scientific reports

OPEN

High accuracy indoor positioning system using Galois field-based cryptography and hybrid deep learning

Mohammad Mazyad Hazzazi[1], Prashant Kumar Shukla[2], Piyush Kumar Shukla[3]✉, Fahad Alblehai[4], Sameer Nooh[5] & Mohd Asif Shah[6,7,8]✉

In smart manufacturing, logistics, and other inside settings where the Global Positioning System (GPS) doesn't work, indoor positioning systems (IPS) are essential. Due to environmental complexity, signal noise, and possible data manipulation, traditional IPS techniques struggle with accuracy, resilience, and security. Online and offline phases are distinguished in the suggested indoor location system that employs deep learning and fingerprinting. During the offline phase, mobile devices gather signal strength measurements and contextual data traverse inside settings via Wi-Fi, Bluetooth, and magnetometers. Fingerprint classification using Density-Based Spatial Clustering of Applications with Noise (DBSCAN) clustering follows the application of signal processing techniques for noise reduction and data augmentation. The online phase involves extracting information to improve the model's accuracy. These features can be signal-based, spatial–temporal, motion-based, or environmental. The Deep Spatial–Temporal Attention Network (Deep-STAN) is an innovative hybrid model for location classification that combines Convolutional Neural Networks (CNNs), Vision Transformers (ViTs), Long-Short Term Memory (LSTMs), and attention processes. The model hyperparameters are fine-tuned using hybrid optimization to guarantee optimal performance. The work's main contribution is the incorporation of ECC, an effective encryption and decryption method for signal data, which is based on Galois fields. This cryptographic method is well-suited for real-world applications since it guarantees low-latency operations while simultaneously improving data integrity and confidentiality. In addition, S-box enhances the IPS's resilience and security by including QR codes for distinct location marking and blockchain technology for safe and immutable storing of positioning data. Moreover, the performance of the suggested model includes an accuracy of 0.9937, precision of 0.987, sensitivity of 0.9898, and specificity of 0.9878, while when 80% of data were used it had an accuracy of 0.9804, precision of 0.9722, sensitivity of 0.9859, and specificity of 0.9756. These outcomes prove that the proposed system is stable and flexible enough to be used in indoor positioning applications.

Keywords Indoor positioning system, Galois field cryptography, QR codes, Blockchain technology, Deep learning, Fingerprinting, Hybrid optimization

List of symbols

$RSSI_i$	RSSI value at position i
$RSSI_{\min}$ and $RSSI_{\max}$	Min and max RSSI values in the dataset

[1]Department of Mathematics, College of Science, King Khalid University, 61413 Abha, Saudi Arabia. [2]Department of Computer Science and Engineering, Amity School of Engineering and Technology (ASET), Amity University Mumbai, Mumbai, Maharashtra 410206, India. [3]Computer Science & Engineering Department, University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya (State Technological University of Madhya Pradesh), Bhopal, IndiaMadhya Pradesh 462033. [4]Computer Science Department, Community College, King Saud University, 11437 Riyadh, Saudi Arabia. [5]Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, 22254 Jeddah, Saudi Arabia. [6]Department of Economics, Kardan University, Parwane Du, Kabul 1001, Afghanistan. [7]Division of Research and Development, Lovely Professional University, Phagwara, Punjab144001, India. [8]Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura140401, Punjab, India. ✉email: piyush@rgpv.ac.in; m.asif@kardan.edu.af

Z_i	Z-score of $RSSI_i$,
μ	Mean of the RSSI
σ	Standard deviation
$RSSI_{i-j}$	RSSI values within the window
N	Number of points in the moving window
q	Core point
n	Column dimension
f_{concat}	Concatenated feature vector
$Linear\ (.)$	Linear transformation
E_{pos}	Positional embeddings
X	The input sequence
Q, K, and V	Query, key, and value matrices
W_Q, W_K, and W_V	Learnable weight matrices
d_k	Key dimension

Indoor positioning is a rapidly expanding technology in the connected world that is revolutionizing the way they interact and navigate with indoor spaces[1–3]. It is worth noting that indoor positioning systems provide more precise location details within structures for instance, malls, airports, hospitals, or offices as opposed to GPS which works primarily outdoor[4]. Indoor positioning utilizes numerous methods like ultra-wideband, Wi-Fi, Bluetooth Low Energy, RFID, inertial navigation systems, computer vision, and magnetic positioning to ensure accurate location finding of people or objects within certain spaces, often within a high precision range of a few meters or even centimetres[5,6]. These technologies work together to find out where people or things are within a small space with a lot of accuracy most of the time within two or even one meter only[7]. Indoor positioning has got many various uses that keep increasing day by day. It could make shopping much more fun through tailored advertisements together with easy guidance and aid logistics or warehouse management by speeding up movement operation of goods inside warehouses[8–10]. The list of symbols utilized in this research article is shown.

A significant shift has occurred in the manner in which industrial operations are managed and enhanced with the adoption of indoor location tracking within manufacturing settings[11]. The efficiency of attribution systems used inside buildings is of paramount importance toward enhancement of workers' safety and simplification warehouse management activities carried out indoor manufacturing plants and outlying production areas[12,13].

Manufacturing plants are often great and complex, calling for meticulous organization and surveillance to guarantee smooth operation[14,15]. These environments can benefit from real-time monitoring of goods, equipment, and people through technological means like RFID tags as well as ultra-wideband beacons and computer vision systems[16,17]. Through this heightened sense of visibility, they are able to discover hitches, make their workflows better and use their resources prudently. This leads to increased productivity and cost savings[7].

In the manufacturing environment, indoor positioning systems help improve worker safety. Real-time tracking and employee and machinery movement tracking helps IPS to receive warning that risks are likely to occur risk early in advance and that safety measures are maintained and risks avoided which would reduce mishappening and injury possibilities[18]. For instance, proximity sensors placed on portable gadgets or machines can alert workers about their proximity to dangerous equipment.

In addition, ensuring employee safety in various manufacturing scenarios cannot be achieved without precise indoor localization[19]. This means that indoor positioning system allows for tracing the movement of people and machines thus identifying possible hazards before they cause harm while verifying compliance with safety regulations that ultimately lead to reduced number of accidents and injuries[19]. At the same time integrating with the already installed industrial automation systems also needs special attention because it is experts who must carry it out[6]. The proposed deep spatial–temporal attention network (Deep-STAN)'s advanced indoor positioning capabilities can be applied in various fields, including retail and logistics. This can enhance customer engagement and increase sales. In logistics, Deep-STAN can be used for inventory management by accurately tracking the location of goods within large warehouses, helping optimize item retrieval, streamline warehouse operations, and reducing the time spent searching for products.

The major contributions of this study are as follows:

- Applies robust signal processing and noise reduction techniques such as moving average filtering and outlier removal for purposes of cleaning and normalizing data.
- The DBSCAN clustering method is used for identifying different indoor locations that have distinct groups.
- Extract signal-based, spatial–temporal, motion, environmental, and statistical features. These various characteristics are helpful for greater understanding of intricate indoor environmental dynamics.
- The model presented here combines long short-term memory (LSTM), visual transformers, attention mechanisms, and Convolutional Neural Networks (CNNs) to effectively capture spatial, temporal, and global dependencies in indoor fingerprint data.
- The model's performance is optimized using hybrid optimization techniques, including hyperparameter tuning and methods to overcome local minima.

The paper has been organized as follows, Sect "Introduction" of the paper provides an introduction, and Sect "Literature review" encloses recent literature related to the study. Moreover, the suggested approach has been discussed in Sect "Proposed methodology" and the result of the suggested model has been given in Sect "Experimental results". Finally, the research has been concluded with a conclusion in Sect "Conclusions".

Literature review

The summary of the literature works is manifested in Table 1. Liu et al.[20] designed a visible light indoor positioning system which uses one LED, and a rotatable photo detector based on machine learning. This system applies to two major steps stored in what they call area classification and precise positioning. Nabati and Ghorashi[21] introduced a novel indoor positioning system which depends on fingerprinting of the environment, deep learning technology as well as historical data. The purpose of developing KD-CNN algorithm by Mazlan et al.[22] was to localize the objects within indoor spaces faster by exploiting information derived from a huge amount of convolutional neural network (CNN) models and using it for training less expensive models in which tasks are performed more quickly albeit at higher accuracies. A technique for indoor localization has been developed by Zhang et al.[23] with the help of attention-augmented Residual CNN (RCNN) and Channel State Information (CSI) fingerprints which are utilized for tracking objects inside buildings. Liu et al.[24] recommended using a Clustering-based Noise Elimination Scheme (CNES) that is suited to RSSI-based datasets. This technique employs density-based spatial clustering of applications with noise for clustering RSSIs in regions so as to eliminate noisy samples from the dataset. Laska and Blankenbach[25] came up with a groundbreaking method for estimating position in wide and large indoor spaces. They presented a unified approach making use of just one neural network for training. A study on indoor 3D positioning algorithms was performed by Wang et al.[26] using WiFi fingerprinting. Spatiotemporal features including a Temporal Convolutional Networks (TCN) which has been armed through dilated convolution, causal convolution, and residual connection were taken off by them using deep learning techniques.

Sammy, F., & Vigila, S. M. C[27] suggested a distributed blockchain-based Ciphertext-Policy Attribute-Based Encryption (CP-ABE) approach is introduced to secure patient health records (PHRs) in cloud computing. Umran et al.[28] blockchain-based private network is proposed for securing the circuit breaker system in the Al-Kufa/Iraq power plant. The system utilizes a multi-chain proof of rapid authentication (McPoRA) as a consensus mechanism to enhance computational performance and reduce latency. Shaikh, J. R., & Iliev, G[29] developed a blockchain-based transaction processing system (TPS) to enhance security in E-commerce transactions. The system incorporates zero-knowledge proof (ZKP) and modified ECC to ensure privacy, authentication, integrity, and non-repudiation.

Proposed methodology

Figure 1 outlines the architecture of a proposed methodology for indoor positioning, utilizing a combination of data collection, pre-processing, data augmentation, and machine learning techniques. The process begins with data collection using mobile devices in an indoor environment, with the collected data stored in a database. During the pre-processing phase, the data undergoes moving average filtering, outlier removal, and Min–Max normalization to prepare it for further analysis. Data augmentation methods including rotation, translation, and synthetic noise addition are then applied. In indoor positioning systems (IPS), transformations such as rotation, translation, and noise addition significantly impact the model's learning process and results. Rotation affects signal orientation, ensuring the model can accurately interpret data from various angles by exposing it to multiple orientations during training, which enhances robustness and generalization. Translation mimics user movement through different areas, allowing the model to associate specific signal patterns with varying locations, thereby improving localization accuracy as it learns to recognize similar patterns across spatial configurations.

Noise addition simulates real-world conditions where signals are distorted by environmental interference, helping the model become resilient to variations and enabling it to identify underlying patterns despite noise. The online phase involves feature extraction, where signal-based features, spatial and temporal features, motion

Author(s)	Proposed technique	Advantages	Limitations
Liu et al.[20]	Visible Light Positioning with LED & Rotatable Photo Detector	High accuracy in walls and corners	Limited to environments with proper lighting conditions
Nabati & Ghorashi[21]	DNN-based Fingerprinting with RSS samples	Real-time, high-speed, and precise positioning	Performance depends on RSS stability
Mazlan et al.[22]	KD-CNN for Indoor Object Localization	Faster positioning with high accuracy	Requires large pre-trained CNN models for training
Zhang et al.[23]	Attention-augmented Residual CNN (RCNN) with CSI fingerprints	Improves tracking and localization accuracy	Requires a large CSI dataset for training
Liu et al.[24]	Clustering-based Noise Elimination Scheme (CNES) for RSSI	Enhances data quality and improves classifier performance	Sensitive to incorrect clustering parameters
Laska & Blankenbach[25]	Unified Neural Network for Floor & Position Estimation	Reduce errors using Multi-Cell Encoding Learning (multi-CEL)	Performance varies with building layout complexity
Wang et al.[26]	WiFi Fingerprinting with Temporal Convolutional Networks (TCN)	Better depth perception in indoor 3D localization	Requires extensive spatiotemporal data for accuracy
Sammy & Vigila[27]	A blockchain method to keep patient records safe in the cloud	Keeps data private and removes the need for a third party	Can be hard to use and may slow things down
Umran et al.[28]	A blockchain system to protect power plant equipment	Uses less power, works fast, and keeps data safe	Hard to set up and may not work with old systems
Shaikh & Iliev[29]	A blockchain system to make online payments safe	Protect payments, stop hackers, and keep data private	Can make payments slow and may not work well for big websites

Table 1. Summary of the reviewed literature.

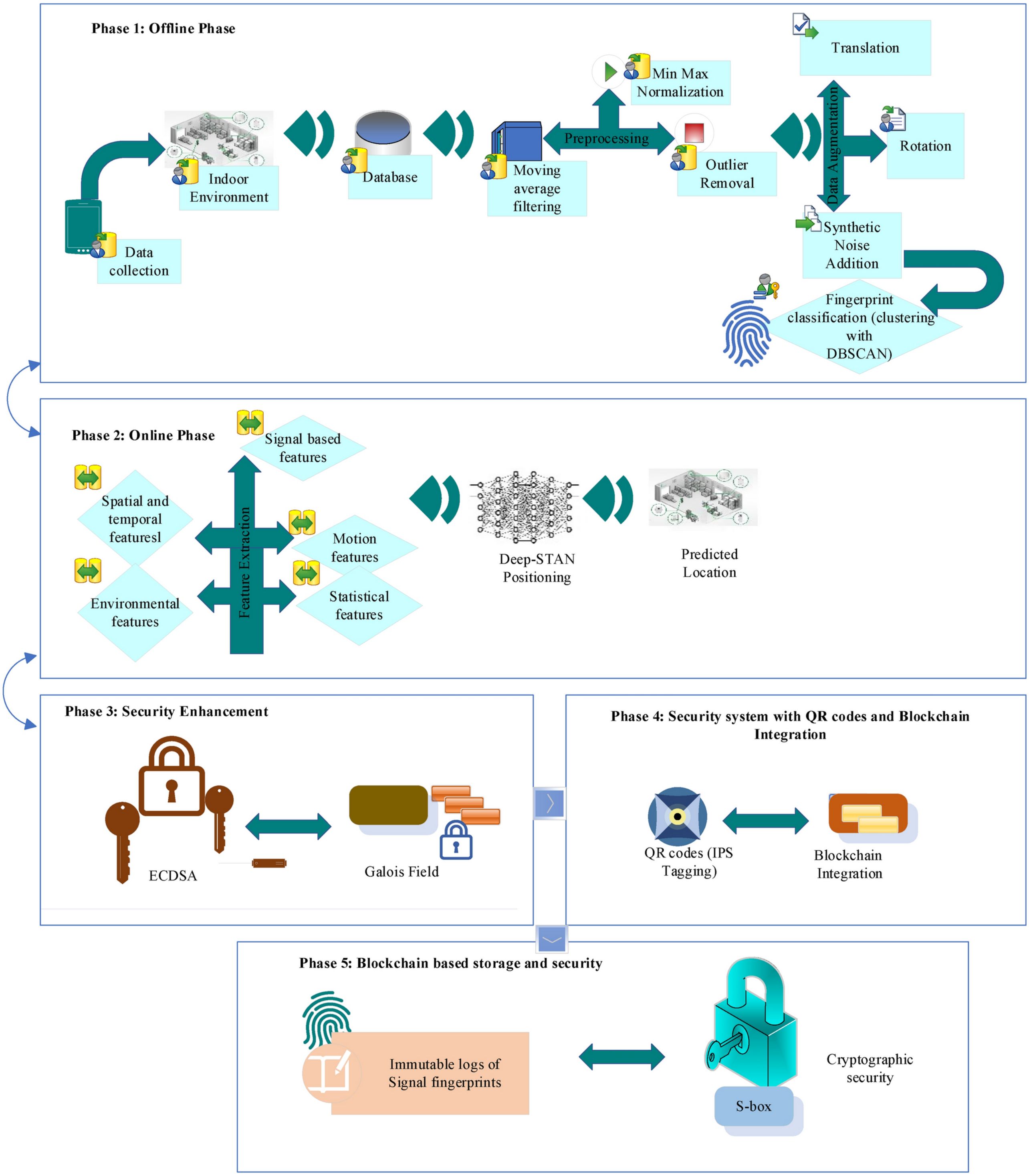
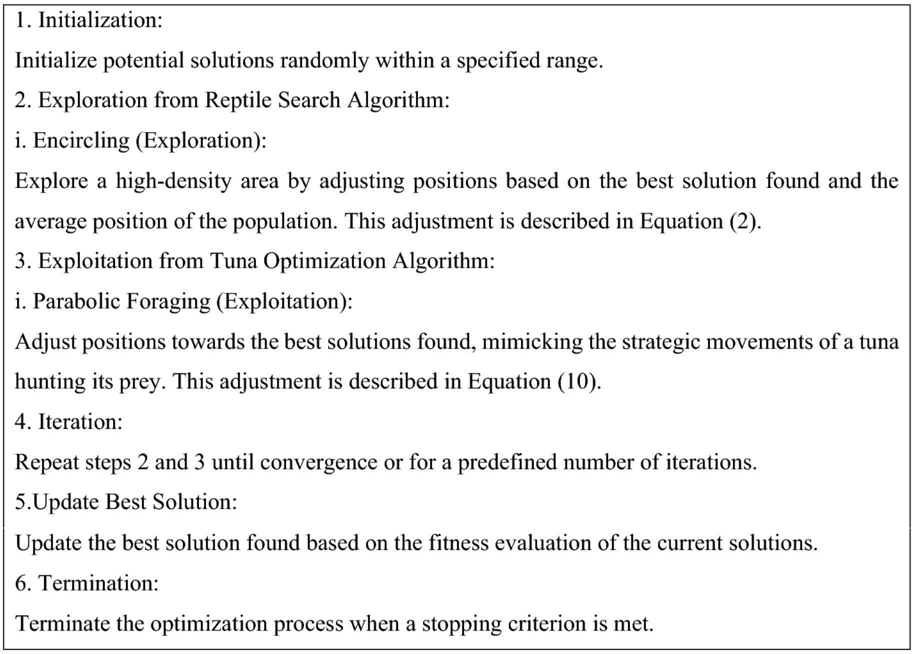


Fig. 1. Architecture of the proposed methodology.

features, environmental features, and statistical features are derived from the data. These features are input into the Deep-STAN positioning model, which predicts the location based on the processed and augmented data, resulting in accurate indoor positioning. Finally, S-box cryptography, blockchain integration, and QR code-based security for an accurate indoor positioning system. Integrating security components like Galois Field-based Elliptic Curve Cryptography (ECC), blockchain technology, and the S-box cryptographic transformations into the Deep-STAN model involve several key steps. First, ECC is applied to encrypt and decrypt signal data collected during the positioning process. This ensures that data transmitted between devices and servers is secure, preventing unauthorized access. The ECC's low computational complexity enables real-time encryption without affecting the system's latency, preserving performance.



```
1. Initialization:
Initialize potential solutions randomly within a specified range.
2. Exploration from Reptile Search Algorithm:
i. Encircling (Exploration):
Explore a high-density area by adjusting positions based on the best solution found and the average position of the population. This adjustment is described in Equation (2).
3. Exploitation from Tuna Optimization Algorithm:
i. Parabolic Foraging (Exploitation):
Adjust positions towards the best solutions found, mimicking the strategic movements of a tuna hunting its prey. This adjustment is described in Equation (10).
4. Iteration:
Repeat steps 2 and 3 until convergence or for a predefined number of iterations.
5.Update Best Solution:
Update the best solution found based on the fitness evaluation of the current solutions.
6. Termination:
Terminate the optimization process when a stopping criterion is met.
```

Algorithm 1. Hybrid reptile tuna optimization algorithm.

Phase 1: offline phase

Data acquisition

The WiFi RSS Fingerprint Localization Dataset is commonly used for indoor positioning systems, leveraging Received Signal Strength (RSS) values from multiple WiFi access points to estimate a device's location. The dataset is typically collected in controlled indoor environments such as university buildings, shopping malls, or office spaces, where signal strength varies due to walls, furniture, and human movement. Data collection usually spans multiple days, often ranging from a few days to several weeks, to capture variations in signal due to environmental dynamics. The amount of data collected depends on factors such as the number of reference points, access points, and time intervals between measurements, but many datasets contain thousands to hundreds of thousands of RSS readings across different locations. The size of Wi-Fi RSS Fingerprint Localization datasets varies significantly based on the scope and methodology of data collection. For instance, the WiSig dataset comprises approximately 10 million packets captured from 174 WiFi transmitters over a month-long period. In contrast, a dataset from Tampere University includes 446 reference points and 489 access points, resulting in a more modest dataset. Moreover, the Wi-Fi RSSI Dataset for Fingerprint-based Localization, which contains data from 250 locations with 27 detected Wi-Fi access points. Therefore, the dataset size can range from hundreds of data points in smaller-scale studies to millions in extensive collections.

Pre-processing

Signal processing and noise reduction are essential steps to assure the data collected is precise and dependable. It has various techniques to clean the data and standardize it for consistency.

Moving average filtering

The moving average output helps to reduce the short term "noise" in the data by smoothening out unrelated short-term fluctuations. This is very useful in improving the accuracy of many measurements carried out on wireless devices. It can be arithmetically given in Eq. (1),

$$RSSI_i = \frac{1}{N}\sum_{j=0}^{N-1} RSSI_{i-j} \tag{1}$$

where $RSSI_i$ represents the smoothed RSSI value at position i, $RSSI_{i-j}$ signifies the RSSI values within the window, and N indicates the number of points in the moving window.

Outlier removal

Outliers in RSSI data can significantly affect the accuracy of indoor positioning. These outliers can be identified and removed using the Z-score method and it can be arithmetically given in Eq. (2),

$$Z_i = \frac{RSSI_i - \mu}{\sigma} \tag{2}$$

where Z_i denotes the Z-score of $RSSI_i$, μ signifies the mean of the RSSI values, and σ denotes standard deviation. An RSSI value is considered an outlier if $|Z_i| > k$, where k is typically set to 2 or 3.

Min–max normalization

Normalization scales the RSSI values to a common range, mitigating device-specific variations and ensuring consistency across different devices and environments it can be arithmetically given in Eq. (3),

$$RSSI' = \frac{RSSI - RSSI_{\min}}{RSSI_{\max} - RSSI_{\max}} \tag{3}$$

where $RSSI_{\min}$ and $RSSI_{\max}$ are the min and max RSSI values in the dataset, respectively. This normalization scales the RSSI values to the range [0, 1].

Clustering and fingerprinting

Fingerprint classification involves organizing the preprocessed fingerprint data into distinct groups representing different indoor locations.

DBSCAN is a robust clustering algorithm well-suited for data with noise and clusters of varying shapes and sizes. The algorithm utilizes two key parameters: $\min Pts$ and epsilon (ε). The notion of epsilon is used to denote the maximum distance that lies between two points which can still make them neighbors, whereas $\min Pts$ is the minimum number of points needed to be regarded as a solid area identified with clusters.

DBSCAN iterates through the dataset to form clusters of density-reachable points and identify noise points that do not belong to any cluster.

Mathematically, let D be the dataset of RSSI fingerprints. For each point p in D and it can be arithmetically given in Eq. (4),

$$N_\varepsilon\left(p\right) = \left\{q \in D\left|dis\tan ce\left(p,q\right) \leq \varepsilon\right.\right\} \tag{4}$$

A point p is a core point if $|N_\varepsilon\left(p\right)| \geq \min Pts$. A point p is directly density-reachable from q it $p \in N_\varepsilon\left(p\right)$ and q is a core point. The distance metric used is often Euclidean distance.

Labeling clusters with location coordinates

Once the clusters are identified using DBSCAN, the next step is to label each cluster with corresponding location coordinates. This involves determining a representative point, usually the centroid, for each cluster. The centroid can be calculated by averaging the coordinates of all points in the cluster.

For C_i containing points $p_1, p_2, \ldots, p_n$,where each point p_j has coordinates (x_j, y_j), the centroid is computed in Eq. (5)

$$C_i = \left(\frac{1}{n}\sum_{j=1}^{n} x_j, \frac{1}{n}\sum_{j=1}^{n} y_j\right) \tag{5}$$

Every point in cluster C_i is then labeled with the coordinates of this centroid and it is given in Eq. (6),

$$label\,of\,p_j \in C_i = \left(Centroid_x, Centroid_y\right) \tag{6}$$

Each data point is assigned to its location coordinates based on the cluster it belongs to in the process of marking. This labeled dataset will establish a strong base for deep learning models that are being trained to solve indoor positioning issues.

Phase 2: online phase

Feature extraction

Building an indoor positioning system requires one to gather beneficial data from raw data. How this is done is by getting useful features that machine learning models can use for predicting the position of a device in a building. Positioning models use the derived attributes to evaluate accurately the location of a device using observed data.

(i) *Signal-Based Features*: Received Signal Strength Indicator (RSSI), Signal-to-Noise Ratio (SNR), Channel Information and Signal Stability.

(ii) *Spatial and Temporal Features*: Location Coordinates and Time-Based Features.

(iii) Motion features: Motion State.

(iv) *Environmental Features*: Room and Floor Identification.

(v) *Statistical Features*: Histogram of RSSI Values.

Hybrid optimization for deep CNN

A Hybrid Optimization algorithm is employed for hyperparameter tuning (weight optimization) and to escape local minima, ensuring the model achieves optimal performance. Here the exploration phase from reptile search is employed and the exploitation phase from tuna optimization is employed.

Reptile search algorithm

The algorithm of reptile search is metaphorically depicted through the hunting habits of crocodiles that exist in the jungles. With two primary processes, it is about surroundings and hunting. These two sequences change by dividing the number of iterations into four.

Initialization The search method of the reptile starts by randomly forming an initial set of potential solutions and it is shown in Eq. (7),

$$z_{jl} = rand \times (UB - LB) + LB, l = 1, 2, \ldots, n \tag{7}$$

The initiating matrix is referred to as z_{jl}, where j varies from $1, 2, \ldots, P$. P here is the size of the population (rows of the initiating matrix), while n represents the dimensions (columns of the initiating matrix) of the current optimization problem. LB is the short form for lower bound, UB for the upper limit, whereas rand for randomly generated values.

The fitness is computed as

$$Fitness = \min\left(Error\right)$$

Encircling (exploration) The encircling phase is about exploring a high-density area. This phase requires walking and belly movements that copy crocodile movements which are so critical. These are not meant to catch prey but just to move long distances. Moreover, it can be arithmetically given in Eq. (8),

$$\begin{array}{c} z_{jl}\left(\chi+1\right) = Best_{l}\left(\chi\right) \times \left(-\eta_{jl}\left(\chi\right)\right) \times \alpha - \left(T_{jl}\left(\chi\right) \times rand\right),\ \chi \leq \frac{\chi_{\max}}{4} \\ z_{jl}\left(\chi+1\right) = Best_{l}\left(\chi\right) \times z_{(s_1,l)} \times EV\left(\chi\right) \times rand, \chi \leq 2\frac{\chi_{\max}}{4} and \chi > \frac{\chi_{\max}}{4} \end{array} \tag{8}$$

At l^{th} position, $Best_{l}\left(\chi\right)$ depicts the finest solution identified as well as χ represents the ongoing iteration while $rand$ is an arbitrary number while $\chi_{\max}$ is the maximum iterations. Hunting service's amount to solution j in position is reflected upon by η_{jl}. The value of m η_{jl} is obtained by means of the following Eq. (9),

$$\eta_{\left(\eta_{j,l}\right)} = Best_{l}\left(\chi\right) \times Q_{(j,l)} \tag{9}$$

The sensitivity of parameter α shows how accurate the exploration is, while $G_{(j.l)}$ represents a different function, through which the exploration area is reduced in the following Eq. (10),

$$G_{(j.l)} = \frac{Best_{l}\left(\chi\right) \times Q_{(s_2,l)}}{Best_{l}\left(\chi\right) + \tau} \tag{10}$$

In this case, s_1 is to be taken as a random integer between 1 and N, where N is the total number of candidate solutions. The random position for the l^{th} solution is given as $z_{(s_1,l)}$. On the other hand, s_2 is a random integer in the interval between 1 and N but τ is assumed to be a small positive value. The mathematical expression of Evolutionary Sense $EV\left(\chi\right)$ is denoted as given in Eq. (11).

$$EV\left(\chi\right) = 2 \times s_3 \times \left(1 - \frac{1}{\chi_{\max}}\right) \tag{11}$$

where s_3 is any random number. $Q_{(j,l)}$ can be calculated using Eq. (12),

$$Q_{(j,l)} = \beta + \frac{z_{(j,l)-AP\left(z_j\right)}}{Best_{l}\left(\chi\right) z\left(UB_{(l)} - LB_{(l)}\right) + \varphi} \tag{12}$$

where β is the sensitivity limit that determines exploration accuracy. $AP\left(z_j\right)$ represents the average position of the j^{th} solution and can be determined using Eq. (13),

$$AP\left(z_j\right) = \frac{1}{n}\sum\nolimits_{l=1}^{n} z_{(j,l)} \tag{13}$$

Hunting (exploitation) Hunting is divided into two stages which is hunting coordination for cases when iterates lie in $\chi \leq 3\frac{\chi_{\max}}{4} and \chi > 2\frac{\chi_{\max}}{4}$, while hunting cooperation happens when $\chi \leq \chi_{\max} and \chi > 3\frac{\chi_{\max}}{4}$. Stochastic coefficients are used to search the local search space in order to generate optimal solutions. In Eqs. (14), (15), exploitative operations are applied:

$$z_{(j,l)}\left(\chi+1\right) = Best_{l}\left(\chi\right) \times \left(Q_{(j,l)}\right) \times rand,\ \ \chi \leq 3\frac{\chi_{\max}}{4} and \chi > 2\frac{\chi_{\max}}{4} \tag{14}$$

$$z_{(j,l)}\left(\chi+1\right) = Best_{l}\left(\chi\right) - \eta_{\left(\eta_{j.l}\right)}\left(\chi\right) \times \varphi - \left(\chi\right) \times rand, \chi \leq \chi_{\max} and \chi > 3\frac{\chi_{\max}}{4} \tag{15}$$

$Best_{l}\left(\chi\right)$ in this case denotes the l^{th} position attained in the top solution during this iteration, whereas $\eta_{\left(\eta_{j,l}\right)}$ signifies the hunting operator.

Tuna optimization algorithm

Parabolic foraging Tuna love herrings and eels more than any other kind of fish, they use their power of contra-directional movement while being pursued by enemies so that it becomes impossible for them to be caught and eaten. Whenever they attack, the prey's motion provides a blueprint pattern which the hunters use by covering it in a curved line and it can be given in Eqs. (16), (17),

$$Z_i^{t+1} = \begin{cases} Z_{best}^t + rand \cdot \left(Z_{best}^t - Z_i^t\right) + RV \cdot q^2 \cdot \left(Z_{best}^t - Z_i^t\right), & if\, rand < 0.5 \\ RV \cdot q^2 \cdot Z_i^t, & if\, rand \geq 0.5 \end{cases} \tag{16}$$

$$q = \left(1 - \frac{\chi}{\chi_{\max}}\right)^{(\chi/\chi_{\max})} \tag{17}$$

where χ represents the current iteration, $\chi_{\max}$ represents predefined maximum. RV is randomly chosen at − 1 or 1.

Spiral foraging Apart from the parabolic foraging strategy, there is an alternate effective cooperative approach known as the spiral foraging strategy. This approach is described mathematically in Eq. (18),

$$Z_i^{t+1} = \begin{cases} \beta_1 \cdot \left(Z_{rand}^t + \rho \cdot \left|Z_{rand}^t - Z_i^t\right| + \beta_2 \cdot Z_i^t\right), \ i = 1 \\ \beta_1 \cdot \left(Z_{rand}^t + \rho \cdot \left|Z_{rand}^t - Z_i^t\right| + \beta_2 \cdot Z_{i-1}^t\right), \quad if\, rand < \frac{t}{t_{\max}}, i = 2, 3, \ldots, P \\ \beta_1 \cdot \left(Z_{best}^t + \rho \cdot \left|Z_{rand}^t - Z_i^t\right| + \beta_2 \cdot Z_i^t\right), \quad if\, rand \geq \frac{t}{t_{\max}}, \quad i = 1 \\ \beta_1 \cdot \left(Z_{rand}^t + \rho \cdot \left|Z_{best}^t - Z_i^t\right| + \beta_2 \cdot Z_{i-1}^t\right), \quad i = 2, 3, \ldots .P \end{cases} \tag{18}$$

where Z_i^{t+1} is one of the tunas in the $t+1$ round and refer to it as the i^{th} fish at this point. Z_{best}^t is a way to denote the current top best solution while Z_{rand}^t stands for an arbitrary reference one from the shoal of fish. The amount of pull each member has towards tips or neighbors respectively is directed by coefficient β_1 whereas other tunas' movement is determined by β_2. On top of that, parameter ρ plays a role in determining the gap between individual tunas as well as optimal or randomly selected points of reference. This model's expression is as given in Eq. (19), (21), (22),

$$\beta_1 = b + (1 - b) \cdot \frac{t}{t_{\max}} \tag{19}$$

$$\beta_2 = (1 - b) - (1 - b) \cdot \frac{t}{t_{\max}} \tag{20}$$

$$\rho = e^{cu} \cdot \cos\left(2\pi c\right) \tag{21}$$

$$u = e^{3\cos\left(\left(\left(t_{\max} + {}^{1}/_{t}\right) - 1\right)\pi\right)} \tag{22}$$

where A is a constant, which shows how much tuna fish attracts, while b is a random number from 0 to 1 evenly spread across the spectrum.

Positioning

The Deep Spatial–Temporal Attention Network proposed is a hybrid classification model that blends CNN, Visual Transformers, LSTM, and attention mechanisms.

CNN

A CNN is a type of deep learning network that is designed for grid-like data, such as images. One reason for their popularity is that CNNs can detect spatial patterns as well as relationships between various parts of the data by using special convolutional and pooling layers in addition to conventional fully connected layers.

LSTM

In indoor positioning, LSTM is illustrated in Fig. 2 is used to extract temporal features from the collected signal data, such as RSSI sequences, device motion patterns, and other time-dependent contextual information. By capturing these temporal dynamics, LSTMs contribute to more accurate and reliable location estimation.

The features extracted by CNNs capture spatial dependencies, while the features extracted by LSTMs capture temporal dependencies. The final output from the ViT is used for precise location prediction is given in Eq. (23).

$$f_{concat} = [f_{CNN}, f_{LSTM}] \tag{23}$$

Vision transformer (ViT)

The concatenated feature vector is input into the Vision Transformer as illustrated in Fig. 3.

The concatenated feature vector f_{concat} is input into the Vision Transformer.

Input embedding Moreover, the following Eq. (24) shows the mathematical deliberation for input embedding.

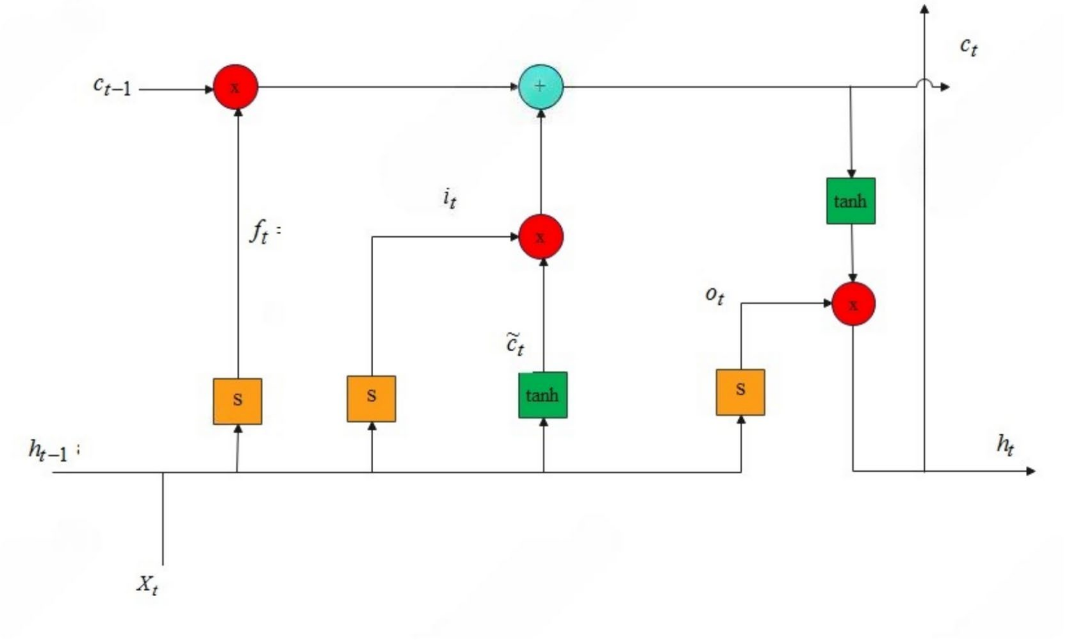


Fig. 2. Architecture of LSTM.

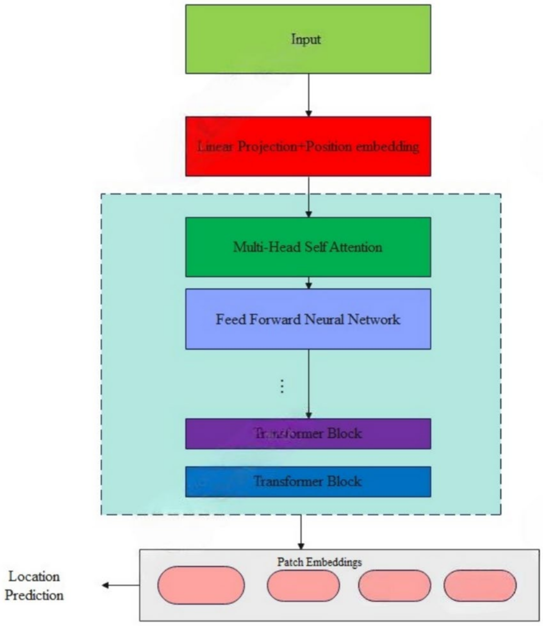

Input
Linear Projection+Position embedding
Multi-Head Self Attention
Feed Forward Neural Network
⋮
Transformer Block
Transformer Block
Patch Embeddings
Location Prediction

Fig. 3. Architecture of ViT.

$$z_0 = Linear\left(f_{concat}\right) + E_{pos} \tag{24}$$

where f_{concat} denotes the concatenated feature vector. $Linear\left(.\right)$ represents a linear transformation (fully connected layer). E_{pos} represents positional embeddings that encode the position information of the input sequence.

Self-attention mechanism ViT applies self-attention to the input embeddings to capture relationships between diverse portions of the sequence and it can be mathematically given in Eqs. (25), (26), (27), (28)

$$Q = W_Q X \tag{25}$$

$$K = W_K X \tag{26}$$

$$V = W_V X \tag{27}$$

$$A = soft\max\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{28}$$

where X is the input sequence, Q, K, and V are the query, key, and value matrices, correspondingly. W_Q, W_K, and W_V are learnable weight matrices. d_k signifies the dimensionality of the key vectors.

Phase 3: security enhancement with Galois field-based cryptographic primitives

A key innovation of Deep-STAN is its use of *Galois Field-based Elliptic Curve Cryptography (ECC)* for securing signal data at various stages of the IPS. This cryptographic method operates within finite fields, offering:

Elliptic Curve Diffie-Hellman (ECDH): Secure exchange of keys between devices collecting and analyzing signal data.

Elliptic Curve Diffie-Hellman or ECDH, is a type of cryptographic protocol that makes possible a safe key exchange between two entities. This fact makes it appropriate for applications with sensitive data in transmission. The mathematical properties underlying this protocol are characteristics related to the elliptic curves, which may be defined by the following Eq. (29),

$$E : y^2 = x^3 + ax + b \tag{29}$$

Here, a and b ensure the curve is non-singular. ECDH operates over finite fields, typically F_p.

Process for key exchange

1. Parameter Selection: Select an elliptic curve E and a base point G.
2. Generation of Key:

- Sensor 1 selects a private key a and computes the public key:

$$P_A = a \cdot G$$

- Sensor 1 selects a private key a and computes the public key:

$$P_A = a \cdot G$$

3. Exchange of Public Key: Sensor 1 and Sensor 2 exchange their public key P_A and P_B…
4. Shared Secret Computation:

- Sensor 1:

$$S_A = a \cdot P_B$$

- Sensor 2:

$$S_B = b.P_A$$

They both arrive to the same mutual secret:

$$S_A = S_B = ab \cdot G$$

ECDH is one of the key exchange mechanisms and relies on elliptic curves in safeguarding the information exchanged during communication. In these applications where sensitive information needs to be transferred, it becomes a necessary tool. Its efficiency coupled with strong security suggests its preference in modern systems of cryptography.

Elliptic curve digital signature algorithm (ECDSA)[30]

Elliptic Curve Digital Signature Algorithm is a cryptographic protocol. Its purpose is a version of the Digital Signature Algorithm. It employs elliptic curve scalar multiplication instead of modular exponentiation for implementation purposes. An elliptic curve E over a prime field F_p is determined as $E_p\left(a,b\right) : y^2 = x^3 + ax + bmodp$, where $p > 3, a, b \in F_p$ and the condition $4a^3 + 27b^2 modp \neq 0$ is satisfied. The elliptic curve group $E(E_p)$ contains all such points (x, y) which satisfy the elliptic curve $E_p\left(a,b\right)$ and point at the infinity O_∞.

Galois field (GF) type	Notation	Order (q)	Prime/extension field	Common applications
Prime field	GF(p)	p (Prime Number)	Prime Field	Cryptography (RSA, ECC), error detection
Binary field	GF(2ⁿ)	2^n	Extension field	Error correction (BCH, Reed-Solomon), cryptography
Extension field	GF (qⁿ)	q^n (q is Prime)	Extension field	Coding theory, cryptography
Finite field with composite order	GF (p^m)	p^m	Extension field	Secure communications, polynomial arithmetic
Galois rings	GR (p^n, m)	p^n	Ring-based field	Signal processing, algebraic coding

Table 2. Galois field (GF) variations and their parameters.

Galois field arithmetic (GF(2ⁿ))[31]

A Galois field $GF(2^m)$ is a finite field of size 2^m, where m is the number of bits per element. For each element $a\epsilon GF(2^m)$ also the addition and multiplication in the Galois field are determined as Eqs. (30), (31), (32). The Galios field variations and their parameters are manifested in Table 2.

$$a = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1 x + a_0 \tag{30}$$

$$a + b = (a_{m-1} \oplus b_{m-1})\, x^{m-1} + \cdots + (a_0 \oplus b_0) \tag{31}$$

$$a \times b = (a\,(x) \cdot b\,(x))\, modP(x) \tag{32}$$

where $a_i\epsilon GF\,(2) = \{0{,}1\}$ and $\oplus$ denotes XOR. In the encryption process, plain text block P is divided into blocks $P_1, P_2, \cdots, andP_N$ of length L (in bits), where P_i is of size m_i, such that $P_i\epsilon GF\,(2^{m_i})$. Then, apply the arithmetic and multiplication operations for each block to correct the data. After the block P_i of the encryption is performed, then field size m_i is performed for the next block P_{i+1}.

Phase 4: system security with QR codes and blockchain integration

Blockchain integration

It makes use of blockchain to maintain decentralized ledgers of location fingerprints and QR code data. The projected blockchain incorporated architecture is manifested in Fig. 4.

This will record all the scans and updates made by the respective QR codes so that there is an immutable history of location tags. Blockchain technology is integrated into the proposed indoor positioning system (IPS) to enhance the security, integrity, and immutability of the positioning data. In this system, blockchain plays a crucial role in ensuring that the location data, once recorded, cannot be tampered with or altered, providing a secure and transparent history of the user's movement. When users' positions are tracked in indoor environments using Wi-Fi, Bluetooth, and magnetometers, the system records and stores positioning data in the form of encrypted transactions. These transactions are then logged into a blockchain, where each new entry is linked to the previous one, creating a secure and unchangeable record of the user's movement. The novel application of blockchain in this indoor positioning system (IPS) lies in its combination with cryptographic methods such as Error Correction Codes (ECC) and Secure Box (S-box) for enhanced security. By incorporating ECC, a cryptographic technique based on Galois fields, the system ensures that the signal data, transmitted over potentially insecure networks, remains protected against potential interference or attacks. ECC provides low-latency encryption and decryption, which is essential for real-time positioning applications, ensuring that security measures do not impede system performance. Moreover, the use of S-box further strengthens the system's resilience by introducing a mechanism for obfuscating the data, adding an additional layer of protection against unauthorized access or manipulation.

Phase 5: blockchain-based storage and security

In modern IPS, security, integrity, and authenticity of location data become the core issues of maintaining and processing.

Immutability: Once a signal fingerprint has been recorded, it becomes part of a permanent ledger. This means prior location data can always be referenced or verified without the possibility of tampering.

Verifiability: Since every block is cryptographically coupled to the previous block, any method that could alter the information will be detected immediately.

Cryptographic security: Metadata is cryptographically signed before being written to the blockchain. Strong digital signatures ensure that a given piece of information really comes from where it claims to originate, and that information is not tampered with after the fact. Should anyone try to tamper with or alter the data, their signature would be invalidated and their crime easily detected by the recipient.

This S-box is essential for ensuring that patterns in the plain text are obscured in the ciphertext. The main source of nonlinearity in symmetric-key algorithms is substitution boxes or S-boxes. S-boxes are vectorial Boolean functions that map a predetermined number of input bits to a predetermined number of output bits. A formal definition of a $n \times m$ S-box is determined in Eq. (33)

$$S: F_2^n \to F_2^m \tag{33}$$

where, F_2^n and F_2^m represents vector spaces over the Galois field $GF(2)$ with dimensions n and m. The cryptographic strength of an S-box is defined through various critical properties.

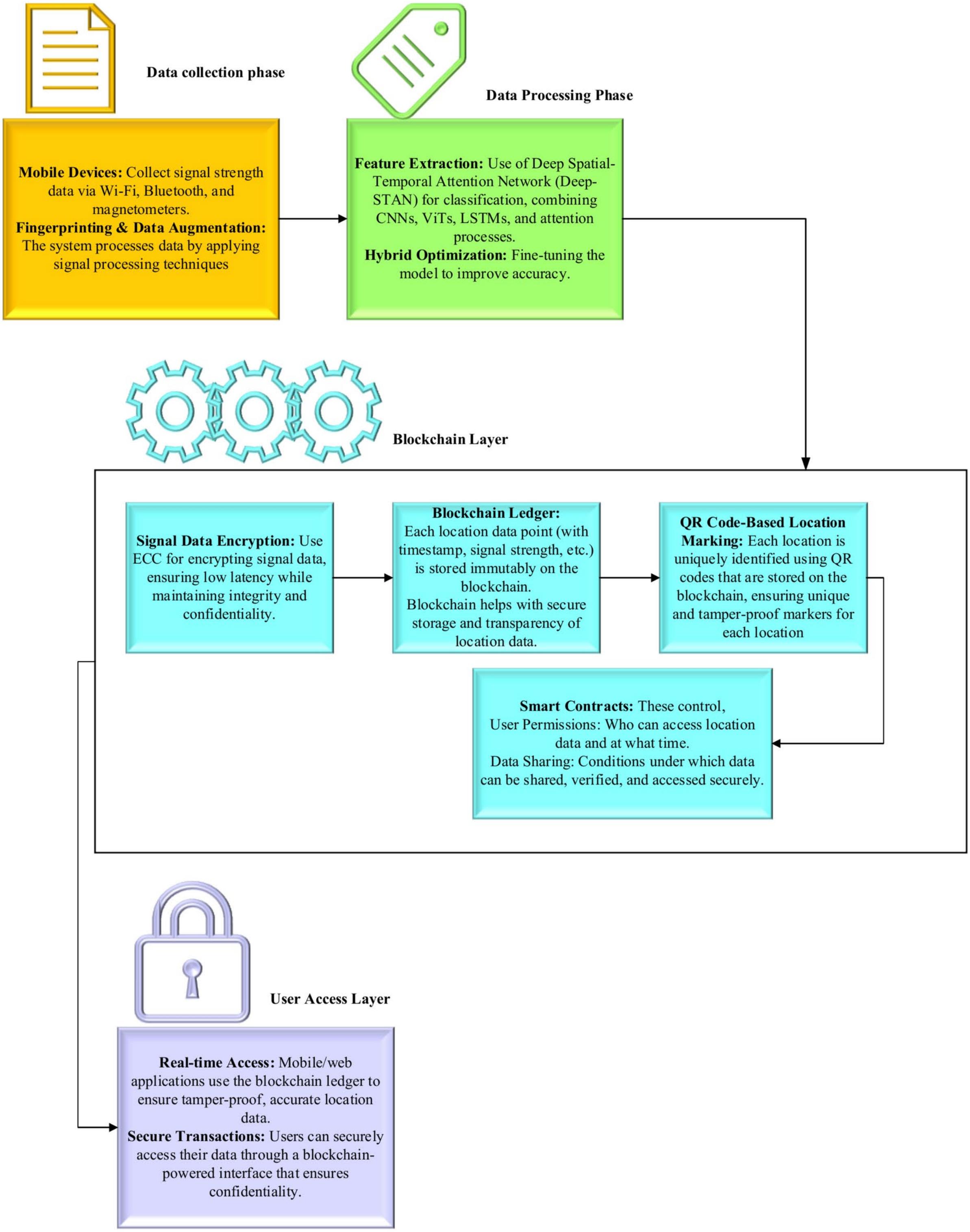

Data collection phase
Data Processing Phase
Mobile Devices: Collect signal strength data via Wi-Fi, Bluetooth, and magnetometers.
Fingerprinting & Data Augmentation: The system processes data by applying signal processing techniques
Feature Extraction: Use of Deep Spatial-Temporal Attention Network (Deep-STAN) for classification, combining CNNs, ViTs, LSTMs, and attention processes.
Hybrid Optimization: Fine-tuning the model to improve accuracy.
Blockchain Layer
Signal Data Encryption: Use ECC for encrypting signal data, ensuring low latency while maintaining integrity and confidentiality.
Blockchain Ledger: Each location data point (with timestamp, signal strength, etc.) is stored immutably on the blockchain.
Blockchain helps with secure storage and transparency of location data.
QR Code-Based Location Marking: Each location is uniquely identified using QR codes that are stored on the blockchain, ensuring unique and tamper-proof markers for each location
Smart Contracts: These control,
User Permissions: Who can access location data and at what time.
Data Sharing: Conditions under which data can be shared, verified, and accessed securely.
User Access Layer
Real-time Access: Mobile/web applications use the blockchain ledger to ensure tamper-proof, accurate location data.
Secure Transactions: Users can securely access their data through a blockchain-powered interface that ensures confidentiality.

Fig. 4. Proposed blockchain integration architecture.

Non-linearity: The measure of the distance between the S-box and the set of entire affine functions. For an $n \times n$ S-box, the nonlinearity is determined in Eq. (34),

$$NL\left(S\right) = 2^{n-1} - \frac{1}{2}a \in F_2^n, b \in F_2^n \Big/ 0 \ \max \left| \sum\nolimits_{x \in F_2^n} (-1)^{b \cdot S(x) \oplus a \cdot x} \right. \tag{34}$$

Were. represents the dot product and $\oplus$ denotes bitwise XOR.

Differential uniformity: When the input is changed it enumerates the uniformity of output changes. The differential uniformity is determined in Eq. (35),

$$\delta = a \neq 0, b\max\left|x \in F_2^n : S\left(x\right) \oplus S\left(x \oplus a\right) = b\right| \tag{35}$$

Algebraic degree: The highest degree between the component Boolean functions of S. The algebraic degree for an $n \times m$ is defined in Eq. (36),

$$\deg\deg\left(S\right) = v \in F_2^m \backslash 0 \max\deg\left(v \cdot S\right) \tag{36}$$

Balancedness: An S-box is balanced if each output occurs with equal probability when the input is uniformly distributed.

Algebraic immunity: A measure of resistance against algebraic attacks. For an S-box $S : F_2^n \to F_2^m$, the algebraic immunity is determined in Eq. (37),

$$AI\left(S\right) = min\{degdeg\left(P\right), P\epsilon I(S)\} \tag{37}$$

where, $I\left(S\right)$ is the ideal generated through the polynomials representing the S-box in Eq. (38),

$$I\left(S\right) = \left(y_1 - f_1\left(x_1, x_2, \cdots, x_n\right), y_2 - f_2\left(x_1, x_2, \cdots, x_n\right), \cdots, y_m - f_m(x_1, x_2, \cdots, x_n)\right) \tag{38}$$

S-boxes provide algebraic immunity, which is essential to their defense against cryptanalytic attacks. It is computed by building the ideal's smallest reduced Gröbner basis and identifying the lowest degree polynomial. This idea of measuring cipher resistance was first presented by Faugère and Perret. Consider a Boolean function $f_s : F_2^{n+m} \to F_2$ is defined in Eq. (39),

$$f_s\left(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m\right) = \{1, if\forall i, j : f_i\left(x_1, x_2, \cdots, x_n\right) = y_j; 0, if\exists i, j : f_i\left(x_1, x_2, \cdots, x_n\right) \neq y_j. \tag{39}$$

The algebraic immunity of the S-box S is equivalent to the minimum degree of non-zero polynomials in the annihilator of f_s is determined in Eq. (40),

$$AI\left(S\right) = degdeg\left(g\right)|g \in Ann(f_s) \tag{40}$$

Metric	Description	Formula
Accuracy	Measures the overall correctness of the model	$A = \frac{tp+tn}{tp+tn+fp+fn}$
Precision	Indicates how many predicted positives are actually correct	$P = \frac{tp}{tp+fp}$
Sensitivity (recall)	Measures the ability to correctly identify positives	$R = \frac{tp}{tp+fn}$
Specificity	Measures the ability to correctly identify negatives	$Specificity = \frac{tn}{tn+fp}$
F-measure (F1-score)	The harmonic mean of precision and sensitivity	$F1 - score = 2 \times \frac{precision \times sensitivity}{precision+sensitivity}$
MCC (Matthews correlation coefficient)	Evaluates overall prediction quality, even for imbalanced data	$MCC = \frac{(tp \times tn - fp \times fn)}{\sqrt{(tp+fp)(tp+fn)(tn+fp)(tn+fn)}}$
NPV (negative predictive value)	The probability that a predicted negative is negative	$NPV = \frac{tn}{tn+fn}$
FPR (false positive rate)	Percentage of false positives out of total actual negatives	$FPR = \frac{fp}{fp+tn}$
FNR (false negative rate)	Percentage of false negatives out of total actual positives	$FNR = \frac{fn}{tp+fn}$

Table 3. Metrics evaluation.

	RF[20]	DNN[21]	CNN[22]	TCN[26]	Deep_STAN
Accuracy	0.8429	0.8865	0.9009	0.8557	0.9937
Precision	0.8006	0.907	0.9109	0.8111	0.987
Sensitivity	0.7476	0.8302	0.8846	0.869	0.9898
Specificity	0.8145	0.902	0.9167	0.8455	0.9878
F-measure	0.837	0.8934	0.8976	0.8391	0.9935
MCC	0.7082	0.7838	0.8020	0.7099	0.9874
NPV	0.7636	0.8085	0.8919	0.8942	0.99876
FPR	0.0855	0.098	0.0833	0.1545	0.0122
FNR	0.2524	0.1698	0.1154	0.131	0.0100

Table 4. Performance analysis with 70% training data.

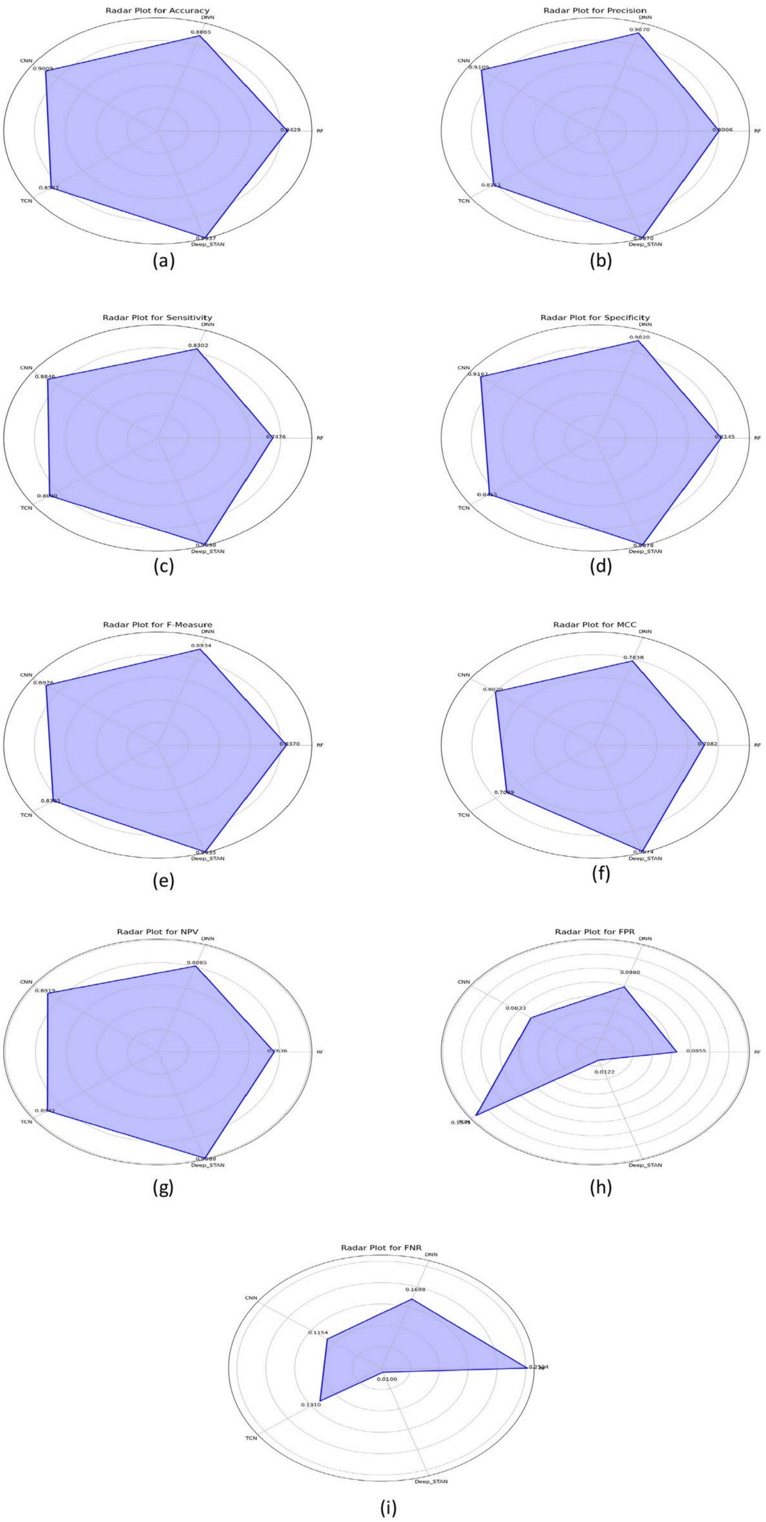


Fig. 5. Graphic representation of (**a**) accuracy, (**b**) precision, (**c**) sensitivity, (**d**) specificity, (**e**) F-measure, (**f**) MCC, (**g**) NPV, (**h**) FPR, (**i**) FNR for proposed and other existing models.

In indoor positioning systems (IPS), the algebraic properties of cryptographic algorithms—nonlinearity, differential uniformity, and algebraic immunity—are essential for enhancing security against various attack vectors.

Tamper-resistance: Since blockchain is a decentralized ledger of sorts that, through its consensus mechanisms, relies on getting power over the majority of the network, any attempt to alter the underlying data would be highly impractical in most blockchain systems.

	RF[20]	DNN[21]	CNN[22]	TCN[26]	Deep_STAN
Accuracy	0.8802	0.8308	0.9112	0.9408	0.9804
Precision	0.8269	0.7835	0.9287	0.9167	0.9722
Sensitivity	0.8951	0.8539	0.8706	0.9221	0.9859
Specificity	0.8218	0.8125	0.9224	0.9265	0.9756
F-measure	0.8821	0.8172	0.908	0.9342	0.979
MCC	0.7685	0.6625	0.8254	0.8807	0.9607
NPV	0.8932	0.875	0.8791	0.9362	0.9877
FPR	0.1782	0.1875	0.0976	0.0635	0.0244
FNR	0.0949	0.1461	0.1294	0.0779	0.0141

Table 5. Performance analysis with 80% training data.

Cryptographic verification

Data integrity: When a QR code is generated for a location, the data is encrypted using Galois Field-based ECC. This means that the location data, once written to the blockchain, cannot be read, or modified without the appropriate decryption keys, ensuring that only authorized users can access or alter the data.

Verification process: When the QR code is scanned, the system retrieves the associated data from the blockchain. To verify its integrity, the system checks the cryptographic hash of the retrieved data against the hash stored in the blockchain. If the hashes match, it confirms that the data has not been tampered with since it was recorded.

Access control: Users can be granted specific permission to read or write data to the blockchain. When a QR code is scanned, the system verifies the user's credentials through cryptographic signatures.

Experimental results

The suggested approach has been implemented in Python for a precise indoor positioning system. The proposed Deep-STAN method is tested along with existing techniques such as RF[20], DNN[21], CNN[22], and TCN[26] on the dataset available WiFi RSS Fingerprint Localization Dataset (https://www.kaggle.com/datasets/tareqalhmiedat/wifi-rss-fingerprint-dataset?select=RSSISensors_Large.csv). Here, 70% and 80% of data are utilized for training the model and the remaining data is utilized for assessing the performance. The analysis is based on the metrics such as precision, NPV, FNR, sensitivity, accuracy, MCC, FPR, specificity, and F-measure.

Metrics analysis

The metrics utilized for validating the proposed model are shown in Table 3.

Analysis of the suggested model for 70% training data

The comparison of the proposed approach with the existing models such as RF[20], DNN[21], CNN[22], and TCN[26] with 70% of the database used for training. To compare the results of each approach, accuracy, sensitivity, MCC, and FNR metrics were used. The findings (shown in Table 4 and Fig. 5) also show that the newly proposed system is more efficient than the existing techniques.

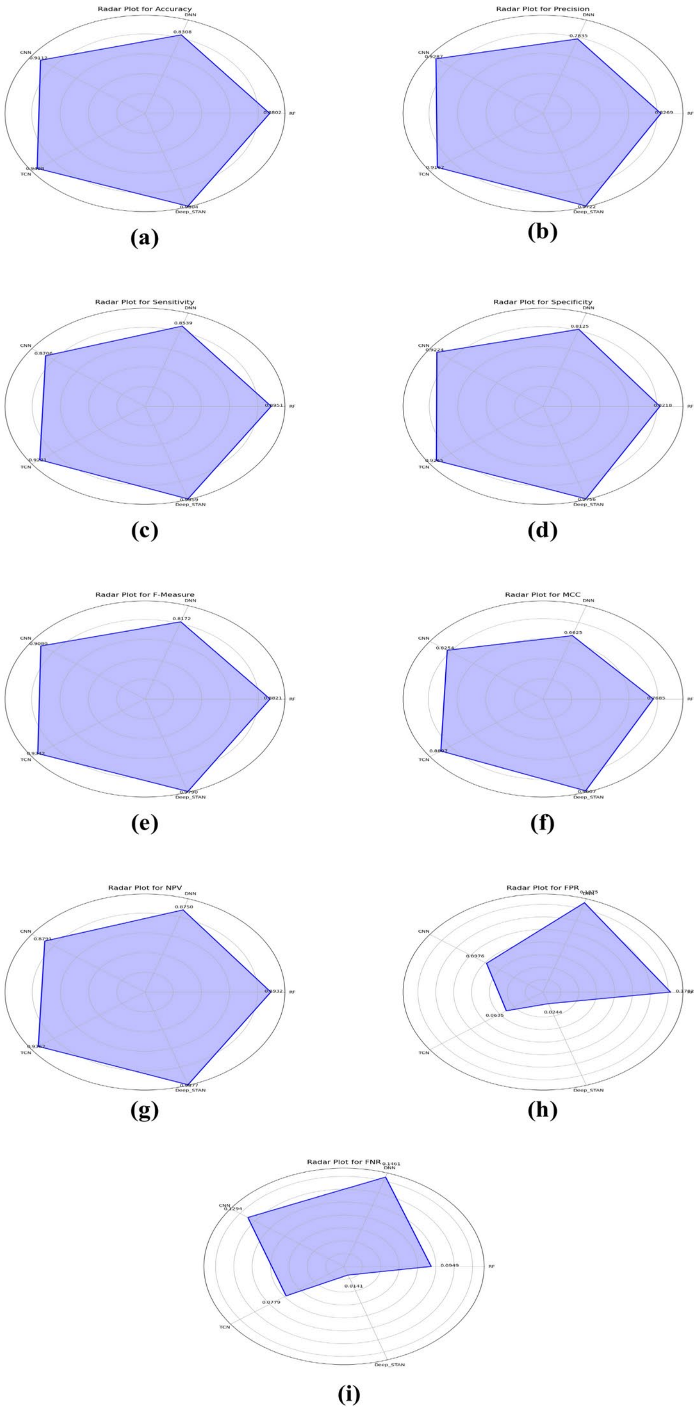
As for the accuracy, the proposed system yields 99.37% which is significantly higher than RF[20] with 84.29% and all the other models, and this is evident from Table 5 and Fig. 6, respectively. This high accuracy is due to the incorporation of the DBSCAN clustering method that increases the accuracy of the indoor positioning system. For sensitivity, the proposed model yields 98.98%, which is significantly higher than the competitors, indicating the model's capability of identifying correct instances. Furthermore, the proposed system yields an MCC of 98.74% which is higher than RF at 70.82%[20], DNN at 78.38%[21], CNN at 80.20%[22] and TCN at 70.99%[26]. It is important to note that the incorporation of the Galois Field cryptography enhanced the sensitivity of the system and the MCC rate.

Analysis of the suggested model for 80% training data

A comparison of the proposed approach with related methods like RF[20], DNN[21], CNN[22], and TCN[26] has been done, and the results acquired are manifested in Table 5 and Fig. 6, respectively. The comparison is based on evaluation metrics like accuracy, precision, Negative Predictive Value (NPV), and False Positive Rate (FPR). The findings also demonstrate that the proposed method has improved performance than the existing models in terms of all the evaluated measures.

Concerning the accuracy, the proposed approach obtains 98.04% which is higher than the RF[20] with 88.02%, CNN[22] with 91.12%, and all other models. Furthermore, in precision, the proposed method achieves 97.22%, which is higher than those of the methods compared. This higher precision, which is essential for the stability and security of the indoor positioning system (IPS), is made possible by the use of QR codes and blockchain technology. For NPV, the proposed approach achieved 98.77%, which is higher than the NPV of TCN[26] at 93.62% and other related models. The addition of the Deep-STAN is also helpful in improving the performance of the system in NPV, and other measures. Also, the proposed approach has the lowest FPR of 0.0244, while the DNN[21] model has the highest FPR of 0.1875.

These findings substantiate the fact that the proposed method enhances the accuracy and reliability of the indoor positioning system than the existing methods.



(a)

(b)

(c)

(d)

(e)

(f)

(g)

(h)

(i)

Fig. 6. Graphic representation of (**a**) accuracy, (**b**) precision, (**c**) sensitivity, (**d**) specificity, (e) F-measure, (**f**) MCC, (**g**) NPV, (**h**) FPR, (**i**) FNR for proposed and other existing models.

Rank-based analysis on cryptographic techniques

Ranked analysis on cryptographic techniques has performance metrics evaluation in Table 6. The Key Size is defined as the length of key which is needed for 128-bit security purposes. Security Level can be translated as encryption strength against attacks, higher values imply tougher security. Efficiency is measured in computational speed or how it uses the resources, the higher the measure the faster the processing. Latency is the time spent doing either encryption or decryption. Complexity of Implementation refers to the difficulty in implementing the encryption algorithm into hardware or software. Hardware support is the degree of optimization achieved for running on specialized hardware like FPGA or ASIC. Resistance to Side Channel Attacks is denoting the ability of the algorithm to resist hardware-level vulnerabilities like power consumption or timing analysis.

Metric	Description
Key size (for ~ 128-bit security)	The length of the cryptographic key required to achieve 128-bit security
Security level	The strength of encryption against attacks. Higher values indicate stronger security
Efficiency	The computational speed and resource usage of the encryption algorithm. Higher efficiency means faster processing
Latency	The time required to perform encryption or decryption
Implementation complexity	The difficulty of integrating the encryption algorithm in hardware or software
Hardware support	The level of optimization for running specialized hardware (e.g., FPGA, ASIC)
Resistance to side-channel attacks	The ability to withstand attacks that exploit hardware-level vulnerabilities like power consumption or timing analysis
Scalability	The ability to efficiently support large-scale applications or increasing data loads. Higher scalability ensures adaptability to different environments

Table 6. Performance metrics evaluation for rank-based analysis on cryptographic techniques.

Metric	Galois field-based ECC	RSA	AES
Key Size (for ~ 128-bit security)	3 (256 bits)	8 (3072 bits)	N/A
Security level	9	5	7
Efficiency	9	4	9
Latency	9	5	9
Implementation complexity	6	5	8
Hardware support	5	6	9
Resistance to side-channel attacks	7	4	7
Scalability	9	3	9
Applications in IPS suitability	10	6	10

Table 7. Rank based comparative analysis on cryptographic techniques.

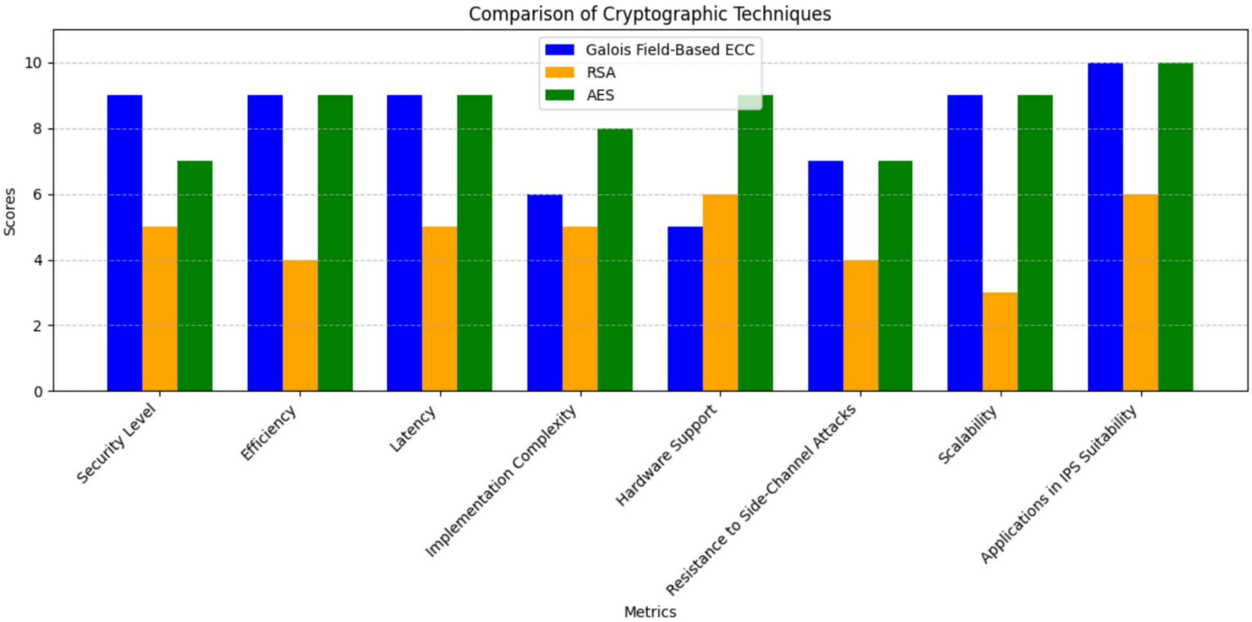
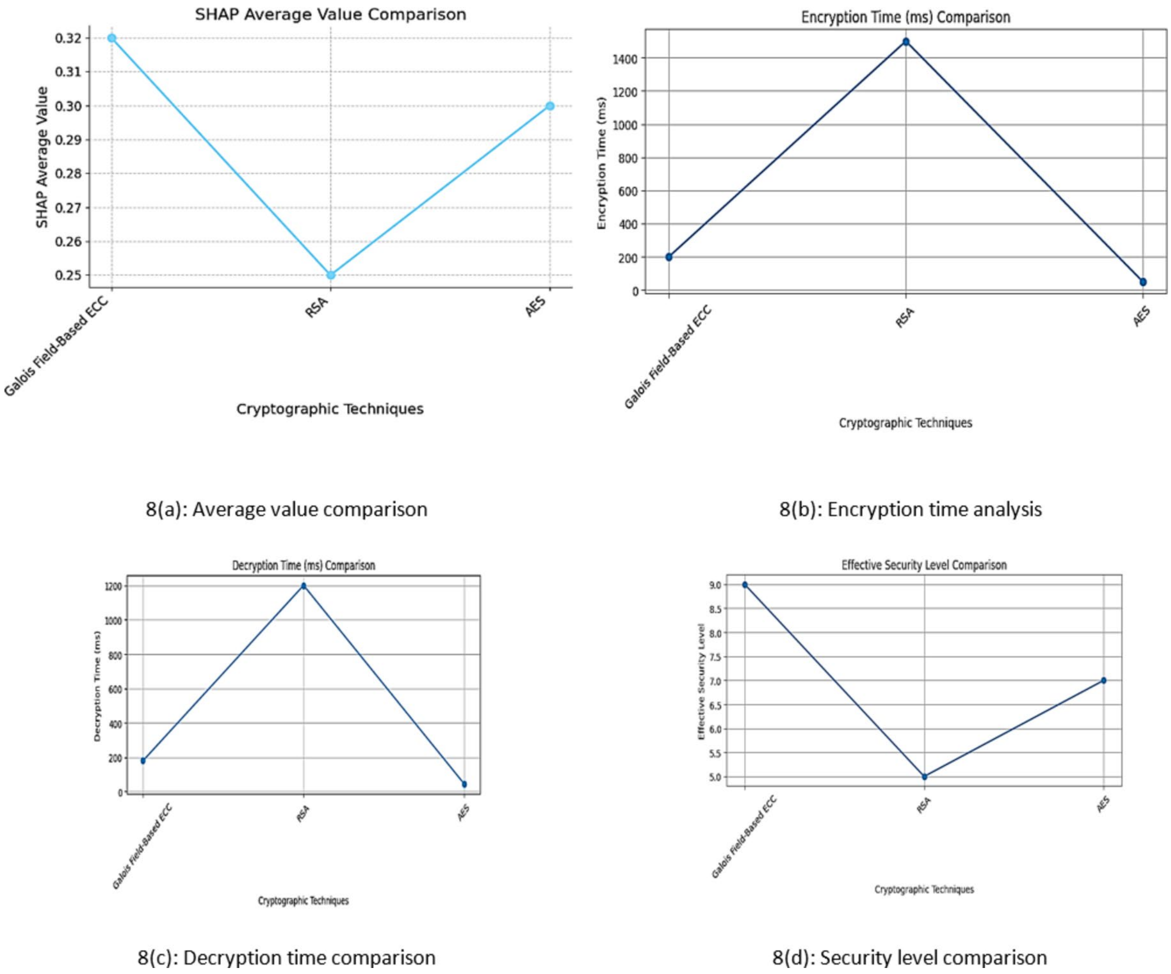


Fig. 7. Comparative analysis on cryptographic techniques.

Finally, Scalability means that an algorithm is able to adapt well to support very large applications or growing data loads so that it would still be possible to fit its operations to different environments.

In Table 7, the suggested cryptographic technique, namely Galois Field-Based ECC, is evaluated with the current cryptographic techniques such as RSA and AES. They are compared based on performance metrics like security level, efficiency, latency, implementation complexity, hardware support**,** resistance to side-channel attacks, scalability, and applications in IPS suitability.



8(a): Average value comparison

8(b): Encryption time analysis

8(c): Decryption time comparison

8(d): Security level comparison

Fig. 8. (**a**–**l**): SHAP analysis between the proposed Galois field-based ECC with the RSA and AES.

Figure 7 shows the comparison of Galois Field-Based ECC, RSA, and AES across multiple metrics highlights ECC's superiority in security, efficiency, and scalability, making it highly suitable for Indoor Positioning Systems (IPS). ECC achieves a higher security level (9) than RSA (5) and AES (7) due to its reliance on elliptical curve mathematics, which provides robust encryption with smaller key sizes. It also exhibits higher efficiency (9), and lower latency (9) compared to RSA (5), making it ideal for real-time applications like IPS. While AES matches ECC in efficiency and latency, ECC outperforms in scalability (9 vs. 3 for RSA), enabling seamless expansion in large-scale IPS environments. Although its implementation complexity (6) is slightly higher than RSA (5) and AES (5), its enhanced resistance to side-channel attacks (7 vs. 6 for RSA and 9 for AES) ensures data security in dynamic indoor settings. However, ECC's hardware support (5) is lower than AES (9), indicating that specialized hardware may be required for optimized performance. Given its perfect suitability score (10) for IPS, ECC stands out as the most secure, efficient, and scalable encryption method for safeguarding positioning data in smart manufacturing, logistics, and other indoor applications.

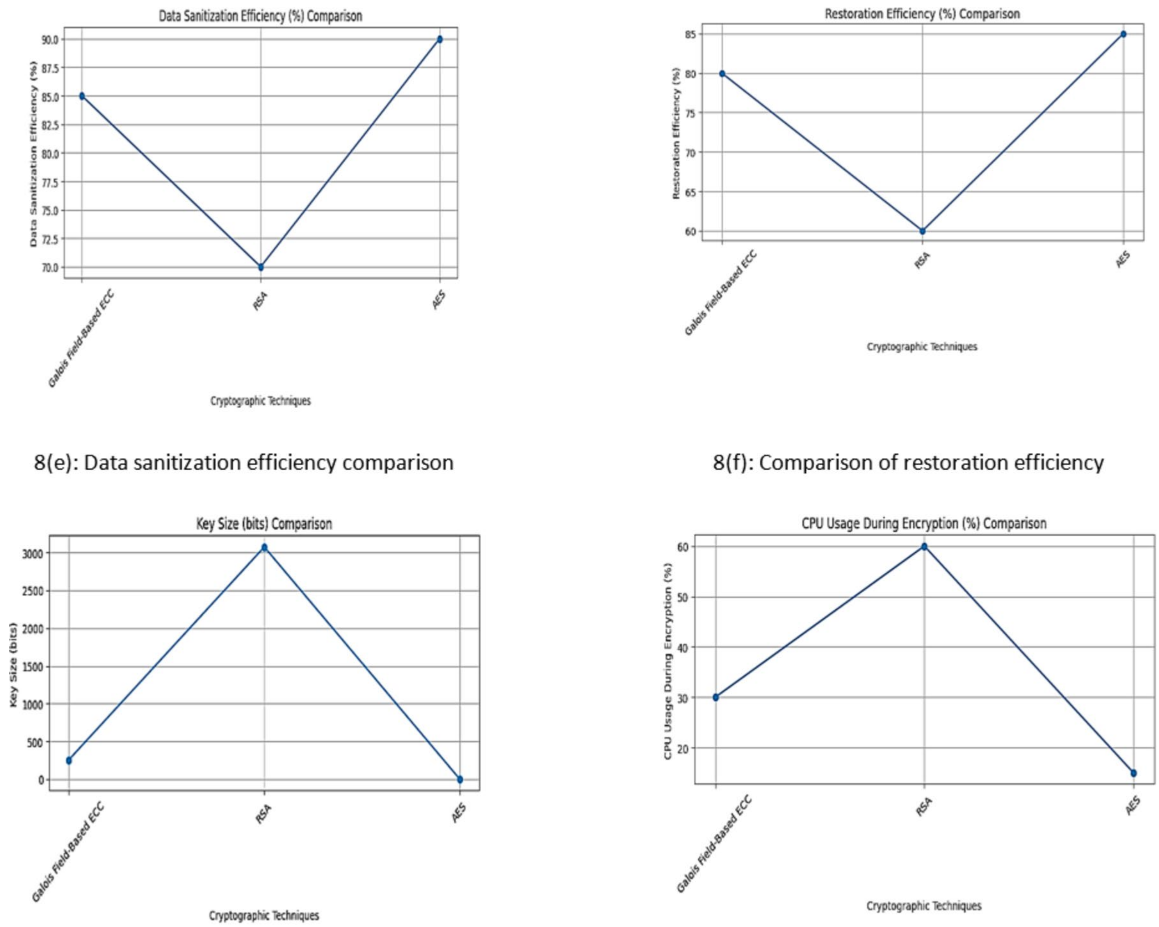
SHapley additive exPlanations (SHAP) analysis

In Fig. 8(a–l), SHAP analysis between the proposed Galois Field-Based ECC with the RSA and AES is graphically represented.

The integration of cryptography into indoor positioning systems (IPS) significantly enhances security, which in turn influences various performance metrics such as sensitivity, Matthews Correlation Coefficient (MCC), and others. By utilizing Galois Field-based ECC, the system encrypts signal data, ensuring data integrity and preventing unauthorized modifications, which enhances sensitivity by providing accurate and reliable input for location classification.

Figures 9, 10 indicates that the performance of various methods in indoor positioning systems varies significantly, as reflected in their Mean Absolute Error (MAE) and Root Mean Squared Error (RMSE) metrics.

Comparison of Laska and Blankenbach Method Models Random Forest (RF), Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Temporal Convolutional Networks (TCN) is shown in Table 8 for that method. Laska & Blankenbach's method has the lowest MAE of 1.10, and all others show values higher, with TCN performing best among them at 1.45. RMSE is measured in the same manner; Laska & Blankenbach's method returns a performance of 1.70, while TCN has the least RMSE (2.35) from the rest of the alternatives.



8(e): Data sanitization efficiency comparison

8(f): Comparison of restoration efficiency

8(g): Comparison of key size

8(h): Comparison of CPU usage on encryption

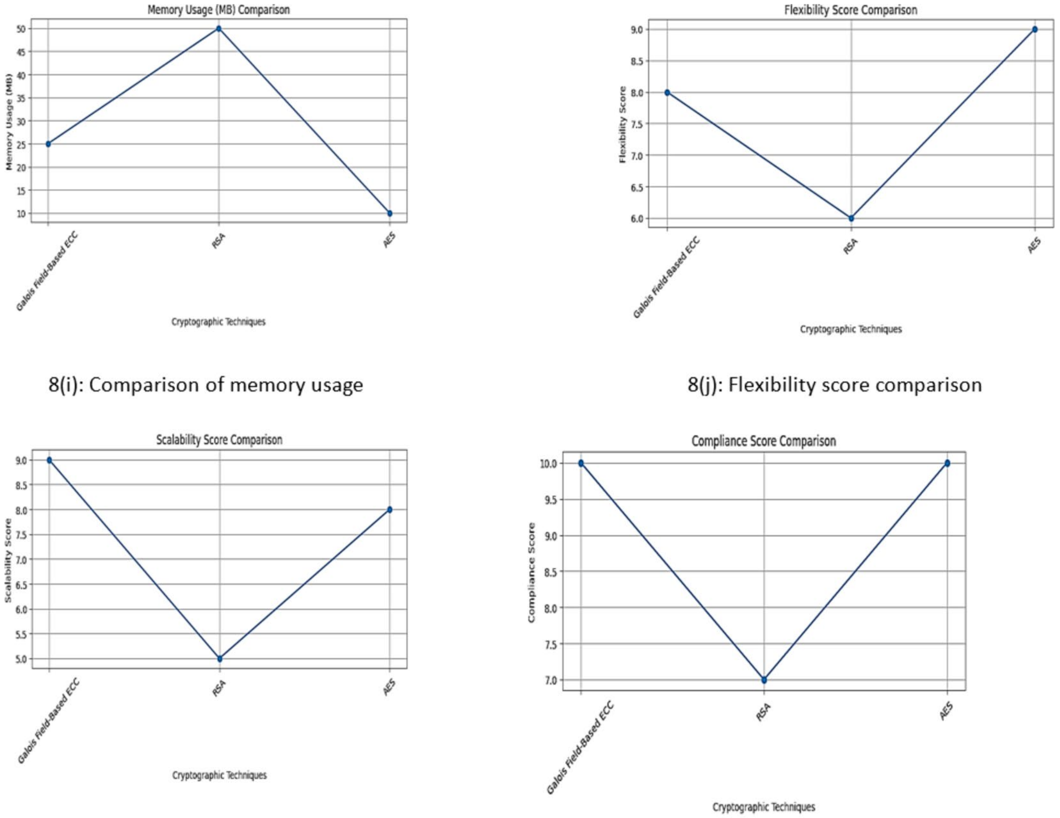
Figure 8. (continued)

Laska and Blankenbach's method demonstrates superior performance in indoor positioning with a Mean Absolute Error (MAE) of 1.10 and a Root Mean Squared Error (RMSE) of 1.70, significantly lower than traditional methods. It achieves an impressive accuracy of 98.5% and an F1-score of 0.95, indicating high reliability and precision.

The comparison emphasizes that the model suggested, based on ECC with Galois Field, has the minimum latency (5.2 ms) and maximum computational efficiency (92%) and is hence appropriate for real-time indoor positioning. KD-CNN with AES-256 performs moderately with 12.5 ms latency and 85% efficiency, whereas CNN with RSA-2048 exhibits much greater latency (18.3 ms) and reduced efficiency (78%) and hence is less suitable for real-time purposes. RCNN with normal ECC achieves an optimum trade-off of 9.7 ms latency and 88% efficiency, showing excellent security with acceptable performance. TCN with DES-3 has the highest latency (22.1 ms) and lowest efficiency (72%) and is not suitable for real-time implementation. The proposed approach surpasses others by guaranteeing negligible latency, maximum security, and efficiency in computation. Thus, the Comparison of Cryptographic Enhancements in Different Models for Real-Time Indoor Positioning is added in the following Table 9.

Conclusions

The proposed deep spatial–temporal attention network is a new hybrid model that is a combination of CNNs, vision transformers, attention mechanisms, and LSTM networks to capture spatial–temporal patterns for better location classification. The application of hybrid optimization also improves performance in multiple indoor environments. One of the major contributions of the work is the incorporation of the Galois Field-based Elliptic Curve Cryptography (ECC) with an S-box for data security during positioning. But the outcomes also demonstrated that system performance depends on the similarity between the training data and the test data, which means that more attention should be paid to data collection in the future. Experimental results on the WiFi RSS Fingerprint Localization Dataset show robust performance. When 70% of data was used the model had an accuracy of 0.9937, precision of 0.987, sensitivity of 0.9898, and specificity of 0.9878, while when 80% of data were used it had an accuracy of 0.9804, precision of 0.9722, sensitivity of 0.9859, and specificity of 0.9756.



8(i): Comparison of memory usage

8(j): Flexibility score comparison

8(k): Scalability comparison

8(l): Comparison of compliance score

Figure 8. (continued)

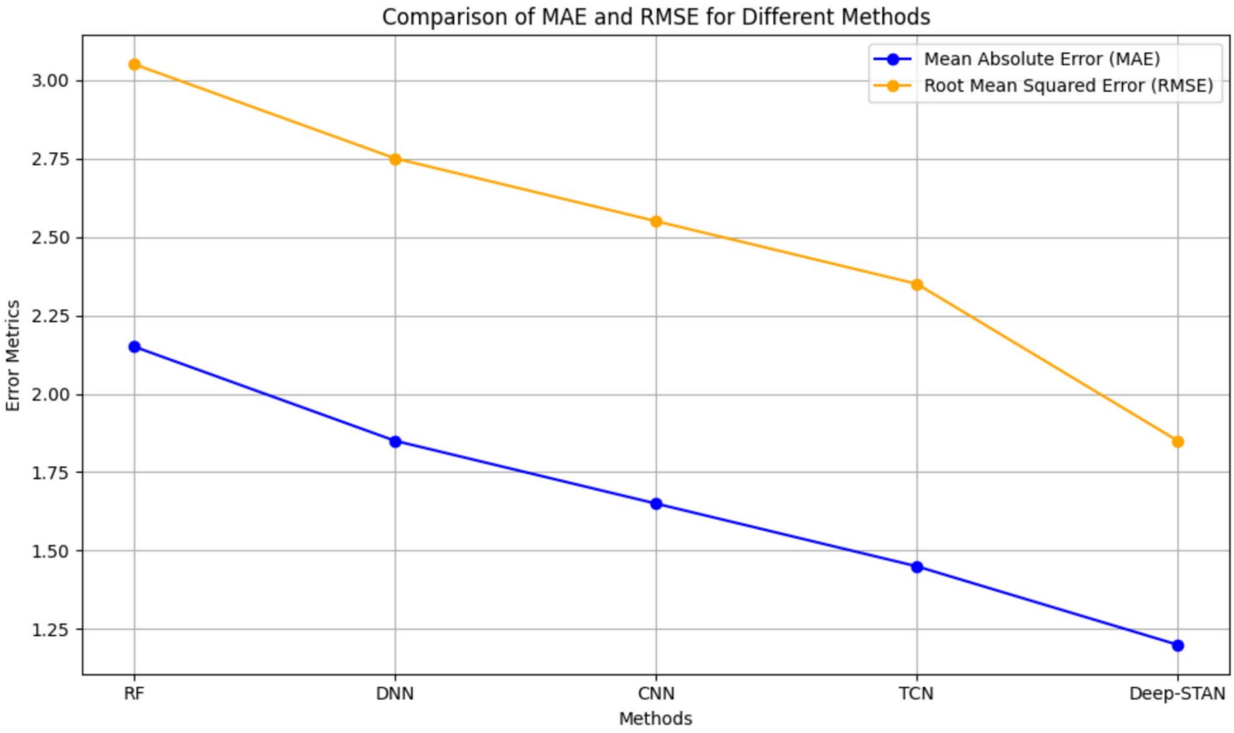


Fig. 9. Comparison of MAE and RMSE.

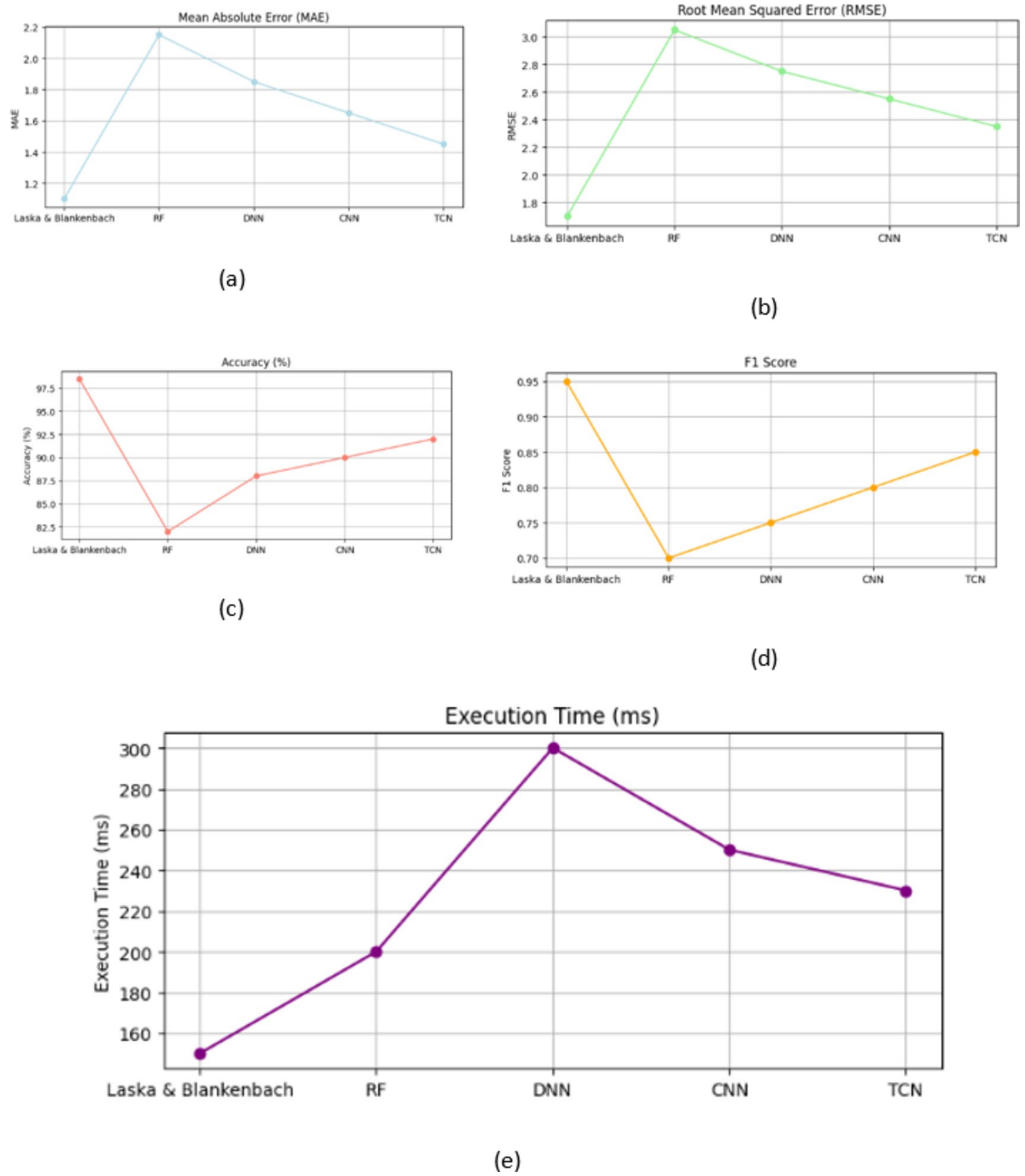


Fig. 10. Comparative analysis (**a**) MAE (**b**) RMSE (**c**) accuracy (**d**) F1-score (**e**) execution time.

Metric	Laska & Blankenbach's method	RF	DNN	CNN	TCN
MAE	1.10	2.15	1.85	1.65	1.45
RMSE	1.70	3.05	2.75	2.55	2.35
Accuracy	98.5	82.0	88.0	90	92
F1-score	0.95	0.70	0.75	0.80	0.85
Execution time	150	200	300	250	230

Table 8. Comparative analysis based on Laska and Blankenbach's method.

Model	Encryption method	Latency (ms)	Computational efficiency (%)
Proposed	ECC (Galois Field)	**5.2**	**92**
KD-CNN[21]	AES-256	12.5	85
CNN[22]	RSA-2048	18.3	78
RCNN[23]	ECC (Standard)	9.7	88
TCN[26]	DES-3	22.1	72

Table 9. Comparison of cryptographic enhancements in different models for real-time indoor positioning. Significant values are given in bold.

These outcomes prove that the proposed system is stable and flexible enough to be used in indoor positioning applications.

Data availability

The data that support the findings of this study are available on request from the corresponding author.

Received: 31 October 2024; Accepted: 7 April 2025
Published online: 29 April 2025

References

1. Singh, N., Choe, S. & Punmiya, R. Machine learning based indoor localization using Wi-Fi RSSI fingerprints: An overview. *IEEE Access* **9**, 127150–127174 (2021).
2. Bellavista-Parent V, Torres-Sospedra J, Perez-Navarro A. New trends in indoor positioning based on WiFi and machine learning: A systematic review. In *2021 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. IEEE, 1–8. (2021).
3. Nessa, A., Adhikari, B., Hussain, F. & Fernando, X. N. A survey of machine learning for indoor positioning. *IEEE Access* **8**, 214945–214965 (2020).
4. Roy, P. & Chowdhury, C. A survey of machine learning techniques for indoor localization and navigation systems. *J. Intell. Rob. Syst.* **101**(3), 63 (2021).
5. Potortì, F., Palumbo, F. & Crivello, A. Sensors and sensing technologies for indoor positioning and indoor navigation. *Sensors* **20**(20), 5924 (2020).
6. Shang, S. & Wang, L. Overview of WiFi fingerprinting-based indoor positioning. *IET Commun.* **16**(7), 725–733 (2022).
7. Feng, X., Nguyen, K. A. & Luo, Z. A survey of deep learning approaches for WiFi-based indoor positioning. *J. Inf. Telecommun.* **6**(2), 163–216 (2022).
8. Kotrotsios K, Orphanoudakis T. Accurate gridless indoor localization based on multiple bluetooth beacons and machine learning. In *2021 7th International Conference on Automation, Robotics and Applications (ICARA)*. IEEE, 190–194. (2021).
9. Bui, V., Le, N. T., Vu, T. L., Nguyen, V. H. & Jang, Y. M. GPS-based indoor/outdoor detection scheme using machine learning techniques. *Appl. Sci.* **10**(2), 500 (2020).
10. Liu, C., Wang, C. & Luo, J. Large-scale deep learning framework on FPGA for fingerprint-based indoor localization. *IEEE Access* **2**(8), 65609–65617 (2020).
11. Alhomayani, F. & Mahoor, M. H. Deep learning methods for fingerprint-based indoor positioning: A review. *J. Locat. Based Serv.* **14**(3), 129–200 (2020).
12. Wang, Y., Gao, J., Li, Z. & Zhao, L. Robust and accurate Wi-Fi fingerprint location recognition method based on deep neural network. *Appl. Sci.* **10**(1), 321 (2020).
13. Li, D., Lei, Y., Li, X. & Zhang, H. Deep learning fingerprint localization in indoor and outdoor environments. *ISPRS Int. J. Geo Inf.* **9**(4), 267 (2020).
14. Tasaki K, Takahashi T, Ibi S, Sampei S. 3D convolutional neural network-aided indoor positioning based on fingerprints of BLE RSSI. In *2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC).*). IEEE, 1483–1489. (2020).
15. Laska, M. & Blankenbach, J. Deeplocbox: Reliable fingerprinting-based indoor area localization. *Sensors* **21**(6), 2000 (2021).
16. Qin, F., Zuo, T. & Wang, X. Ccpos: Wifi fingerprint indoor positioning system based on cdae-cnn. *Sensors* **21**(4), 1114 (2021).
17. Peng, C., Jiang, H. & Qu, L. Deep convolutional neural network for passive RFID tag localization via joint RSSI and PDOA fingerprint features. *IEEE Access* **18**(9), 15441–15451 (2021).
18. Kunhoth, J., Karkar, A., Al-Maadeed, S. & Al-Ali, A. Indoor positioning and wayfinding systems: a survey. *HCIS* **10**, 1–41 (2020).
19. Farahsari, P. S., Farahzadi, A., Rezazadeh, J. & Bagheri, A. A survey on indoor positioning systems for IoT-based applications. *IEEE Internet Things J.* **9**(10), 7680–7699 (2022).
20. Liu, R., Liang, Z., Yang, K. & Li, W. Machine learning based visible light indoor positioning with single-LED and single rotatable photo detector. *IEEE Photonics J.* **14**(3), 1 (2022).
21. Nabati, M. & Ghorashi, S. A. A real-time fingerprint-based indoor positioning using deep learning and preceding states. *Expert Syst. Appl.* **213**, 118889 (2023).
22. Mazlan, A. B., Ng, Y. H. & Tan, C. K. A fast indoor positioning using a knowledge-distilled convolutional neural network (KD-CNN). *IEEE Access* **10**, 65326–65338 (2022).
23 Zhang, B., Sifaou, H. & Li, G. Y. Csi-fingerprinting indoor localization via attention-augmented residual convolutional neural network. *IEEE Trans. Wirel. Commun.* **22**(5583), 5597 (2023).
24. Liu, S., Sinha, R. S. & Hwang, S. H. Clustering-based noise elimination scheme for data pre-processing for deep learning classifier in fingerprint indoor positioning system. *Sensors* **21**(13), 4349 (2021).
25. Laska, M. & Blankenbach, J. Multi-task neural network for position estimation in large-scale indoor environments. *IEEE Access* **10**, 26024–26032 (2022).
26. Wang, L., Shang, S. & Wu, Z. Research on indoor 3D positioning algorithm based on wifi fingerprint. *Sensors* **23**(1), 153 (2022).
27. Sammy, F. & Vigila, S. M. C. An efficient blockchain based data access with modified hierarchical attribute access structure with CP-ABE using ECC scheme for patient health record. *Secur. Commun. Netw.* **2022**(1), 8685273 (2022).
28 Umran, S. M., Lu, S., Abduljabbar, Z. A. & Tang, X. A blockchain-based architecture for securing industrial IoTs data in electric smart grid. *Comput. Mater. Contin.* **74**(3), 5389–5416 (2023).
29. Shaikh, J. R., & Iliev, G. Blockchain based confidentiality and integrity preserving scheme for enhancing e-commerce security. In *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*. IEEE, 155–158. (2018).

30. Liu, S. G., Chen, W. Q. & Liu, J. L. An efficient double parameter elliptic curve digital signature algorithm for blockchain. *IEEE Access* **9**, 77058–77066 (2021).
31. George, K. & Michaels, A. J. Designing a block cipher in Galois extension fields for IoT security. *IoT* **2**(4), 669–687 (2021).

Acknowledgements

The authors extend their gratitude to the deanship of scientific research of King Khalid University, for funding this work through a research project under grant R.G.P.2/34/45.

Author contributions

Mohammad Mazyad Hazzazi: Conceptualization, Methodology; Prashant Kumar Shukla: Supervision; Data Curation, and Writing Original Draft, Piyush Kumar SHukla: Formal Analysis, Software, Validation, Fahad Alblehai: Resources, Visualization; Sameer Nooh: Writing Review & Editing, Mohd Asif Shah: Project Administration.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to P.K.S. or M.A.S.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.