





An Enhanced Privacy-Preserving Federated Learning Framework Using Attribute-Based Encryption for Smart IoT Systems

Somireddy Pavani*, Arun Sahayadhas

Department of Computer Science and Engineering, VELS Institute of Science, Technology & Advanced Studies, Chennai 600117, India

Corresponding Author Email: somi.phd@velsuniv.ac.in

Copyright: ©2025 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijssse.150508>

ABSTRACT

Received: 12 April 2025
Revised: 15 May 2025
Accepted: 24 May 2025
Available online: 31 May 2025

Keywords:

disruptive technologies, attribute based encryption, heterogeneous chaotic layered encryption, secured information system, federated learning

With the initiation of disruptive technologies like Internet of Things (IoT), Artificial Intelligence (AI), 5G/6G wireless communication, data plays a significant factor as an economic asset encompassing all aspects of existence. With maximising number of data resources, privacy breaches and information leakage have become the major bottleneck in terms of maintaining the secured data exchange that creates the major threat in every human's life. Collaborative Learning is considered to be secured learning framework which is deployed for the prevention of data leakage by allowing the user's intelligent applications to run locally. But still there exist the daunting challenges in Federated Learning (FL) frameworks when applied for the IoT based Smart Systems such as mode of sharing with designing the satisfactory incentive mechanism. In this context, novel FL framework which employs the attribute based encryption (ABE) with the Heterogeneous Chaotic Layered Encryption (HCLE) schemes that provides the fine-grained access control and assures more secure data management for the secured information sharing process in IoT based systems. The proposed FL framework encrypts the intelligent model updates through ABE-HCLE schemes, ensuring more privacy under the multiple attacks and in fully dishonest environment. The complete environment was simulated using Python 3.19 using TensorFlow-FATE FL and Charm-Crypto Libraries to deploy the proposed model in the IoT environment. The comprehensive experimentation has been conducted using BotNET datasets thereby analysing the performance of the proposed framework in leveraging the numerous threats. Extensive simulation outcomes depict the resilience of the recommended approach to varied assaults, attaining over the 95% convergence in the privacy elevated FL rounds within 70 Interaction phases and offering solid privacy measures. Using the Optimized Light Weight Learning Model (OPLWLM), to Categorise the multiple attacks achieving the average performance of 98.5% on larger datasets. ABE-HCLE relied encryption protects the weight attributes and prevents the reliable data leakages while reducing the computational cost to 0.010 seconds every round. Theoretical and empirical outcomes assure the approach's strength to elevate the privacy and offer the impressive operation in mitigating the multiple attacks in the smart IoT systems.

1. INTRODUCTION

The IoT hold a prominent place in modern urban development discussions, where the infusion of Information and Communication Technology (ICT) is crucial for revolutionizing personal living environments and lifestyles [1-3]. These systems make utilize of the advanced data analytics and wireless communication techniques to elevate the resources, enhance the service delivery and scales the life of people to comfort zone. These systems define the people's life by their capability to effectively organize enormous data constructed from the multiple sources –ranging from health records to traffic data.

1.1 Threats in existing IoT systems

Despite numerous advantages offered by these systems, the challenge of collecting data remains significant. This issue is further intensified by stringent data protection laws and the increasing emphasis on privacy, leading to the creation of fragmented data environments, often referred to as 'data islands,' within urban landscapes. Information stored on cloud platforms is vulnerable to cyber threats, thereby risking the exposure of users' sensitive information. Additionally, consolidating vast amounts of data into centralized repositories raises critical concerns regarding data privacy and security [4-6]. For example, centralized storage systems can create single points of failure, making them highly prone to network breaches and unauthorized intrusions. Furthermore,

third-party cloud service providers may not always be fully reliable, and challenges associated with key management and data storage amplify the risks. A single security breach has the potential to completely compromise data confidentiality.

1.2 FL models

FL is a kind of distributed training that prevents the direct uploads of user private data. These learning models typically utilize multiple participants to train the model with the local data which are contributed to model development while maintaining the data privacy. This distributed training model prevents the model poisoning and opt individuals for the next round of training to favour model convergence. The implementation of FL for IoT devices encounters several challenges, including substantial communication overhead, difficulties in achieving model convergence across heterogeneous ambient, and the pressing require for strong security measures to prevent data breaches regarding training processes [7-11]. To address these concerns, Privacy-Preserving FL (PPFL), a secure variant of FL, mitigates potential privacy risks by incorporating advanced procedures like differential privacy (DP), secure multiparty computation (SMPC), and homomorphic encryption (HE). DP enhances data confidentiality by initiating noise to obfuscate training data or model attributes, assuring that individual data points minimally influence the final results [12]. However, this addition of noise often slows model convergence and reduces accuracy during aggregation [13, 14]. SMPC, a cryptographic framework, enables Joint computations among multiple parties with input privacy protection. Despite its advantages, SMPC involves intricate cryptographic protocols and frequent network communications, leading to increased computational demands and latency, particularly in large-scale deployments.

1.3 Motivation and contribution of the research article

As discussed above, FL and PPFL remains susceptible to many attacks due to high computation cost implementation, high latency and non-resistant against the multiple data. To overcome this aforementioned problem, hybrid encryption scheme which combines the attribute based encryption (ABE) with heterogeneous chaotic layers(HCL) to form the high secured data transmission with the les computational overhead. The key features of the proposed hybrid encryption-based PPFL include:

1. Provides the Strong Encryption Scheme against challenging attacks such as unintentional data leakage, GAN-based inference attacks [15, 16], and membership inference attacks [17] that remain poorly handled by the present frameworks.
2. Non-Linear Chaotic behaviours are explored to provide the high resistant to the growing attacks by reducing the computational costs [18], resource constraints, and optimization issues within PPFL for real-time applications.
3. This Study explores scalability and efficiency of ABE systems for large-scale, datasets.

In this context, the key contributions of this research article are as follows:

- a. The paper proposes the Hybrid Encryption (HE)

scheme which integrates the advantages of ABE and Chaotic behaviour to ensure the security in PPFL against the attacks.

- b. The paper introduces the novel Optimized X-Long Short Term Memory (X-LSTM) architectures that combines global and local training incorporating the hybrid chaotic encryption schemes.
- c. The novel heterogeneous chaotic encryption layers which essence the advantages of the Logistic Maps, Henon and HCL Maps to form the hybrid encryption model to secure the weights of the learning framework.
- d. The recommended approach is examined by utilizing the BoTNET approach with heterogeneous and non-independent, identically distributed (non-i.i.d.) datasets to evaluate the resilience of encryption techniques and the precision of federated models under practical scenarios
- e. The computational overhead and intricacies associated with both global and local training, as well as the integration of hybrid encryption procedures, are thoroughly evaluated to establish the feasibility and applicability of the recommended approach in practical scenarios.
- f. Extensive assessment of the proposed framework utilizing performance measures like accuracy, precision, recall, specificity, and F1-score reveals its superior capability, achieving an accuracy rate of 98%, thereby surpassing existing learning systems in both consistency and performance.

1.4 Structure of the research paper

The remaining of the manuscript is structured as pursues: Section-2 depicts the relevant studies by varied researchers. The preliminaries background of ABE, Chaotic Systems are described in Section-3. The system model, dataset description, model description, proposed PPFL with the encryption schemes are illustrated in the Section-4. The experimental outcomes, results analysis and comparative investigations are depicted in Section-5. Finally, the paper is wrapped up with the future endeavours in Section-6.

2. RELATED WORKS

Narkedimilli et al. [19] introduced FL-DABE-BC, an advanced FL framework that integrated Decentralized Attribute-Based Encryption, HE, Secure Multi-Party Computation, and blockchain technology for IoT scenarios. The framework enabled secure local data encryption through DABE for decentralized authentication and performed secure computations on encrypted data via HE. Initial deep learning models were distributed via blockchain to edge devices. While the framework effectively addressed secure decentralized learning challenges in IoT environments, its performance overhead in resource-constrained environments remained a major concern.

Xiong et al. [20] proposed an effective privacy-elevated asynchronous FL scheme for multimedia data in edge-based IoT, combining revocable attribute-relied encryption and DP. The framework introduced an asynchronous weight-relied aggregation scheme to elevate training efficacy and model caliber while maintaining privacy throughout the process.

Performance evaluation showed significant improvements with 63.3% reduction in cryptography runtime and 61.9% reduction in global model aggregation time compared to existing procedures. The approach maintained competitive accuracy rates across multiple datasets while ensuring privacy preservation. However, the framework's performance in highly heterogeneous IoT environments required additional optimization.

Saidi et al. [21] developed an integrated approach combining CP-ABE and CKKS encryption to enhance privacy in FL environments without compromising performance. Secret sharing procedures protected model weights by preventing single points of failure while maintaining strong data privacy guarantees. The framework demonstrated promising results compared to existing approaches in terms of security and efficiency. Nevertheless, the system's scalability with increasing numbers of attributes and participants needed further exploration.

Nabi et al. [22] proposed a distributed privacy-preserving learning-based chaotic encryption framework designed for cognitive healthcare IoT systems. This framework ensured secure data transmission while maintaining the confidentiality of sensitive medical information. By leveraging chaotic encryption, the model enhanced security in cognitive IoT applications and addressed privacy concerns in healthcare systems. The authors validated the framework's performance using extensive experimental analysis, demonstrating its robustness and efficiency in securing IoT-based healthcare systems. However, a significant drawback of the study was the potential computational overhead associated with chaotic encryption, which might limit its scalability for large-scale IoT deployments in resource-constrained environments.

Shen et al. [23] introduced a security-elevated FL procedure incorporating homomorphic encryption and secret sharing after identifying vulnerabilities in the PEPFL framework. Their analysis uncovered an attack strategy that succeeded in retrieving private information when participant numbers remained below 300. The proposed solution implemented private gradient inference. Experimental results confirmed

significant reduction in collusion risks while maintaining uninterrupted training capability. Meanwhile, the scheme showed minimal impact on model training accuracy, but its performance was limited under varying network conditions.

Garcia-Rodriguez and Skarmeta [24] developed a comprehensive privacy-preserving attribute-relied approach for IoT device lifecycle management using p-ABC schemes with distributed issuance capability. The solution integrated with W3C's standards to facilitate adoption and compatibility with existing systems. The framework addressed device lifecycle challenges following self-sovereign principles and demonstrated practical applicability through implementation in the H2020 ERATOSTHENES project. While the framework effectively addressed IoT identity management requirements, it fell short in terms of performance optimization for resource-constrained environments.

Ma et al. [25] introduced xMK-CKKS, an enhanced variant of the MK-CKKS multi-key HE protocol tailored for secure FL. This method encrypted model updates by utilizing a collective public key prior to server transmission and required cooperation among all involved devices for decryption. Their solution safeguarded against privacy breaches from shared model updates and proved resilient to collusion between the server and participating devices. The evaluation highlighted its superior approach. However, the system's scalability with large numbers of participating devices required further investigation.

Arumugam et al. [26] proposed ECC-BFL, combining Elliptical Curve Cryptography with Blockchain-relied FL to ensure user privacy and gradient confidentiality. The framework achieved impressive metrics including 95% classification accuracy and 92% transaction speed, with significant improvements in communication and computation overhead. Comparative analysis against existing methods demonstrated superior performance across multiple parameters. The solution effectively balanced security requirements with system efficiency. Nevertheless, the blockchain component's scalability in large-scale deployments remained constrained.

Table 1. Quick summary of the different existing works

S. No	Author & Year	Technology	Key Advantages	Main Limitation
1	Narkedimilli et al. [19]	Decentralized Attribute-Based Encryption, Blockchain	Secure local encryption with decentralized authentication	Performance overhead in resource-constrained IoT
2	Xiong et al. [20]	Revocable attribute-based encryption , Differential privacy	63.3% reduced cryptography runtime	Poor performance in heterogeneous IoT
3	Saidi et al. [21]	CP-ABE, CKKS encryption, Secret sharing	Granular access control with secure computation	Limited scalability with increasing attributes
4	Nabi et al. [22]	Chaotic encryption for secure data transmission	Ensures data security and privacy in cognitive IoT systems	Computational overhead may limit scalability in resource-constrained environments
5	Shen et al. [23]	Homomorphic encryption, Secret sharing	Significant reduction in collusion risks	Poor performance in varying networks
6	Garcia-Rodriguez and Skarmeta [24]	p-ABC schemes, W3C Verifiable Credentials	Compatible with W3C standards	Poor resource optimization
7	Ma et al. [25]	Multi-key HE protocol	Superior communication costs	Increased computational complexity
8	Arumugam et al. [26]	Elliptical Curve Cryptography, Blockchain	95% classification accuracy	Limited blockchain scalability
9	Lin et al. [27]	Attribute-based access control, Federated deep learning	High data integrity	Scalability issues in dynamic setups
10	Islam and Madria [28]	Revocable ABE, DMG-SDS	Unlimited user revocation	High computational cost

Lin et al. [27] introduced SACM, an attribute-relied Secure Access Control Mechanism for IoT-Health leveraging FL. The framework innovatively correlated users' social attributes with trust levels based on social influences using graph convolutional networks. Access permissions were determined through trust thresholds specific to each occupation, with federated deep learning optimizing control parameters. Experimental results showed effective access control. However, the system's performance in highly dynamic social networks required additional investigation.

Islam and Madria [28] proposed a revocable collusion-resistant ABE scheme supporting unlimited user revocation without affecting non-revoked users' secret membership keys. The framework extended to DMG-SDS, enabling dynamic multi-group operations while maintaining key integrity. Performance assessment showed significant advantages over contemporary schemes in multi-group data sharing scenarios. The approach effectively addressed security requirements while maintaining practical implementation capabilities. Meanwhile, the system's efficiency with extremely large user groups might benefit from further optimization. Table 1 highlights the summary of distinct existing procedures.

3. SYSTEM OVERVIEW

This section details about the overview of attribute encryption system used as the hybrid model for the proposed framework.

3.1 Attribute based encryption system (ABE)-An overview

Attribute-based encryption (ABE) is a cryptographic method that offers precise control over who can access encrypted data. Unlike traditional encryption procedures, where a secret key is required for decryption and only authorized individuals can utilize it, ABE enables encryption using attributes such as an Individual's role or location. The ability to access the encrypted data depends on the parameters of the individual making the request. In 2005, Abebe and Hussain [29] proposed ABE as a framework for managing data access through the use of attributes. Since then, ABE has gained considerable attention in research and found applications in areas like wireless networks, IoT and cloud computing.

ABE provides varied benefits compared to conventional encryption scheme. It desires for detailed utilization control, enabling the granting or revocation of access rights which relies on changing conditions like user role updates. This characteristic makes ABE especially applicable in IoT settings, where many devices with diverse utilities and access levels interact within a network. Additionally, ABE ensures data confidentiality and privacy, as only those whose features meet the access policy are able to decrypt the data. This means that whenever if a malicious entity gains entry to the encrypted data, they cannot decrypt it without possessing the required attributes. While, ABE has few drawbacks. For instance, the decryption process can be computationally demanding, as it involves evaluating complex access policies. Furthermore, the use of ABE can lead to larger cipher texts, which may pose challenges for storing and transmitting large datasets over the network.

4. PROPOSED METHODOLOGY

Figure 1 shows the proposed framework deployed for PPFL to mitigate the different attacks. The suggested framework consists of four major parts such as Key generation, Data Collection from IoT devices, Centralised Model design using Optimized X-LSTM model and proposed PPFL training model. The Thorough description of the recommended approach is as pursues

4.1 System model

As portrayed in Figure 1, the system model comprises of pursuing components: 1) Key Manager 2) Cloud Manager 3) Communication layers 4) User Nodes

a. Key manager: The key manager (KM) generates the keys for the both the central server and IoT systems using ABE-HCL techniques. This module automatically computes the system public key and system master keys which are distributed to the nodes and cloud for formulating the strong encryption and decryption process.

b. Cloud Manager: This layer of cloud Seeks to create the global approach by opting a set of attributes that produce various attribute value keys for potential entities. The cipher text is generated by the models are generated using the Cloud manager.

c. Communication layer: This layer enables for transmission of the encrypted local models and weights from the nodes to cloud layer.

d. User Nodes: The user nodes are IoT nodes which are used to collect the local data thereby training the local schemes and sends to the cloud server in an encrypted manner.

4.2 Centralized model design

The centralized model design for the recommended approach consists of Extended Long Short-Term Memory and Optimized Learning networks for the detection of multiple attacks.

4.2.1 Recurrent Neural Networks (RNN)-An overview

In RNN, the hidden layers of one network are linked to the hidden layers of further nodes in a new network. RNNs are primarily designed for applications involving time series and large-scale data analysis because they can recall past information and encode historical data within a few milliseconds. This approach allows for the direct creation of graph structures using nodes and their sequences. Consequently, it can demonstrate dynamic behaviour for synchronizing sequences. By utilizing an internal state (memory), RNNs process input sequences, leveraging prior data to forecast future outcomes. However, in practical service platforms, while the gap among past and future data is significant, this approach hurdles to retain meaningful information from earlier data, causing to the vanishing gradient challenge. As a result, the outcomes may not be ideal for real-time scenarios. To resolve this issue, the performance of RNNs has been enhanced through the constructing of Long Short-Term Memory (LSTM) networks [30].

4.2.2 LSTM-An overview

LSTM networks are widely used learning models, known for their flexibility in handling memory and reliability for large databases. The LSTM architecture is given in Figure 2.

output state is L_t (with its preceding state L_{t-1} , the gates' states are represented by k_t , T_f , and T_o). The structure of LSTM operates such that both L_t and h_t are transmitted to the subsequent NN layer in the Recurrent Neural Network (RNN). The LSTM mechanism merges the output of the prior unit with the recent input state, where the output and forget gates facilitate updates to the memory. To determine G_t and h_t , the pursuing equations are utilized.

$$I.G: k_t = \theta(L_t^i \cdot D_t + L_h^i \cdot e_{t-1} + s_i) \quad (1)$$

$$F.G: T_f = \theta(G_t^f \cdot D_t + L_h^f \cdot e_{t-1} + s_f) \quad (2)$$

$$D.G: T_o = \theta(L_t^o \cdot D_t + L_h^o \cdot e_{t-1} + s_o) \quad (3)$$

$$V.I: \widetilde{T}_C = \tanh(L_t^c \cdot D_t + L_h^c \cdot e_{t-1} + s_c) \quad (4)$$

The weight matrices among the input gates and output layers are denoted as $L_t^0, L_t^f, L_t^i, L_t^c$, while the weight criteria among the hidden and input layers are represented by $L_t^0, L_t^f, L_t^i, L_t^c$. The bias vectors are labelled as s_i, s_f, s_o, s_c and the hyperbolic function \tanh is applied. The output state of the cell is ascertained by the pursuing formulas:

$$T_c = k_t * \widetilde{T}_C + T_f * T_{t-1} \quad (5)$$

$$e_t = T_o * \tanh(T_c) \quad (6)$$

The equation above yields the final output score.

4.3 Extended LSTM model –Its working mechanism

To elevate the storage capacity of LSTMs, the memory cell is extended from a scalar $c \in \mathbb{R}$ to a matrix $C \in \mathbb{R}^{d \times d}$, allowing for retrieval via matrix multiplication. At a given time, t , a pair of vectors—a key $k_t \in \mathbb{R}^d$ and a value $v_t \in \mathbb{R}^d$ stored, following the terminology used in Transformers. Subsequently, at time $t+\tau$, the value v_t is acquired using a query vector $q_{t+\tau} \in \mathbb{R}^d$. This mechanism aligns with the framework of Bidirectional Associative Memories (BAMs). The process employs the covariance update rule to encode the key-value pairs effectively.

$$C_t = C_{t-1} + v_t k_t^T \quad (7)$$

We presume a layer normalization step is performed prior to projecting inputs into key and value spaces, ensuring these projections have a mean of zero. The rule for updating the covariance matrix is designed to optimize the separability of retrieved binary vectors. This optimal separability corresponds to achieving the highest possible signal-to-noise ratio. Enhanced separability can be achieved by restricting acquired to pairwise interactions and accepting the quadratic computational complexity associated with attention mechanisms.

Building on this foundation, we embed the covariance update rule within the LSTM architecture. In this setup, the forget gate f_t acts as a decay factor, controlling how much of the previous memory is retained. The input gate i_t regulates the learning rate by controlling the flow of new information into memory. The output gate O_t adjusts the influence of the current memory state on the output. These gates are standard in LSTM architectures and are integrated here to manage the

dynamics of memory update and retrieval.

Within this matrix memory framework, the normalizer state n_t is defined as a weighted summation of key vectors, with weights determined by the input gate and the cumulative influence of all subsequent forget gates. This normalizer state effectively captures the dynamics of gate strengths. Given that the dot product among the query and the normalizer state can approach zero, taking the magnitude of this dot product and setting a minimum threshold (commonly 1.0) to ensure stability. Consequently, the forward propagation in the mLSTM model proceeds as:

$$C_t = f_t C_{t-1} + i_t v_t k_t^T \quad (8)$$

Cell state

$$n_t = f_t n_{t-1} + i_t k_t \quad (9)$$

Normalizer state

$$h_t = o_t \odot \widetilde{h}_t, \widetilde{h}_t = C_t q_t / \max\{|n_t^T q_t|, 1\} \quad (10)$$

Hidden state

where, the intermediate vectors are computed as:

$$q_t = W_q x_t + b_q \quad (11)$$

Query input

$$k_t = \frac{1}{\sqrt{d}} W_k x_t + b_k \quad (12)$$

Key input

$$v_t = W_v x_t + b_v \quad (13)$$

Value input

Gate activations are calculated using:

$$i_t = \exp(\widetilde{i}_t), \widetilde{i}_t = w_i^T x_t + b_i \quad (14)$$

Input gate

$$f_t = \sigma(\widetilde{f}_t) \text{ OR } \exp(\widetilde{f}_t), \widetilde{f}_t = w_f^T x_t + b_f \quad (15)$$

Forget gate

$$o_t = \sigma(\widetilde{o}_t), \widetilde{o}_t = w_o^T x_t + b_o \quad (16)$$

Output gate

The mLSTM framework, similar to the traditional LSTM, accommodates multiple memory cells. In the context of mLSTM, having multiple heads is synonymous with having multiple cells due to the absence of memory integration.

4.4 X-LSTM architecture

An xLSTM block is designed to non-linearly condense past information within a high-dimensional space, which enhances the ability to distinguish between different historical contexts or sequences. This separation of histories is crucial for accurately predicting the subsequent sequence element, such as the next token. The approach is grounded in Cover's Theorem [31], which suggests that patterns non-linearly embedded into a higher-dimensional space are more likely to attain linear separation compared to the original space.

The advantages of two configurations for residual block architectures:

1. **Residual Block with Post Up-Projection:** Similar to the design in Transformers, this configuration

initially condenses past information non-linearly within the original space. It then projects this representation linearly into a high-dimensional space, applies a non-linear activation function, and afterward, restores it to the original space.

2. **Residual Block with Pre Up-Projection:** Aligned with the architecture of State Space Models, this variant starts by projecting the data linearly into a high-dimensional space, where the past is non-linearly summarized. The representation is then linearly mapped back to the original space.

4.5 Optimized learning model

In this work, Ashera CAT Swarm Optimized Deep Learning Networks, inspired by Cat Swarm Optimization [32], are used for the effective prediction of multiple attacks in IoT systems. Training and testing is done using 10-fold cross-validation to reduce the bias vectors during testing. The thorough representation of the approach is explained below.

4.5.1 Ashera CAT Swarm Optimization model

The Ashera CAT Swarm Optimization (CSO) algorithm is a contagious, single-objective optimization technique aspired by the traits of Ashera cats, particularly their resting and tracing actions. Ashera cats appear to be lethargic, spending most of their time resting. Despite their idle state, they maintain heightened awareness of their environment. During these periods of rest, they stay alert and observant, and upon recognition of a target, they quickly move towards it. The CSO approach mimics this dual behavior by combining these two characteristics into its framework. The algorithm operates in two phases: the seeking and tracing modes. Each Ashera CAT in the algorithm represents a potential solution, with a position in the search space, a fitness value, and a flag. The location consists of multiple dimensions, each with an associated velocity, while the fitness value indicates the quality of the resolution. The flag serves to categorize the cat as either in seeking or tracing mode. In practice, the number of Ashera

CATs participating in each iteration needs to be specified. These cats are processed through the approach, with the best performing one at every loop being stored in memory. The cat with the highest fitness at the final loop is selected as the solution. Figure 3 depicts the flow of the Ashera CSO approach, and the workings of the seeking and tracing phases are further explored in the subsequent segment.

Seeking Modes. This phase mimics the dormant trait of Ashera cats, here four key factors are crucial: the memory pool search (MPS), the search scope of the chosen dimension (SSCD), the number of dimensions to alter (NDA), and the consideration of self-position (CSP). These parameters are all adjusted and established by the individual through a trial-and-error process.

SMP determines the quantity of potential positions to be considered by an Ashera CAT, essentially defining how many candidate locations are generated, from which one will be selected for the Ashera CAT's next move. For instance, if SMP is set to 5, five random positions will be generated for each Ashera CAT, and one will be chosen as the next location. The method used to randomize these locations depends on the values of the varied dual attributes: CDC and SRD. CDC indicates the proportion of dimensions to be altered, which ranges from 0 to 1. For instance, if the search space has five dimensions and CDC is set to 0.2, then four dimensions will be randomly chosen for modification, leaving the remaining one unchanged. SRD specifies the mutation ratio for the chosen dimensions, indicating how much of the selected dimensions (as determined by CDC) will be adjusted. Finally, SPC is a Boolean flag that indicates while the recent location position of an Ashera CAT should be included as a candidate for the upcoming loop or not.

If the SPC flag is enabled, for each Ashera CAT, the system should generate (SMP-1) candidates instead of the usual SMP. This adjustment accounts for the recent location being included as one of the candidates. The steps involved in seeking phase are outlined as pursues:

- (1) Initiate multiple SMP duplicates of the recent location of Ashera CAT.

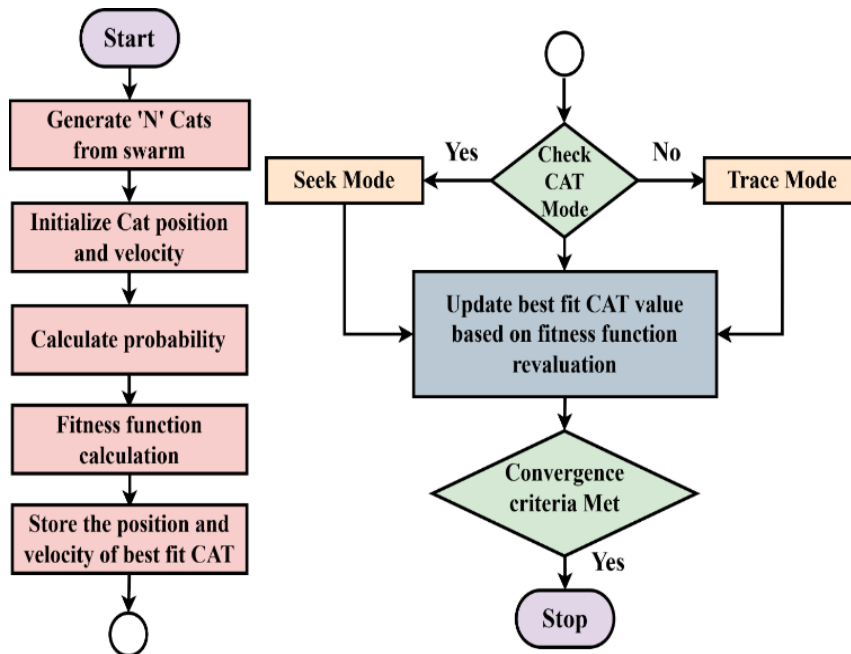


Figure 3. Entire working process for the Ashera CAT swarm optimization

(2) For every instance, randomly choose a set number of CDC dimensions to undergo mutation. Additionally, randomly increase or decrease the SRD values from the existing values, which will interchange the previous locations, as described in Eq. (17).

$$x(new_cat) = (1 + rand + SRD) * x(old_cat) \quad (17)$$

where, $x(new_Ashera\ CAT)$ is new Ashera CAT's new location, $x(old_Ashera\ CAT)$ is Ashera CAT's initial location and $rand$ is random interval of time among $[0,1]$.

The Fitness Function (FF) is calculated as per the following expression (18), and the candidate location is chosen which relies on the highest probability corresponding to the Fitness Function value. This approach selects the position with the highest FF, ensuring the optimal candidate is selected based on its fitness ranking.

$$P(i) = |(FF(i) - FF(b)) / (FF_{max} - FF_{min})| \quad (18)$$

The fitness of the recent Ashera CAT is denoted as $FF(i)$, while $FF(b)$ represents the total population of Ashera CAT. FF_{max} indicates the highest value of the FF, and FF_{min} refers to the lowest value of the FF.

Tracing Modes. In this phase, the trait of Ashera Cats is replicated by mimicking their tracing actions. Initially, random velocity values are assigned to each dimension of an Ashera Cat's position. However, in subsequent iterations, the velocity values must be modified accordingly. This method of movement for Ashera Cats is described as pursues:

(i) Upgrade velocities (V (ASHERA CAT)) for all dimensions regarding to below Eq. (19):

$$V(CAT) = V(CAT) + a * c (x(new_cat) - x(old_cat)) \quad (19)$$

where, a and c are constants.

4.5.2 Hyper parameter tuning process

The proposed Optimized are utilized to optimize the weights of X_LSTM dense networks. Initially, the hyperparameters are opted at random and moved to the X_LSTM training network. The novel FF which is coined based on ACO model is given in Eq. (20).

$$Fitness\ Function = Min(MSE(Predicted\ value - Actual\ Value)) \quad (20)$$

The fitness function is computed based on the minimum error which is measured by MSE (mean Square Error) among the predicted value and actual value. Once the hyperparameters are optimized using Eq. (16), dense training layers classifies data into normal and attacks. The complete phase of operation of the recommended approach is represented in Algorithm-1.

Steps	Algorithm-1 // Pseudo Code for the Proposed Model
01	Input = Bias weights, Hidden layers, Epochs, Learning Rate
02	Output: Prediction of Normal/Attack
03	Randomly allocate the bias weights, learning rate, hidden layers and epochs.
04	Commence the three parameters such as
05	While (true)

06	Compute the output from XLSTM cells utilizing Eq. (8) to (16)
07	Compute the Fitness function utilizing the Eq. (19)
08	For $t=1$ to N where N = Maximum Iteration
09	Allocate the bias weights and input layers by Eq. (8) to (16)
10	Compute the fitness function by utilizing Eq. (19)
11	If (Fitness function = = Eq. (19))
12	Go to Step 17
13	Else
14	Go to Step 08
15	End
16	End
17	If (output value ≤ 1)
18	//Normal is Ascertained
19	Else if (output value > 1 && output value ≤ 2)
20	// Attacks are Ascertained
21	Else
22	Go to Step 09
23	End
24	End
25	End

4.6 FL model for the proposed network

FL is considered to be promising framework that used to construct the privacy-preserving learning models that guards the privacy. In the progress of learning framework, global model based on the ACAT-X-LSTM model is trained with the help of other participants and the decentralized data overseen by the central cloud/server. The individual receives a common global scheme from the server and execute training on their individual local datasets. Afterward, they pass the weights or gradients of their locally trained scheme to the task publisher for updating the global approach. (Algorithm-2 presents the working mechanism of the proposed model). Specifically, Fed-X-LSTM is formulated with the objective function is rewritten relied on the Fed-Avg functions which are represented as follows:

$$f(w) = \sum_{j=1}^j \frac{N(i)}{N} * F(W) \quad (21)$$

The algorithm follows a straightforward approach, where j portrays the total count of participants, and $n(i)$ portrays the count of training samples for the j -th participant. Initially, specific nodes are chosen within each batch for training across epochs. Subsequently, each node transmits its weight upgrades to the central server.

$$w < - - - w < - - - \eta \alpha L(w, h) \quad (22)$$

The server then gathers all the w_{t+1k} values to compute the weighted average of the updated global w_{t+1} , which is subsequently transmitted to each participant.

$$(w) = \sum_{j=1}^j \frac{N(i)}{N} * W(j + 1) \quad (23)$$

Steps	Algorithm-2 //FL for the Recommended Optimized Model
1	The Central transfers sends a weights of the model to each user nodes in an Encryption framework (Section-4.7).
2	All the weights are encrypted by using proposed

encryption schemes (As mentioned in 4.7).

- 3 Every Ch-IoT nodes trains the retrieved weights utilizing decryption process using their own private data and transfers to server in an encrypted.
- 4 The server systems aggregate the partial models using Eq. (23) through their parameters and builds the federated model.
- 5 The main server examines a stopping criterion by assessing the FF, represented by Eq. (22). If the criterion is met, the FL (FL) progress wraps up; instead, it begins again from step 1.

4.7 HCL schemes for techniques

As discussed PPFL requires more security in sharing of the private data to train the federated model. Therefore, the chaotic preserving procedures are used in FL. In this research, chaotic procedures are utilized along with ABE for maintaining the privacy and encrypting the data from the nodes to server. To establish the chaotic principles, a heterogeneous combination of the Henon and HCL maps is employed in the proposed framework. The multi-HCL attractors are favoured over varied residing chaotic maps like circle, sine, logistic maps and tent due to their superior randomness and the capability to manipulate chaotic trajectories by adjusting initial phases.

4.7.1 HCL attractors

Dynamic systems that exhibit multi-HCL attractors often demonstrate more intricate behaviour compared to typical chaotic systems with single-HCL attractors. The equation governing the state space for an automatic chaotic system is expressed as:

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (24)$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (25)$$

$$\dot{x}_3 = ex_3 - fx_1x_2 \quad (26)$$

The above Eqs. (24)-(26) could be revised by the adding the hyperbolic equation $p_1 \tanh(x_2 + g)$ which is given in below equations:

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (27)$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (28)$$

$$\dot{x}_3 = ex_3 - fx_1x_2 + p_1 \tanh(x_2 + g) \quad (29)$$

Chaotic attractor is acquired when $a = 2$, $b = 6$, $c = 6$, $d = 3$, $e = 3$, $f = 1$, $p_1 = 1$, $g = 2$ and the chosen initial factors are $[x_1(0), x_2(0), x_3(0)] = [0.1, 0.1, 0.6]$.

When the hyperbolic function is applied originally with a parameter value of $g=-3$ and the starting conditions $[0.1, -0.1, -0.6]$, a double-HCL attractor is observed, as portrayed in Figure 4.

4.7.2 Henon maps-its principles of working

Henon Maps [33] are the disruptive quadratic and non-linear maps given by its characteristic equation.

$$X_{n+1} = 1 - aX_n^2 + Y_n \quad (30)$$

$$Y_{n+1} = 1 - bX_n \quad (31)$$

The classical maps rely on the dual parameters a and b which has the values of $a=1.4$ and $b=1.3$. For the classical values, Henon map is chaotic. For the varied values of a and b , henon maps may exhibit the chaotic behavior which can be identified with the several times of iteration. Figure 5 represents the chaotic behavior of the henon maps using classical values.

In the proposed HCL techniques, HCL and henon maps are combined to form the ensemble techniques. The random output from the henon maps will be the input to the HCL attractors. The integration of the two maps leads to the high randomness outputs that can be used to create the strong keys against the multiple keys. Figure 6 shows the bifurcation diagram for the proposed HCL technique. The mathematically HCL is expressed by modifying the Eq. (30) and Eq. (31).

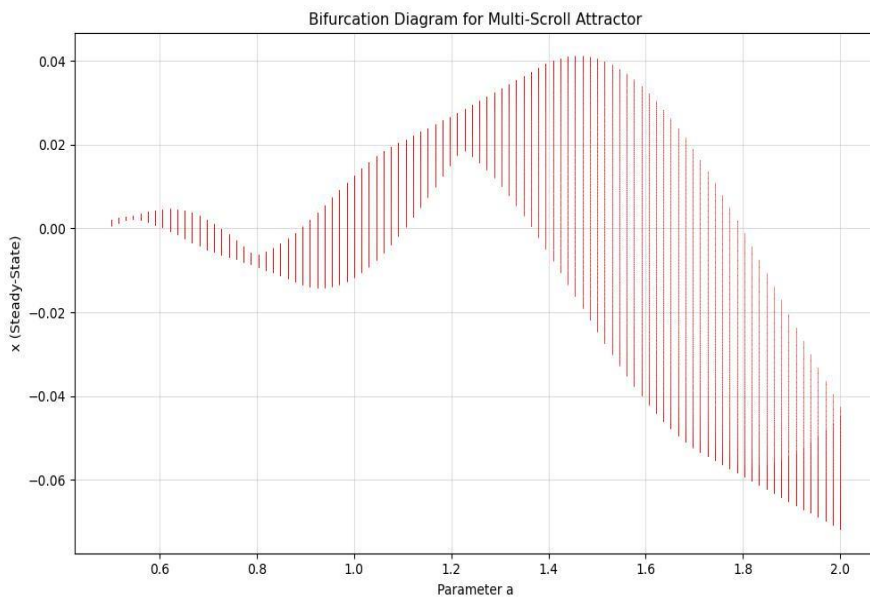


Figure 4. Non –linear behaviour diagram of multi-HCL attractors

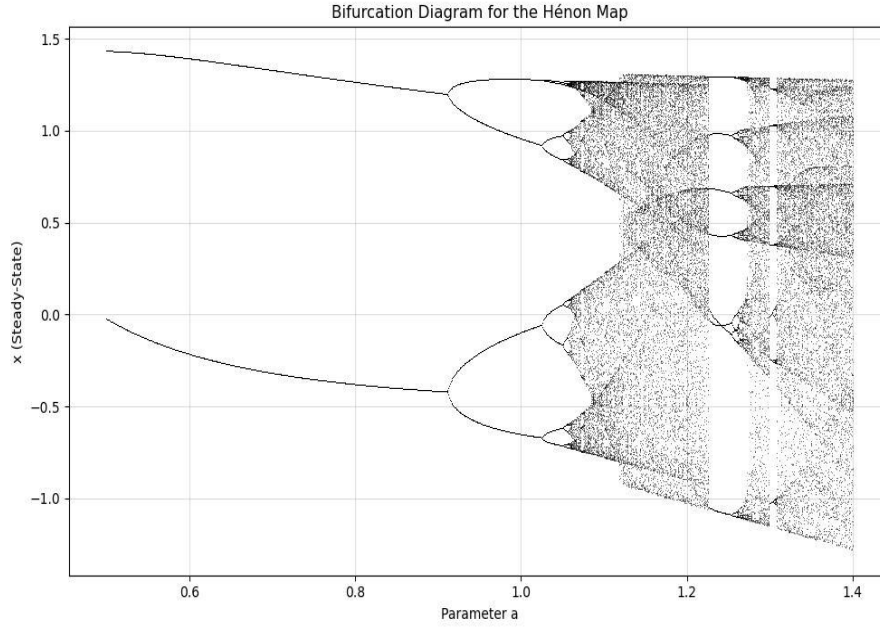


Figure 5. Non –linear behaviour diagram of Henon MAPS

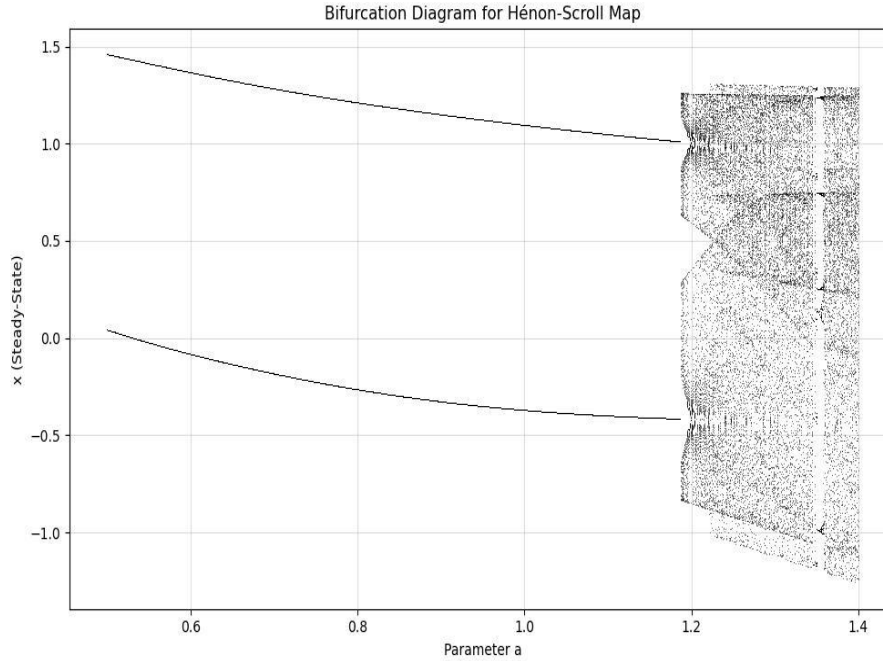


Figure 6. Non–linear behaviour diagram of HCL maps at the initial condition when a=0.3, b=0.1

$$X_{n+1} = 1 - aX_n^2 + Y_n + F(s) \quad (32)$$

$$Y_{n+1} = 1 - bX_n + F(s) \quad (33)$$

where, $F(s)$ is HCL maps.

4.7.3 ABE-HCL encryption technique

In this study, Cipher text policy based attribute relied encryption schemes (CP-ABE) based on the HCL techniques. For the encryption process, access policies (AP) are initiated by utilizing user attributes and the data can only be decrypted by the receiver if their attributes fulfil the AP's conditions. As the first step, public key(PK) and master key(MK) are constructed. By utilizing the AP and PK, a ciphertext is created. The secret keys are generated by utilizing mater keys and an attribute sets. To make the model as more resistant against the

collusion attacks, the proposed study incorporates the heterogeneous chaotic encryption schemes to be more resistant against the collusion attacks. In the existing technique, attribute-based encryption (CP-ABE) procedures often rely on bilinear pairings of elliptic curves, known as pairing-friendly curves. Let G_1 and G_2 be cyclic groups of prime order p , and let $e: G_1 \times G_1 \rightarrow G_2$ be a bilinear map. In this proposed research, all the maps are generated based on the HCL technique which produces the more random keys which are unpredictable for tampering.

Encryption using HCL maps introduces additional security and privacy levels by modifying the input parameters (Algorithm-3). For encryption with HCL maps, a permutation operation is performed between each element of the input data and a chaotic value constructed by the HCL maps. The i th element of the plaintext data is diffused with the random value

from the HCL maps to generate robust encrypted data. Prior to encryption, both the HCL maps and the data are scaled to a common factor of 16 to reduce process challenge. Similarly, in the reversible operation (Algorithm-4), a diffusion operation is performed among the encrypted data and the same encryption key (or parameter), which restores the original plaintext. The unique properties of chaotic systems, like ergodicity, sensitivity and determinism to initial phases, make them an attractive option for designing cryptographic systems. A prominent strength of chaos-relied encryption approaches is their computational efficiency [34].

Step	Algorithm-3// ABE-HCL based privacy Encryption Schemes
1	Input: Data Parameters (D)
2	Output: Encrypted Data (E)
3	Key generation Process (PK) using HCL maps
4	Initial conditions selections
5	Generate the HCL maps (G) and encrypts in accordance to the access policies AP
6	For i= 1 to n_iteration
7	F= Data.G ⁽ⁱ⁾ Formation of Cipher text in according to the access policies AP
8	End
9	The output from the encryption process

	Algorithm-4// ABE-HCL based privacy Decryption Schemes
1	Input: Encrypted Data (E)
2	Output: Plain Data (P)
3	First checks the attribute set satisfies access policy AP
4	If Satisfies the AP
5	Recover the messages
6	Else
7	Decryption Fails
8	End
9	The output from the decryption process

The encryption and decryption processes, as detailed in Algorithm-3 and Algorithm-4, comprise several stages: 1) Key Generation: The keys are created by looping among varied originating criteria of the HCL maps. 2) Diffusion: This phase facilitates the interaction among the data and the HCL keys to generate the encrypted data. The primary goal of this research is to establish a multi-variable relationship among the original and the encrypted data. Furthermore, during encryption, numerous loops are applied to refresh the HCL maps and keys. Each iteration may modify the key to initiate additional randomness, thereby enhancing the security of the encryption process as per the AP. 4) The final encrypted outcome unveils increased Irregularity and greater Quantitative independence from the original data.5) The reversible progress of decryption is involved by checking the cipher text in accordance to AP if matches, decryption starts otherwise it ends.

5. RESULTS AND DISCUSSIONS

This segment demonstrates about the experimentation setup, outcomes discussion and comparative analysis of the proposed model.

This segment furnishes about the experimentation procedures, discussion for outcomes and atleast wrapped with the thorough comparison with the varied cutting-edge approaches.

5.1 Experimental outcomes

Experimental evaluations are carried out using TensorFlow version 2.3.3 along with Pandas 1.22 and Numpy 1.20. For the implementation of the FL framework, the TensorFlow Federated Library Flower is leveraged [35]. All the cryptographic algorithms are implemented in Crypto-charm libraries. Additionally, the proposed model was evaluated from the BoTNET-IoT datasets [36]. The data used for the evaluation in which the 70% of total data were used for training, 20% of data were used for testing and at last 10% of data is used for validation.

The ablation experimentation is utilized in the four folded mode to prove the effectiveness of every segment of recommended approach. The detailed descriptions of the recommended approach are presented below.

5.2 Ablation experiment outcomes

5.2.1 Model evaluation

To assess the efficiency of the recommended approach, performance metrics like specificity, precision, accuracy, F1-Score, and recall are calculated. Additionally, AUC (Area under ROC) and confusion matrix to validate supremacy of the recommended approach. The mathematical formulations for computing the performance metrics are outlined in Table 2. Greater values for these metrics signify superior performance. To address the network's overfitting challenge and elevate generalization, the early stopping procedure [37] is utilized. This approach halts the training process of the proposed network when the validation performance fails to improve over a specified number of consecutive iterations. To prove the effectiveness of the proposed framework, variants of federated LSTM such as Fed-LSTM [38], mLSTM [39], Fed-Hybrid LSTM [40], FAF-LSTM [41], Fed-Stacked LSTM [42] and Conventional LSTM [43].

Table 2. Mathematical expressions for the performance metrics' calculation

Performance Metrics	Mathematical Expression
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$
Recall	$\frac{TP}{TP + FN} \times 100$
Specificity	$\frac{TN}{TN + FP}$
Precision	$\frac{TP}{TP + FP}$
F1-Score	$2 \cdot \frac{Precision * Recall}{Precision + Recall}$

5.2.2 Discussions

Figure 7 depicts the performance of the recommended approach with the changes in the drop-out ratios. Even though the drop-outs are increased, model is capable of showing the stable performance in the detecting the attacks. As shown in Figure 7 Ashera CAT optimized LSTM with its FL technology has maintained the average accuracy of 0.974, precision of 0.965, recall of 0.96, Specificity of 0.96 and F1-score of 0.965 with the increase in the drop-out ratios. Figure 8-17 illustrates the performance of the recommended and residing approach with the changes in the number of participants. In the first and second round of experimentation with the reduced count of individuals, every approach has shown the stable performance in recognizing the assaults. As the participants increases,

performance of conventional LSTM drops by 12%, Fed-LSTM by 11.4%, mLSTM by 19.2%, Fed-FAF-LSTM by 10.5%, Fed-Hybrid_LSTM by 9.3%, Fed-Stacked-LSTM by 14,3% respectively. But the performance of the proposed

federated framework drops only 1.5% as the participants increases. The role of federated optimized learning layers has portrayed the greater performance than the varied residing approaches.



Figure 7. Performance of the recommended approach in recognizing the varied attacks with the varied drop-outs

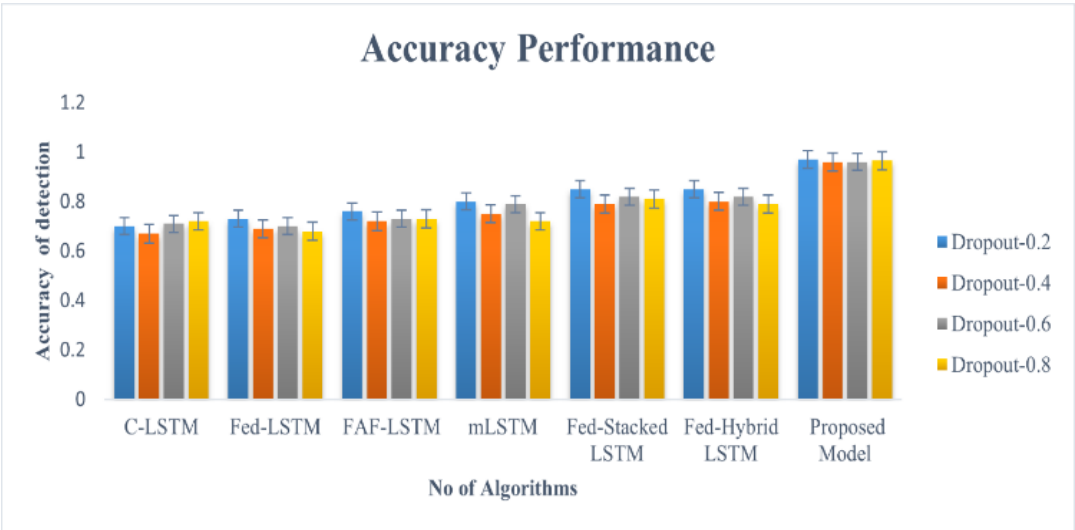


Figure 8. Accuracy of the varied approach in recognizing the varied threats with the varied drop-outs

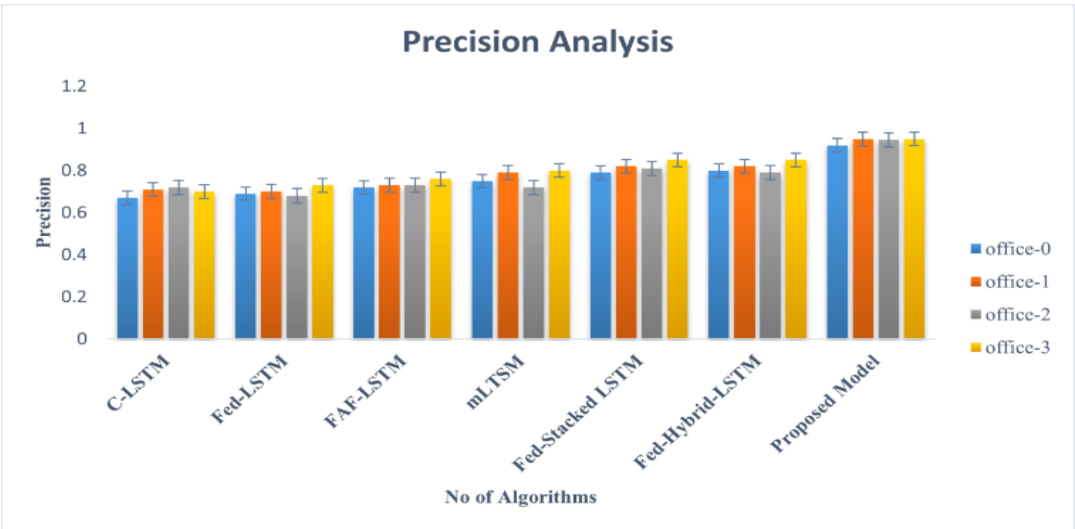


Figure 9. Precision of the varied approach in recognizing the varied threats with the varied drop-outs

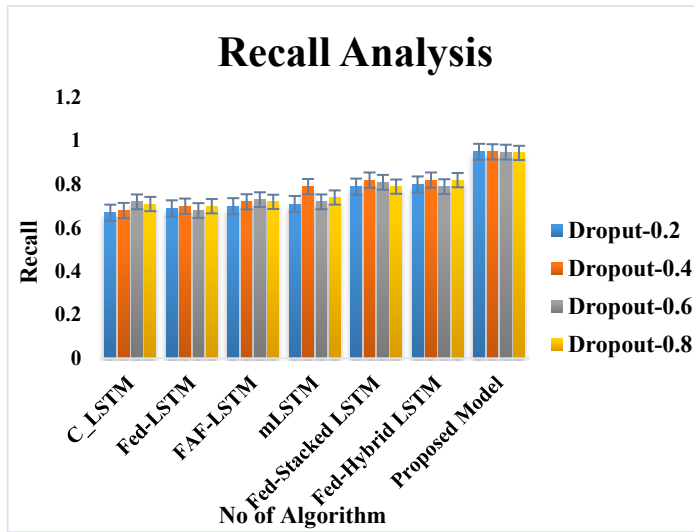


Figure 10. Recall of the varied approach in recognizing the varied threats with the varied drop-outs

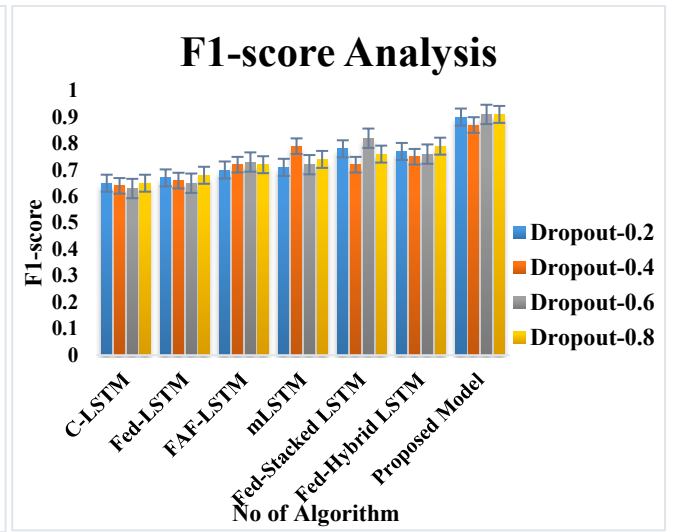


Figure 11. F1-scores of the varied approach in recognizing the varied threats with the varied drop-outs

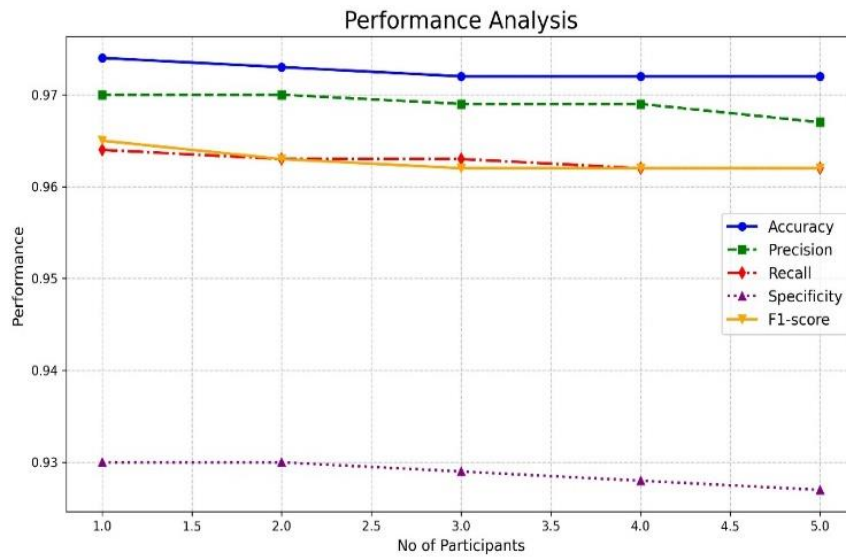


Figure 12. Performance of the recommended fed approach with the maximising number of the participants

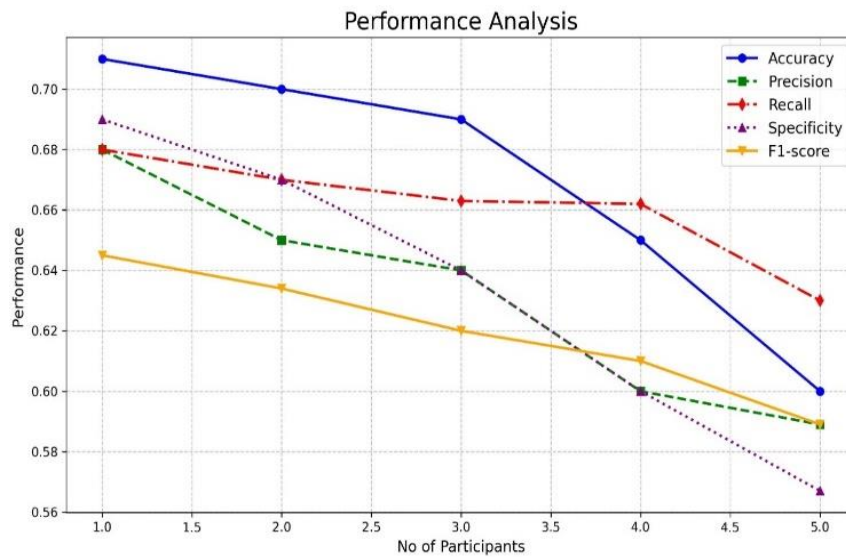


Figure 13. Performance of the traditional LSTM model with the maximising number of the participants

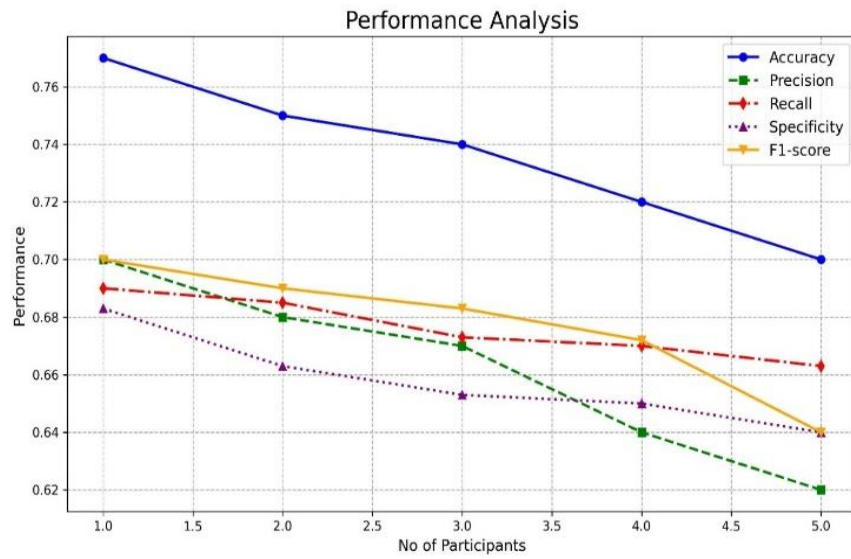


Figure 14. Performance of Fed-mLSTM approach in detecting the different attacks for the maximising number of participants

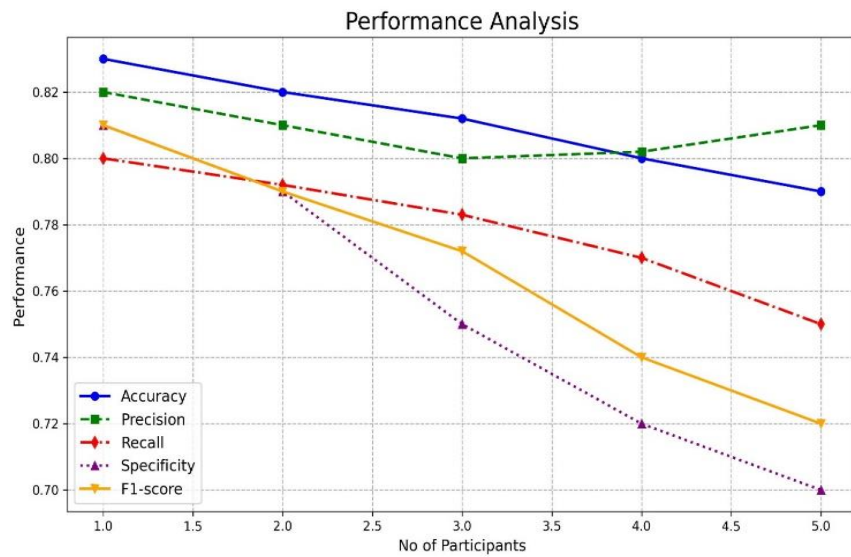


Figure 15. Performance of Fed-LSTM approach in recognizing the varied attacks for the maximising count of individuals

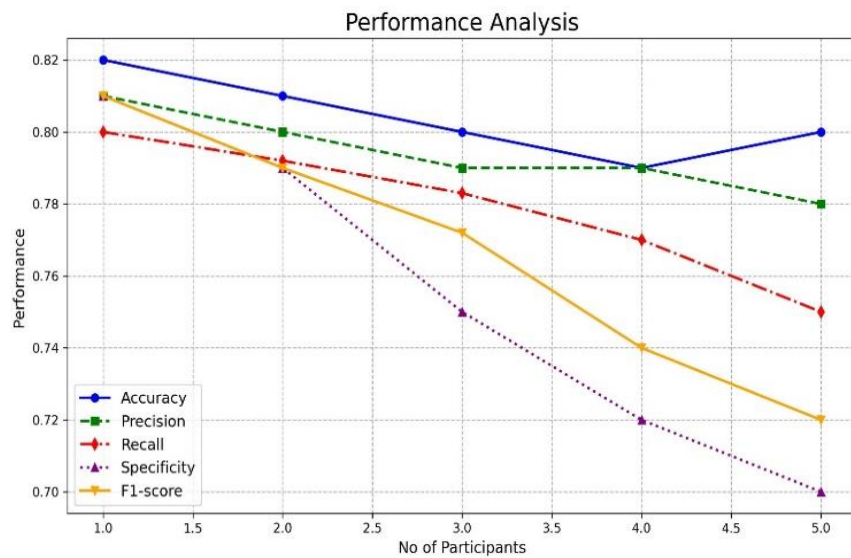


Figure 16. Performance of Fed-FAF-LSTM approach in recognising the varied threats for the increased count of individuals

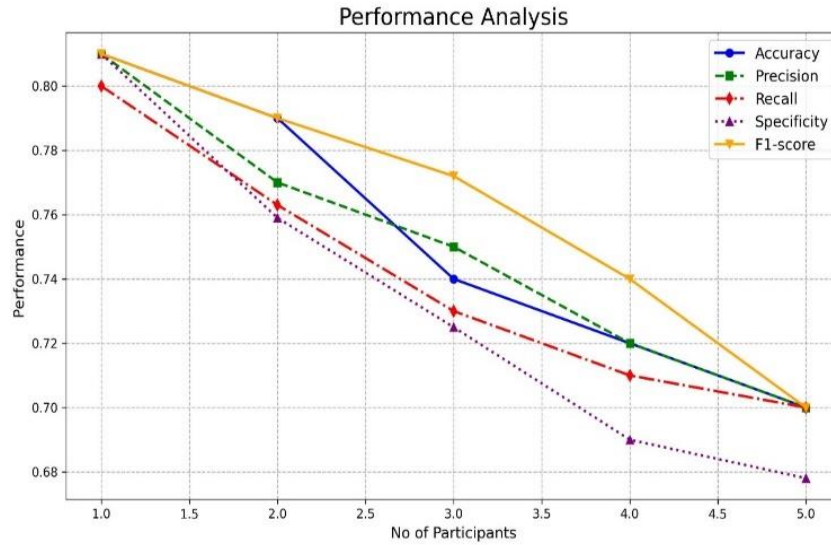
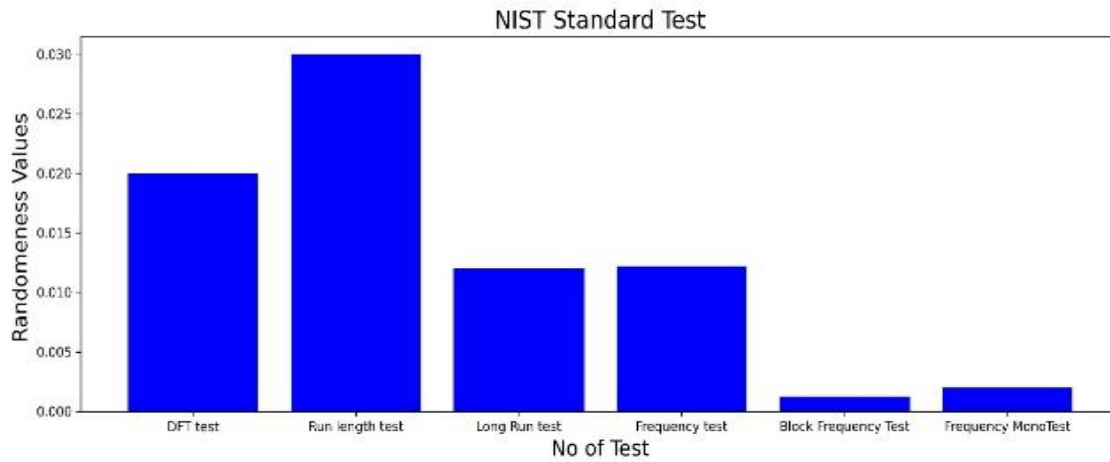
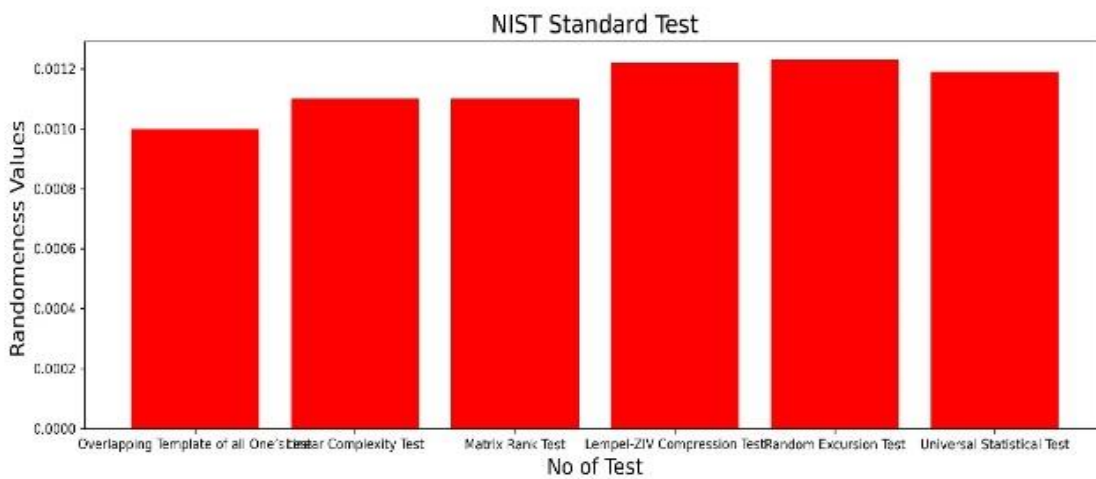


Figure 17. Performance of Fed-Hybrid-LSTM approach in recognizing the varied threats for the increased number of participants



(a)



(b)

Figure 18. NIST standard test results a) Result of first six standard test b) Result of second six standard test

5.3 Security analysis and its outcomes

In this experimentation, the security robustness of the encrypted bits was assessed and examined through the implementation of the National Institute of Standards and

Technology (NIST) tests. These tests ensure the randomness of the encrypted bits, adapting them for the secure communication of private models to central servers. The 12 essential NIST were performed, and the experimentation results are shown in Figure 18 (a) & (b).

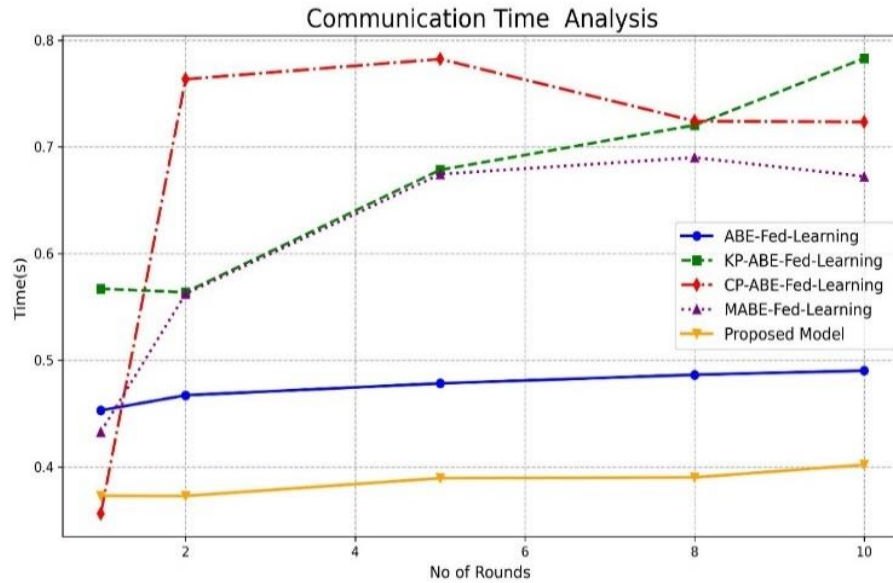


Figure 19. Communication time analysis for the different ABE encryption models integrated in the FL process

Table 3. Comparison analysis between the existing works and proposed works

Work Details	Proposed Model	Performance Analysis			
		Accuracy	CT (Sec)	ET (Sec)	DT (Sec)
Shen et al. [23]	PPFL-MKFHE	0.92	0.567	2.45	2.89
Narkedimilli et al. [19]	FL_DABE-BC	N/A	0.833	n/a	n/a
Lin et al. [27]	DeepFeed	0.90	0.892	1.89	1.90
Xiong et al. [20]	ABE-FL	0.91	0.67	2.99	3.01
Saidei et al. [21]	Chaotic Encryption with FL	0.92	0.453	1.64	1.56
Proposed Model	ABE-HCL with FL	0.965	0.390	1.92	1.99

To validate the randomness of the recommended encryption procedure, 12 tests of NIST suite has to be passed in which the randomness value of P is set to be greater than 0.001. From the Figures 18(a)-(b), it is evident that the proposed encryption scheme has passed the NIST test which has proved its strength of protecting the PPFL in mitigating the multiple attacks.

5.4 Communication time analysis

The communication time analysis has been calculated by the time of transmitting update from clients to server. The mathematical expression of the communication time is expressed as follows

$$\text{Communication Time} = N \times T_{\text{send}} + T_{\text{aggregate}} \quad (34)$$

where, T_{send} is the time for transmitting the data from devices to server whereas $T_{\text{aggregate}}$ is the time taken by the server/cloud for aggregation process. N represents the number of rounds. For this experimentation, different existing Communication time for ABE techniques with FL models and proposed ABE-HCL integrated in FL process are considered.

Based the Figure 19, it is very obvious that the recommended FL process has consume only 0.45secs with the maximum number of 10 which is 45% lesser than ABE technique, 35% lesser than KP-ABE, 27% lesser than CP-ABE and 25% lesser than MABE techniques. Hence the communication cost of using the proposed encryption model in FL has consumed only lesser communication overhead in transmitting and aggregating the global model.

5.5 Comparative analysis by different works

Table 3 presents a performance comparison between the recommended approach and various methods proposed by authors discussed in Section 2 (Related Works), using a bandwidth of 500 megabytes.

From the Table 3, recommended approach has yielded the best performance in recognising the multiple threats but still has higher encryption and decryption time than the residing works.

This is due to the fact that the recommended approach has integrated with the HCL with ABE to produce the best randomness values. But still it has scope of improvisation in reducing the encryption and decryption time suitable for the IoT devices.

6. CONCLUSION AND FUTURE ENHANCEMENT

This current study, recommended protocol based on the FL with the novel ABE-HCL encryption techniques has been presented The optimized LSTM network works on the principle of Ashera CAT optimization approach was recommended for an effective detection of multiple attacks. Later, Optimized approaches are transformed from conventional training approaches into federated distributed networks, enabling more efficient resource utilization and improved performance. The ABE-HCL maps are utilized to encrypt and decrypt the local schemes, transforming the distributed scheme into a privacy-preserving mechanism capable of mitigating various types of attacks. Comprehensive

experiments were conducted using the BotNET datasets, and several performance metrics are evaluated and analysed. In the initial experimentation, metrics like F1-score, accuracy, recall, and precision were computed for the recommended federated approach and varied residing cutting-edge LSTM procedures. The outcomes portray that the recommended approach surpasses the others, achieving the highest accuracy of 0.97, an F1-score of 0.965, precision of 0.96 and recall of 0.96. Computational time was also assessed, with the distributed model showing shorter processing times examined to the varied approaches. Finally, the approach's privacy was validated through NIST standard tests. Across all experimentations, the recommended distributed learning approach exhibited optimal performance, establishing their strong potential for IoT systems.

In future, Computational overhead is needed to be infused for varied Edge/Fog gateway devices to enhance the approach's efficiencies including computation, communication and secured storage. Moreover, full approach would be refined for managing real-time datasets.

REFERENCES

- [1] Lin, Y., Xie, Z., Chen, T., Cheng, X., Wen, H. (2024). Image privacy protection scheme based on high-quality reconstruction DCT compression and nonlinear dynamics. *Expert Systems with Applications*, 257: 124891. <https://doi.org/10.1016/j.eswa.2024.124891>
- [2] Khan, M.J., Chauhan, R.C.S., Singh, I., Fatima, Z., Singh, G. (2024). Mobility management in heterogeneous network of vehicular communication with 5G: Current status and future perspectives. *IEEE Access*, 12: 86271-86292. <https://doi.org/10.1109/ACCESS.2024.3382917>
- [3] Haghrah, A., Haghrah, A., Niya, J.M., Ghaemi, S. (2023). Handover triggering estimation based on fuzzy logic for LTE-A/5G networks with ultra-dense small cells. *Soft Computing*, 27: 17333-17345. <https://doi.org/10.1007/s00500-023-08482-0>
- [4] Xu, S., Nikraves, A., Mao, Z.M. (2019). *Leveraging Context-Triggered Measurements to Characterize Lte Handover Performance*. Springer, pp. 3-17. https://doi.org/10.1007/978-3-030-15986-3_1
- [5] Sun, C., Ma, S., Zheng, C., Wu, S., Cui, T., Lyu, L. (2023). FL over a wireless network: Distributed user selection through random access. *arXiv preprint arXiv:2307.03758*. <https://doi.org/10.48550/arXiv.2307.03758>
- [6] Yin, B., Chen, Z., Tao, M. (2020). Joint user scheduling and resource allocation for FL over wireless networks. In *2020 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6. <https://doi.org/10.1109/GLOBECOM42002.2020.9322263>
- [7] Huang, W., Wu, M., Yang, Z., Sun, K., Zhang, H., Nallanathan, A. (2022). Self-adapting handover parameters optimization for SDN-enabled UDN. *IEEE Transactions on Wireless Communications*, 21(8): 6434-6447. <https://doi.org/10.1109/TWC.2022.3184163>
- [8] Liu, Q., Kwong, C.F., Wei, S., Li, L., Zhang, S. (2021). Intelligent handover triggering mechanism in 5G ultra-dense networks via clustering-based reinforcement learning. *Mobile Networks and Applications*, 26: 27-39. <https://doi.org/10.1007/s11036-020-01591-7>
- [9] Angjo, J., Shaye, I., Ergen, M., Mohamad, H., Alhammadi, A., Daradkeh, Y.I. (2021). Handover management of drones in future mobile networks: 6G technologies. *IEEE Access*, 9: 12803-12823. <https://doi.org/10.1109/ACCESS.2021.3051620>
- [10] Lopez-Perez, D., Guvenc, I., Chu, X. (2012). Mobility management challenges in 3GPP heterogeneous networks. *IEEE Communications Magazine*, 50(12): 70-78. <https://doi.org/10.1109/MCOM.2012.6384451>
- [11] Tan, K., Bremner, D., Le Kernec, J., Sambo, Y., Zhang, L., Imran, M.A. (2022). Intelligent handover algorithm for vehicle-to-network communications with double-deep Q-learning. *IEEE Transactions on Vehicular Technology*, 71(7): 7848-7862. <https://doi.org/10.1109/TVT.2022.3179805>
- [12] Priyanka, A., Gauthamarayathirumal, P., Chandrasekar, C. (2023). Machine learning algorithms in proactive decision making for handover management from 5G & beyond 5G. *Egyptian Informatics Journal*, 24: 100389. <https://doi.org/10.1016/j.eij.2022.10.002>
- [13] Luo, Y., Zhang, Y., Du, C., Zhang, H., Liu, Y. (2024). Handover algorithm based on Bayesian-optimized LSTM and multi-attribute decision making for heterogeneous networks. *Ad Hoc Networks*, 157: 103454. <https://doi.org/10.1016/j.adhoc.2023.103454>
- [14] Lima, J.P., de Medeiros, Á.A., de Aguiar, E.P., Silva, E.F., de Sousa, V.A., Nunes, M.L., Reis, A.L. (2023). Deep learning-based handover prediction for 5G and beyond networks. In *ICC 2023 - IEEE International Conference on Communications*, Rome, Italy, pp. 3468-3473. <https://doi.org/10.1109/ICC45041.2023.10279486>
- [15] Kaur, G., Goyal, R.K., Mehta, R. (2022). An efficient handover mechanism for 5G networks using hybridization of LSTM and SVM. *Multimedia Tools and Applications*, 81: 37057-37085. <https://doi.org/10.1007/s11042-021-11608-0>
- [16] Bandani, A.K., Riyazuddin, S., Bidare Divakarachari, P., Patil, S.N., Arvind Kumar, G. (2023). Multiplicative long short-term memory-based software-defined networking for handover management in 5G network. *Signal, Image and Video Processing*, 17: 2933-2941. <https://doi.org/10.1007/s11760-023-02714-4>
- [17] Yin, X., Qiu, H., Wu, X., Zhang, X. (2024). An efficient attribute-based participant selecting scheme with blockchain for FL in smart cities. *Computers*, 13(5): 118. <https://doi.org/10.3390/computers13050118>
- [18] Park, Y., An, J., Oh, Y., Lee, J. (2023). A blockchain-based secure FL mechanism for autonomous vehicles. *Sensors*, 23(1): 267. <https://doi.org/10.3390/s23010267>
- [19] Narkedimilli, S., Sriram, A.V., Raghav, S. (2024). FL-DABE-BC: A privacy-enhanced, decentralized authentication, and secure communication for FL framework with decentralized attribute-based encryption and blockchain for IoT scenarios. *arXiv preprint arXiv:2410.20259*. <https://arxiv.org/abs/2410.20259>
- [20] Xiong, H., Yan, H., Obaidat, M.S., Chen, J., Cao, M., Kumar, S., Agarwal, K., Kumari, S. (2024). Efficient and privacy-enhanced asynchronous FL for multimedia data in Edge-based IoT. *ACM Transactions on Multimedia Computing, Communications and Applications*. <https://doi.org/10.1145/3688002>
- [21] Saidi, A., Amira, A., Nouali, O. (2025). Securing decentralized federated learning: Cryptographic mechanisms for privacy and trust. *Cluster Computing*,

- 28(2): 1-17. <https://doi.org/10.1007/s10586-024-04957-8>
- [22] Nabi, S.A., Kalpana, P., Chandra, N.S., Smitha, L., Naresh, K., Ezugwu, A.E., Abualigah, L. (2024). Distributed private preserving learning based chaotic encryption framework for cognitive healthcare IoT systems. *Informatics in Medicine Unlocked*, 49: 101547. <https://doi.org/10.1016/j.imu.2024.101547>
- [23] Shen, C., Zhang, W., Zhou, T., Zhang, L. (2024). A security-enhanced FL scheme based on homomorphic encryption and secret sharing. *Mathematics*, 12(13): 1993. <https://doi.org/10.3390/math12131993>
- [24] García-Rodríguez, J., Skarmeta, A. (2023). A privacy-preserving attribute-based framework for IoT identity lifecycle management. *Computer Networks*, 236: 110039. <https://doi.org/10.1016/j.comnet.2023.110039>
- [25] Ma, J., Naas, S.A., Sigg, S., Lyu, X. (2022). Privacy-preserving FL based on multi-key homomorphic encryption. *International Journal of Intelligent Systems*, 37(9): 5880-5901. <https://doi.org/10.1002/int.22818>
- [26] Arumugam, S., Shandilya, S.K., Bacanin, N. (2022). FL-based privacy preservation with blockchain assistance in IoT 5G heterogeneous networks. *Journal of Web Engineering*, 21(4): 1323-1346. <https://doi.org/10.13052/jwe1540-9589.21414>
- [27] Lin, H., Kaur, K., Wang, X., Kaddoum, G., Hu, J., Hassan, M.M. (2021). Privacy-aware access control in IoT-enabled healthcare: A federated deep learning approach. *IEEE Internet of Things Journal*, 10(4): 2893-2902. <https://doi.org/10.1109/JIOT.2021.3112686>
- [28] Islam, M.A., Madria, S.K. (2022). Attribute-based encryption scheme for secure multi-group data sharing in cloud. *IEEE Transactions on Services Computing*, 15(4): 2158-2172. <https://doi.org/10.1109/TSC.2020.3038836>
- [29] Abebe, B.T., Hussain, F.K. (2022). FL for preserving privacy and enhancing trust in healthcare and medical systems: A survey. *IEEE Access*, 10: 50040-50055. <https://doi.org/10.1109/ACCESS.2022.3173933>
- [30] Kaissis, G., Makowski, M., Rückert, D., Braren, R. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. *Nature Machine Intelligence*, 2: 305-311. <https://doi.org/10.1038/s42256-020-0186-1>
- [31] Zhang, Y., Xie, F., Wang, Q., Shi, W. (2021). A survey on FL. *IEEE Transactions on Big Data*, 10(1): 1-19. <https://doi.org/10.1109/TBDATA.2021.3122224>
- [32] Chu, S.C., Tsai, P.W., Pan, J.S. (2006). Cat swarm optimization. In *Pacific Rim International Conference on Artificial Intelligence*, Berlin, Heidelberg, pp. 854-858. https://doi.org/10.1007/978-3-540-36668-3_94
- [33] Wang, J., Yurochkin, M., Sun, Y., Papailiopoulos, D., Khazaeni, Y. (2021). FL with matched averaging. In *International Conference on Learning Representations*. <https://openreview.net/forum?id=BkluqISFDS>
- [34] Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., et al. (2021). Advances and open problems in FL. *Foundations and Trends® in Machine Learning*, 14(1-2): 1-210. <https://doi.org/10.1561/22000000083>
- [35] Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., et al. (2019). Towards federated learning at scale: System design. *Proceedings of machine learning and systems*, 1: 374-388.
- [36] Li, T., Sahu, A.K., Zaheer, M., Sanjabi, M., Talwalkar, A., Smith, V. (2020). Federated optimization in heterogeneous networks. In *Proceedings of Machine Learning and Systems*, pp. 429-450.
- [37] Wang, H., Joshi, J. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 83: 395-411. <https://doi.org/10.1016/j.future.2017.11.022>
- [38] Al-Bassam, M. (2018). Scalable and trustworthy FL for IoT. *arXiv preprint arXiv:1811.12201*. <https://doi.org/10.48550/arXiv.1811.12201>
- [39] Kalpana, P., Anandan, R. (2023). A capsule attention network for plant disease classification. *Traitement du Signal*, 40(5): 2051-2062. <https://doi.org/10.18280/ts.400523>
- [40] Liu, X., Yu, J., Lin, X., Yu, H. (2020). Privacy-preserving federated recommender systems. In *Proceedings of the Web Conference 2020*, pp. 921-931. <https://doi.org/10.1145/3366423.3380177>
- [41] Kalpana, P., Kodati, S., Smitha, L., Sreekanth, N., Smerat, A., Ahmad, M.A. (2025). Explainable AI-driven gait analysis using Wearable Internet of Things (WIoT) and human activity recognition. *Journal of Intelligent Systems & Internet of Things*, 15(2): 55-75. <https://doi.org/10.54216/JISIoT.150205>
- [42] Mohammadi, M., Al-Fuqaha, A., Sorour, S., Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*, 20(4): 2923-2960. <https://doi.org/10.1109/COMST.2018.2844341>
- [43] Kalpana, P., Narayana, P., Smitha, L., Madhavi, D., Keerthi, K., Smerat, A., Nazzal, M.A. (2025). Health-Fots-A latency aware fog based IoT environment and efficient monitoring of body's vital parameters in smart health care environment. *Journal of Intelligent Systems & Internet of Things*, 15(1): 144-156. <https://doi.org/10.54216/JISIoT.150112>