Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.048621

ARTICLE

Correlation Composition Awareness Model with Pair Collaborative Localization for IoT Authentication and Localization

Kranthi Alluri and S. Gopikrishnan*

School of Computer Science and Engineering, VIT-AP University, Amaravathi, Andhra Pradesh, 522241, India

*Corresponding Author: S. Gopikrishnan. Email: gopikrishnan.s@vitap.ac.in

Received: 13 December 2023 Accepted: 29 February 2024 Published: 25 April 2024

ABSTRACT

Secure authentication and accurate localization among Internet of Things (IoT) sensors are pivotal for the functionality and integrity of IoT networks. IoT authentication and localization are intricate and symbiotic, impacting both the security and operational functionality of IoT systems. Hence, accurate localization and lightweight authentication on resource-constrained IoT devices pose several challenges. To overcome these challenges, recent approaches have used encryption techniques with well-known key infrastructures. However, these methods are inefficient due to the increasing number of data breaches in their localization approaches. This proposed research efficiently integrates authentication and localization processes in such a way that they complement each other without compromising on security or accuracy. The proposed framework aims to detect active attacks within IoT networks, precisely localize malicious IoT devices participating in these attacks, and establish dynamic implicit authentication mechanisms. This integrated framework proposes a Correlation Composition Awareness (CCA) model, which explores innovative approaches to device correlations, enhancing the accuracy of attack detection and localization. Additionally, this framework introduces the Pair Collaborative Localization (PCL) technique, facilitating precise identification of the exact locations of malicious IoT devices. To address device authentication, a Behavior and Performance Measurement (BPM) scheme is developed, ensuring that only trusted devices gain access to the network. This work has been evaluated across various environments and compared against existing models. The results prove that the proposed methodology attains 96% attack detection accuracy, 84% localization accuracy, and 98% device authentication accuracy.

KEYWORDS

Sensor localization; IoT authentication; network security; data accuracy; precise location; access control; security framework

1 Introduction

The Internet of Things (IoT) is a network of interconnected electronic and mechanical devices that can communicate autonomously without human intervention. IoT is dependent on connectivity to function, enabling sensors, actuators, and controllers to communicate with one another and the cloud. Connected devices are changing industries, homes, and lives, paving the way for an intelligent, connected future. IoT devices possess diverse internet connections during real-time deployment. The connectivity of IoT devices is impacted by various issues, including security vulnerabilities, reliability concerns, limited scalability, and the need for seamless integration of connectivity technologies to ensure accurate position estimation. Additionally, the deployment of localization devices such as anchors or beacons poses challenges. Sensor localization improves IoT security, dependability, and efficiency. IoT applications can improve authentication, access control, data accuracy, and resource allocation by knowing sensor locations [1]. Sensor localization uses many methods and technologies. The Global Positioning System (GPS) is used to accurately measure latitude, longitude, and altitude. GPS works best outdoors and may struggle indoors or in obstructed areas with weak satellite signals [2].

Network Grouping: IoT authentication groups devices by parameters using network grouping. Effective management and security of large IoT networks require this grouping strategy. Clustering devices help network managers manage authentication, access, and security. IoT devices include sensors, actuators, gateways, and controllers. Authentication and security processes tailored to each device type's demands and vulnerabilities can be applied by administrators. Another major network grouping factor is device proximity [3]. IoT devices are commonly spread between zones. Administrators can implement context-aware access controls and authentication by grouping devices by location.

Sensor Identification: Each IoT sensor has a unique identity, either a globally unique identifier (GUID) [4] or a device-specific key. This digital fingerprint distinguishes the sensor from other network devices. An IoT sensor's unique identifier is registered with the network or a central authentication authority during setup or deployment. Registering the sensor with the network verifies its presence and involvement. **Sensor Authentication:** Sensor authentication usually involves a challenge-response system [5] while connecting to the network or other devices. The sensor must correctly answer a cryptographic inquiry like a nonce or random value using its identification credentials. IoT sensor authentication often uses public key cryptography. A sensor may have a private key that matches the network's public key.

2 Background and Literature Review

The fundamentals of sensor discovery, localization algorithms, and IoT authentication schemes employed in our proposed scheme are covered in this section. To distinguish themselves from other devices, sensor devices should have Media Access Control (MAC) addresses or digital certificates [6]. During authentication, this identification verifies the device. To authenticate the sensor and IoT platform before data sharing, robust authentication protocols [7], such as mutual authentication, should be used. Role-Based Access Control (RBAC) should be used to design and enforce permissions and access restrictions for each sensor device [8] to ensure they only execute authorized actions and access relevant data.

2.1 Localization Techniques

IoT authentication relies on device geolocation [9]. Many IoT devices position themselves using GPS or Wi-Fi triangulation [10]. The IoT platform can use this data to verify the device's location before giving access. Virtual "fences" surround geographic locations in geofencing. IoT devices can perform actions or authentication checks while entering or exiting specific zones. Place Bluetooth beacons in recognized places to transmit signals. IoT devices with Bluetooth can detect beacons for proximity-based authentication. Nearby Wi-Fi SSIDs and access point signal intensity are identified. Radio-Frequency Identification (RFID) and Near Field Communication (NFC) offer proximity-based verification. Nearby readers or devices can read IoT RFID or NFC tags. As a summary, the magnetic calibration technique is employed in [11] to attain energy efficiency. However, the incorporation of cloud computing is necessary in this model. The paper [12] introduces convolutional neural networks, highlighting their offline preprocessing advantage. However, it necessitates the exploration of optimising algorithms. The concept of dead reckoning is introduced in [13], highlighting the advantage of magnetic calibration. However, there is still a need to improve its performance in localization. The Time Difference of Arrival (TDOA) technique, as described in [14], is utilised to attain a high level of precision. However, it is necessary to further investigate and employ advanced positioning techniques. The Rivest-Shamir-Adleman cryptosystem technique, proposed in [15], aims to leverage blockchain technology for trust management. However, optimisation is necessary in order to decrease the computational cost.

2.2 Authentication Schemes

Device authentication and secure communication in IoT environments depend on authentication schemes [16]. Based on IoT deployment requirements and constraints, many approaches and schemes can be used [17]. Password-Based Authentication is a simple IoT platform authentication mechanism that uses a username and password [18]. However, improper security can make this strategy vulnerable to password-guessing attacks. Certificate-based authentication, which uses X.509 certificates, is safer. A trusted Certificate Authority (CA) issues a unique certificate for each device. Certificates are more secure than passwords and resistant to common attacks. The desired level of security, IoT device capabilities, and use case determine the authentication strategy [19]. To strengthen security, many IoT implementations use various authentication mechanisms. The Rivest Shamir Adleman cryptosystem is proposed in [15]. Blockchain technology improves wireless sensor network (WSN) security and trust. Optimisation for scalability and computational cost. Based on mobile terminal radio signal quality, the paper [20] locates Narrowband IoT (NB-IoT) nodes using RF fingerprinting and machine learning. The location of NB-IoT nodes using mobile terminal radio signal quality without hardware is proposed in the article. Reference [21] proposes blockchain-based cascade encryption and trust evaluation. Malicious node localization and detection increase network security and service. Consider blockchain-based secure IoT-WSNs with hybrid machine learning for large, safe deployments. Reference [22] proposes machine learning-based correlation analysis for feature selection. Faster Message Queuing Telemetry Transport (MQTT) anomaly detection helps. Advanced correlation analysis can improve research efficiency. The model [23] leverages blockchain for authentication, data exchange, and non-repudiation. For security and decentralisation, the proposed approach saves legitimate nodes' identities on a consortium blockchain.

2.3 Attack Detection Techniques

The federated intrusion detection system, (F-IDS) [24], uses federated learning. This model uses deep, convolutional, and recurrent neural networks as classifiers. Local learning allows devices to benefit from their peers' knowledge by sharing only model updates with an aggregation server to improve detection models while protecting data privacy. When one or more edge nodes are malicious, the model's robustness can be improved. B-LSTM [25] is a hybrid IDS model that uses Map Reduce, Black Widow Optimised Convolutional-Long Short-Term Memory (BWO-CONV-LSTM), and the Artificial Bee Colony (ABC) algorithm for feature selection. Improving the B-LSTM to adapt to other public intrusion detection datasets and investigate adaptive strategies to detect higher-similarity attack classes like low-frequency Distributed Denial of Service (DDoS) attacks is still required. The paper [26] uses lightweight federated learning. This method uses ambient sensor and wearable device data from mobile user entities and equipment (UEs) to collaboratively and privately learn medical symptoms like COVID-19 with high accuracy. Investigating the seamless integration of asynchronous federated learning and blockchain can address open research issues and improve B5G network security and privacy. FC-IDS [27] is a machine learning-based, two-layer hierarchical intrusion detection method for IoT networks. This two-layer fog-cloud intrusion detection model finds intrusions into IoT networks while working with limited resources. It is better than other methods in terms of accuracy, precision, recall, and F1-score. Our security architecture relies on the CCA model, which introduces unique device correlation methods that greatly increase IoT attack detection and localization. Using coarse-grained IoT device correlations like delay and network quality, our strategy aims to detect active attacks and geolocate hostile IoT devices. Data is used to develop dynamic implicit authentication systems. Our method uses PCL to precisely locate hostile IoT devices and CCA model insights into attack detection. Faster response times and better isolation and mitigation increase IoT security.

2.4 Requirements and Challenges

Sensor localization in IoT authentication is difficult. IoT devices can operate in low-network environments [28]. Localization algorithms may use offline or delayed processing to circumvent network difficulties. Securing it is another priority. Privacy and the integrity of location data matter. Thus, safe IoT authentication requires robust encryption and authentication. IoT sensors localise using GPS, Wi-Fi, Bluetooth, and RFID. Integrating various sensor data consistently and accurately is tough. Environmental variables like signal interference can also impair sensor data accuracy. Effective localization algorithms must withstand various environmental challenges in diverse environments. Managing and tracking many sensors in large IoT deployments is complex. Location data is crucial, making privacy a priority. IoT authentication must protect user location data and authorised access [29]. Automated cars need real-time localization with low latency [30]. Meeting these rigorous timing criteria is tough but critical for application safety and efficiency.

2.5 Problem Statement

Growing IoT use has enhanced connectivity and convenience. IoT networks face security risks as they grow. Underusing coarse IoT device correlations like delay and link quality to secure networks is troublesome. This problem demands a full security solution that uses these correlations to detect active attacks, locate rogue IoT devices, and establish dynamic implicit authentication. The framework must easily connect to existing IoT networks for practicality and scalability. This study has many goals. First, update the Correlation Composition Awareness model, which uses unique device correlation methods to detect and localise assaults. Second, localise malicious IoT devices with Pair Collaborative Localization. Behaviour and performance measurement authentication are needed to restrict network access to trusted devices. This issue shows that IoT network security requires a coarse device correlation security architecture.

3 Proposed Identification and Authentication Algorithm

This section covers the basic system model, identification, authentication, and verification processes for detecting assaults, malicious nodes, and suspicious devices. Fig. 1 demonstrates a multi-layered beacon node and signal processing system for IoT network attacker detection. Edge servers calculate and notify hostile nodes' positions to cloud servers for network protection from data theft and disturbances. Sensor nodes report signal strength.

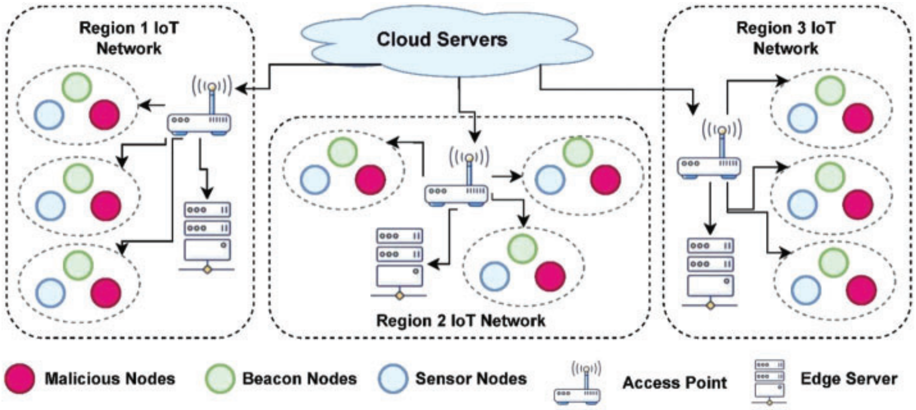

Figure 1: Process of localizing malicious nodes of the proposed model

3.1 System Model

Wireless sensor nodes are divided into ten regions and clusters as sink, cluster head, and sensor nodes based on computational capabilities in the network model. Sensor nodes lack location knowledge; thus, beacon and sink nodes find locations and identify malicious nodes with unique identifiers. Organising nodes into clusters, correct position determination, detecting and addressing rogue nodes, and using unique identities for node support are model priorities for efficient performance. The system model establishes the wireless sensor node network structure and assumptions for algorithms 1, 2, and 3. The system model separates the network into sink, cluster head, and sensor node areas and clusters. The algorithms improve IoT network performance and security by addressing system model challenges. The CCA-PCL model uses coarse IoT device correlations, targeting latency, and network quality to make attack detection and localization better. Bayesian Sensor Relocation and Traffic Monitoring (BSRTM) [15], Weighted K-Nearest Neighbours (WKNN) [20], Block-Based Sparse Localization (BBSL) [21], Improved Range-Free Detection Algorithm (IRDA) [22], Adaptive Detection of Sybil Nodes (ADSN) [23], Flow-based Intrusion Detection System (F-IDS) [24], Bidirectional Long Short-Term Memory (B-LSTM) [25], Low-Frequency Logistic Model (LFLM) [26], Fuzzy-based Classification Intrusion Detection System (FC-IDS) [27], and High-Performance Boundary-based Feature Learning (HBFL) [28] offer IoT security insights, whereas CCA-PCL uses correlation composition awareness. The proposed methodology is unique in its ability to scale and evaluate the chain of trust using intelligent communication among IoT nodes in a specific area. The security performance of the system is isolated for each area, ensuring that DoS attacks are unable to manipulate and gain simultaneous access to multiple regions.

Algorithm 1: Pair Collaborative Identification Algorithm

```
Input: $\overline{A} = \overline{A_L}.\frac{d}{dx}\left(A_D\left(x\right)\right)\ UntrainedD_d$
Initialize: N = Number of the training epochs, SGD = Stochastic gradient descent
Output: A = $A_L\frac{d}{dx}\left(A_D\left(x\right)\right)$
IoT Node Identification
Begin
While (i←N) do
```

(Continued)

Algorithm 1 (continued)

```
        Update $\overline{A_D}$ with SGD
         L$\overline{A_D}\left(C1\left(\left(A_D\left(x_{i,}y_i\right)\right)\right), \forall (x_i, y_i) \in D_D$
End
Finalize $A_D \rightarrow C1(A_D)$
 $D_L \leftarrow A_D(x)$
 $\forall x \in D_D \rightarrow Predicted\ usingF_D(x)$
Returned trained IoT Node Identification model $A_D, D_L, D_D$
End
```

3.2 Identification Phase

The proposed method uses correlation analysis to detect and localise wireless network assaults using Gated Recurrent Units (GRU) machine learning. It addresses wireless channel randomness-related latency and link quality correlations. GRU helps the attack detection model, trained on dataset DL with pairings (G; ML), detect attacks with comparable correlations. Delays and link quality are correlated between devices. Attack localization auxiliary model is trained on HL, where labels (ML) represent adversary zones, using the detection model's outcome. The system has an early exit feature and two auxiliary classifiers for robustness. Gated Recurrent Units overcome wireless channel randomization by using correlation information across IoT devices to identify and localise assaults.

1. If denotes the count of IoT devices, the correlation of link quality (Q) or packet delay (D) between IoT devices *i* and *j* is computed according to Eq. (1). Here, N {Q, D} and T represent the size of the window.

$$r_{i,j}^{N} = \frac{\sum_{i,j=0}^{T}(N_i-\overline{N}_i)\left(N_j-\overline{N}_j\right)}{\sqrt{\sum_{i,j=0}^{T}\left(N_i-\overline{N}_i\right)^2\sum_{i,j=0}^{T}\left(N_j-\overline{N}_j\right)^2}} \tag{1}$$

For the training of our attack detection model, we generated a training dataset. Where the input features consist of correlations between pairs of devices in terms of delay and link quality.

2. For training the attack detection model, a data set was constructed incorporating delay and link quality $\{(\mathrm{G}, Y_D|\mathrm{G} = (r_{i,j}^{D}, r_{i,j}^{Q}))\}$, where Y_D represents the results from the detection model. Additionally, to train the auxiliary attack localization model, a separate dataset was generated leveraging the outcomes obtained from the detection model. Algorithm 1 discovers IoT nodes collaboratively. Start model optimisation by initialising training epochs and stochastic gradient descent. A training loop updates the model with paired data and calculates losses. The final model predicts dataset node IDs. Algorithms train models to detect IoT nodes in networks.

Algorithm 2: Pair Collaborative Localization Algorithm

```
Input: $\overline{A} = \overline{A_L}.\frac{d}{dx}(A_D(x))\ UntrainedD_d$
Initialize: S = Number of the Security configurations, SGD = Stochastic gradient descent
Output: A = $A_L\frac{d}{dx}(A_D(x))$
IoT Node Localization:
```

(Continued)

Algorithm 2 (continued)

```
Begin
Call Algorithm1
While (j←S) do
    Update $\overline{A_D}$ with SGD
        L$\overline{A_L}$ $\left(C2\left(\left(A_L\left(x_{i,}y_i\right)\right)\right)\right)$
        $\forall\,(x_i, y_i) \in D_L$
        Update (A) with dynamic-range quantization
        RETURN fully –trained detection and localization
End
```

3.3 Authentication Phase

Continuous device authentication in IoT networks reduces battery life due to communication and computational issues. CCA-PCL has a Device Anomaly Detection module to address this. This module detects malicious IoT devices by analysing CPU and memory consumption. Based on Pair Collaborative Localization results, CCA-PCL dynamically narrows suspect devices, implicitly authenticating them and minimising system overhead for longer device life spans. It optimises authentication by targeting threats and exploiting performance metrics to improve accuracy and reduce network load. The algorithm detects anomalies in behavior and performance measurement to protect IoT devices by comparing data points to a model. Designing dynamic and adaptive implicit authentication solutions for IoT systems to address changing threats and network conditions while protecting user privacy and system integrity is difficult. Continuous authentication tracking of user and device activities is essential. With anomaly detection and machine learning to generate behavioral profiles, systems can dynamically adjust authentication criteria and identify questionable activities to trigger re-authentication. To minimise CCA model and PCL strategy effects from network heterogeneity and device variability, the proposed security architecture must be thoroughly reviewed. The CCA model adapts to IoT devices and networks via adaptive learning and feature engineering for robustness.

Algorithm 3: Correlation Composition Aware Attack Detection Algorithm

```
Input: Set of target devices (∅)
Output: Adversary$\varnothing'$, $ZVERIFY\,(P\varnothing') = 0$
P = GENERATE – CHALLENGE ($1^n$)
While $\varnothing \in \varnothing do$
    Assign (P) to ∅
    $K \leftarrow 0$, Z← 0, $Lf = \{\}$ ►∅ Operations Start
    Tstart Integrate EPOCH (Current)
    PID PROC(P)
    while (S PROC(P)) do
    $u1 \leftarrow K_i^{PID}, u2 \leftarrow Z_i^{Total}$ and $Z_{factor} \leftarrow K + \frac{U_1}{U_2}$
$U \leftarrow \frac{K_{factor}}{i+1}$
```

(Continued)

Algorithm 3 (continued)

```
$v1 \leftarrow Z_i^{PID}, v2 \leftarrow Z_i^{Total}$ and $Z_{factor} \leftarrow Z + \frac{V_1}{V_2}$
$Z \leftarrow \frac{Z_{factor}}{i+1}$
Lf←ptrace
$T_{End} \leftarrow$ *Integrate* EPOCH (Current)
T $= T_{Start} - T_{End}$
$P_{\varnothing} =$ (K,Z,TLf,SHA256(S))
Assign ($P_{\varnothing}$) to server ▶∅ Operations end
{0,1}←Meta Verify ($P_{\varnothing}$)
```

3.4 Verification Phase

Validating and confirming network transactions is called verification. To ensure transaction accuracy and integrity, many peers run the verification algorithm. Due to the many computations and communication overhead, this verification procedure can diminish operational efficiency and energy waste. The verification step authenticates people, devices, and data using various authentication protocols and cryptographic algorithms. A chaos-based privacy-preserving cryptographic algorithm and MAC can safeguard smart home data communications. Specialised smart contracts and authorization mechanisms can also help implement blockchain authentication and access control. Using lightweight anti-malware solutions to protect IoT devices from malware and developing lightweight cryptographic algorithms and efficient key management schemes to secure data while allowing authorised access can reduce computational overhead and speed up verification. The Algorithm 2 helps grid devices locate themselves like a GPS. Data is collected from reliable "anchor" points first. It then analyses patterns in paired data points, adjusts internal data representations, and minimises inconsistencies to improve its grid comprehension. This optimization process, fueled by "stochastic gradient descent," produces a revised map that lets each device calculate its position depending on its neighbors.

3.5 Attack Detection Phase

The correlation composition-aware attack detection algorithm (Algorithm 3) and the performance algorithm hunt for hidden attackers in a network. It challenges target devices, analyses their responses, and uses extracted features to train a model that identifies malicious patterns. Suspicious devices are flagged with confidence scores, helping system defenders prioritise and neutralise potential threats. Real-world testing and validation of the proposed security framework across IoT domains are essential to assessing its flexibility and efficacy. The validation procedure will include many evaluations to verify robustness in various environments and attack vectors. First, we will run lab tests to simulate different assault situations and environmental conditions. This lets us assess the framework's attack detection accuracy, malicious device localization precision, and dynamic implicit authentication effectiveness. By integrating privacy-enhancing features alongside powerful security procedures, the proposed IoT sensor localization architecture addresses changing data protection legislation and standards. To comply, the CCA model prioritises anonymized data aggregation, reducing sensitive information while using correlations for attack detection and location. PCL uses encrypted communication channels and encryption to locate rogue IoT devices, enhancing privacy. The BPM device authentication approach follows privacy-by-design principles to rigorously validate trusted devices without compromising user data.

4 Result Evaluation

Our method uses trust evaluation to discover rogue sensor nodes in the network. To prevent network intrusion, we added authentication. A trust value is calculated for each beacon node to determine its reliability and security. The model was tested using a large-scale network simulation model. This research needed several implementations of state-of-the-art current models to compare the proposed model's performance to existing models. Fig. 2 shows the simulation model. For the two main aims of this work, the suggested model was compared against two sets of similar models. In the initial phase, the proposed model's attack detection performance is assessed using metrics like accuracy, F1-score, precision score, and recall score, and the results are compared to F-IDS [24], B-LSTM [25], LFLM [26], FC-IDS [27], and HBFL [28]. The proposed model's localization performance is assessed in the second phase. The proposed model was compared to BSRTM [15], WKNN [20], BBSL [21], IRDA [22], ADSN [23], and the proposed CCA-PCL model on accuracy, F1-score, precision score, and other parameters. In conclusion, the suggested localization model is evaluated for transaction delay, energy utilisation, throughput, and honesty. Comparing the suggested model to localization analysis models confirmed its improvement.

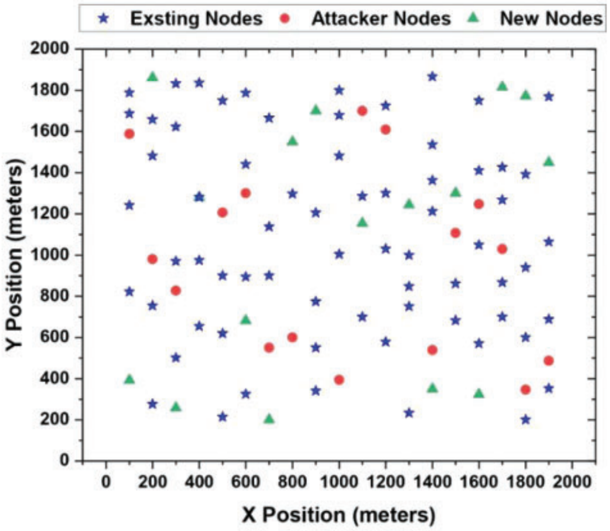

Figure 2: Simulation model

4.1 Simulation Model

Simulation findings from numerous scenarios validate the suggested system model. Our models' network planning and simulation were done in MATLAB R2021a on a workstation with an Intel(R) Xeon(R) Silver 4214 CPU @ 2.20 GHz 2.19 GHz (2 processors), 128 GB of RAM (128 GB useable), 64-bit Windows 10, and an x64-based processor. Python was used for data analysis and processing. Table 1 summarizes network deployment and extensive security analysis simulation setup parameters. We used Solidity to create smart contracts and consensus processes in addition to Python and MATLAB.

Table 1: Simulation setup for proposed network model

Parameter	Values	Parameter	Values
Platform 10	MATLAB	Cluster heads	10
Number of IoT nodes	100 to 1000	Number of regions	10
Total unknown nodes	10	Attacks	DDoS
Deployment area	20000 × 20000 m^2	Protocol type	MQTT
Mobility	Random way path	Sink position	500, 2000
Data size	64 KB	Transmission radius	250

4.2 Performance Metrics

The proposed system's performance is assessed through the examination of the following four metrics: Localization error (LE): This measure quantifies how far away the estimated position of a sensor node is from its true position. This can be calculated as LE $= \sqrt{\left(x_i' - x_i\right)^2 + \left(y_i' - y_i\right)^2}$ and average localizationerror (ALE) is calculated as ALE $\frac{= \sum_{i=1}^{n} LE}{pQ}$. In the anonymous node I, while (x_i, y_i) represent its computed coordinates. The variable p signifies the number of unknown nodes, and Q denotes the communication radius of the network. Localization errors are standardised by normalising them to the radio range of sensor nodes. This involves dividing the localization errors by the radio range of the sensor nodes, simplifying the comparison of performance across different localization systems [30]. This research area's average localization accuracy assesses node placement precision. This is calculated using all study nodes' average localization errors. Unknown sensor node location: It assesses how well the system finds new sensor nodes. A confusion matrix: This matrix rates the system's attack classification. The system is tested using the publicly available CICIDS 2017 benchmark dataset with varied assaults. Localization error and ALE are calculated from predicted sensor node coordinates and dataset positions. Localization of unknown sensor nodes assesses the system's ability to find new ones. The dataset has training and test sets. The system is taught and tested on training and test sets. The confusion matrix measures system attack classification. Compare system-predicted attack labels to ground-truth labels. Calculate precision, recall, and F1-score from the confusion matrix. The system's effectiveness is measured by its average detection rate, accuracy, precision, and recall. The system's attack detection and classification metrics are calculated in [21].

4.3 Energy Utilization Performance

Energy optimisation and node-to-node communication in wireless sensor networks are crucial. It assesses the trustworthiness of network nodes. We examined energy use in low-power IoT nodes to boost energy. For a data transmission of k bits across a distance D and a threshold distance D_o, the required transmission energy is calculated as $E_{TX(s)} = k \times (E_e + E_f) \times D^2$, for beacon packets $E_{TX(b)} = 0.2 \times (E_e + E_f)$. Hence the total energy utilization for the time slice t is calculated as $E_t = E_{TX(s)} + E_{TX(b)}$. Here, E_f is the energy being received, and E_e is the power being lost somewhere along the line. Innovative integration of correlation composition analysis awareness and pair collaborative localization into a single framework improves model efficiency at low-power IoT nodes and reduces communication overhead. Fig. 3 compares Region 1's average energy use. Energy utilisation performance of the proposed model with 10 IoT sensor nodes: BSRTM 70%, WKNN 71.5%, BBSL

72.5%, IRDA 71.86%, ADSN 72.68%, and our proposed method 71.234%. With 100 IoT sensor nodes, BSRTM uses 91.254% of energy, whereas our proposed technique uses 75.648%, a 15.606% variation, and a minimum of 5.587%. Attack detection is done internally during localization. The region's reward function from the previous round updates peer node location process outcomes. This reduces computational costs and improves low-power IoT node location accuracy.

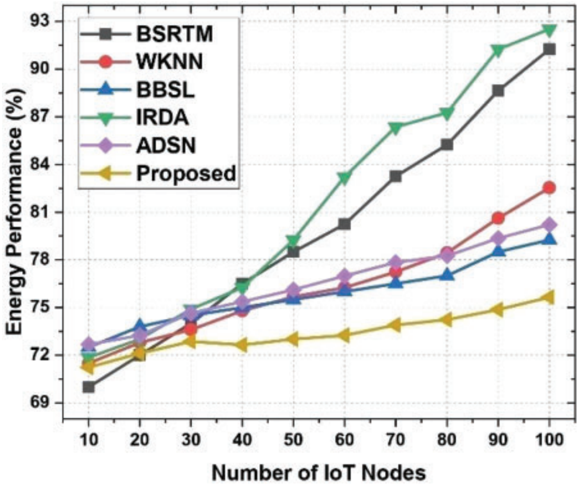

Figure 3: Energy utilization comparison

4.4 *Honesty Analysis*

We analyse honesty to calculate behavioral trust for secure attack localization and detection in IoT-based wireless sensor networks. This honesty performance metric is calculated as ho $= K_s/K_n$ that proves the behavioral trust. There are K_n interactions between source and destination nodes, and K_s interactions between source and destination nodes which lead to successful results. Behavioral trust in beacons is compromised when malicious nodes are within the radius of an anchor node. Impaired beacon node trust leads to incorrect selection of anchor and cluster head nodes for accurate localization of malicious nodes in the IoT. We have calculated the honesty of each IoT node, and the average honesty performance of all the IoT nodes in a region is depicted in Fig. 4. We calculated each IoT node's honesty, and Fig. 4 shows the region's average honesty performance. When we assessed 10 IoT sensor nodes, BSRTM gave honesty as 97.0085%, WKNN 96.4379%, BBSL 96.4379%, IRDA 96.7308%, and ADSN 98.0842%. Our proposed method is 2%–3% more honest than our comparative methods.

4.5 *Transaction Delay Performance*

The transaction delay between base and sensor nodes was studied by adjusting the number of IoT nodes from 10 to 100 and setting the communication packets to 100 64 KB packets. We tested 10 IoT sensor nodes and found that BSRTM took 4 s, WKNN 7 s, BBSL 5 s, IRDA 6 s, ADSN 8 s, and our proposed solution 3 s. For 100 IoT sensor nodes, IRDA offers 88 s transaction delay while our proposed technique gives 78 s with 10 s fluctuations which is depicted in Fig. 5.

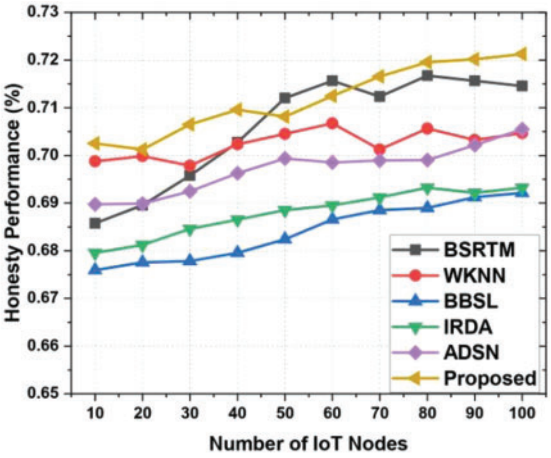

Figure 4: Honesty comparison

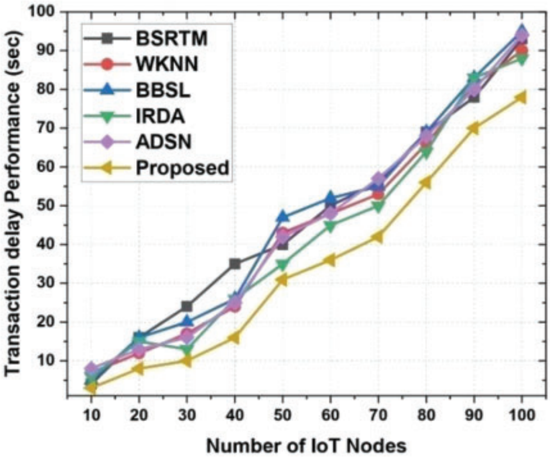

Figure 5: Transaction delay comparison

4.6 Attack Detection Analysis

This method aims to detect and locate rogue nodes in IoT-based wireless sensor networks to improve security. It uses a comprehensive strategy that incorporates correlation composition and pair-wise collaborative localization. Investigation of IoT device-initiated assaults on network security and operation. Denial-of-service (DoS) attacks, unauthorised access attempts, and other malicious activities designed to disrupt the IoT network are evaluated.

The system uses benchmark datasets like CICIDS 2017 and UNSW-NB15 to evaluate its performance, which cover normal network behavior and popular attacks. Many present and past intrusion detection experiments use the UNSW-NB15 dataset. The IXIA Perfect Storm programme created regular and anomalous network traffic packets. The tool simulates nine attack classes to update security vulnerabilities and exposures in the collected packets. Fig. 6 depicts attack detection accuracy. When we evaluated 10 IoT sensor nodes, F-IDS had an 85% accuracy attack, B-LSTM had 85%, LFLM had 84%, FC-IDS had 86%, HBFL had 85%, and our proposed method had 87%. The HBFL technique delivers a 94% accuracy attack for 100 IoT sensor nodes, whereas our method gives 98.5%

with 4.5% fluctuation. The assault detection F1-score is in Fig. 7. When we tested 10 IoT sensor nodes, BSRTM gave F1-score attack 86.82%, WKNN 85.4%, BBSL 85.4%, IRDA 86.24%, ADSN 83.5%, and our suggested method 89.2%. The ADSN technique yields an 86.85% F1-score attack for 100 IoT sensor nodes, while our method gives 91.9% with a 5.05% variance. The attack detection precision score is presented in Fig. 8. When we evaluate with 10 IoT sensor nodes, by applying BSRTM technique we got precision attack as 91.82%, WKNN technique 91.65%, BBSL technique 96.2%, IRDA technique 94.2% ADSN technique 97.6%. where our proposed method gives precision attack as 93.6%. When we evaluate this for 100 IoT sensor nodes ADSN method gives precision attack as 91.9% and our proposed method gives 96.5% with 4.6% variation. The recall score performance is presented in Fig. 9. When we evaluate with 10 IoT sensor nodes, by applying BSRTM technique we got recall attack as 70.82%, WKNN technique 85.2%, BBSL technique 80.52%, IRDA technique 84.92% ADSN technique 93.5% gives recall attack as 93.5% where our proposed method gives recall accuracy as 94.6%. When we evaluate with 100 IoT Sensor nodes BSRTM gives recall attack as 85.2% and our proposed method gives the recall attack as 94.8%.

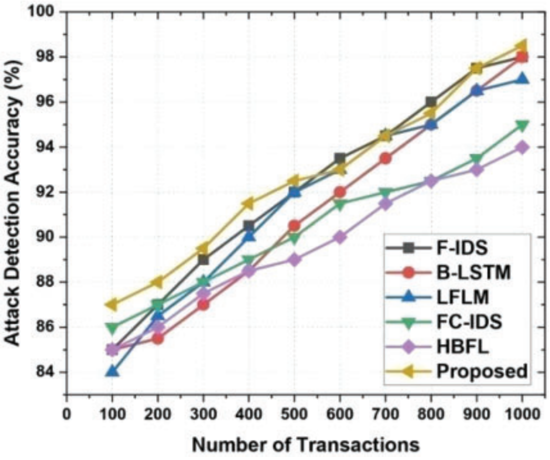

Figure 6: Attack detection accuracy

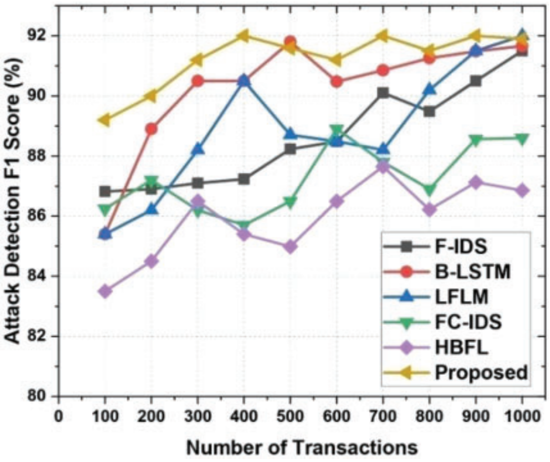

Figure 7: Attack detection F1-score

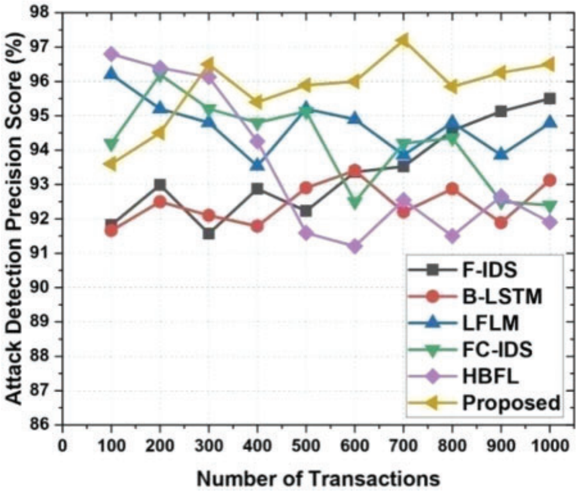

Figure 8: Attack detection precision score

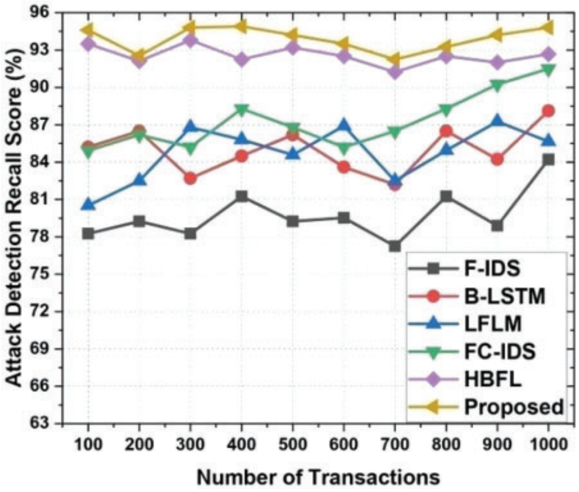

Figure 9: Attack detection recall score

4.7 Localization Performance

In the proposed localization scheme, we calculate all node positions and deviations. Fig. 1 shows how malicious nodes are organized. False negatives misclassify honest nodes as malevolent in network traffic. Along with honesty, intimacy is one technique to measure the behavioral trustworthy values of anchor nodes. It may be computed as $I_n = \frac{m_i}{m_{i+m_a}}$, where m_a is the time consumed for the node to communicate with the anchor node and m_i is the collaboration time of a particular node with beacon i.

Fig. 10 shows localization precision. Localizing 10 IoT sensor nodes using BSRTM gives 92.13% accuracy. WKNN 91.52%, BBSL 91.68%, IRDA 91.78%, ADSN 91.89%, and our technique gives 92% localization accuracy. BBSL localizes 100 IoT sensor nodes with 92.84% accuracy, while our method has 94.21%, a 1.37% difference. These F1-score performance can be observed from Fig. 11. The localization precision score is in Fig. 12. BSRTM locates 10 IoT sensor nodes: 81.54%, WKNN

91.25%, BBSL 85.45%, IRDA 90.5%, and ADSN 85.23%. Overall, our localization method is 79.25% accurate. ADSN's 90.245% accuracy with 100 IoT sensor nodes is 5% lower than our suggested method's 95.24% precision score localization. The localization recall score is in Fig. 13. BSRTM locates 71.15% of 10 IoT sensor nodes, WKNN 70.45%, BBSL 73.5%, IRDA 71.25%, and ADSN 76.89%. This localization approach has a 79.25% recall. Localizing 100 IoT sensor nodes with BBSL yields a 75.542% recall score, 4.448% lower than our suggested method's 79.99%. Simulations show that 10 IoT sensor nodes can detect and locate rogue nodes with 100% honesty, 71.234% energy use, and a 3-s transactional latency.

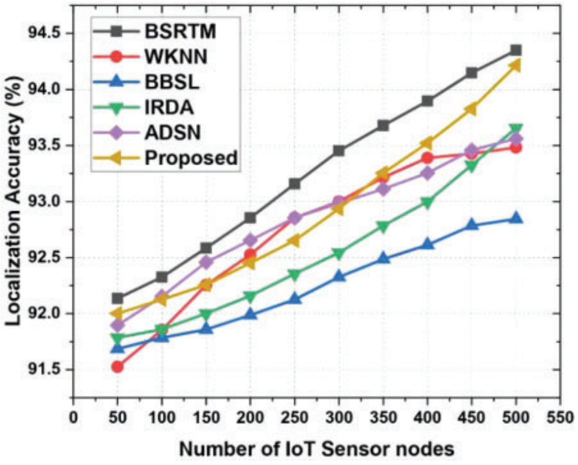

Figure 10: Localization accuracy

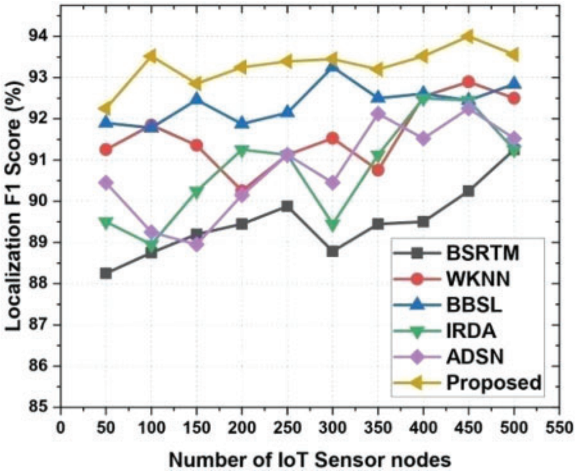

Figure 11: Localization F1-score

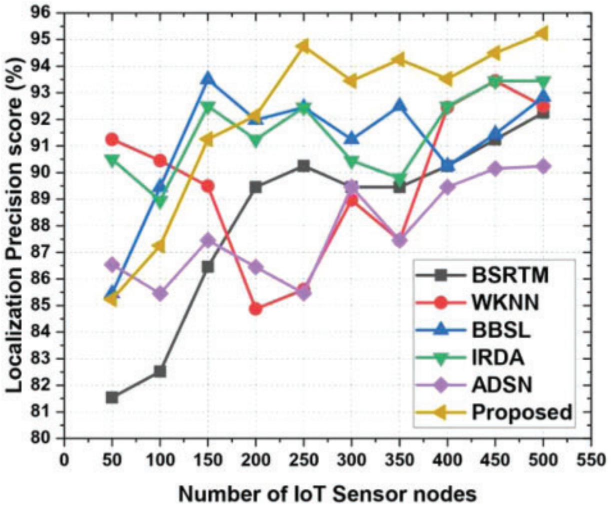

Figure 12: Localization precision score

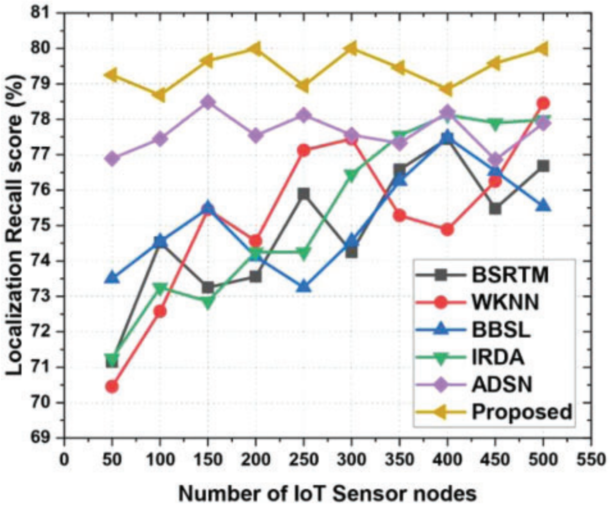

Figure 13: Localization recall score

5 Conclusion

The correlation composition awareness model and the pair-collaborative localization technique are crucial to attack detection and localization accuracy. By simultaneously addressing numerous security objectives, the framework provides a strong defence against potential threats and improves IoT system security, dependability, and efficiency. The Behavior and Performance Measurement (BPM) scheme ensures strict device authentication, allowing only trusted devices to access the network, boosting framework effectiveness. The system's dynamic implicit authentication algorithms adapt to changing security environments, protecting the IoT ecosystem. Overall, this research offers practical methods that advance IoT security and promise secure IoT implementations in the future.

Acknowledgement: We acknowledge the support for the evaluation of the proposed model from Intel IoT Center for Excellence, VIT-AP University.

Funding Statement: The authors received no specific funding for this research.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Kranthi A; data collection: Kranthi A; analysis and interpretation of results: Kranthi A, Gopikrishnan S; draft manuscript preparation: Kranthi A., Gopikrishnan S; supervision and result analysis: Gopikrishnan S. All authors reviewed the results and approved the final version.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. M. A. Janabi and S. Kurnaz, "A new localization mechanism in IoT using grasshopper optimization algorithm and DVHop algorithm," *Wirel. Netw.*, vol. 18, pp. 1–21, 2023. doi: 10.1007/s11276-023-03247-2.

[2] G. N. Kar, P. Verma, S. Mahato, A. Santra, S. Kundu and A. Bose, "An IoT-enabled multi-sensor system with location detection for agricultural applications," *MAPAN*, vol. 38, pp. 1–8, 2023. doi: 10.1007/s12647-022-00617-7.

[3] S. Yoon, S. Han, and E. Hwang, "Joint heterogeneous PUF-based security-enhanced IoT authentication," *IEEE Internet Things J.*, vol. 10, no. 20, pp. 18082–18086, 2023. doi: 10.1109/JIOT.2023.3279847.

[4] P. Razmjoui, A. Kavousi-Fard, T. Jin, M. Dabbaghjamanesh, M. Karimi and A. Jolfaei, "A blockchain-based mutual authentication method to secure the electric vehicles' TPMS," *IEEE Trans. Indust. Inf.*, vol. 20, pp. 158–168, 2023. doi: 10.1109/TII.2023.3257294.

[5] Z. Ren *et al.*, "Cost-effective colorimetric sensor for authentication of protected designation of origin (PDO) Longjing green tea," *Food Chem.*, vol. 427, no. 10, pp. 136673, 2023. doi: 10.1016/j.foodchem.2023.136673.

[6] G. Mudra, H. Cui, and M. N. Johnstone, "Survey: An overview of lightweight RFID authentication protocols suitable for the maritime internet of things," *Electron.*, vol. 12, no. 13, pp. 2990, 2023. doi: 10.3390/electronics12132990.

[7] Y. Jin and M. Tomoishi, "A named-entity-based TTP-free authentication and authorization architecture for IoT systems," in *IEEE 47th Annu. Comput., Softw. Appl. Conf. (COMPSAC)*, Torino, Italy, IEEE, 2023, pp. 985–986.

[8] T. Schläpfer, D. Lorenz, and S. Künzli, "Dynamic approach to IoT security: A new security solution for IoT," in *Embedded World Conf.*, Nuremberg, Germany, Mar. 14–16, 2023, pp. 261–266.

[9] J. Singh, A. Gimekar, and S. Venkatesan, "An efficient lightweight authentication scheme for human-centered industrial internet of things," *Int. J. Commun Syst.*, vol. 36, no. 12, pp. e4189, 2023. doi: 10.1002/dac.4189.

[10] C. Wang, D. Wang, Y. Duan, and X. Tao, "Secure and lightweight user authentication scheme for cloud-assisted internet of things," *IEEE Trans. Inform. Forensic Secur.*, vol. 18, pp. 2961–2976, 2023. doi: 10.1109/TIFS.2023.3272772.

[11] R. C. Shit, S. Sharma, D. Puthal, and A. Y. Zomaya, "Location of Things (LoT): A review and taxonomy of sensors localization in IoT infrastructure," *IEEE Commun. Surv. & Tutor.*, vol. 20, no. 3, pp. 2028–2061, 2023. doi: 10.1109/COMST.2018.2798591.

[12] W. Njima, I. Ahriz, R. Zayani, M. Terre, and R. Bouallegue, "Deep CNN for indoor localization in IoT-sensor systems," *Sens.*, vol. 19, no. 14, pp. 3127, 2019. doi: 10.3390/s19143127.

[13] S. Anoopa, A. Salim, and D. S. Pankaj, "Crowdsourcing of internet of things: Applications, trends in technology and the future," in *Int. Conf. Power, Instrum., Control Comput. (PICC)*, Thrissur, India, 2023, pp. 1–6.

[14] S. Ghorpade, M. Zennaro, and B. Chaudhari, "Survey of localization for Internet of Things nodes: Approaches, challenges and open issues," *Future Internet*, vol. 13, no. 8, pp. 210, 2021. doi: 10.3390/fi13080210.

[15] 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," *Sens.*, vol. 22, no. 2, pp. 411, 2022. doi: 10.3390/s22020411.

[16] S. S. Sahoo, S. Mohanty, K. S. Sahoo, M. Daneshmand, and A. H. Gandomi, "A three-factor-based authentication scheme of 5G wireless sensor networks for IoT system," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 15087–15099, 2023. doi: 10.1109/JIOT.2023.3264565.

[17] F. Tang, C. Ma, and K. Cheng, "Privacy-preserving authentication scheme based on zero trust architecture," *Digit. Commun. Netw.*, 2023. doi: 10.1016/j.dcan.2023.01.021.

[18] E. Gambi, L. Senigagliesi, A. Barbaresi, M. Mellini, and A. de Santis, "A WKNN-based approach for NB-IoT sensors localization," *Digit. Commun. Netw.*, vol. 9, no. 1, pp. 175–182, 2023. doi: 10.1016/j.dcan.2022.04.033.

[19] 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," *Clust. Comput.*, vol. 26, no. 2, pp. 945–960, 2023. doi: 10.1007/s10586-022-03722-z.

[20] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, K. K. Choo and M. Nafaa, "FELIDS: Federated learning-based intrusion detection system for agricultural internet of things," *J. Parallel Distr. Comput.*, vol. 165, pp. 17–31, 2022. doi: 10.1016/j.jpdc.2022.03.003.

[21] H. Goswami and H. Choudhury, "An eSIM-based remote credential provisioning and authentication protocol for IoT devices in 5G cellular network," *Internet of Things*, vol. 23, pp. 100876, 2023. doi: 10.1016/j.iot.2023.100876.

[22] A. A. Al-Saggaf, T. Sheltami, H. Alkhzaimi, and G. Ahmed, "Lightweight two-factor-based user authentication protocol for IoT-enabled healthcare ecosystem in quantum computing," *Arab. J. Sci. Eng.*, vol. 48, no. 2, pp. 2347–2357, 2023. doi: 10.1007/s13369-022-07235-0.

[23] P. R. Kanna and P. Santhi, "Hybrid intrusion detection using MapReduce-based black widow optimized convolutional long short-term memory neural networks," *Expert. Syst. Appl.*, vol. 194, pp. 116545, 2022. doi: 10.1016/j.eswa.2022.116545.

[24] 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," *Comput. Networks*, vol. 205, pp. 108672, 2022. doi: 10.1016/j.comnet.2021.108672.

[25] S. Roy, J. Li, and Y. Bai, "A two-layer fog-cloud intrusion detection model for IoT networks," *IEEE Internet Things J.*, vol. 19, pp. 100557, 2022. doi: 10.1016/j.iot.2022.100557.

[26] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection," *Computers and Electrical Engineering*, vol. 103, pp. 108379, 2022. doi: 10.1016/j.compeleceng.2022.108379.

[27] S. Nematzadeh, M. Torkamanian-Afshar, A. Seyyedabbasi, and F. Kiani, "Maximizing coverage and maintaining connectivity in WSN and decentralized IoT: An efficient metaheuristic-based method for environment-aware node deployment," *Neural Comput. Appl.*, vol. 35, no. 1, pp. 611–641, 2023. doi: 10.1007/s00521-022-07786-1.

[28] F. Zuo, Y. Li, G. Wang, and X. He, "Towards accurate and privacy-preserving localization using anchor quality assessment in internet of things," *Future Gener. Comput. Syst.*, vol. 148, no. 7, pp. 524–537, 2023. doi: 10.1016/j.future.2023.06.025.

[29] M. Orfanos, H. Perakis, and V. Gikas, "RF-based localization (WiFi RTT/LoRa) in underground quarrying for agent supervision and mapping applications," *Int. Arch. Photogramm, Remote Sens. Spat. Inf. Sci.*, vol. 48, pp. 353–361, 2023. doi: 10.5194/isprs-archives-XLVIII-1-W1-2023-353-2023.

[30] Y. Wang, Z. Tian, Y. Sun, X. Du, and N. Guizani, "LocJury: An IBN-based location privacy preserving scheme for IoCV," *IEEE Trans. Intell. Transport. Syst.*, vol. 22, no. 8, pp. 5028–5037, 2020. doi: 10.1109/TITS.2020.2970610.