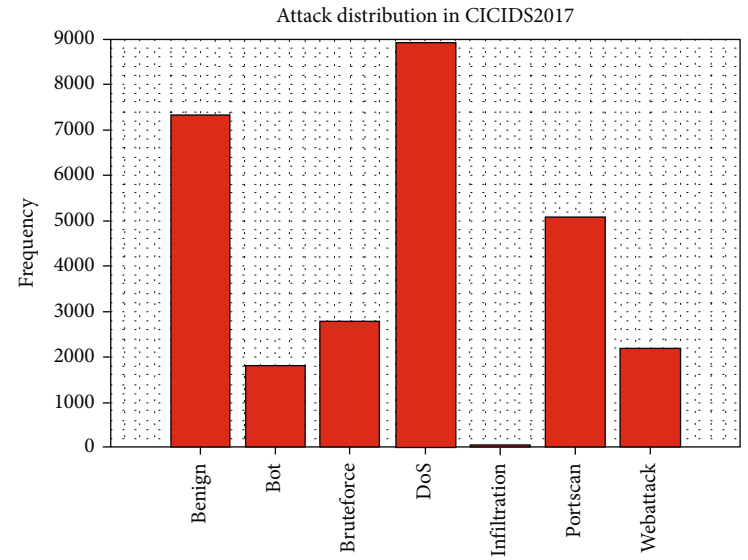


FIGURE 4: Secure data collection and transfer via IoT-WSNs that entail multiple steps, including authentication, registration, and transmission.

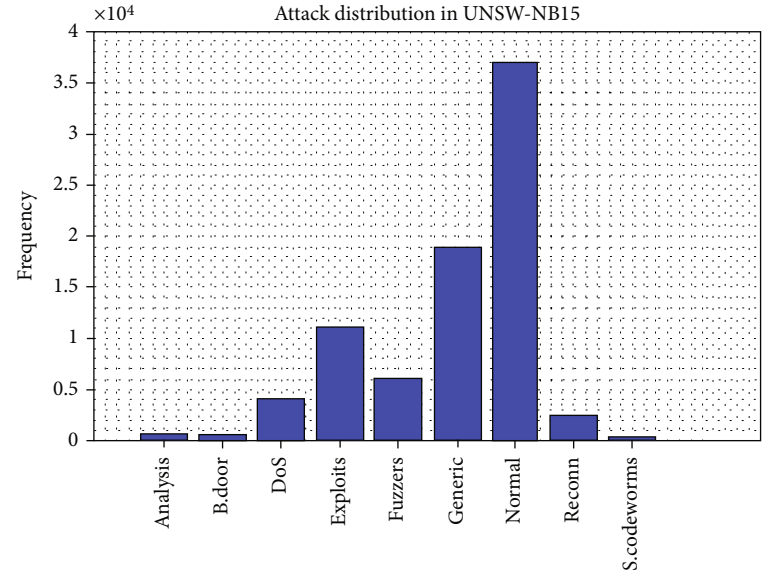
frequency distribution of these attacks is depicted in Figure 5(b). The dataset is divided into 80% training and 20% testing samples for building the predictive models for classification and regression tasks using machine learning models.

4.4.1. Data Preprocessing and Feature Selection. The traffic data can be collected from a local network or the benchmark dataset using the Data collection module [40]. The preprocessing module receives these data and filters them before they are used. These details are also supplied to the cluster and the trust-based safer routing module for more efficient data transmission. The data preprocessing agent makes excellent use of available data preparation methods. Data cleansing, integration, and modification are also undertaken before preprocessing. The data preprocessing step starts with data cleaning and normalization to improve the data quality for training and testing for building the predicting machine learning models. The preprocessing is important for vectorizing, consisting of feature extraction, feature selection, and dimensional reduction [41]. The dataset can be cleaned by removing the duplicated values, replacing the mission data, and removing and fixing unwanted structures from the samples. After cleaning the dataset, it is essential to normalize using the minimum and maximum scaling values as in the following equations:

$$Z_{\text{norm}} = \frac{Z - \min(z)}{\max(z) - \min(z)}, \tag{8}$$



(a) Frequency distribution of attacks in CICIDS2017



(b) Frequency distribution of attacks in UNSW_NB15

Figure 5: Attack occurrences in the CICIDS2017 and UNSW_NB15 benchmark datasets were plotted as a frequency distribution.

where min (z) is the minimum value, and max (z) is the maximum value of the attribute Z, respectively. Z_{norm} is a normalized feature value, and Z is an original feature value [42].

K-means cluster sampling is utilized to improve the classification and detection accuracies of the machine learning model by generating a small K-number of clusters of the original dataset to reduce the training complexity [43]. The K-means sampling technique generates highly representative small groups by removing redundant data to increase efficiency, computational power, and resource. The synthetic minority oversampling process (SMOTE) creates high-quality samples to avoid class imbalance. After the data preprocessing technique, a feature engineering technique is applied to produce sensitive, high-quality features, reduce dimensionality, and remove redundant features by computing the correlation features between features.

4.5. Federated Learning and Security. Currently, the federated cybersecurity (FC) model communicates and collaborates at several levels to provide security solutions for IoT applications. However, privacy and security risks are associated with the standard method of transmitting data within the cluster and across different groups. As a result, federated learning (FL) has emerged as a viable option for exchanging data and information in a method that is both secure and private as in Figure 6. To ensure the security of the IoT network, an FC model that works in tandem with FL to share and discuss data at any level is essential. Most FC strategies based on FL as a cyberdefense mechanism have concentrated

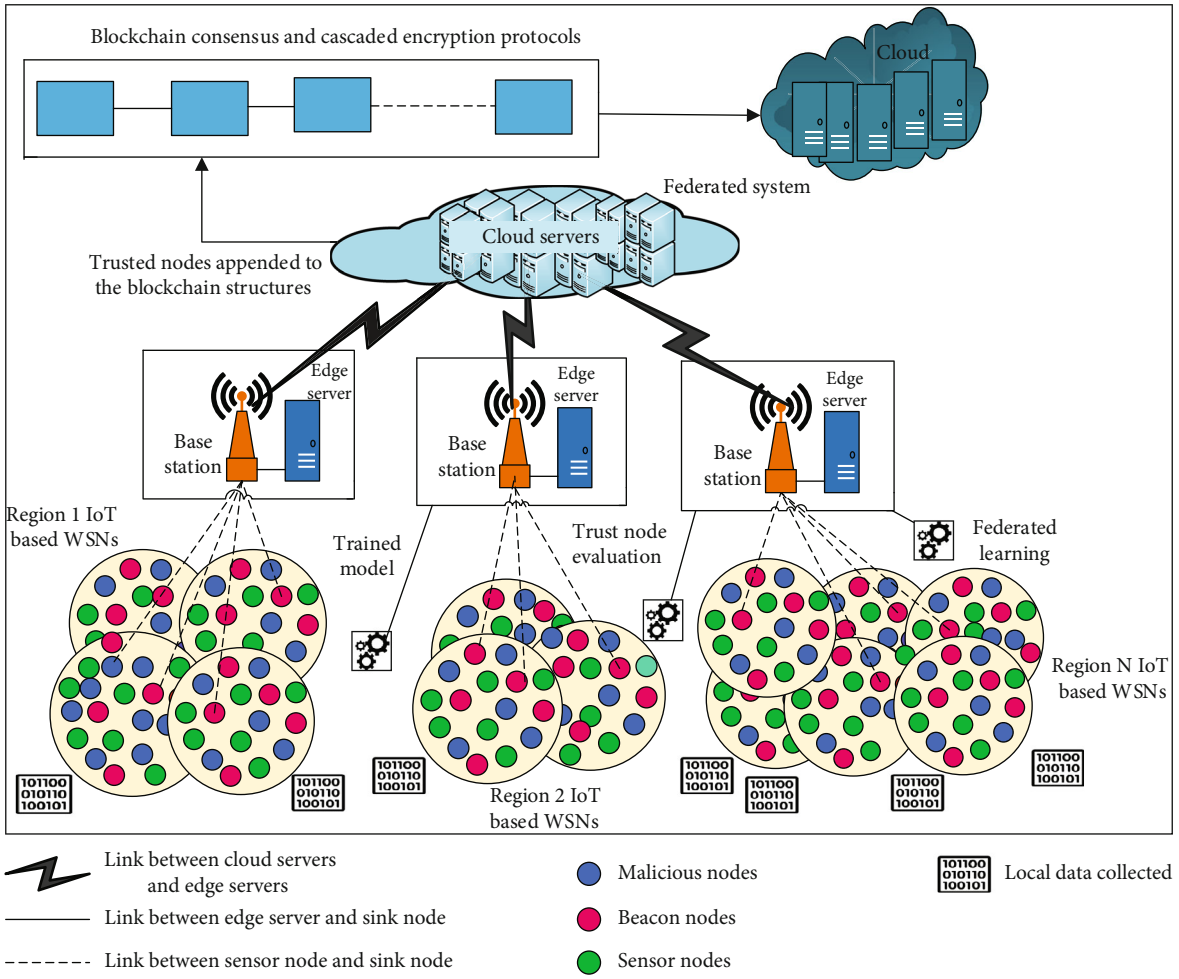


Figure 6: Secure hybrid federated IoT-based WSN model for detection and localization of malicious attacks.

on protecting IoT networks while assuming a unified, worldwide service offering. The method has been developed for a single global model managed by a single service provider; however, it may be readily generalized to a collaborative scenario with several global models managed by numerous service providers. Only a tiny amount of study has developed a federated security model that integrates different international approaches [44]. Machine learning techniques identify resource allocation, security and privacy, communication cost, localization of malicious nodes, and enhancing network lifetime in IoT-based WSNs [45].

Some of the learning techniques utilized in this work include a support vector machine, XGBoost, random forest, and ensemble stacking to improve the performance and evaluate the effectiveness of the proposed system using various evaluation metrics. They are effective and practical techniques for knowledge extraction and finding the relations in wireless sensors that make detecting malicious nodes in the network more accessible. Trusted nodes valuated by the beacon nodes and base station are allowed to enter the block structure as shown in Figure 6 in IoT-based WSNs.

Machine learning models are statistical algorithms with the ability to infer meaningful insights about future data by learning complex patterns in existing data [25]. These ML models are designed using a training procedure in which the learning models glean relevant meanings from the accessible data logs. Training log sets in an IoT ecosystem are produced locally by a wide variety of digital endpoints including smartphones, smart appliances, sensors, and the like. The efficacy of ML-based IDSs is directly impacted by the quality and quantity of data utilized in training and evaluating learning models. The first type, known as localized learning, involves training a model locally using data sets generated by a single endpoint; the second, known as centralized learning, involves training a model centrally using data sets collected from multiple endpoints, and the third, known as federated learning, involves training a model across multiple endpoints using local data sets without exchanging them.

4.5.1. Random Forest. Random forest (RF) is an ensemble learning model that operates by constructing many decision trees for predicting a class [46]. Random forest manages high-dimensional data by judging the importance of the features for solving overfitting and stability problems by reducing the variance. This makes the random forest technique effective for detecting and classifying malicious attacks using

a heterogeneous benchmark dataset in wireless sensor networks. The random forest also handles the missing values and is robust to outliers with less effect for nosy data. The scheme also needs more computational power and more resources due to the construction of many trees. Random forest constructs a forest of several decision trees to predict the model's detection accuracy [47]. It is successful in detecting and classifying attacks using a benchmark dataset.

4.5.2. Gradient Boost. Extreme gradient boosting (XGBoost) is a classification technique for large datasets with a minimum amount of time, making it popular nowadays [48]. The gradient boosting technique uses the extraction of essential features to improve the computational speed and provides a precise output for intrusion detection by reducing memory consumption during the training and testing of the dataset for classification [49]. It is an efficient machine learning technique for optimizing the loss function and computed features, as shown below:

$$\phi(\mathrm{X}) = \sum_{k=1}^{K} f_k(X) \quad f_k \epsilon F, \tag{9}$$

where $\phi(X)$ is the final result of the K sequential classifier and f_k is the decision tree for the K number of iterations in the gradient descent algorithm. The technique also performs parallel computing for getting results in classifying the target results. The XGBoosting improves the gradient descent and regularization strategy for optimizing and managing the process and overfitting factor. The parameters of the classifiers are related as in the following equation shown below:

$$\mathscr{L}(\phi)_{\mathrm{t}} = \sum l(f_{t-1} + f_t) + \Omega(f_t), \tag{10}$$

where $\mathscr{L}(\phi)_t$ is the loss function and $\Omega(f_t)$ is the regularization term to optimize the step size t. The gradient boosting technique uses feature metrics to retrieve the scores according to the features for each attribute.

4.5.3. Ensemble Learning. Ensemble machine learning techniques are classifiers with averaged accuracy to reduce the risk of overfitting and bias from a single classifier [50]. The classification machine learning models are set of tree structures and enhance the overall accuracy. Ensemble techniques are meta-algorithms combining various machine learning techniques into a unified machine learning prediction model for evaluating variation and stacking [51]. The ensemble technique integrates different machine learning results into a single robust model and improves the overall performance. Stacking, bagging, and boosting are the essential ensemble technique concepts. In this scheme, stacking is used for combining and increasing the prediction power of the machine learning models.

4.5.4. Support Vector Machine. The term "support vector machine" (SVM) refers to a family of statistical methods for categorizing network activity under the guidance of an experienced teacher [52]. The fundamental purpose of a support vector machine (SVM) classifier is to build a hyperplane in the feature spaces using a set of vectors called support vectors. Here, we use a dispersed binary classifier for normal and abnormal, which enables the detection of any harmful behavior.

$$w = \sum_{i=1}^{n} a_i y_i x_i \quad \min \left\{ \frac{\|w\|^2}{2} + \mathrm{C} \sum_{i=1}^{n} \varepsilon_i \right\}. \tag{11}$$

$\sum_{i=1}^{n} \varepsilon_i$ is the bounds on the learning vectors, C is the constant that determines the tradeoff between the number of false positives and the margin, and a_i is the Lagrange multiplier. The input and output variables, x and y, are for the demo data set.

Support vector machine (SVM) is a technique for classification, outlier detection, and regression of data samples using hyperplane mapping the data into feature space [47]. It is used for multiclass classification techniques using nonlinear data as a benchmark for evaluation. The SVM technique is used to detect and classify attacks in WSNs to improve the performance and detection accuracy of the system. The SVM has some key features, including more training time, nonlinear data usage, and a higher false alarm rate. It is most beneficial for the classification and prediction of performance evaluation.

4.6. Optimization Techniques. To further enhance the classification of machine learning models for the proposed method on the benchmark dataset, we combine two hyperparameter optimization strategies with Bayesian optimization using a tree based on the Parzen estimation (BO-PTE). Hyperparameters are used by every machine learning method in order to fine-tune the settings and achieve the best possible results. Machine learning performance is enhanced while human labour is reduced thanks to hyperparameter optimization (HPO) [53]. Hyperparameter optimization is also utilized in a black box and global optimization for enhancing functional evaluation. This enables us to describe the black box Bayesian optimization techniques. Bayesian optimization (BO) is a framework for global optimization with expensive black box functions gaining attraction in HPO for deep neural networks. Bayesian optimization is an iterative technique with an acquisition function and probabilistic surrogate model evaluating the decision-making points by applying the Gaussian process. The hyperparameters are handled by tree-based methods, including random forest and tree Parzen estimators (PTE). In this proposed work, Bayesian-based optimization is used with tree Parzen estimators (BO-PTE) for evaluating the best point of evaluation for automatic machine learning.

5. Simulation Results

The validation of the proposed system model is presented using simulation results with different simulation scenarios. The simulation results confirmed that the proposed scheme effectively detects and localizes malicious nodes in IoT-based wireless sensor networks. Our suggested approach employs a

Table 1: Simulation setup for the proposed network model.

Parameter	Values	Parameter	Values
Software	MATLAB	Total sink nodes	10
Number of sensors	1600	Number of clusters	53
Total unknown nodes	1480	Sink position	500, 2000
Protocol type	Clustering and routing	Attacks	Routing
Deployment area	$20000 \times 20000\,m^2$	Mobility	Random
Total beacon nodes	110	Transmission radius	250
Total edge servers	10	Data size	4000 KB

trust evaluation mechanism to pinpoint malicious sensor nodes in the network. In addition, we have included an authentication method to prevent unauthorized access to our network. An energy-efficient and real-time routing system between SNs and BSs is also proposed. Based on authentication, the proposed model is contrasted with the current paradigm. Since authentication's impact is difficult to see in real-time, we measure it in terms of how long a network lasts, how much power it uses, and how fast it can transfer data. In addition, Solidity is employed in the creation of the smart contract. PoW and PoA are used together as part of a consensus process to verify the integrity of the network. The implemented algorithms are compared based on their gas consumption and transaction delay [12].

In our experiments, we used Python 3 and MATLAB as the primary language of code [17]. Popular libraries like NumPy, which facilitates the manipulation of multidimensional arrays and matrices, have been used to implement the proposed strategy. These matrices and arrays are used in the analysis and classification of attacks. Pandas python library provides easy access to advanced data structure modification and analysis tools. Frameworks like TensorFlow and Keras have become increasingly common in deep learning and machine learning. Both supervised and unsupervised ML techniques can be developed with the scikit-learn toolkit. SMOTE was created to oversample people from underrepresented groups systematically. The network planning and simulation of the models were conducted using MATLAB R2021a running on a machine having a Processor Intel(R) Xeon(R) Silver 4214 CPU @ 2.20GHz 2.19 GHz (2 processors), Installed RAM 128 GB (128 GB usable), windows ten 64-bit operating system, and ×64-based processor. Python is also used for data processing and analysis. Table 1 shows the parameters of the simulation setup for network deployment and performs a comprehensive security analysis. Solidity programming language is also employed for creating smart contacts and consensus processes. Both proof-of-work and proof-of-audit are used as network-wide consensus techniques for validation. Measures such as gas consumption, transaction delay, geolocation accuracy, and classification precision are used to evaluate the developed algorithms.

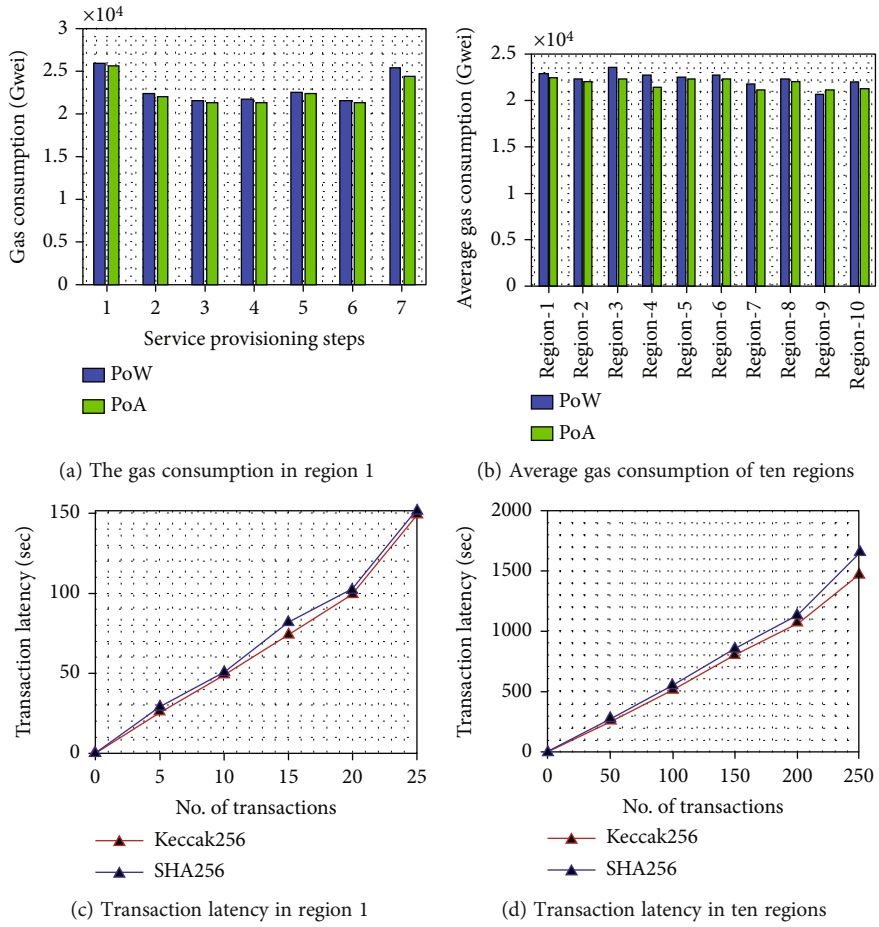
The proposed localization technique uses blockchain for detecting malicious attacks, and the models are deployed into ten independent IoT-based regions for IoT-based WSNs. The PoW and PoA consensus algorithms are used in the region for validating the transactions and adding blocks for detecting malicious nodes and service provisioning. Minor nodes validate the transactions and add blocks for localization of the unknown nodes so that attacks can be removed. This blockchain-based technique enables localizing routing attacks that degrade the network performance and lifetime.

Table 1 also contains the simulation parameters for the models we have proposed. Ten distinct IoT-WSN areas have implemented in this proposed blockchain-based localization for detecting malicious attacks and various simulation parameters for the proposed models. Predesignated nodes are liable for approving transactions and putting blocks onto the blockchain under these models, which use the PoA consensus method Figure 7(a) illustrates how IoT-WSN gas usage varies by power level and area in region 1 IoT-WSNs for service provisioning. For example, Figure 7(b) compares the average gas consumption of the IoT-WSNs in all ten regions to that of PoW and PoA. PoW uses more gas than PoA, as evidenced by these numbers. This is because in proof-of-work (PoW), the miner nodes in charge of validating transactions are chosen through a rigorous mathematical process. On the other hand, in PoA, miners are selected based on their stakes rather than their qualifications. A group of miners is chosen to validate and run blockchain transactions and add new blocks.

5.1. Evaluation Metrics. A trust value is determined for each beacon node to choose the most reliable and secure beacon nodes [4]. According to the trust value calculation, the network has numerous nodes that do not know their specific location. These nodes cannot locate themselves without the help of nearby beacon nodes why they should be the most reliable and trustworthy in a network. The confidence of each anchor node is calculated using the triangulation process and distance vector routing to identify the most reliable beacon nodes. Behavioural, feedback, and trusted data values contribute to the total trust level. Four criteria are used to measure behavioural trust:

(1) Frequency of interaction: anchor nodes' interactions with other anchor nodes are counted as the rate of interactions

(2) Friend nodes and list of neighbors: the ratio of the total amount of one-hope nodes in any beacon node



(a) The gas consumption in region 1

(b) Average gas consumption of ten regions

(c) Transaction latency in region 1

(d) Transaction latency in ten regions

FIGURE 7: The gas consumption and transaction latency of different regions in IoT-based wireless sensor networks.

to the whole number of nodes except for this particular beacon node is an essential statistic for calculating behavioural trust. It is the quickest route from the beacon node to the rest of the network. The number of nodes in the vicinity of anchor node is called its range

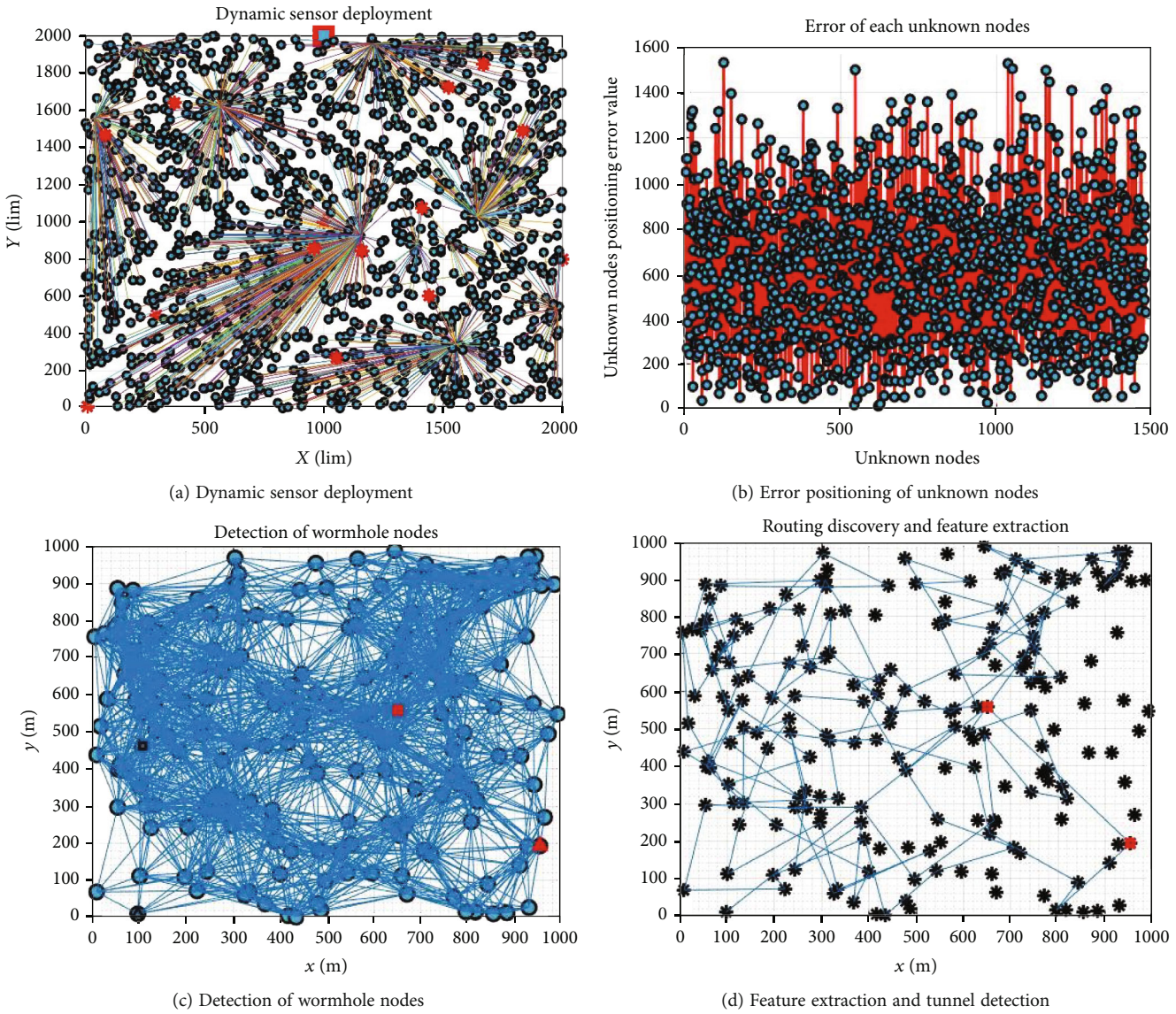
5.1.1. Localization Accuracy. The performance of the proposed system is measured using localization error (LE), average localization error (ALE), localization accuracy of the unknown sensor nodes, and the confusion matrix taking the CICIDS2017 benchmark dataset for classification of attacks. The localization error measures how far away the estimated position is from the true position [54]. To facilitate a standard means of comparison, localization errors are normalized to the radio range of sensor nodes. The average localization accuracy measures how precisely the nodes in the study area are located [55]. The average error localization (ALE) [34] is computed as in equations (12)-(14), respectively. The average detection rate, accuracy, precision, and recall are also used to evaluate the effectiveness the proposed system. In order to calculate the ALE, add up the LE of all the unknown nodes and divide by the total number of unknown nodes [29].The LE represents the discrepancy between the estimated and true locations of any undiscovered nodes.

$$\mathrm{LE} = \sqrt{\left(u_i' - u_i\right)^2 + \left(v_i' - v_i\right)^2},$$

$$\mathrm{ALE} = \sum_{i=1}^{n} \frac{\sqrt{\left(u_i' - u_i\right)^2 + \left(v_i' - v_i\right)^2}}{\mathrm{nR}},$$

$$\mathrm{ALA} = \left(1 - \left(\sum_{i=1}^{n} \frac{\sqrt{\left(u_i' - u_i\right)^2 + \left(v_i' - v_i\right)^2}}{\mathrm{nR}}\right)\right) \times 100\%, \tag{12}$$

where (u'_i, v'_i) and (u_i, v_i) are the real and computed coordinates of the anonymous node I, respectively; n represents unknown nodes, and R represents the communication radius of the network. In Figure 8(b), we can see the deviation of the unknown sensor nodes (b). Using the localization scheme, the positions and deviations of all nodes are calculated. The performance of the proposed scheme is evaluated using the performance metrics including detection rate, false



(a) Dynamic sensor deployment

(b) Error positioning of unknown nodes

(c) Detection of wormhole nodes

(d) Feature extraction and tunnel detection

Figure 8: Dynamic deployment and clustering of sensor nodes for computing unknown node positioning in IoT-based WSNs.

alarm, precision, and recall. Equations (15)-(17) provide a mathematical representation of this:

$$\begin{aligned} \text{Accuarcy} &= \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}, \\ \text{Detection rate} &= \frac{\text{TP}}{\text{TP} + \text{FN}}, \\ \text{F1} - \text{score} &= \frac{2 \times \text{TP}}{2 \times \text{TP} + \text{FP} + \text{FN}}. \end{aligned} \tag{13}$$

Accuracy determines how well the learning model functions are [56]. We put the proposed method to the test by doing experiments and comparing the outcomes to those obtained using an established secure blockchain based on federated hybrid machine learning models. To accomplish this, we must first determine the proportion of attacks that were correctly classified as true positive, trusted nodes that were correctly classified as true negative, false positives that were incorrectly classified as true negative, and false negatives that were incorrectly classified as true positive.

The detection rate is a measure of correctively classified normal traffic and is regarded as a positive value over the total samples in the dataset. The detection rate is the same as the actual positive rate computed in equation (14). The precision is the number of correctly classified attacks over the total number of instances of attacks in the networks.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \tag{14}$$

where true positive (TP) is the number of attacks correctly classified as attacks [57, 58], and false positive (FP) is the number of attacks incorrectly classified in the network [59]. The true negative (TN) is the legitimate nodes organized as

legitimate, and the false negative is the honest nodes incorrectly as malicious nodes in the network traffic.

The detection accuracy is the fraction of trusted sensor nodes that correctly identify malicious nodes relative to the total number of harmful nodes in the network [6]. When compared to the false negative rate (FNR), which is the total number of malicious nodes that are incorrectly classified as legitimate nodes by the suggested model, it is computed by the following equation:

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TP}}. \tag{15}$$

5.1.2. Intimacy. It is one way to gauge the behavioural trusted values of the anchor nodes. It is the time consumed that anchor nodes spend for communicating. It is computed by using the following formula:

$$\mathrm{In} = \frac{t_i}{t_i + t_a}, \tag{16}$$

where t_a is the time consumed for node to communicate with the a anchor node and t_i is the collaboration time of a particular node with beacon i.

5.1.3. Honesty. Another metric that is used to calculate behavioural trust is honesty. The equation used to calculate it is presented below.

$$h_{\mathrm{o}} = \frac{P_s}{P_n}. \tag{17}$$

There are P_n interactions between source and destination nodes and P_s interactions between source and destination nodes that result in successful outcomes. Truthfulness tells the overall amount of interactions between nodes, both successful and unsuccessful. The interactions take into account end-to-end delay for classifying interactions among nodes. The amount of time it takes, on average, for data packets to be transported from source nodes to sinks, including both valid and faulty data packets, is referred to as end-to-end latency [60]. It is the amount of time required for a data packet to travel from its point of origin to the location where it will be stored permanently.

When malicious nodes are inside the radius of any anchor node, the behavioural trust in those beacons is compromised. Beacon nodes' overall trust is impacted, resulting in an incorrect selection of anchor node and cluster head nodes for accurate localization malicious nodes in WSNs. The number of neighbour nodes, distance error, security, mobility, and localization techniques all plays a role in determining where rogue nodes can be found in WSNs [61].

After calculating behavioural trust, each beacon node's feedback trust is determined. A beacon or an unknown node must supply the other with its coordinates to figure it out. After verifying that the sender beacon node gave it the correct coordinates, this node provides feedback on the sender beacon node. Last, each beacon node's data-based trust is calculated by comparing the actual distance of the beacons to their anticipated distance. Equation (18) gives the Euclidean theorem to calculate the exact distance for estimating distance.

$$D_{\mathrm{ac}} = \sqrt{\left(u_i - u_j\right)^2 + \left(v_i - v_j\right)^2}, \tag{18}$$

where D_{ac} is the actual distance, u_i and v_i denote the positions of the sender anchor node, and u_j and v_j are the positions of the destination anchor node.

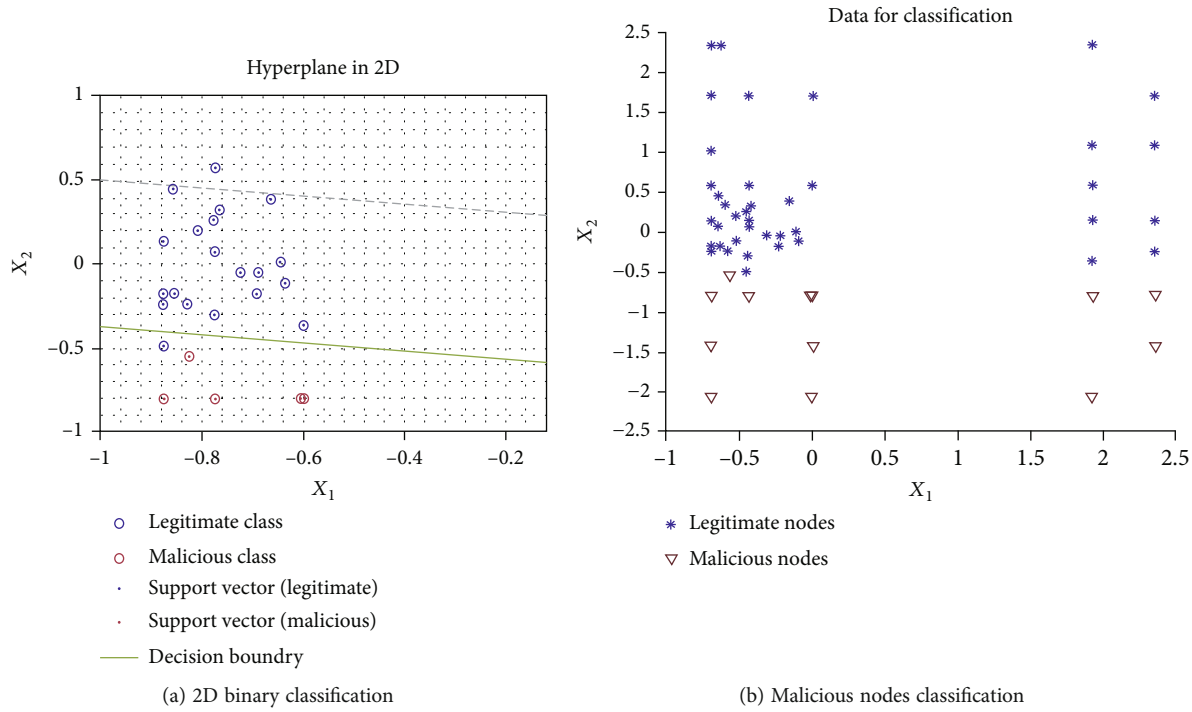
The novelty of the proposed methodology is scalability and chain of trust evaluation using intelligent communication of the wireless sensor nodes within a given region. The security performance of the system is independent for each area; hence, the DoS attacks cannot manipulate and access multiple religions simultaneously.

6. Performance Evaluation and Validation

The evaluation and validation of the proposed system are computed through simulating and classification of hybrid and federated machine learning models. Our simulation results demonstrate the efficacy of the proposed system's federated-based machine learning algorithms for identifying, localizing, and classifying malicious nodes in the simulated network. The proposed model has been simulated to determine its gas consumption, delay, time response, data aggregation, remaining network energy, and dropped packet count.

The practical steps of our model are deployment, as shown in Figure 8(a) and computing in Figure 8(b), for localization error of unknown nodes, registration, authentication, routing calculation, and malicious node detection and classification using hybrid federated machine learning models. The wormhole attacks were detected by computing the distances and position of the sensor nodes marked with red colors as in Figure 8(c). Wormhole tunnels were created and detected using routing discovery and feature extraction between two malicious nodes as depicted in Figure 8(d).The simulation result shows that the proposed system achieved the localization accuracy of the routing attacks is 99.14% by training the extracted features as shown in Figure 8(d). This shows that the localization accuracy of the wormhole attack is effective compare to Kim et al. [1] with localization accuracy of 82.17%.

As a result of this research, the network's malicious nodes have been located and deleted. XGBoost, random forest, extra tree, and ensemble stacking are utilized for evaluating the performance and test the effectiveness of the proposed system utilizing benchmark datasets with various evaluation metrics to classify genuine and malicious nodes. Hyperplanes are used by SVM to classify data points into one of two categories. As a result of this model, a line (hyperplane) is generated that splits the data samples into two distinct categories. A hyperplane is constructed for comparing these data point. The SVM model then determines the class of each data point. SVM's primary goal is to build a decision border that is effective for separating the data samples of each course, as shown in Figure 9(a), for malicious node classification as in Figure 9(b).



(a) 2D binary classification

(b) Malicious nodes classification

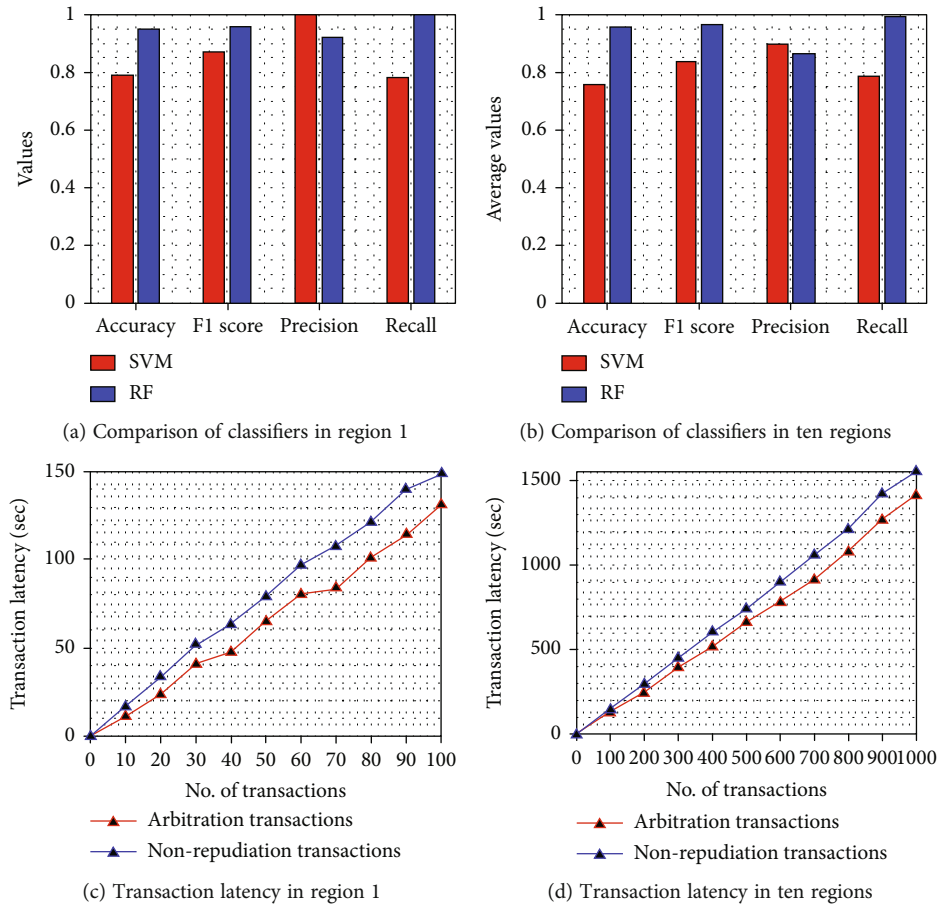
Figure 9: Classification of legitimate nodes from malicious nodes using decision boundary with SVM.

The dataset is imported and labelled when the honesty and end-to-end delay calculations are completed. After that, it is separated into datasets for training and testing. Following the division of the dataset, the model is trained to predict the node categorization based on its predictions. The benchmark dataset demonstrates the SVM model's extensive methodology for detecting malicious nodes.

The results also show that the proposed approach is efficient for malicious node detection using the blockchain technique for ten independent and nonrepudiation regions in IoT-based wireless sensor networks. Preselected network nodes, as depicted in Figure 7(a) and Figure 7(b), in the next generation's IoT-based wireless sensor networks will use the proof-of-authority (PoA) consensus process to validate transactions and add blocks to the block. The majority of consortium blockchains use the PoA consensus technique. To add new blocks to the blockchain, PoA chooses a set of validators. Validators are chosen according to their standing in the system. Since validators can be preselected using PoA, it uses far fewer computing resources than PoW. Contrary to PoW, the PoA consensus technique does not include any form of mining. Proof-of-work (PoW) is a consensus technique utilized by public blockchains like Bitcoin and Ethereum. A cryptographic problem is broadcast over the network to determine a miner in proof-of-work (PoW). The node chosen will be the one that figures out the solution to the challenge quickly and accurately. The chosen miner verifies the transactions and creates the block hash. The hash is then sent across the network to establish an agreement. Figure 7(a) compares the gas consumption in the secure service provisioning method between PoW and PoA in region 1 of an IoT-based wireless sensor network. The gas consumption is a small amount of cryptocurrency, as shown in Figure 7(a). The amount is deducted from the user's account performing the transaction on the Ethereum blockchain [62]. The cryptocurrency is removed from the user account. Figure 7(a) shows the gas consumption of events of the secure service provisioning process in gas units.

Similarly, Figure 7(b) compares the average gas consumption of IoT-based wireless sensor networks between PoW and PoA in all ten regions. PoW uses more gas than PoA, as evidenced by these numbers. This is because in proof-of-work (PoW), the miner nodes in charge of validating transactions are chosen through a rigorous mathematical process. On the other hand, in PoA, miners are selected based on their stakes rather than their qualifications. A group of miners is chosen to validate transactions and add new blocks to keep the blockchain running. Since all transactions depend on a limited number of miners, the PoA process weakens distributed nature of the blockchain. This is partly because PoA makes blockchain networks more centralized. The transaction delay of Keccak-256 and SHA-256 hashing algorithms in region 1 IoT-based wireless sensor networks and across all ten IoT sensor networks is shown in Figures 7(c) and 7(d). The secure hashing method has been expanded, and the Keccak256 hashing algorithm is the result (SHA3). There is a built-in implementation of the Keccak256 algorithm in the Solidity programming language. Keccak256 may hash any data into a hexadecimal value of a predetermined size.

Because the hashing process is irreversible, this hash cannot be used to retrieve the original data. When compared to other hashing algorithms like SHA256 and RIPEMD160, Keccak256 offers a lower cost profile. Hence, we choose to



(a) Comparison of classifiers in region 1

(b) Comparison of classifiers in ten regions

(c) Transaction latency in region 1

(d) Transaction latency in ten regions

Figure 10: Performance compression of classifiers and transaction latency using blockchain technique for detecting and localizing malicious nodes in IoT-based WSNs.

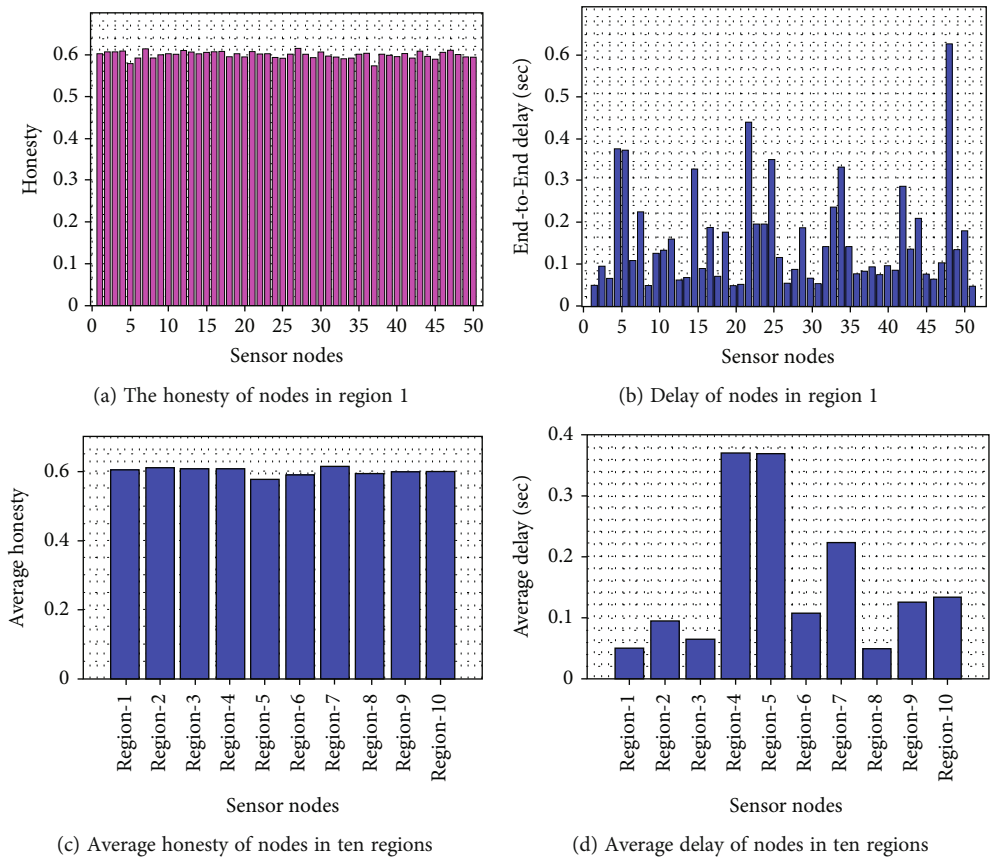
employ it. Network sensors in region 1 of Figure 7 perform 25 transactions per second, while all Figure 7 sensors perform 250 transactions per second (d).

Figures 7(c) and 7(d) depict a network with one and ten areas of IoT sensors, respectively. SHA-256 and Keccak-256 hashing methods behave identically in both figures. It can be deduced from the data that SHA-256 takes almost twice as long as Keccak-256 to execute. SHA-256 lacks an infinite input space, which makes it easier for Keccak-256 to do hashing. A nonrepudiation model based on a support vector machine, XGBoost, random forest, and ensemble stacking classifiers is effectively used for scalable and large networks. The model also provides effective actions for detecting and localizing malicious nodes in the network model using federated machine learning techniques. Linear separability in the SVM hyperplane allows for categorizing data points into two distinct categories.

As a genuine class, the one with the highest honesty value and the least delay from beginning to end is considered the best candidate. However, malicious nodes have a high end-to-end delay and a poor integrity rating. The recall, precision, accuracy, and F1 score of RF and SVM in IoT-based wireless sensor networks are shown in Figures 10(a) and 10(b). IoT wireless sensor networks with rogue nodes can be detected more effectively by using radio frequency identification (RFID) technology. Figure 10(a) shows that SVM has an accuracy of 89%, but RF has an accuracy of 99%.

It shows that support vector machine (SVM) has an average accuracy of 86%, and RF has an average accuracy of 99.3% in all ten regions of interest. According to the findings, RF outperforms SVM in detecting malicious nodes across several regions' networks based on honesty and end-to-end latency. Ensemble learning multiple decision trees are another explanation for RF's better accuracy. Many trees are produced for training and testing to solve the same problem of identifying malicious nodes. Figure 10(a) shows that the F1 score of SVM in a single region is 87.95%, while RF has a 96% F1 score. As depicted in Figure 10(b), SVM and RF have an average F1 score of 84% and 97% in all ten regions of IoT based WSNs, respectively. Because of this, hostile nodes in sensor networks, whether in a single part or over numerous areas, are less likely to be mistaken for legitimate nodes via RF.

In addition, as shown in Figures 10(a) and 10(b), SVM's recall score is lower than RF's because RF is better at predicting harmful nodes. In addition, these results show that SVM's precision is superior to RF's. As a result, SVM can correctly identify the positive observations thanks to its support vector. Our suggested nonrepudiation model was shown to be effective in all ten clusters of the regions of



(a) The honesty of nodes in region 1

(b) Delay of nodes in region 1

(c) Average honesty of nodes in ten regions

(d) Average delay of nodes in ten regions

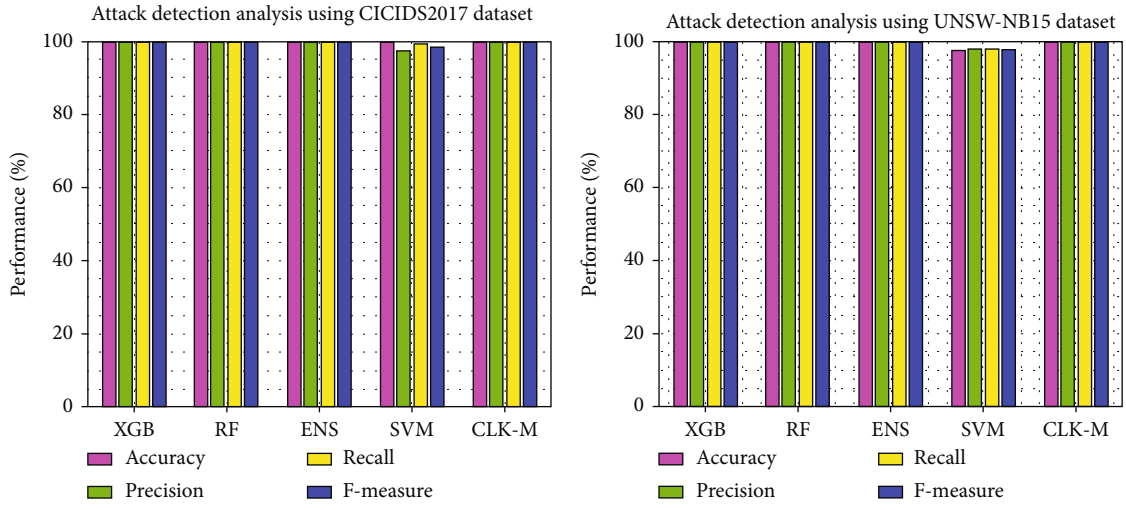
Figure 11: Honesty of wireless sensor nodes and end-to-end delay of nodes in IoT-WSNs.

IoT-WSNs, as shown in Figures 10(c) and 10(d). A varied number of disagreements are reflected in the numbers. Transaction latency is the time it takes a network to process a transaction. Client and service provider latency for arbitration transactions is also depicted. Both the service provider and the customer are found to be vicious in these transactions. According to the diagrams in Figure 10, our suggested system can process a high number of transactions in a short period. As a result, no data is exchanged between the features indicated and the service supplied during these transactions, allowing for a fair comparison. It demonstrates that the arbitration transactions use the bare minimum of network resources including throughput and bandwidth. In addition, the results reveal that the nonrepudiated transactions have relatively low latency. This proves that our suggested nonrepudiation strategy is effective to protect a large number of users over a wide area of IoT-WSNs while being efficient in terms of quality of services and security.

Nodes from region 1 IoT-WSNs are shown to be honest in Figure 11(a). From the region 1 IoT-WSNs, a random sample of fifty nodes is chosen randomly. Shown in the graph are various levels of trustworthiness for each node. For this reason, each node has a varied number of successful interactions. All ten areas' IoT-WSNs' honesty is calculated in the same method, as illustrated in Figure 11(c). Nodes with a high honesty rating are more likely to be legitimate.

This indicates that the node has many interactions and connections with other sensor nodes in WSNs. Honesty is a critical criterion for determining the authenticity of nodes in our networks. Nodes' validity can also be verified by looking at the end-to-end delay, transmission delay, propagation delay, processing delay, and queuing delay and can all be calculated. The malicious nodes are those that have end-to-end delays that are higher than the predefined threshold value. Nodes are not responding quickly enough when other nodes send them messages. Furthermore, their limited processing skills cannot process the data packet, resulting in service denial.

There is a high end-to-end delay with this type of node that broadcasts this information (latency). Figure 11 shows the end-to-end latency of region 1 IoT-WSNs and the average end-to-end delay of all ten regions' IoT-WSNs (Figures 11(b) and 11(d)). Figure 11 depicts the random selection of fifty ordinary nodes from each location. Figure 11(b) shows that the end-to-end delay for each node varies. This is because each node responds to requests in a different period. The malicious nodes in the network are those that have a higher end-to-end delay than a predetermined threshold. Another interesting finding from Figure 11 is that different IoT-WSN region networks have varied range of honesty and end-to-end delay average values, demonstrating the performance of different IoT-WSN region networks in providing secure services.



(a) Hybrid machine learning models using CICIDS2017

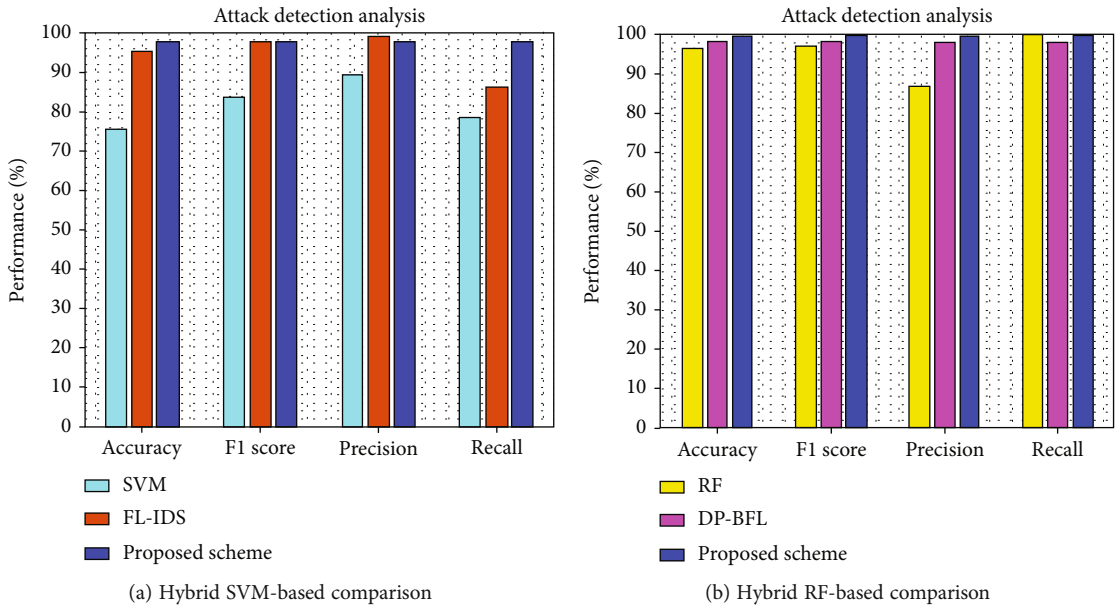
(b) Hybrid machine learning models using UNSW_NB15

Figure 12: The utilization of CICIDS2017 and UNSW_NB15 benchmark datasets for comparison performance of several machine learning models is conducted based on a variety of performance measures.

6.1. Attack Detection Analysis. The performance of the proposed system is evaluated using machine learning models using a benchmark dataset containing a class of attacks in WSNs. The hybrid optimized machine learning also utilizes the same benchmark dataset to evaluate the proposed routing attack localization and detection effectiveness in wireless sensor networks. Figure 12(a) shows the comparative performance of the various machine learning schemes. The performance of the proposed system is further improved with the application of cluster labeling (CL) K-means binary classification techniques.

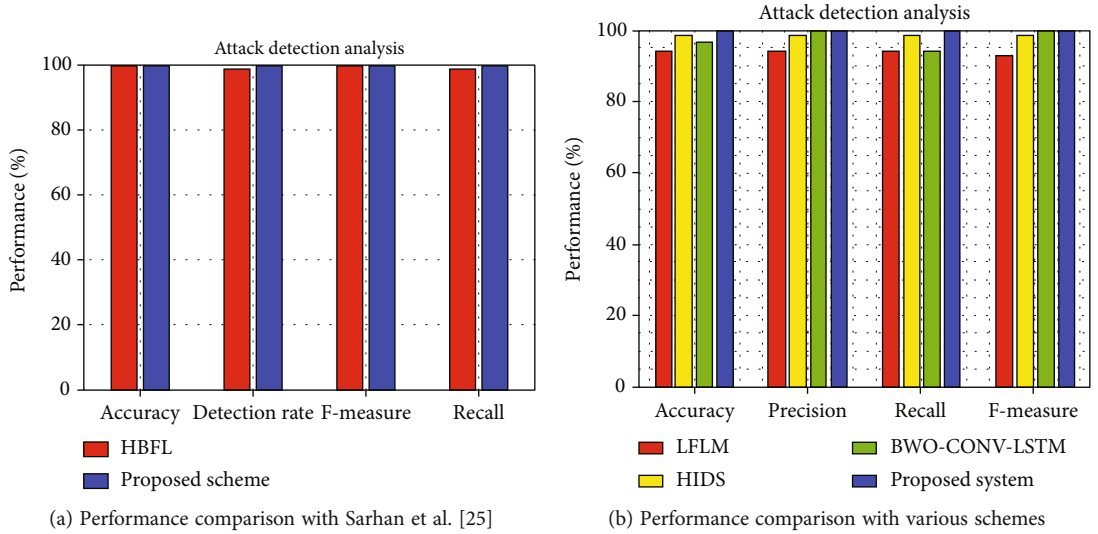
The performance of the proposed scheme is also evaluated using a UNSW_NB15 benchmark dataset with the application of various machine learning models, as shown in Figure 12(b). The binary classification technique using hybrid cluster labeling K-means achieves better classification accuracy of 100% using the benchmark dataset. As shown in Figure 12, the proposed system's performance is adequate for detection and localization attacks in IoT-based wireless sensor networks using benchmark datasets. This can be validated and confirmed by comparing the simulation and experimental results with other research works. Abubaker et al. [4] proposed blockchain-based malicious node detection and localization using federated machine learning using SVM and RF in IoT-based WSNs, as depicted in Figures 13(a) and 13(b). Figure 11 shows that the proposed approach effectively detects and localizes malicious nodes in IoT-WSNs using a hybrid federated machine learning approach. Using the dynamic power of SM 3.0 networks and MNSIT datasets as a benchmark evaluation method, Salim et al. [63] present a differentially privacy blockchain-based explainable FL (DP-BFL) architecture as shown in Figure 13(b). Any Internet-connected device can now contribute data to a globally secure model thanks to this platform. Rehman et al. [64] explored the interplay between blockchain technology and federated learning in healthcare and provides a thorough analysis of the results 5.0. The goal of this research is to build a safe healthcare monitoring system 5.0 by using a blockchain-enabled, federated-learning-based intrusion detection system (FL-IDS) to detect any malicious activity within a healthcare network and allowing doctors to keep tabs on patients via sensors and take preventative measures on a regular basis by foreseeing diseases, as shown in Figure 13(a). The results of the suggested system show that the method is well suited to healthcare monitoring.

The results show that the proposed scheme is better compared to Awan et al. [12] which presented a trust evaluation process based on blockchain for storing the identities of the sensor nodes (SN) and aggregator nodes (AN). The scheme utilized the private and public blockchains for detecting malicious nodes with the detection accuracy of 75% taking malicious nodes 20-80, whereas the proposed technique achieves a detection accuracy of 95%, bringing the number of malicious nodes to 5-30. Otoum et al. [14] proposed a framework using blockchain and federated learning for trust evaluation and security and achieved average detection rate accuracy of 96% and 93%, respectively. Kim et al. [1] achieved average localization detection accuracy and average localization error of 96.5% and 6.97 using secure blockchain based on trust management and evaluation, respectively. Friha et al. [17] designed DNN, CNN, and RNN learning techniques and achieved average detection accuracy of 98.63%, 99.71%, and 99.05% for FELIDS using a benchmark dataset for measuring the detection performance of the system. Kim et al. [41] presented collaborative security system-based federated learning for the internet of things. They achieved a training accuracy of 98.47% using the NSL-KDD benchmark dataset with various classes of attacks for training and testing. This suggests that the proposed scheme is enhanced for detecting and localizing attacks in IoT-based WSNs. The proposed blockchain-based technique for attack detection and localization enhances security. It reduces energy consumption and



(a) Hybrid SVM-based comparison (b) Hybrid RF-based comparison

Figure 13: Performance comparison of the proposed scheme with various evaluation metrics for identification of malicious nodes in IoT-WSNs using benchmark dataset.



(a) Performance comparison with Sarhan et al. [25] (b) Performance comparison with various schemes

Figure 14: Performance comparison of the proposed scheme using various evaluation metrics and benchmark dataset with previous works.

effective data aggregation using the trust values of the beacon nodes for improved network lifetime compared to Ahmed et al. [45]. Mahmood and Jusas [65] proposed blockchain-enabled federated learning for data security and privacy in IoT-WSNs and decentralized nodes and sent global data sharing and achieved average detection accuracy of 95%. The scheme also aggregates the data from the local model to the global model for secure transactions. This shows that the proposed method achieves better classification accuracy. Sarhan et al. [25] proposed a hierarchical blockchain-based federated learning (HBFL) for a secure collaborated intrusion detection system in IoT-based wireless sensor networks as shown in Figure 14(a). The scheme achieves an average detection accuracy of 99.71% using a benchmark dataset UNSW-NB15 containing various classes of attacks. Hassan et al. [66] proposed self-learning and the adaptive protocol to transmit multiuser data automatically by efficiently using channel spectral features and achieved average attack classification accuracy of 98.98 using a nonlinear SVM classification model for IoT-based WSNs. Nasser et al. [67] presented a lightweight federated learning model (LFLM) to learn medical symptoms with high accuracy from data collected by individuals utilizing ambient IoT based-sensors and wearable devices for the COVID-19 response in a collaborative yet private manner with evaluation metrics a shown in Figure 14(b). Roy et al. [68] present a two-layer hierarchical intrusion detection system (HIDS) based on machine learning to successfully detect intrusions

in IoT networks while meeting the IoT resource restrictions. Kanna and Santhi [69] proposed a MapReduce-based black widow optimized convolutional-long short-term memory (BWO-CONV-LSTM) networks for building a hybrid IDS model that efficiently addresses these problems in IoT-based WSNs.

Kumar et al. [56] proposed a federated machine learning-based intrusion detection system for detecting and localizing malicious nodes. They achieved an average detection accuracy of 92.7% using KDD-99 in IoT-based WSNs. The proposed approach is further compared with Mohar et al. [70], and Kumar et al. [71] performed an average localization error of 0.43 with four beacon nodes using a hybrid scalable, secure collaborative localization technique for WSNs. Sajid et al. [72] presented models based on genetic algorithms are presented for identifying malicious nodes, specifically the GA-SVM and GA-DT. After a rogue node has been identified, the Dijkstra algorithm is used to determine the most efficient route through the network. Both GA-DT and GA-SVM are highly accurate, with a 96% and 98% success rate, respectively. The GA-DT and GA-SVM each score 94% and 96%, respectively, when it comes to their accuracy. Nagalakshmi et al. [73] designed and presented detection and localization of black hole attacks based on machine learning models using 114 samples and achieved localization accuracy of 98.01% for WSNs. This demonstrates that the suggested approach performance is more sufficient for identifying and categorising attacks in IoT-based WSNs.

7. Conclusion

The proposed solution utilizes a blockchain-based security technique to detect and localize malicious nodes in hierarchically distributed IoT-WSNs. Using XGBoost and CLK-means machine learning federated classifiers for multiclass and binary classification approaches, the blockchain technique successfully identifies and pinpoints rogue nodes in IoT-based wireless sensor networks. Service delivery without the risk of attack and improved network speed was other goals of this technique, which also made use of feature evaluation and cascading encryption techniques. Results from simulation and classification demonstrate that the proposed system is sufficient for malicious node detection and localization, with average detection accuracies of 99.95% and 100% for XGBoost and CLK-means, respectively, based on the multiclass and binary classification approach with the CICIDS2017 benchmark dataset. Detecting and localizing attacks in IoT-WSNs with the use of a hybrid federated machine learning approach are a novel approach. The outcomes demonstrate that random forest is superior to other methods for classifying diverse network traffic data and detecting malicious nodes. Node honesty, end-to-end delay, and transaction latency are also measured to gauge the effectiveness of the proposed paradigm in delivering services safely and promptly. Since sensor nodes are typically placed in unattended environments where they are susceptible to various routing attacks, more research into how to identify the location of malicious nodes is warranted.

In the future, we want to investigate and develop cutting-edge blockchain-based secure IoT-WSNs with hybrid federated and hybrid machine learning methodologies for massive, safe, and intelligent IoT-WSN deployments in the near future. To locate and identify malicious nodes in IoT-WSNs, we will investigate blockchain-based sophisticated hybrid access control mechanisms. In addition, we will implement cutting-edge multiclass and binary classification evaluation metrics utilizing a wide range of benchmark datasets and hybrid routing protocols.

Data Availability

Data used in this article are available from the corresponding author upon request.

Conflicts of Interest

Authors confirm that they have no financial or personal ties to any parties that might influence the results of this study.

Authors' Contributions

Compiling, writing, and conceptualizing are done by Gebrekiros. Prof. J. Panda, and Prof. S. Indu did the discussion, validation, and evaluation.

References

[1] T. H. Kim, R. Goyat, M. K. Rai et al., "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184133–184144, 2019.

[2] A. Sagu, N. S. Gill, and P. Gulia, "Hybrid deep neural network model for detection of security attacks in IoT enabled environment," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, pp. 120–127, 2022.

[3] R. Bharathi, S. Kannadhasan, B. Padminidevi, M. S. Maharajan, R. Nagarajan, and M. M. Tonmoy, "Predictive model techniques with energy efficiency for iot-based data transmission in wireless sensor networks," *Journal of Sensors*, vol. 2022, Article ID 3434646, 18 pages, 2022.

[4] Z. Abubaker, N. Javaid, A. Almogren, M. Akbar, M. Zuair, and J. Ben-Othman, "Blockchained service provisioning and malicious node detection via federated learning in scalable Internet of Sensor Things networks," *Computer Networks*, vol. 204, article 108691, 2022.

[5] C. Ming, C. Xiaoting, D. Wensheng, and G. Jiahui, "A secure blockchain-based group key agreement protocol for IoT," *The Journal of Supercomputing*, vol. 77, no. 8, pp. 9046–9068, 2021.

[6] S. Agrawal, S. Sarkar, O. Aouedi et al., "Federated learning for intrusion detection system: concepts, challenges and future directions," *Computer Communications*, vol. 195, pp. 346–361, 2022.

[7] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain- enabled IoT network," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55–68, 2022.

[8] O. Cheikhrouhou and A. Koubaa, "BlockLoc: secure localization in the Internet of Things using blockchain," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 629–634, Tangier, Morocco, 2019.

[9] S. Algarni, F. Eassa, K. Almarhabi et al., "Blockchain-based secured access control in an IoT system," *Applied Sciences*, vol. 11, no. 4, article 1772, 2021.

[10] M. P. Nath, S. N. Mohanty, and S. B. B. Priyadarshini, "Application of machine learning in wireless sensor network," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 7–12, New Delhi, India, 2021.

[11] R. Goyat, G. Kumar, M. K. Rai, R. Saha, R. Thomas, and T. H. Kim, "Blockchain powered secure range-free localization in wireless sensor networks," *Arabian Journal for Science and Engineering*, vol. 45, no. 8, pp. 6139–6155, 2020.

[12] S. Awan, N. Javaid, S. Ullah, A. U. Khan, A. M. Qamar, and J. G. Choi, "Blockchain based secure routing and trust management in wireless sensor networks," *Sensors*, vol. 22, no. 2, pp. 1–24, 2022.

[13] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for Internet of Things," *Sensors*, vol. 21, no. 3, pp. 1–26, 2021.

[14] S. Otoum, I. A. Ridhawi, and H. Mouftah, "Securing critical IoT infrastructures with blockchain-supported federated learning," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2592–2601, 2022.

[15] W. She, Q. Liu, Z. Tian, J. Sen Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[16] K. Fan, S. Wang, Y. Ren et al., "Blockchain-based secure time protection scheme in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4671–4679, 2019.

[17] 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.

[18] N. Javaid, "A secure and efficient trust model for wireless sensor IoTs using blockchain," *IEEE Access*, vol. 10, pp. 4568–4579, 2022.

[19] D. Wu and N. Ansari, "A trust-evaluation-enhanced blockchain-secured industrial iot system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5510–5517, 2021.

[20] A. U. Khan, M. B. E. Sajid, A. Rauf, M. N. Saqib, F. Zaman, and N. Javaid, "Exploiting blockchain and RMCV-based malicious node detection in ETD-LEACH for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 7281872, 15 pages, 2022.

[21] R. Goyat, G. Kumar, M. Alazab, R. Saha, R. Thomas, and M. K. Rai, "A secure localization scheme based on trust assessment for WSNs using blockchain technology," *Future Generation Computer Systems*, vol. 125, pp. 221–231, 2021.

[22] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1-2, pp. 1–13, 2018.

[23] Z. Ma, L. Wang, and W. Zhao, "Blockchain-driven trusted data sharing with privacy protection in IoT sensor network," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25472–25479, 2021.

[24] X. Yang, Y. Chen, X. Qian, T. Li, and X. Lv, "BCEAD: a blockchain-empowered ensemble anomaly detection for wireless sensor network via isolation forest," *Security and Communication Networks*, vol. 2021, Article ID 9430132, 10 pages, 2021.

[25] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: a hierarchical blockchain-based federated learning framework for a collaborative iot intrusion detection," 2022, https://arxiv.org/abs/2204.04254.

[26] S. J. Hsiao and W. T. Sung, "Employing blockchain technology to strengthen security of wireless sensor networks," *IEEE Access*, vol. 9, pp. 72326–72341, 2021.

[27] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed, and A. Radwan, "Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things," *IEEE Access*, vol. 9, pp. 139739–139754, 2021.

[28] E. H. Abualsauod, "A hybrid blockchain method in Internet of Things for privacy and security in unmanned aerial vehicles network," *Computers and Electrical Engineering*, vol. 99, article 107847, 2022.

[29] G. G. Gebremariam, J. Panda, and S. Indu, "Localization and detection of multiple attacks in wireless sensor networks using artificial neural network," *Wireless Communications and Mobile Computing*, vol. 2023, Article ID 2744706, 29 pages, 2023.

[30] Z. Cui, F. Xue, S. Zhang et al., "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[31] A. U. Khan, N. Javaid, M. A. Khan, and I. Ullah, "A blockchain scheme for authentication, data sharing and nonrepudiation to secure internet of wireless sensor things," *Cluster Computing*, vol. 112, pp. 1–16, 2022.

[32] Z. Ullah, "A survey on hybrid, energy efficient and distributed (HEED) based energy efficient clustering protocols for wireless sensor networks," *Wireless Personal Communications*, vol. 112, no. 4, pp. 2685–2713, 2020.

[33] S. Messous and H. Liouane, "Online sequential DV-hop localization algorithm for wireless sensor networks," *Mobile Information Systems*, vol. 2020, Article ID 8195309, 14 pages, 2020.

[34] S. Dong, X. G. Zhang, and W. G. Zhou, "A security localization algorithm based on DV-hop against Sybil attack in wireless sensor networks," *Journal of Electrical Engineering & Technology*, vol. 15, no. 2, pp. 919–926, 2020.

[35] A. Hadir, K. Zine-Dine, M. Bakhouya, and J. El Kafi, "An improved DV-hop localization algorithm for wireless sensor networks," in *2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, pp. 330–334, Wuhan, China, 2014.

[36] H. Chen, W. Lou, Z. Wang, J. Wu, Z. Wang, and A. Xi, "Securing DV-hop localization against wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, vol. 16, pp. 22–35, 2015.

[37] F. Khelifi, A. Bradai, A. Benslimane, P. Rawat, and M. Atri, "A survey of localization systems in Internet of Things," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 761–785, 2019.

[38] R. Jeet, S. S. Kang, S. S. Hoque, and B. N. Dugbakie, "Secure model for IoT healthcare system under encrypted blockchain framework," *Security and Communication Networks*, vol. 2022, Article ID 3940849, 11 pages, 2022.

[39] S. M. Kasongo, "An advanced intrusion detection system for IIoT based on GA and tree based algorithms," *IEEE Access*, vol. 9, pp. 113199–113212, 2021.

[40] S. Subramani, *Deep learning based IDS for secured routing in wireless sensor networks using fuzzy genetic approach*, Research Square, 2022.

[41] S. Kim, H. Cai, C. Hua, P. Gu, W. Xu, and J. Park, "Collaborative anomaly detection for Internet of Things based on federated learning," in *2020 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 623–628, Chongqing, China, 2020.

[42] Y. Kayode Saheed, A. Idris Abiodun, S. Misra, M. Kristiansen Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting Internet of Things network attacks," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 9395–9409, 2022.

[43] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: a multitiered hybrid intrusion detection system for Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 616–632, 2022.

[44] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8229–8249, 2022.

[45] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, and Z. Mushtaq, "An energy-efficient data aggregation mechanism for IoT secured by blockchain," *IEEE Access*, vol. 10, pp. 11404–11419, 2022.

[46] P. Roy and C. Chowdhury, "A survey of machine learning techniques for indoor localization and navigation systems," *Journal of Intelligent & Robotic Systems*, vol. 101, no. 3, pp. 1–34, 2021.

[47] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges," *Soft Computing*, vol. 25, no. 15, pp. 9731–9763, 2021.

[48] S. Pande, A. Khamparia, and D. Gupta, "Feature selection and comparison of classification algorithms for wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 2021, pp. 1–13, 2021.

[49] D. Upadhyay, J. Manero, M. Zaman, and S. Sampalli, "Gradient boosting feature selection with machine learning classifiers for intrusion detection on power grids," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 1104–1116, 2021.

[50] S. Taleb, A. Al Sallab, H. Hajj, Z. Dawy, R. Khanna, and A. Keshavamurthy, "Deep learning with ensemble classification method for sensor sampling decisions," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 114–119, Paphos, Cyprus, 2016.

[51] M. Sri Vidya and G. R. Sakthidharan, "Accurate anomaly detection using various machine learning methods for IoT devices in indoor environment," in *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 308–316, Palladam, India, 2021.

[52] L. Moulad, H. Belhadaoui, and M. Rifi, "Implementation of a hierarchical hybrid intrusion detection mechanism in wireless sensors network," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 10, pp. 270–278, 2017.

[53] M. Feurer and F. Hutter, *Hyperparameter optimization*, Springer, 2019.

[54] M. Farooq-I-Azam, Q. Ni, and E. A. Ansari, "Intelligent energy efficient localization using variable range beacons in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2206–2216, 2016.

[55] S. Karagol and D. Yildiz, "A novel path planning model based on nested regular hexagons for mobile anchor-assisted localization in wireless sensor networks," *Arabian Journal for Science and Engineering*, vol. 47, no. 8, pp. 9833–9848, 2022.

[56] K. P. S. Kumar, S. A. H. Nair, D. Guha Roy, B. Rajalingam, and R. S. Kumar, "Security and privacy-aware artificial intrusion detection system using federated machine learning," *Computers and Electrical Engineering*, vol. 96, article 107440, 2021.

[57] Z. Tan, A. Jamdagni, P. Nanda, X. He, and R. P. Liu, "Evaluation on multivariate correlation analysis based denial-of-service attack detection system," in *SecurIT '12: Proceedings of the First International Conference on Security of Internet of Things*, pp. 160–164, Kollam India, 2012.

[58] Z. Tan, "Detection of Denial-of-Service Attacks Based on By," pp. 1–14, University of Technology Sydney Australia, 2013.

[59] M. Nivaashini and P. Thangaraj, "Computational intelligence techniques for automatic detection of Wi-Fi attacks in wireless IoT networks," *Wireless Networks*, vol. 27, no. 4, pp. 2761–2784, 2021.

[60] C. Lyu, X. Zhang, Z. Liu, and C. H. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks," *IEEE Access*, vol. 7, pp. 31068–31082, 2019.

[61] B. Kaur and D. Prashar, "Localization in wireless sensor network: techniques, algorithms analysis and challenges," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1–7, Noida, India, 2021.

[62] T. A. Alghamdi, I. Ali, N. Javaid, and M. Shafiq, "Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain," *IEEE Access*, vol. 8, pp. 1048–1061, 2020.

[63] S. Salim, B. Turnbull, and S. Member, "A Blockchain-Enabled Explainable Federated Learning for Securing Internet-of-Things-Based Social Media 3. 0 Networks," *IEEE Transactions on Computational Social Systems*, pp. 1–17, 2021.

[64] A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. Muhammad, and A. Mosavi, "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Computers in Biology and Medicine*, vol. 150, article 106019, 2022.

[65] Z. Mahmood and V. Jusas, "Blockchain-enabled: multi-layered security federated learning platform for preserving data privacy," *Electronics*, vol. 11, no. 10, p. 1624, 2022.

[66] T. Hassan, S. Aslam, and J. W. Jang, "Fully automated multi-resolution channels and multithreaded spectrum allocation protocol for IoT based sensor nets," *IEEE Access*, vol. 6, pp. 22545–22556, 2018.

[67] N. Nasser, Z. M. Fadlullah, M. M. Fouda, A. Ali, and M. Imran, "A lightweight federated learning based privacy preserving B5G pandemic response network using unmanned aerial vehicles: a proof-of-concept," *Computer Networks*, vol. 205, article 108672, 2022.

[68] S. Roy, J. Li, and Y. Bai, "A two-layer fog-cloud intrusion detection model for IoT networks," *Internet of Things*, vol. 19, article 100557, 2022.

[69] P. R. Kanna and P. Santhi, "Hybrid intrusion detection using MapReduce based black widow optimized convolutional long short-term memory neural networks," *Expert Systems with Applications*, vol. 194, article 116545, 2022.

[70] S. S. Mohar, S. Goyal, and R. Kaur, "Localization of sensor nodes in wireless sensor networks using bat optimization algorithm with enhanced exploration and exploitation characteristics," *The Journal of Supercomputing*, vol. 78, no. 9, pp. 11975–12023, 2022.

[71] A. Kumar, "A hybrid fuzzy system based cooperative scalable and secured localization scheme for wireless sensor networks," *International Journal of Wireless & Mobile Networks*, vol. 10, no. 3, pp. 51–68, 2018.

[72] M. B. E. Sajid, S. Ullah, N. Javaid, I. Ullah, A. M. Qamar, and F. Zaman, "Exploiting machine learning to detect malicious nodes in intelligent sensor- based systems using blockchain," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 7386049, 16 pages, 2022.

[73] T. J. Nagalakshmi, A. K. Gnanasekar, G. Ramkumar, and A. Sabarivani, "Machine learning models to detect the black-hole attack in wireless adhoc network," *Materials Today: Proceedings*, vol. 47, pp. 235–239, 2021.