IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 December 2023, accepted 28 January 2024, date of publication 5 February 2024, date of current version 21 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3362347

RESEARCH ARTICLE

Enhancing Intrusion Detection Through Federated Learning With Enhanced Ghost_BiNet and Homomorphic Encryption

OM KUMAR CHANDRAUMAKANTHAM[1], SUDHAKARAN GAJENDRAN[2], AND SUGUNA MARAPPAN[1]

[1]SCOPE, Vellore Institute of Technology, Chennai Campus, Chennai, Tamil Nadu 600127, India
[2]SENSE, Vellore Institute of Technology, Chennai Campus, Chennai, Tamil Nadu 600127, India

Corresponding author: Om Kumar ChandraUmakantham (omkumar.cu@vit.ac.in)

ABSTRACT Intrusion detection is essential for safeguarding computer systems and networks against unauthorized access, malicious activities, and security breaches. Its application domains include network security, information security, and cybersecurity across various sectors such as finance, healthcare, government, and industry. Federated learning-based intrusion detection offers improved performance compared to conventional mechanisms by leveraging decentralized data sources, preserving data privacy, and enhancing model generalization through collaboration among multiple organizations. However, challenges faced by existing federated learning-based intrusion detection mechanisms include ensuring data privacy and security, mitigating communication overhead, and enhancing detection accuracy. In order to overcome these issues, this research article proposes a federated learning-based intrusion detection methodology that leverages Enhanced Ghost_BiNet, a novel deep learning model, to enhance the security of information sharing and detection accuracy. Federated learning, a privacy-preserving machine learning technique, is utilized to enable multiple entities to collaboratively train a global intrusion detection model without sharing sensitive data. The proposed system first trains local models using Enhanced Ghost_BiNet, which integrates GhostNet and Bidirectional Gated Recurrent Unit (BiGRU). To optimize the model's performance, the Chaotic Chebyshev Artificial Humming Bird (CAh) algorithm is employed. Homomorphic encryption is applied to encrypt the local model updates, enhancing data privacy and security. Server-side aggregation of updates and collaborative optimization are introduced to minimize communication rounds during data aggregation. The results demonstrate that the Enhanced Ghost_BiNet outperforms traditional models like GhostNet, BiGRU, RNN, Auto Encoder, and CNN in terms of accuracy, precision, recall, F-Score, and mean square error (MSE). For instance, the Enhanced Ghost_BiNet achieves an accuracy of 99.24% on the KDD CUP 99 dataset, surpassing the other models by a significant margin. The proposed methodology provides a robust and secure approach to intrusion detection, ensuring the confidentiality of sensitive data while improving detection accuracy.

INDEX TERMS Federated learning, intrusion detection, hybrid deep learning, homomorphic encryption, enhanced Ghost_BiNet, privacy.

I. INTRODUCTION

The volume of data created and stored has grown dramatically in the age of digitalization. Database instances are proliferating as a result of the present tendency to record and analyze every technological contact as well as the declining cost of infrastructure and storage devices [1], [2]. Deep learning in many areas and machine learning models, in general, have improved opportunities because of the massive volume of data that is incorporated into our daily activities [3]. Machine

The associate editor coordinating the review of this manuscript and approving it for publication was Sangsoon Lim.

learning has been used for a wide range of products and services, from cyber-physical systems (CPS) and IoT sensors like small handheld devices and large corporations like Netflix, Amazon, Google, and Facebook [4]. A few well-known machine learning services where models may be utilized and deployed at scale include Microsoft Azure, Google Cloud, and Amazon Web Services [5], [6]. In addition to enhancing user experience and business modeling, machine learning has become essential for identifying and thwarting cyber threats and assaults [7]. Because of how much data is used in today's society, protecting its privacy and integrity is crucial. Communication links are necessary for the transfer of sensitive data about people, governments, and organizations [8].

Most of the time, traditional cybersecurity mitigation techniques only shield devices after particular kinds of attacks have taken place. But threats on today's internet are very different in terms of their kinds and patterns [9]. Persistently altering their profile, polymorphic viral attacks are hard to identify and anticipate. In light of this, the machine learning method of identifying and forecasting risks, irregularities, or any type of cyberspace security breach and implementing appropriate countermeasures has garnered a lot of attention lately [10], [11]. It is well established that the performance of the learning model may be enhanced by forming a centralized learning model through local training data exchange [12]. Machine learning-based cybersecurity is implemented using several approaches, including centralized, decentralized, and federated approaches each with pros and cons [13], [14]. These models have recently been expanded to include the federated learning paradigm for cybersecurity. The novel distributed machine learning method known as federated learning makes use of edge device processing capacity without transferring user data samples [15]. Before being sent to the centralized server, the local models are trained on user data on the device. As a result, because federated learning prevents the transfer of enormous volumes of data, it is somewhat efficient in terms of communication and privacy [16], [17]. Unfortunately, since federated learning is trained on sensitive user data, reverse engineering might compromise its privacy protection [18].

Federated learning-based intrusion detection techniques, underpinned by deep learning, offer a host of compelling advantages [19]. Firstly, they excel in preserving data privacy, a critical factor in intrusion detection, as sensitive information remains decentralized and local. Moreover, these techniques are data-efficient, harnessing the collective knowledge of distributed devices to build robust models without the need for extensive data transfers [20]. Real-time learning capabilities enable rapid adaptation to evolving intrusion patterns, enhancing system responsiveness. By aggregating local models, federated learning provides a global view of network security, bolstering intrusion detection accuracy and generalization [21]. The decentralized approach minimizes the risk of a single point of failure, improving system resilience. These techniques can adapt to diverse domains, making them versatile for intrusion detection in various environments [22]. Furthermore, deep learning's ability to capture intricate intrusion patterns results in superior model performance, reducing false alarms and enhancing overall security [23]. Lastly, by minimizing data transfer, they align with data protection regulations and user privacy expectations, making them an attractive choice for modern security challenges [24]. Thus, this research introduced a novel federated learning-based intrusion detection mechanism. The major contributions of the research are:

1. Design of CAh Algorithm: The algorithm for optimizing the loss function of the deep learning model during the information training is employed using the Chaotic Chebyshev Artificial humming bird (CAh), wherein the Chaotic Chebyshev is incorporated into the Artificial Humming Bird for enhancing the exploration criteria for avoiding the issue of local optimal trapping.
2. Design of Enhanced Ghost_BiNet: The intrusion detection is employed using the novel hybrid deep learning method named Ghost Bidirectional Gated Recurrent Unit (Ghost_BiNet), wherein the loss function optimization is devised using the CAh algorithm.

The organization of the research is: Section II details the related works along with the problem statement. Section III elaborates the proposed federated learning based intrusion detection and Section IV presents the results. Finally, Section V concludes the research.

II. RELATED WORKS

The conventional federated learning-based intrusion detection mechanisms are reviewed in this section.

The intrusion detection based on federated learning are: With the main goal of protecting networks, [25] created a Federated Learning technique that attempts to detect and stop unauthorized intrusions. A new model was sent to each local model by the global server after a round of federated learning training. A collective improvement in intrusion detection capabilities was ensured by the introduced model to integrate insights and improvements obtained from all local clients. Following that, the local models trained their corresponding local datasets using these revised models. By actively participating in the improvement of the overall intrusion detection model, the suggested approach allowed individual IoT devices to protect the privacy of their sensitive data. Performance issues with the model as a whole may arise from imbalances in the data distribution among local clients.

In order to overcome the difficulties of generalising in a cross-silo setup for a flow-based network intrusion detection system, [26] developed the stacked-unsupervised Federated Learning technique. A deep autoencoder was first developed, which was intended to learn meaningful representations of data from many network silos. This autoencoder is an effective intrusion detection tool since it retrieves useful features and patterns. The flow-based data was then classified and possible intrusions were found using the energy flow classifier. It was discovered that the proposed federated learning

was a workable and efficient method for accomplishing generalization over heterogeneous networks. Using ensemble learning, which blends several models, can add complexity and processing costs.

Reference [27] created a distributed anomaly detection system intended to identify malicious devices. Initially, carrier frequency offset (CFO), a physical layer property peculiar to a particular device type, was measured for device fingerprinting. The CFO-based method may therefore make it possible to identify anomalous variations in the device's CFO behavior, which may be a sign of hostile intervention. The suggested approach showed improved detection precision, lower storage requirements, and strong defense against cyberattacks. Even when data was transmitted in a dispersed fashion, there was always a risk involved, despite federated learning's goal of protecting data privacy. It was essential to guarantee data security throughout the federated learning process.

To protect federated learning systems against malevolent poisoning assaults, [28] designed Defending Poisoning attacks in Federated Learning (DPA-FL). The primary goal of the DPA-FL's initial phase was to quickly detect prospective attackers by comparing participant model weights. To identify attackers, the combined model was tested using a dataset in the second phase. When the combined model's accuracy fell to a point where it suggested possible hostile intervention, this phase became relevant. One significant benefit of DPA-FL was how quickly and effectively it could identify and rule out attackers. Although the goal of DPA-FL was to increase accuracy and F1-score, it might unintentionally misclassify some innocent participants as attackers, leading to false positives.

To increase the importance of essential devices in the learning process, [29] developed a federated learning technique with an attention mechanism. The number of communication cycles was decreased as a result of the introduced model, which effectively gave devices of larger relevance more weight. The method was able to significantly minimize communication overhead while maintaining learning convergence, which eases the load on network resources and makes the solution more effective and economical. The system's responsiveness may be impacted by latency in the intrusion detection process due to the increased complexity and communication overhead reduction techniques.

A. PROBLEM STATEMENT

Federated learning plays a crucial role in intrusion detection by enabling collaborative, privacy-preserving model training across decentralized devices and networks. This approach empowers intrusion detection systems to learn from local data without the need to share sensitive information centrally. Federated learning's applications extend to a wide range of domains, including the Internet of Things (IoT), Industrial Internet of Things (IIoT), healthcare, finance, and more. In IoT and IIoT, federated learning is vital for detecting network intrusions in distributed, often resource-constrained environments, where data privacy and network security are paramount. Healthcare leverages federated learning to safeguard patient data while improving anomaly detection in medical devices. Financial institutions apply it to enhance fraud detection across multiple branches or devices without risking data exposure. In essence, federated learning democratizes intrusion detection, making it adaptable to various domains while respecting data privacy and security.

Existing federated learning-based intrusion detection methods have shown promising outcome in enhancing cybersecurity for distributed environments. They leverage the power of collaborative machine learning while preserving data privacy. However, several challenges persist in this domain. Firstly, the complexity of implementing federated learning in real-world scenarios can be daunting, demanding expertise in both intrusion detection and machine learning. Secondly, federated learning models may be resource-intensive, particularly in large-scale IoT networks, leading to scalability issues. Moreover, ensuring robustness against a variety of intrusion types and maintaining privacy in the sharing of model updates across participants are persistent challenges. Additionally, the trade-offs between detection accuracy and false positives and negatives must be carefully managed. Thus, a novel federated learning approach based on optimized deep learning is introduced to enhance detection accuracy and minimize false alarms.

The design of proposed model by integrating GhostNet, lightweight neural network architecture, with Bidirectional Gated Recurrent Unit (Bi-GRU) for sequence modeling, the model effectively captures both spatial and temporal patterns in network traffic data, improving its ability to detect complex and evolving intrusion behaviors. In this, the loss function optimization using the CAh algorithm assists to enhance the detection accuracy. Additionally, homomorphic encryption of model weights ensures the privacy and security of sensitive information during model updates, enabling secure collaboration among multiple parties. Server updation using collaborative optimization further enhances the model's performance by aggregating encrypted updates from distributed clients, allowing for efficient and robust model optimization. Overall, the combination of these techniques facilitates more accurate and reliable intrusion detection while safeguarding data privacy and security, ultimately reducing false alarm rates and enhancing cybersecurity defenses.

III. FEDERATED LEARNING BASED INTRUSION DETECTION

Federated learning is a machine learning approach where a model is trained across multiple decentralized devices or servers holding local data samples, without exchanging them. Instead of sending raw data to a central server, local models are trained on each device using their respective data, and only model updates, typically in the form of gradients, are shared with the central server. The server aggregates these updates to improve the global model, which is then sent back

to the devices for further refinement. This process allows for collaborative model training while preserving data privacy and security. The key characteristics of federated learning based intrusion detection are:

Data Privacy: Intrusion detection often involves sensitive and confidential data, such as network traffic logs or security events. Federated learning allows model training to occur locally on individual devices or servers without the need to centralize or share raw data. This preserves data privacy and security, as sensitive information remains on the device where it originated.

Data Distribution: In large-scale network environments, data samples may be distributed across multiple devices or locations. Federated learning enables model training on distributed data sources without the need to consolidate them into a centralized location. This allows for more representative and diverse training datasets, capturing variations and nuances across different network segments or locations.

Resource Constraints: Devices or servers in network environments may have limited computational resources or bandwidth for centralized model training. Federated learning distributes the computational burden of model training across multiple devices, making it suitable for resource-constrained environments. This allows for efficient model training without overloading individual devices or servers.

Real-time Learning: Intrusion detection requires continuous monitoring and adaptation to evolving threats and network conditions. Federated learning supports real-time model updates and continuous learning by training models locally on devices with up-to-date data. This enables intrusion detection models to adapt quickly to emerging threats and changes in network behavior.

The proposed intrusion detection mechanism utilizes the federated learning-based approach for enhancing the security of information sharing and detection accuracy. Federated learning is a privacy-preserving machine learning technique that allows multiple devices or entities to collaboratively train a model without sharing sensitive data. In the context of intrusion detection, this method offers several advantages. Traditional intrusion detection systems rely on centralized data repositories, which can be vulnerable to attacks and privacy concerns. Federated learning, however, distributes the training process across individual devices or network segments, enabling each participant to train a local intrusion detection model using their own data. These locally trained models are then aggregated to create a global intrusion detection model without the need to exchange raw data. This decentralized approach enhances data privacy and security, making it harder for malicious actors to compromise sensitive information. The system model of the proposed intrusion detection model is presented in Figure 1.

Initially, the local models are trained using the novel deep-learning model named Enhanced Ghost_BiNet. In this, the hybrid classifier Ghost_BiNet is designed by integrating the GhostNet and Bidirectional gated Recurrent Unit, which is tuned optimally using the optimization algorithm Chaotic

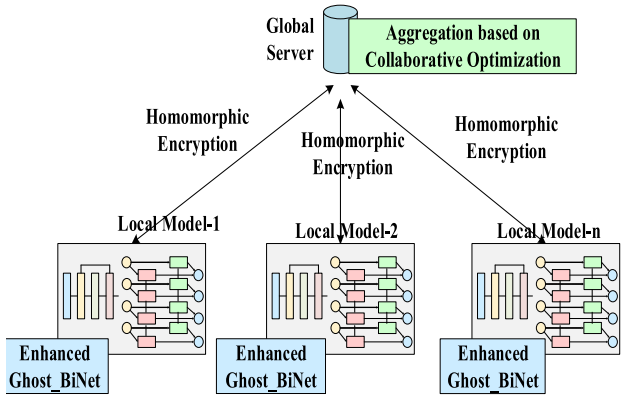

FIGURE 1. Proposed system model for intrusion detection.

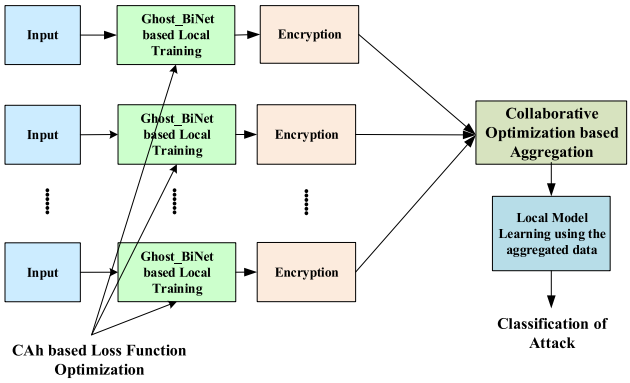

FIGURE 2. Proposed workflow.

Chebyshev Artificial Humming Bird (CAh) Algorithm for minimizing the information loss during the learning phase. After training the local models, the updates are encrypted using the homomorphic encryption algorithm to enhance the privacy of the model. Finally, on the server side, the updates are aggregated for training the global model to enhance the intrusion detection accuracy. In addition, for the reduction of communication rounds during the data aggregation process, collaborative optimization is devised for choosing the more relevant updates from the local models. The workflow is presented in Figure 2.

A. DATA ACQUISITION

The data for processing the proposed federated learning-based intrusion detection is acquired from publically available datasets like KDD CUP 99, CICIDS 2017, and UNSW-NB15.

B. PROPOSED ENHANCED GHOST_BINET

The proposed Ghost_BiNet is designed by combining the GhostNet and Bidirectional Gated Recurrent Unit (BiGRU), wherein the loss function optimization is devised using the Chaotic Chebyshev Artificial Humming Bird (CAh) Algorithm.

1) ARCHITECTURE OF GHOSTNET

GhostNet employs lightweight convolutional operations, which reduce the computational cost of the model. This is

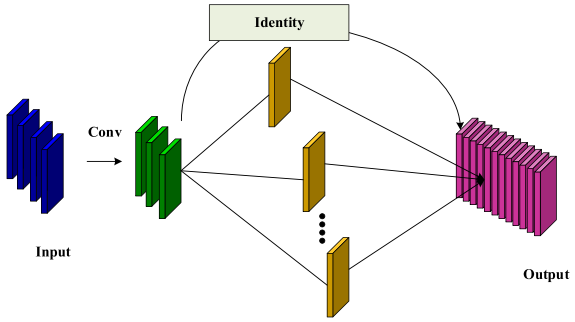

FIGURE 3. Architecture of GhostNet.

especially important in resource-constrained environments like mobile devices or edge devices, where conventional deep learning models can be too computationally intensive. The Ghost Module in GhostNet requires fewer parameters compared to standard convolutional layers, leading to reduced memory, which is crucial for devices with limited memory capacity. Due to its computational efficiency, GhostNet can perform faster inference, making it suitable for real-time applications. This is essential for tasks like real-time image classification and intrusion detection where low latency is critical. GhostNet's lightweight architecture often leads to improved generalization, which means it can perform well on a wider range of data without overfitting. Thus, GhostNet is utilized for feature mapping of the proposed federated learning-based intrusion detection module.

In the Ghost module, the convolutional layer-based mapping is employed initially, and then, the linear operation is employed for obtaining the Ghost features as shown in Figure 3. The two paths utilized by GhostNet are:

Primary Path: This path is the main convolutional operation, which is usually a depth-wise separable convolution. Depth-wise separable convolutions are computationally cheaper than standard convolutions because they separate spatial filtering and channel-wise filtering. The feature mapping obtained through the primary path is formulated as:

$$F_m = A * c + d \tag{1}$$

where, the feature map is defined as, bias is notated as and conventional filters is denoted as.

Ghost Path: The ghost path is a lightweight, low-cost convolution with fewer channels. It's often referred to as a low-complexity operation. The ghost path captures additional features that are less computationally expensive. By fusing information from both paths, the network can achieve higher representational power while being more efficient. The feature mapping obtained through the ghost path is formulated as:

$$F_m = A * c' \tag{2}$$

where, the filter utilized in the ghost path is denoted as

Thus, the outcome of the GhostNet-based feature mapping aggregates the features mapped by the convolutional layer and the GhostModule-based features. The mapped features is fed into the BiGRU for extracting the long-term dependent features by considering both the forward and backward data processing.

2) ARCHITECTURE OF BIGRU

Bidirectional Gated Recurrent Units (BiGRU) play a significant role in intrusion detection compared to other deep learning models due to their ability to capture both past and future contextual information in sequential data, such as network traffic logs. BiGRU models consist of two Gated Recurrent Unit (GRU) layers, one processing data in a forward direction and the other in a backward direction. This bidirectional nature allows them to consider dependencies in both temporal directions, making them more effective at recognizing complex patterns and anomalies. In the context of intrusion detection, where threats can emerge from different sources and exhibit varying temporal characteristics, BiGRU models have a distinct advantage. They can effectively capture the evolving nature of network intrusions by analyzing past and future context, ultimately enhancing the accuracy of anomaly detection compared to traditional models or unidirectional deep learning models. The architecture of BiGRU is depicted in Figure 4.

The candidate state $\widetilde{Q}_T$ is evaluated using the reset gate and the input information is outlined as:

$$\widetilde{Q}_T = \tanh\left(L_Q\left[a_T * Q_{T-1}, E_T\right]\right) \tag{3}$$

Here, weight is notated as L_Q, and the candidate state concerning the past iteration is defined as Q_{T-1}. The expression concerning the reset gate is defined as:

$$a_T = \sigma\left(L_a\left[Q_{T-1}, E_T\right]\right) \tag{4}$$

Here, [0,1] is the limit for the sigmoid function defined as σ, and L_a is the weight. The reset gate is a mathematical function that operates on the input data at each time step in the sequence. It is typically represented as a sigmoid function, which squashes the input values to a range between 0 and 1. The reset gate function is designed to determine which information from the past hidden state should be ignored and which parts should be considered in the current processing. The update gate q_T, like the reset gate, is a mathematical function typically represented as a sigmoid function. It operates at each time step in the sequence and decides how much of the past hidden state information should be used to update the current hidden state. The specific operation of the update gate function is as follows:

$$q_T = \sigma\left(L_q\left[Q_{T-1}, E_T\right]\right) \tag{5}$$

Here, weight is defined as L_q. Finally, the formulation for the hidden state is defined as:

$$Q_T = (1 - q_T) * Q_{T-1} + q_T * \widetilde{Q}_T \tag{6}$$

Here, Q_T defines the hidden state. BiGRU is a powerful neural network architecture for intrusion detection and other sequential data analysis tasks. Its bidirectional processing

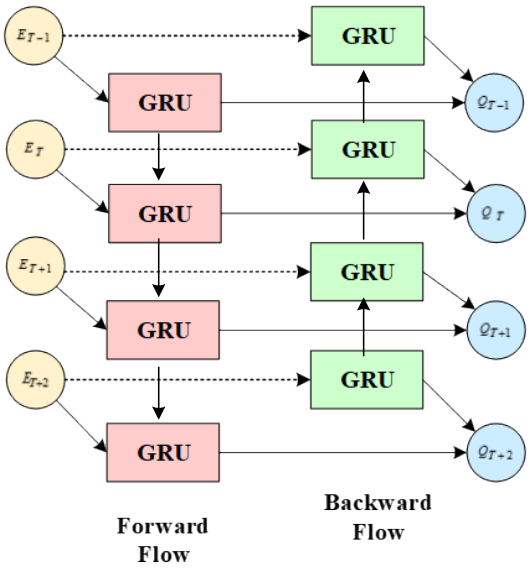

FIGURE 4. Architecture of BiGRU.

capability, combined with the gating mechanisms of the GRU, enables it to capture complex temporal dependencies and improve the accuracy of identifying network intrusions and anomalies. It is particularly effective in scenarios where past and future context is essential for accurate detection of intrusion. The hidden state evaluation for the bidirectional $\overrightarrow{Q_T}$ *and* $\overleftarrow{Q_T}$ processing in forward and backward direction is stated as:

$$\overrightarrow{Q_T} = GRU\left(E_T, \overrightarrow{Q_{T-1}}\right) \tag{7}$$

$$\overleftarrow{Q_T} = GRU\left(E_T, \overleftarrow{Q_{T-1}}\right) \tag{8}$$

$$Q_T = m_T \overrightarrow{Q_T} + n_T \overleftarrow{Q_T} + b_T \tag{9}$$

Here, m_T *and* n_T denotes the forward and backward hidden layer weights at the time T and the hidden layer state is notated as b_T. The outcome of the BiGRU is fed into the fully connected layer and softmax layer for classifying the intrusion types.

3) ARCHITECTURE OF GHOST_BINET

The hybrid deep learning model GhostNet based bidirectional gated recurrent unit (Ghost_BiNet) is designed by integrating the GhostNet and BiGRU, which is portrayed in Figure 5.

Here, the hybrid classifier comprises of weights and biases, which are adjusted optimally using the CAh algorithm for minimizing the information loss during the information training phase.

4) LOSS FUNCTION OPTIMIZATION USING CHAOTIC CHEBYSHEV ARTIFICIAL HUMMING BIRD (CAH) ALGORITHM

The proposed CAh algorithm is designed by integrating the artificial humming bird algorithm with chaotic Chebyshev mapping to enhance the randomness in the algorithm for solving the local optimal trapping issue. Hummingbirds are

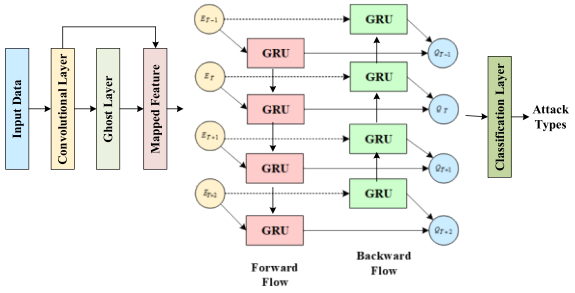

FIGURE 5. Architecture of Ghost_BiNet for intrusion detection.

taken into consideration to address the optimization problem because of their unusual foraging characteristics and flight abilities. One of the tiniest birds with good memory skills and the ability to recall both the spatial and temporal position of the food source is the hummingbird. Due to their flexible shoulder joints, birds can rotate their wings 180 degrees and feed insects while catching them. The distinctive foraging talent of flight based on the diagonal movement of the hummingbird helps to capture the target more easily. To capture the target, the birds use their migratory, territorial, and guided foraging characteristics. The approach to resolving the optimization problem is the identification of the food source. While searching for food sources the hummingbirds use the guided foraging behavior, wherein the searching capability is further enhanced by incorporating chaotic Chebyshev mapping

5) MATHEMATICAL MODELLING

The initialization of the parameters is the first step of the algorithm formulation. Thus, the boundary limits of the feature region, the total count of iteration, and the population size that defines the number of artificial hummingbirds in the feature region are initialized. After initializing the parameters, the candidate solutions (artificial hummingbirds) are randomly placed in the feature region and is expressed as:

$$B_i = K + M\,(L - K) \quad i = 1, 2, \ldots .Z \tag{10}$$

The random number that is represented as falling between limit [0,1], and i^{th} food source is referred as B_i. The search space's borders that correspond to its lower and higher limits are determined by K and L, respectively. Also, the entire population in the feature region is notated as Z. C indicates the dimension for the feature region.

a: SOLUTION UPDATION

The solutions acquired by the candidates are updated in the visit table that has the history of all the search spaces. The solution updation table is defined as:

$$F_{i,j} = \begin{cases} 0 & if\ i \neq j \\ null & i = j \end{cases} \quad i = 1, 2, \ldots Z;\ j = 1, 2, \ldots Z \tag{11}$$

When $F_{i,j} = 0$ in the current iteration, the i^{th} candidate visits the j^{th} target. The food is consumed by the candidate in the current iteration, according to the value $F_{i,j} = null$.

b: DIRECT SEARCHING

In the search criteria based on the direct search for the food reserve, the candidates explore the most frequently visited area. Here, the assumption considered is that, the search must not be visited recently. While foraging for food, the candidates employ various flight skills to identify the food reserve quickly. The various flights made by the candidates in the feature region are represented as:

Horizontal flight:

$$H(i) = \begin{cases} 1 & if\ i = rand\ i\ ([1, C]) \\ 0 & else \end{cases} \quad i = 1, 2, \ldots C \tag{12}$$

Slant flight:

$$H(i) = \begin{cases} 1 & if\ i = N(j), j \in [1, e], \\ & N = D(e), e \in \\ & [2, [U_1(C-2)] + 1] \\ 0 & else \end{cases} \quad i = 1, 2, \ldots C \tag{13}$$

Full-view flight:

$$H(i) = 1 \quad i = 1, 2, \ldots C \tag{14}$$

A random permutation is produced and is denoted as $D(e)$ inside the bounds of the random number M_1 with the range of [0, 1]. The solution's dimension is denoted by C, is chosen at random by the algorithm $rand\ i\ ([1, C])$ from a range $[1, C]$. The outcome of direct searching behaviour is therefore expressed as:

$$h_i(\tau + 1) = B_{i,Q}(\tau) + c \cdot H \cdot \left(B_i(\tau) - B_{i,Q}(\tau)\right) \tag{15}$$

$$c \sim N(0, 1) \tag{16}$$

The target food source is described as $B_{i,Q}(\tau)$ and the i^{th} food source's location is given as in $B_i(\tau)$ at that moment τ. The direct searching factor is denoted by c, which is defined as the normal distribution $N(0, 1)$ with a mean of 0 and a standard deviation of 1. Here, for enhancing the search capability to avoid the solution trapping at local solution, Chaotic Chebyshev randomness is introduced and is expressed as:

$$h_i(\tau + 1) = \cos\left(D.\cos^{-1} h_\tau\right) \tag{17}$$

where, the solution accomplished in the present iteration is indicated as $h_{\tau+1}$, and the solution accomplished in the τ^{th} iteration is indicated as h_τ. D is the control parameter within the range [0, 1] utilized for selecting the best individuals. Then, the solution accomplished by the proposed CAh is expressed as:

$$h_i(\tau + 1) = 0.5\left[h_i(\tau + 1)_{Artificial\ hum\min g\ bird}\right] + 0.5\left[h_i(\tau + 1)_{CC}\right] \tag{18}$$

$$h_i(\tau + 1) = 0.5\left[B_{i,Q}(\tau) + c \cdot H \cdot \left(B_i(\tau) - B_{i,Q}(\tau)\right)\right] + 0.5\left[\cos\left(D.\cos^{-1} h_\tau\right)\right] \tag{19}$$

Thus, the position updation acquired by the combined behavior of the artificial humming bird and the chaotic chebyshev enhances the convergence rate by identifying the food source more accurate due to the incorporation of randomness. After detecting the food source, the feasibility of the solution is evaluated based on the fitness function evaluated in equation (6) and is expressed as:

$$B_i(\tau + 1) = \begin{cases} B_i(\tau)\ \vec{Fit}\left(B_i(\tau)\right) \leq \vec{Fit}\left(h_i(\tau + 1)\right) \\ h_i(\tau + 1)\ \vec{Fit}\left(B_i(\tau)\right) > \vec{Fit}\left(h_i(\tau + 1)\right) \end{cases} \tag{20}$$

where, the fitness function is indicated as $\vec{Fit}$.

c: BOUNDED SEARCHING

The in-depth search of the food based on the solution acquired by the candidates in the direct searching mechanism is devised in the bounded searching criteria. The solution accomplished by the candidates in the feature region is outlined as:

$$h_i(\tau + 1) = B_{i,Q}(\tau) + t \cdot H \cdot B_i(\tau) \tag{21}$$

$$t \sim N(0, 1) \tag{22}$$

where, the territorial factor is represented as t that is defined based on the normal distribution $N(0, 1)$ with standard deviation of 1 and mean of 0.

d: DISPERSED SEARCHING

When the scarcity of food occurs in the present location, then the candidate's moves towards the next location in search of identifying the food reserve. Thus, in the dispersed food search mechanism, the candidates explore more search areas and assist in capturing the global best solution. The solution accomplished by the candidates in the dispersed searching phase is outlined as:

$$B_{bad}(\tau + 1) = K + M \cdot (L - K) \tag{23}$$

where, the worst food source with minimal nectar filling is indicated as B_{bad}.

e: FEASIBILITY OF SOLUTION

The feasibility of the solution accomplished by the proposed CAh algorithm is evaluated based on MSE defined in equation (33).

f: TERMINATION

The attainment of maximal iteration or the global best solution terminates the iteration of algorithm. The pseudo-code for CAh is presented in Algorithm 1.

Algorithm 1 Pseudo-code for proposed CAh Algorithm

Pseudo-code for proposed CAh Algorithm
1 Initialize the population, iteration and dimension
2 While ($\tau < \tau_{\max}$)
3 Estimate the fitness using equation (33)
4 Update the solution in direct searching using equation (20)
5 Update the solution in bounded searching using equation (21)
6 Update the solution in dispersed searching using equation (23)
7 Re-estimate the feasibility using equation (33)
8 $\tau = \tau + 1$
9 End while
10 Return best solution
11 stop

Thus using the solution evaluated by the CAh algorithm, the loss function optimization is employed for minimizing the information loss, which in turn enhances the generalization capability of the classifier. The highly generalized classifier provides the more accurate intrusion detection with minimal false alarm.

C. HOMOMORPHIC ENCRYPTION

The outcome of the local model updates are encrypted using the Homomorphic encryption technique for further enhancing the security of the information. Homomorphic encryption adds a significant layer of privacy and security to federated learning-based intrusion detection because it protects the confidentiality of sensitive network traffic data and allows multiple parties to collaborate without exposing their data. This technique helps in achieving a balance between data sharing and privacy, which is crucial in fields like intrusion detection where the confidentiality of data is of utmost importance. The outcome of the Homomorphic encryption is stated as:

$$H(e) = \frac{G(e)}{(e-\alpha_0)(e-\alpha_1)\ldots..(e-\alpha_{l-1})} + d(e) \quad (24)$$

Here, the updates obtained from the Enhanced Ghost_BiNet is defined as $G(e)$. The outcome after the Homomorphic encryption is denoted as $H(e)$, wherein the keys used for performing the encryption is denoted as $\alpha_0, \alpha_1, \ldots \alpha_{l-1}$.Besides, $d(e)$ refers to the polynomial degree is defined as, wherein t is a positive value.

D. SERVER UPDATION USING COLLABORATIVE OPTIMIZATION WEIGHTS

For the server updation, the server assigns weights for the updates and sets a threshold value for gathering updates from the local model that has the updates greater than the threshold. By doing so, the communications rounds in model update is further reduced. The server utilizes the attention mechanism for assigning weights to the updates and is evaluated as:

$$F = \tanh(w) \quad (25)$$

$$G = soft\max\left(w_f^T F\right) \quad (26)$$

$$w^* = n \cdot G^T \quad (27)$$

Here, the weight matrix is denoted as G, and the parameter matrix is denoted as w_f. The weight estimated by the server is denoted as F, and n denotes the number of local models. The updates that has the weight higher than the threshold t is defined as:

$$w_B = \sum_{x=1}^{X} \frac{|D_x|}{n^*} g_x w_x \quad (28)$$

where, number of chosen models is denoted as n^*, the data sample from x^{th} client is denoted as D_x and the weight matrix of x^{th} client is denoted as g_x. Thus, using the collaborative optimization of weights, the communication rounds of the server model updation is minimized.

IV. RESULT AND DISCUSSION

PYTHON programming tool is utilized for the implementation of the proposed federated learning based intrusion detection mechanism. The measures like Accuracy, Precision, Recall, F-Measure and mean square error (MSE).

Description of Dataset: The dataset utilized for the assessment of proposed intrusion detection mechanism is KDD CUP 99 [30], CICIDS2017 [31], and UNSW-NB15 [32].

KDD CUP 99: The dataset comprises of 23 classes, with a total of 4, 94,020 data. Besides, the dataset comprises of 42 attributes in total.

CICIDS2017: The dataset consists of 2,25, 745 data with two classes like Benign and DDoS attack. A total of 79 features are available in the dataset.

UNSW-NB15: The UNSW-NB15 dataset comprises of 82,332 data with two classes like attack and normal. Besides, the dataset comprises of 45 attributes in total.

Definition for Assessment measures: The federated learning based intrusion detection mechanisms are evaluated based on various measures liked accuracy, precision, recall, F-Score and MSE. The definitions are:

$$FLID_{Acc} = \frac{FLID_{T_P} + FLID_{T_N}}{FLID_{T_P} + FLID_{T_N} + FLID_{F_P} + FLID_{F_N}} \quad (29)$$

$$FLID_{\Pr e} = \frac{FLID_{T_P}}{FLID_{T_P} + FLID_{F_P}} \quad (30)$$

$$FLID_{\text{Rec}} = \frac{FLID_{T_P}}{FLID_{T_P} + FLID_{F_N}} \quad (31)$$

$$FLID_{F-M} = \frac{2\left(FLID_{\Pr e} * FLID_{\text{Rec}}\right)}{\left(FLID_{\Pr e} + FLID_{\text{Rec}}\right)} \quad (32)$$

$$FLID_{MSE} = \frac{1}{T}\sum_{i=1}^{T}(O_i - T_i)^2 \quad (33)$$

Here, accuracy is defined as $FLID_{Acc}$, the precision is notated as $FLID_{\Pr e}$, the recall is denoted as $FLID_{\text{Rec}}$, F-Score is indicated as $FLID_{F-M}$ and MSE is defined as $FLID_{MSE}$. Then, the true positive is notated as $FLID_{T_P}$, the true negative is defined as $FLID_{T_N}$, false positive is indicated as $FLID_{F_P}$ and false negative is represented as $FLID_{F_N}$. The total samples

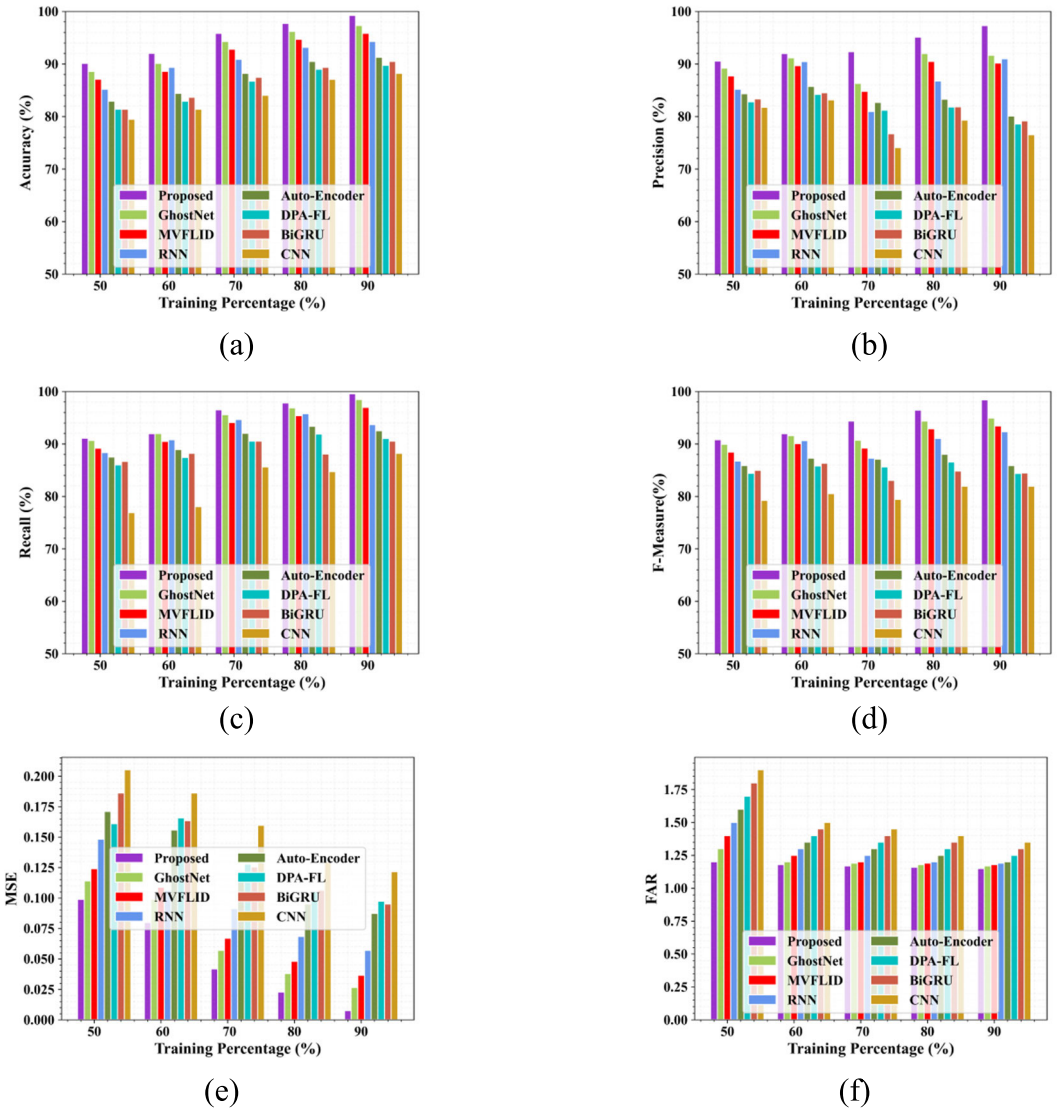

FIGURE 6. Assessment using KDD Cup 99 dataset (a) accuracy, (b) precision, (c) recall, (d) F-Score, (e) MSE and (f) FAR.

is denoted as T, the observed value is referred as O_i and the target is stated as T_i.

Existing methods for comparison: The existing federated learning based deep learning methods like CNN [25], Auto-Encoder [27], RNN [25], BiGRU [33], GhostNet [34], DPA-FL, and MVFLID are compared with proposed method to depict the superiority of the proposed model.

A. ASSESSMENT USING KDD CUP 99 DATASET

The assessment of the federated learning based intrusion detection methods using the KDD Cup 99 is portrayed in Figure 6. Let, the accuracy estimated by the proposed Enhanced Ghost_BiNet is 97.71%; still the conventional methods like GhostNet, BiGRU, RNN, Auto Encoder, CNN, MVFLID and DPA-FL acquired the accuracy of 96.19%, 93.15%, 90.49%, 89.35%, 87.07%, 95.83% and 89.75% respectively with 80% of learning data. Here, the elevated accuracy is accomplished by the Enhanced Ghost_BiNet model due to the design of hybrid deep learning model with the loss function optimization. Likewise, for all the assessment measures, the Enhanced Ghost_BiNet acquires the superior outcome using the KDD Cop 99 dataset.

B. ASSESSMENT USING CICIDS2017 DATASET

The assessment of the federated learning based intrusion detection methods using the CICIDS2017 dataset are portrayed in Figure 7. Let, the Precision estimated by the proposed Enhanced Ghost_BiNet is 90.76%; still the conventional methods like GhostNet, BiGRU, RNN, Auto Encoder, CNN, MVFLID and DPA-FL acquired the accuracy of 85.61%, 80%, 81.88%, 75.91%, 73.49% 84.11%, and 80.38% respectively with 70% of learning data. Similarly, the MSE estimated is 4.9%, 6.08%, 9.88%, 12.54%, 13.30% and 17.73% for the Enhanced Ghost_BiNet, GhostNet, BiGRU, RNN, Auto Encoder, and CNN respectively. Thus, the anal-

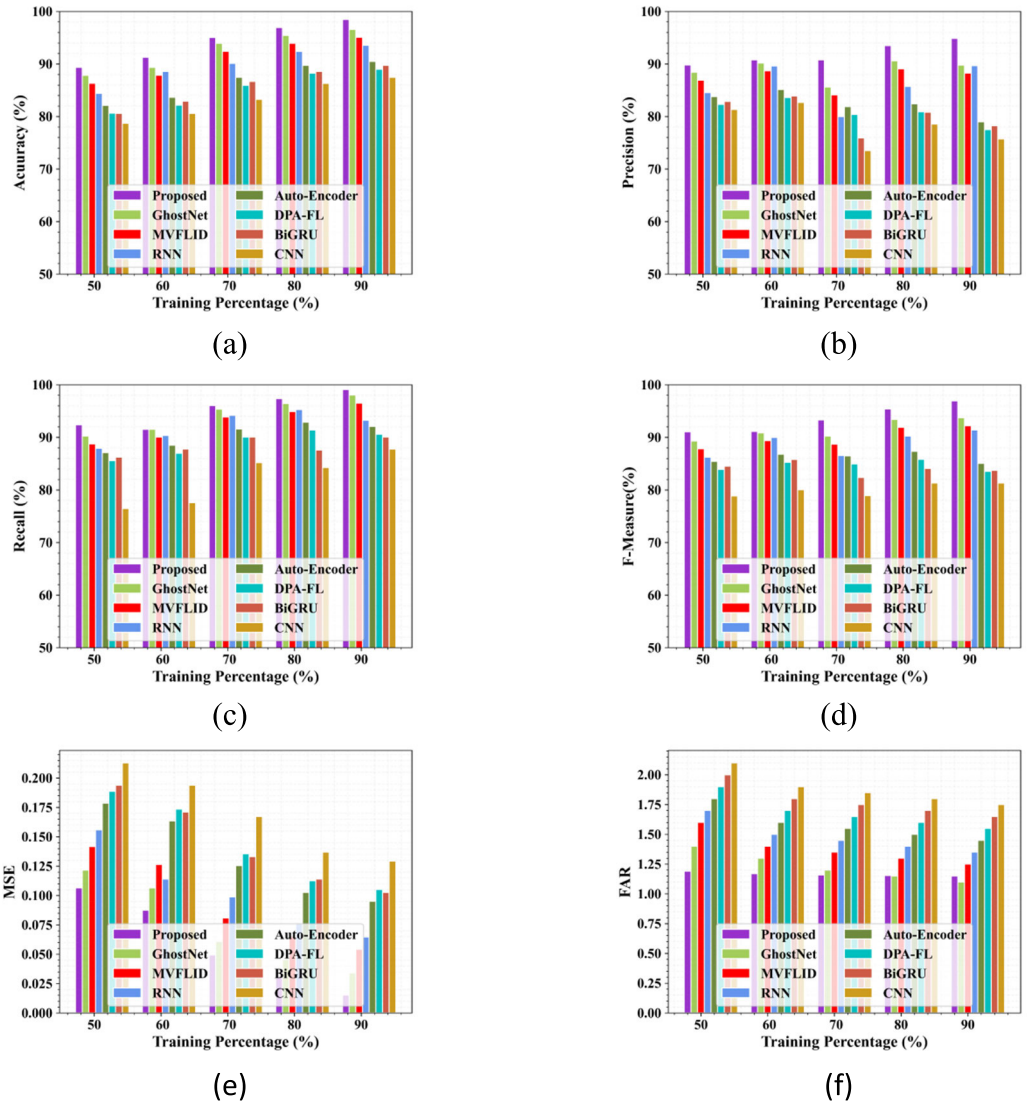

FIGURE 7. Assessment using CICIDS2017 dataset (a) accuracy, (b) precision, (c) recall, (d) F-Score, (e) MSE and (f) FAR.

ysis indicates the better outcome of the proposed Enhanced Ghost_BiNet compared to the existing models.

C. ASSESSMENT USING UNSW-NB-15 DATASET

The assessment of the federated learning based intrusion detection methods using the UNSW-NB-15 dataset are portrayed in Figure 8. Let, the Recall estimated by the proposed Enhanced Ghost_BiNet is 91.29%; still the conventional methods like GhostNet, BiGRU, RNN, Auto Encoder, CNN, MVFLID and DPA-FL acquired the accuracy of 91.32%, 90.14%, 88.26%, 87.561%, 77.36%, 89.82%, and 86.76% respectively with 60% of learning data. Similarly, the F-Score estimated is 90.74%, 90.51%, 89.67%, 86.51%, 85.53%, 79.80%, 89.01%, and 85.01% for the Enhanced Ghost_BiNet, GhostNet, BiGRU, RNN, Auto Encoder, CNN, MVFLID and DPA-FL respectively. Thus, the analysis indicates the better outcome of the proposed Enhanced Ghost_BiNet compared to the existing models.

D. ACCURACY LOSS ASSESSMENT

The accuracy-loss analysis of the proposed Enhanced Ghost_BiNet is presented in Figure 9, wherein the analysis using KDD Cup 99, CICIDS2017 and UNSW-NB-15 is portrayed in Figure 9(a), Figure 9(b) and Figure 9(c). Accuracy-loss analysis is critical for evaluating the effectiveness of FL-based intrusion detection method. While considering the accuracy-loss analysis, the model's performance is evaluated on both the training and testing datasets. The goal is to achieve closer accuracy-loss values for both datasets, indicating that the model generalizes well to unknown data. For example, if the accuracy-loss on the training dataset is significantly higher than on the testing dataset, it indicates that the model may be overfitting to the training data, capturing noise and irrelevant patterns that do not generalize well to new data. Conversely, if the accuracy-loss on the testing dataset is significantly lower than that on the training dataset, it indicates that the model may be underfitting, failing to capture the

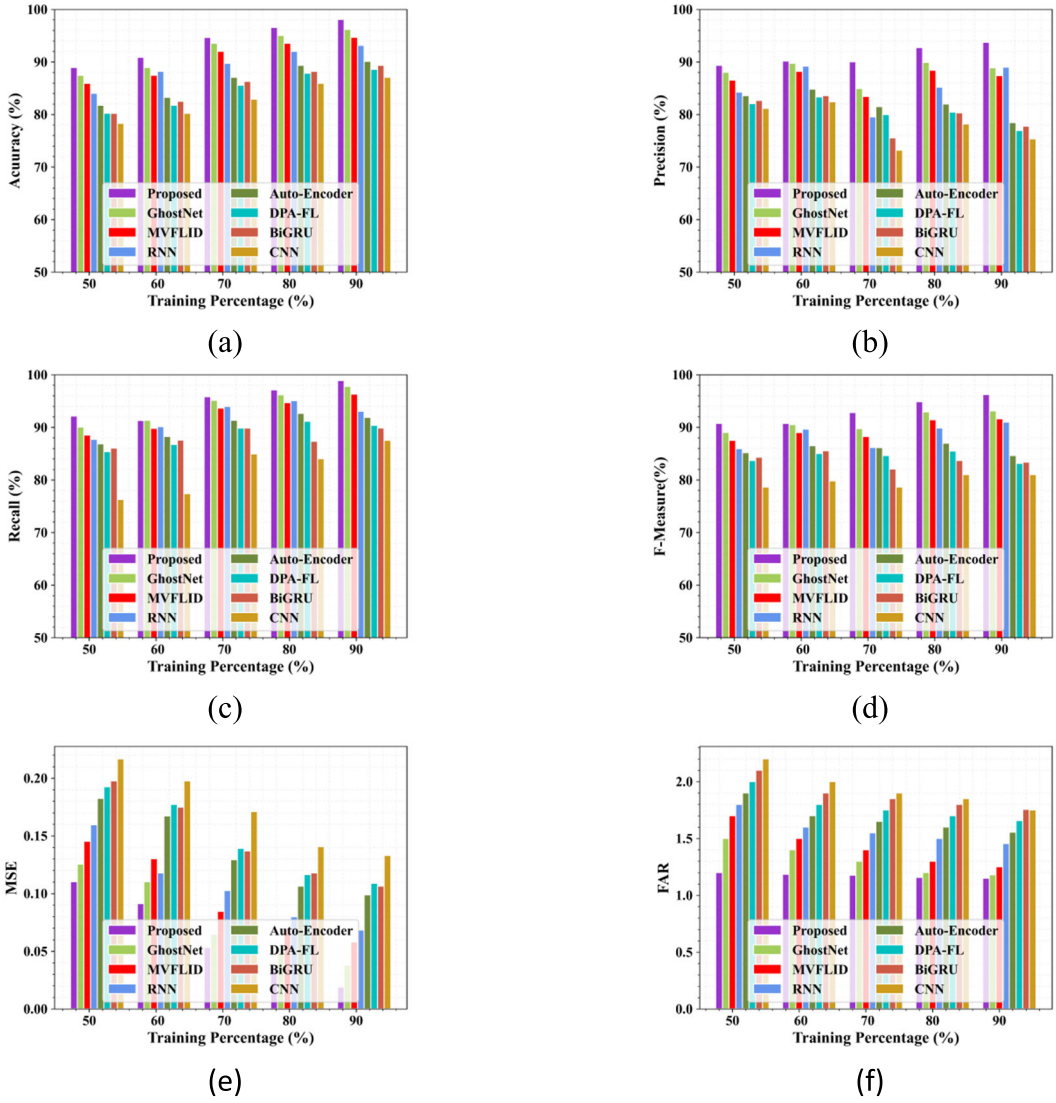

FIGURE 8. Assessment using UNSW-NB-15 dataset (a) accuracy, (b) precision, (c) recall, (d) F-Score, (e) MSE and (f) FAR.

underlying patterns in the data. The testing and training analysis of accuracy-loss for the proposed Enhanced Ghost_BiNet model are closer, which depicts the better generalization capability of the model.

E. CONVERGENCE ANALYSIS

The convergence analysis of the proposed CAh algorithm with the traditional artificial humming bird algorithm (AHA) for the three various datasets is presented in Figure 10. The analysis depicts the better performance of the CAh algorithm. The rate of convergence measures how quickly the optimization algorithm approaches the optimal solution. Here, the proposed CAh algorithm converges faster compared to the existing AHA algorithm due to the incorporation of Chaotic Chebyshev randomness. The faster rate of convergence of CAh indicates that the algorithm converges to the optimal solution more quickly; that is advantageous in practical applications as it reduces the time and computational cost needed to solve optimization problems, making the algorithm more efficient and effective.

F. COMPARATIVE DISCUSSION

The comparative discussion based on the better outcome is presented in Table 1. The maximal accuracy estimated by Enhanced Ghost_BiNet is 99.24%, which is 11.11%, 8.82%, 8.05%, 4.98%, 1.91%, 9.56%, and 3.43% superior compared to CNN, Auto Encoder, RNN, BiGRU, GhostNet, DPA-FL, and MVFLID. The maximal Precision estimated by Enhanced Ghost_BiNet is 97.30%, which is 21.36%, 18.63%, 17.70%, 6.47%, 5.79%, 14.89%, and 1.50% superior compared to CNN, Auto Encoder, RNN, BiGRU, GhostNet, DPA-FL, and MVFLID. The maximal Recall estimated by Enhanced Ghost_BiNet is 99.56%, which is 11.41%, 9.08%, 7.05%, 5.88%, 1.10%, 8.56%, and 2.61% superior compared to CNN, Auto Encoder, RNN, BiGRU, GhostNet, DPA-FL, and MVFLID. The maximal F-Score estimated

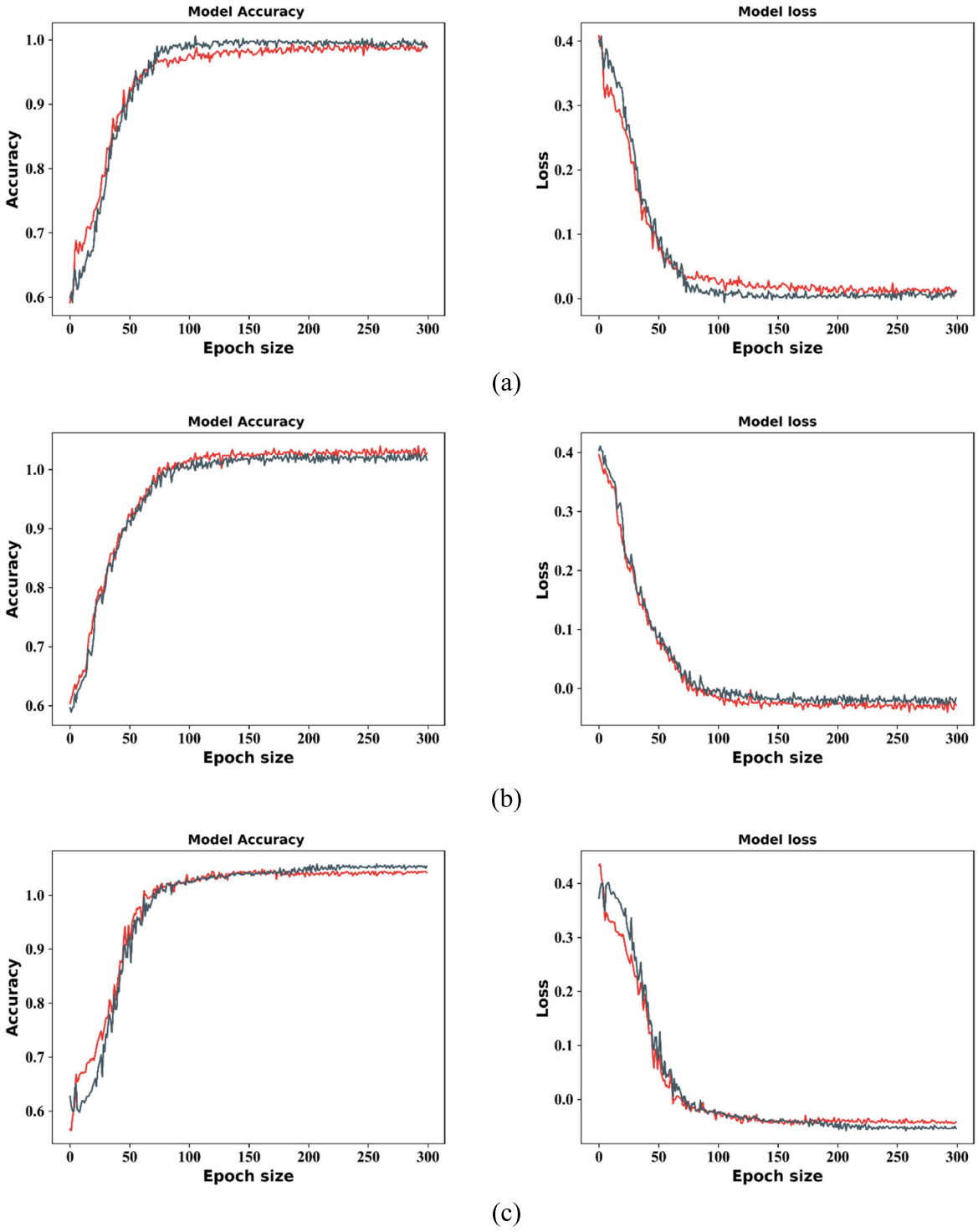

FIGURE 9. Accuracy-Loss: (a) KDD Cup 99, (b) CICIDS2017 and (c) UNSW-NB-15.

by Enhanced Ghost_BiNet is 98.42%, which is 16.74%, 14.18%, 12.76%, 6.18%, 3.54%, 5.06%, and 5.06% superior compared to CNN, Auto Encoder, RNN, BiGRU, GhostNet, DPA-FL, and MVFLID. The minimal MSE estimated by Enhanced Ghost_BiNet is 0.01, which is 91.67%, 90.00%, 88.89%, 83.33%, 66.67%, 89.74%, and 72.69% superior compared to CNN, Auto Encoder, RNN, BiGRU, GhostNet, DPA-FL, and MVFLID. The minimal FAR estimated by Enhanced Ghost_BiNet is 0.13, which is 15.56%, 5.00%, 4.20%, 12.31%, 2.56%, 8.80%, and 3.39% superior compared to CNN, Auto Encoder, RNN, BiGRU, GhostNet, DPA-FL, and MVFLID.

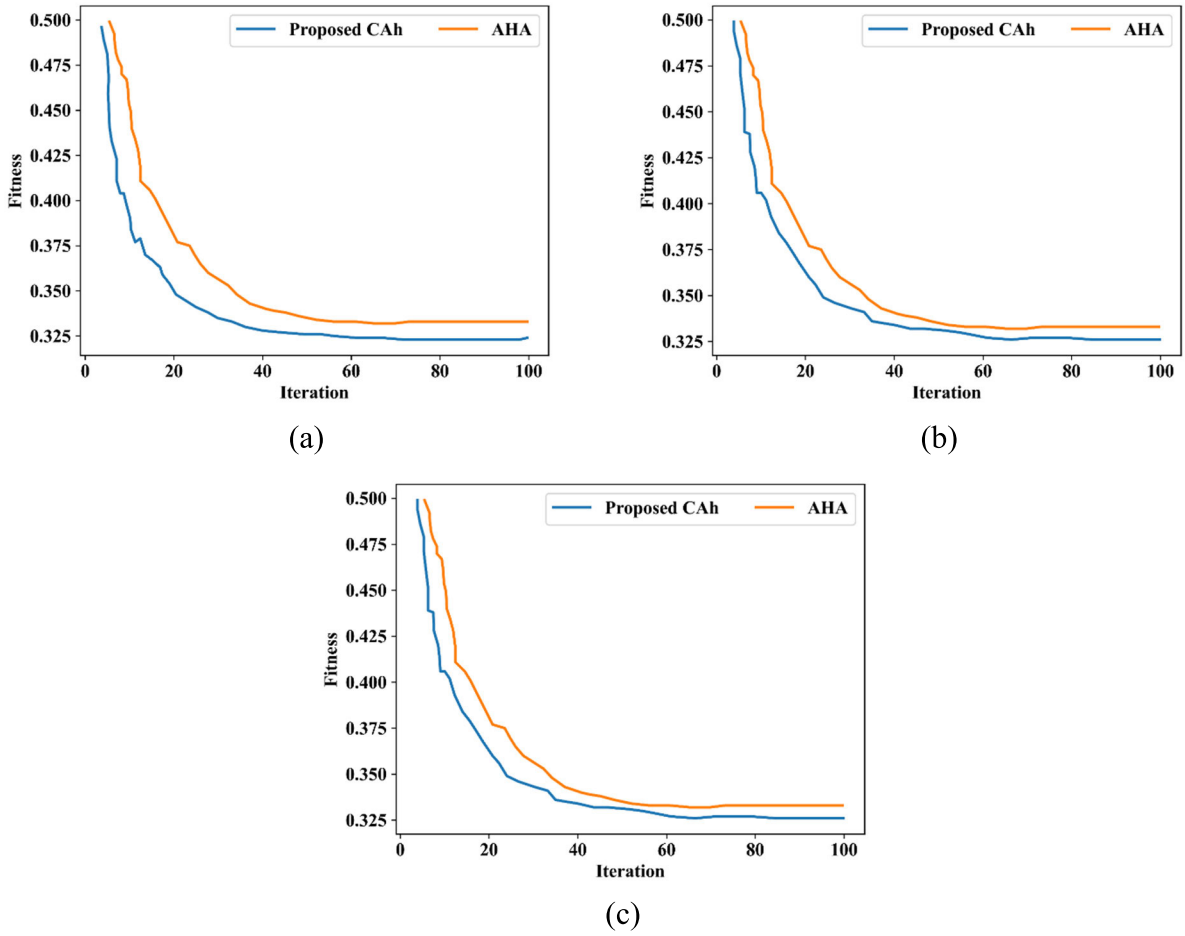

FIGURE 10. Accuracy-Loss: (a) KDD Cup 99, (b) CICIDS2017 and (c) UNSW-NB-15.

A key advantage of using a bidirectional architecture of proposed model allows to consider both past and future data when making predictions. In the context of intrusion detection, network traffic data is often sequential, and understanding the context of data is crucial for identifying patterns and anomalies. The bidirectional nature of proposed Enhanced Ghost_BiNet enables the model to capture dependencies in both directions, improving its ability to detect complex attack patterns that may span over multiple time steps. The ghost concept refers to the idea of training the network on both the original input and a modified or perturbed version of the input. This technique is beneficial for enhancing the model's robustness and generalization capabilities. By exposing the model to variations of the data, it can learn to differentiate between normal and malicious behavior more effectively. Ghost Bi-Net leverages this concept to improve its ability to identify unseen attack variants, making it more adaptable to emerging threats. Besides, the loss function optimization using the CAh algorithm enhances the intrusion detection by fine tuning the optimal parameters like weights and bias and hence enhances the generalization capability.

The proposed federated learning-based intrusion detection method, as demonstrated by the achieved results, offers significant practical implications for improving cybersecurity defenses. The maximal accuracy, precision, recall, and F-score attained by Enhanced Ghost_BiNet outperform several conventional methods, including CNN, Auto Encoder, RNN, BiGRU, GhostNet, DPA-FL, and MVFLID, by substantial margins. This superior performance indicates the effectiveness of the proposed method in accurately detecting and classifying intrusions in network traffic data. Additionally, the minimal mean squared error (MSE) and false alarm rate (FAR) achieved by Enhanced Ghost_BiNet further highlight its superiority over existing approaches, emphasizing its ability to minimize prediction errors and false positives. These results underscore the practical relevance and efficacy of federated learning-based intrusion detection in enhancing cybersecurity defenses and mitigating threats in diverse network environments.

V. CONCLUSION

In conclusion, the proposed intrusion detection mechanism represents a significant advancement in enhancing information security and detection accuracy. The system model of the proposed intrusion detection mechanism leverages a novel deep learning model called Enhanced Ghost_BiNet. This hybrid classifier integrates GhostNet and Bidirectional Gated Recurrent Unit (BiGRU) and optimizes it using the Chaotic

TABLE 1. Comparative discussion based on best outcome with 90% training and 10% testing data.

Metrics/ Methods	CNN	Auto Encoder	RNN	BiGRU	GhostNet	DPA-FL	MVFLID	Enhanced Ghost_BiNet
KDD Cup 99								
Accuracy	88.21	90.49	91.25	94.30	97.34	89.75	95.84	**99.24**
Precision	76.52	79.17	80.08	91.00	91.67	82.81	95.84	**97.30**
Recall	88.20	90.52	92.54	93.71	98.46	91.04	96.96	**99.56**
F-Score	81.94	84.46	85.86	92.34	94.94	93.44	93.44	**98.42**
MSE	0.12	0.10	0.09	0.06	0.03	0.10	0.04	**0.01**
FAR	1.35	1.20	1.19	1.30	1.17	1.25	1.18	**1.13**
CICIDS2017								
Accuracy	87.45	89.73	90.49	93.54	96.58	88.99	95.08	**98.48**
Precision	75.74	78.23	78.98	89.65	89.77	82.31	88.27	**94.87**
Recall	87.76	90.08	92.10	93.27	98.03	90.60	96.53	**99.12**
F-Score	81.31	83.73	85.04	91.43	93.72	83.54	92.22	**96.95**
MSE	0.13	0.10	0.10	0.06	0.03	0.11	0.05	**0.02**
FAR	1.75	1.45	1.35	1.65	1.10	1.55	1.25	**1.15**
UNSW-NB-15								
Accuracy	87.07	89.35	90.11	93.16	96.20	88.61	94.70	**98.10**
Precision	75.36	77.78	78.46	89.02	88.89	82.07	87.39	**93.75**
Recall	87.54	89.86	91.88	93.05	97.81	90.38	96.31	**98.90**
F-Score	81.00	83.38	84.64	90.99	93.13	83.14	91.63	**96.26**
MSE	0.13	0.11	0.10	0.07	0.04	0.11	0.06	**0.02**
FAR	1.75	1.56	1.46	1.76	1.18	1.66	1.25	**1.15**

Chebyshev Artificial Humming Bird (CAh) algorithm. This optimization minimizes information loss during the learning phase, resulting in more accurate intrusion detection. The architecture of GhostNet provides computational efficiency, making it suitable for resource-constrained environments like mobile and edge devices. The BiGRU component of the proposed model is instrumental in capturing both past and future contextual information in sequential data, enhancing its ability to recognize complex patterns and anomalies in network traffic logs. The loss function optimization using the CAh algorithm further fine-tunes the model, improving its generalization and overall performance. Homomorphic encryption is employed to secure the model updates, adding an additional layer of privacy and security to the federated learning process. The research conducted extensive experiments using publicly available datasets, such as KDD CUP 99, CICIDS 2017, and UNSW-NB15, for validation. The results consistently demonstrated the superiority of the proposed Enhanced Ghost_BiNet model compared to existing methods. However, limitations may arise in terms of computational resources, training time, and scalability, particularly in extremely large-scale network environments. Future research could explore addressing these limitations, as well as integrating real-time data streams and continuous learning to adapt to evolving threats and network conditions. Overall, the proposed framework holds promise for improving intrusion detection while safeguarding data privacy and security in diverse cybersecurity scenarios.

ACKNOWLEDGMENT

The authors would like to take this opportunity to thank the management of Vellore Institute of Technology for providing the APC and encouragement to carry out this work.

REFERENCES

[1] E. M. Campos, P. F. Saura, A. González-Vidal, J. L. Hernández-Ramos, J. B. Bernabé, G. Baldini, and A. Skarmeta, "Evaluating federated learning for intrusion detection in Internet of Things: Review and challenges," *Comput. Netw.*, vol. 203, Feb. 2022, Art. no. 108661.

[2] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, S. Bhattacharya, P. K. R. Maddikunta, and T. R. Gadekallu, "Federated learning for intrusion detection system: Concepts, challenges and future directions," *Comput. Commun.*, vol. 195, pp. 346–361, Nov. 2022.

[3] X. Huang, J. Liu, Y. Lai, B. Mao, and H. Lyu, "EEFED: Personalized federated learning of execution & evaluation dual network for CPS intrusion detection," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 41–56, 2023.

[4] N. K. Singh, C. U. O. Kumar, and R. Sridhar, "Flash crowd prediction in Twitter," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–6.

[5] P. R. K. S. Bhama, "Detecting and confronting flash attacks from IoT botnets," *J. Supercomput.*, vol. 75, no. 12, pp. 8312–8338, Dec. 2019.

[6] P. R. K. S. Bhama, "Fuzzy based energy efficient workload management system for flash crowd," *Comput. Commun.*, vol. 147, pp. 225–234, Nov. 2019.

[7] C. U. O. Kumar and P. R. K. S. Bhama, "Proficient detection of flash attacks using a predictive strategy," in *Emerging Research in Computing, Information, Communication and Applications*, vol. 1. Singapore: Springer, 2021, pp. 367–379.

[8] P. R. K. S. Bhama, "Efficient ensemble to combat flash attacks," *Comput. Intell.*, vol. 40, no. 1, pp. 1–20, Nov. 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/coin.12488

[9] A. Belenguer, J. Navaridas, and J. A. Pascual, "A review of federated learning in intrusion detection systems for IoT," 2022, *arXiv:2204.12443*.

[10] O. Aouedi, K. Piamrat, G. Müller, and K. Singh, "FLUIDS: Federated learning with semi-supervised approach for intrusion detection system," in *Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2022, pp. 523–524.

[11] S. Arisdakessian, O. A. Wahab, A. Mourad, H. Otrok, and M. Guizani, "A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 4059–4092, Aug. 2022.

[12] P. Singh, G. S. Gaba, A. Kaur, M. Hedabou, and A. Gurtov, "Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 722–731, Feb. 2023.

[13] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection," *Comput. Electr. Eng.*, vol. 103, Oct. 2022, Art. no. 108379.

[14] C. U. Om Kumar, K. Tejaswi, and P. Bhargavi, "A distributed cloud-prevents attacks and preserves user privacy," in *Proc. 15th Int. Conf. Adv. Comput. Technol. (ICACT)*, Sep. 2013, pp. 1–6.

[15] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection," *J. Netw. Syst. Manage.*, vol. 31, no. 1, pp. 1–23, Jan. 2023.

[16] S. Chatterjee and M. K. Hanawal, "Federated learning for intrusion detection in IoT security: A hybrid ensemble approach," *Int. J. Internet Things Cyber-Assurance*, vol. 2, no. 1, p. 62, 2022.

[17] K. H. Shibly, M. D. Hossain, H. Inoue, Y. Taenaka, and Y. Kadobayashi, "Personalized federated learning for automotive intrusion detection systems," in *Proc. IEEE Future Netw. World Forum (FNWF)*, Oct. 2022, pp. 544–549.

[18] L. Xing, K. Wang, H. Wu, H. Ma, and X. Zhang, "FL-MAAE: An intrusion detection method for the Internet of Vehicles based on federated learning and memory-augmented autoencoder," *Electronics*, vol. 12, no. 10, p. 2284, May 2023.

[19] J. Toldinas, A. Venč kauskas, A. Liutkevič ius, and N. Morkevič ius, "Framing network flow for anomaly detection using image recognition and federated learning," *Electronics*, vol. 11, no. 19, p. 3138, Sep. 2022.

[20] C. U. Om Kumar, J. Durairaj, S. A. Ahamed Ali, Y. Justindhas, and S. Marappan, "Effective intrusion detection system for IoT using optimized capsule auto encoder model," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 13, p. e6918, Jun. 2022.

[21] A. Alazab, A. Khraisat, S. Singh, and T. Jan, "Enhancing privacy-preserving intrusion detection through federated learning," *Electronics*, vol. 12, no. 16, p. 3382, Aug. 2023.

[22] C. U. Om Kumar, S. Kishore, and A. Geetha, "Debugging using MD5 process firewall," in *Proc. Int. Conf. Contemp. Comput. Informat. (IC3I)*, Nov. 2014, pp. 1279–1284.

[23] H. Liang, D. Liu, X. Zeng, and C. Ye, "An intrusion detection method for advanced metering infrastructure based on federated learning," *J. Mod. Power Syst. Clean Energy*, vol. 2022, pp. 1–11, Apr. 2022.

[24] E. Novikova, E. Doynikova, and S. Golubev, "Federated learning for intrusion detection in the critical infrastructures: Vertically partitioned data use case," *Algorithms*, vol. 15, no. 4, p. 104, Mar. 2022.

[25] M. M. Rashid, S. U. Khan, F. Eusufzai, M. A. Redwan, S. R. Sabuj, and M. Elsharief, "A federated learning-based approach for improving intrusion detection in industrial Internet of Things networks," *Network*, vol. 3, no. 1, pp. 158–179, Jan. 2023.

[26] G. de Carvalho Bertoli, L. A. P. Junior, O. Saotome, and A. L. dos Santos, "Generalizing intrusion detection for heterogeneous networks: A stacked-unsupervised federated learning approach," *Comput. Secur.*, vol. 127, Apr. 2023, Art. no. 103106.

[27] S. Halder and T. Newe, "Radio fingerprinting for anomaly detection using federated learning in LoRa-enabled industrial Internet of Things," *Future Gener. Comput. Syst.*, vol. 143, pp. 322–336, Jun. 2023.

[28] Y.-C. Lai, J.-Y. Lin, Y.-D. Lin, R.-H. Hwang, P.-C. Lin, H.-K. Wu, and C.-K. Chen, "Two-phase defense against poisoning attacks on federated learning-based intrusion detection," *Comput. Secur.*, vol. 129, Jun. 2023, Art. no. 103205.

[29] A. Belenguer, J. A. Pascual, and J. Navaridas, "Göwfeda novel federated network intrusion detection system," *J. Netw. Comput. Appl.*, vol. 2023, Jan. 2023, Art. no. 103653.

[30] *KDD CUP 99*. Accessed: Nov. 19, 2023. [Online]. Available: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[31] *CICIDS2017 Dataset*. Accessed: Nov. 19, 2023. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html

[32] *UNSW-NB-15 Dataset*. Accessed: Nov. 19, 2023. [Online]. Available: https://research.unsw.edu.au/projects/unsw-nb15-dataset

[33] K. Kethineni and G. Pradeepini, "Intrusion detection in Internet of Things-based smart farming using hybrid deep learning framework," *Cluster Comput.*, vol. 2023, pp. 1–14, Jun. 2023.

[34] K. Han, Y. Wang, Q. Tian, J. Guo, C. Xu, and C. Xu, "GhostNet: More features from cheap operations," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2020, pp. 1577–1586.

OM KUMAR CHANDRAUMAKANTHAM received the B.Tech. and M.Tech. degrees in CSE from CREC, SVEC affiliated to Jawaharlal Nehru Technological University, Anantapur, in 2010 and 2013, respectively, and the Ph.D. degree in cyber security from Anna University, Chennai, in 2020. He embarked on his teaching career with the SRM Easwari Engineering College, Chennai, from 2013 to 2016, where he discovered his passion for teaching and honed his pedagogical skills. He is currently an Assistant Professor (Sr. G) with the School of Computer Science Engineering, Vellore Institute of Technology, Chennai Campus, and has a distinguished academic and professional journey. His research interests include the IoT and deep learning, leading to the filing of an international patent and the publication of 25 research articles in reputable journals, establishing an H-index value of six.

SUDHAKARAN GAJENDRAN received the B.Tech. degree in information technology from the Vel Tech Engineering College, Anna University, Chennai, in 2009, the M.E. degree in computer science and engineering from the Government College of Engineering, Tirunelveli, Anna University, Chennai, in 2011, and the Ph.D. degree from the Department of Computer Science and Engineering, Anna University, in 2021. He has been a Researcher in bioinformatics and artificial intelligence, since 2015. He is currently an Assistant Professor with the School of Electronics Engineering (SENSE), Vellore Institute of Technology, Chennai, India. His current research is concerned with extracting and analyzing the association between different entities from the biomedical literature text and gene sequence analysis.

SUGUNA MARAPPAN received the B.E. (C.S.E.) degree from the Kumaraguru College of Technology, Coimbatore, the M.E. (C.S.E.) degree from the Government College of Technology, Coimbatore, and the Ph.D. degree in information and communication engineering from Anna University, Chennai. She is currently an Assistant Professor (Senior Grade II) with the School of Computer Science and Engineering, Vellore Institute of Technology, Chennai. She has published more than 20 research articles in international journals and 15 international conferences. Her research interests include data analytics, health care analytics, cloud computing, and agile project management. She is a member of ISTE and IAENG.