[1] Anitha Govindaram

[2] Jegatheesan A

Enhancing Industrial IoT Security: Utilizing Blockchain-Assisted Deep Federated Learning for Collaborative Intrusion Detection

Journal of Electrical Systems

Abstract: - The Industrial Internet of Things (IIoT) is a rapidly evolving features with multiple applications, including critical infrastructure. Privacy policies are required to preserve the protection of user data in the threat intelligence community. Blockchain is a modern technology which used recently to provide more secure storage and efficiency. In this research, Blockchain Assisted Deep Federated Learning (BC_DFL) system is used to detect intruders. The three key processes used in the proposed intrusion detection architecture are data collection, pre-processing and intrusion detection. Data normalization, reduction, cleaning and transformation are used in pre-processing to remove extraneous information and improve data quality. This pre-processed data is sent to the Blockchain Assisted Deep Federated Learning (BC_DFL) system for intrusion detection. To detect intruders, the federated learning-based Capsule Auto-Encoder (FL_CAE) architecture first learns the properties from the inputs. Blockchain technology (BCTech) is not only used for storage but also improves security by eliminating the possibility of threatening node and individual server failure. The ToN_IoT and UNSW-NB15 data sets are used in the implementation and performance evaluation study. The proposed model is evaluated using existing in the Results section. In the UNSW-NB15 dataset, proposed model achieved an accuracy, precision, recall and F1 score of 97.26%, 97.28%, 96.89% and 96.96% respectively as well as in ToN_IoT data set proposed model achieved an accuracy, precision, recall and F1 score of 95.74%, 99.54 %, 99.49% and 99.24%, respectively. The execution of the proposed approach takes 2.31 seconds in the UNSW-NB15 dataset and 1.66 seconds in the ToN_IoT dataset. Blockchain offers a transparent and impenetrable ledger for transaction recording and verification. Within the framework of cooperative intrusion detection, it guarantees a secure and reliable exchange of threat intelligence and detection models between various users of IIoT ecosystem.

Keywords: Data authentication, Industrial Internet of Things, Intrusion Detection, Capsule Network, Federated Learning, Stochastic Gradient Decent method, Data Fusion Vector.

I. INTRODUCTION

The Internet of Things (IoT) is a network of organized devices using computing tools such as processors or sensors to store, transmit and collect data over the Internet [1]. The general function or goal of the IoT environment, for example healthcare, industrial or smart homes processes, is fulfilled by each device fulfilling a specific role. IoT allows remotely managed devices to work together and achieve common goals [2, 3]. In the year 2025, it is anticipated that the quantity of Internet of Things (IoT) devices will escalate to 41.6 billion and need for IoT networks based on data collected by International Data Corporation (IDC). Based on infrastructure and artificial intellect abilities, the IoT ecosystem has much to offer customers and enterprises, such as increasing operational agility and effectiveness [4, 5]. However, one of the biggest obstacles to the development of such networks is their security.

IoT devices gather as well as store highly complex information, such as medical and financial records, which are often the target of cybercriminals [6]. In light of the prevailing security posture of IoT networks, organizations and consumers encounter heightened challenges in upholding the security and integrity of their digital resources. This predicament is primarily attributed to the intricate, vast, and decentralized attack surface created by the placement of IoT devices predominantly at the network periphery, facilitating their role as potential entry points to an organization's central network. [7]. An IoT ecosystem is created by these often networked and constantly communicating gadgets.

[1] *Corresponding author: Research scholar, Department of Computer Science and Engineering,

Saveetha School of Engineering,

Saveetha Institute of Medical and Technical Sciences (SIMATS), Saveetha University, Thandalam, Chennai-602105,India.

gani3086@gmail.com

[2] Professor, Department of Computer Science and Engineering,

Saveetha School of Engineering,

Saveetha Institute of Medical and Technical Sciences (SIMATS), Saveetha University, Thandalam, Chennai-602105,India.

jegatheesana.sse@saveetha.com.

Therefore, any intrusion into any of these networks poses significant problems for the security and confidentiality of the entire network. Furthermore, since the Internet of Things links the physical and digital worlds, hacking IoT devices can have serious consequences [8].

Most network participants, especially end devices, can now provide services due to the developments in wireless communication and devices for the IoT [9]. Through collaboration and cooperation, such devices can offer storage and computing capacities to other network entities in increasingly diverse ways. In addition, a large proportion of these devices are suitable for distributed and decentralized learning and have artificial intelligence (AI) functions [10, 11]. FL can be leveraged to tackle the challenges associated with data centralization, representing a decentralized learning approach aimed at enhancing AI-driven computing Various sectors, including healthcare and e-commerce, have embraced the FL methodology.

The integration of blockchain technology has facilitated the emergence of distributed and decentralized solutions, enabling endpoints to collaborate on tasks that previously necessitated centralized organization oversight. By merging blockchain with FL, activities can now be delegated to IoT devices, thereby enhancing computing capabilities and surpassing traditional centralized systems. Furthermore, the cryptographic features of blockchain technology ensure data integrity, leading to secure data storage and transmission. Moreover, blockchain mechanisms can monitor the addition of new devices to the network through transaction records, thereby ensuring data authenticity and authorization.[14]. Furthermore, storing locally learned data of performing transaction validation and multiple transactions for each device enables secure communication between end devices [15].

A. Motivation

The security of private and sensitive information while transferring data has become critical with the fast development in the amount of data created by various industrial devices in the IoT. At the moment, federated learning for data security has evolved, and it can handle data interchange security challenges via model exchange on the Internet of mutual mistrust. However, hackers continue to build attacks that exploit compound learning flaws (for example, model extraction and model reversal attacks). Many methods are proposed to resist these attacks, but most of them do not provide an effective solution, which motivates us to propose blockchain-based federated learning. This concept has the dual security of federated learning and blockchain, making it harder for an adversary to attack. The major contribution of this work is:

- To enhance the protection of user data within the threat intelligence sharing community, the Blockchain Assisted Deep Federated Learning (BC_DFL) system is proposed.
- To acquire the input data, publically available sources are used
- To pre-process the input data, Data Normalization, Reduction, Cleaning and Transformation are used to decrease the irrelevant information and improve the accuracy
- To detect the intrusions from the provided inputs, the Federated Learning based Capsule Auto-Encoder (FL_CAE) is used to learn the features.
- For enhancing security, Blockchain technology (BCTech) is used for storage purposes, which eliminates the risks of threatening nodes and a single server failure.

The remaining part of the structure delineates as follows: Section 2 delineates the relevant literature. Section 3 elucidates the suggested approach, while Section 4 expounds upon the outcomes and discourse; the final remarks and sources are explicated in Section 5.

II. RELATED WORKS

An integrated framework that advances security, confidentiality, and trust using Deep Learning and BC technologies has been formulated by Kumar et al. [16]. The architecture of the Deep Blockchain-Based Trustworthy Privacy-Preserving Secured Framework (DBTP2SF) utilizes a BC-based reputation system for trust establishment, a two-tier privacy-preserving strategy merging ePoW for data integration preservation and AE for generating novel data dimensions, alongside a privacy-preserving algorithm. Through the adoption of a two-step technique, the vulnerabilities of data poisoning and inference attacks can be circumvented. Subsequently, a deployment framework named BlockCloud-BlockFog was introduced to tackle the challenges within the current Cloud-Fog architecture.

Nevertheless, certain issues surfaced, resulting in prolonged block mining duration and manual pre-processing requirements with the proliferation of IIoT network nodes.In the context of an intelligent industrial setting, Auther et al. [17] have introduced a blockchain-based framework. This approach facilitates the establishment of a decentralized, private IIoT network based on blockchain technology,lightweight and secure, capable of performing a number of critical tasks, including trusted machine operation, data storage and user and device registration. However, this strategy is more difficult to implement.

The traditional blockchain system was developed by Wang et al. [18] using the incremental aggregator subvector commitment (IASVC) and the IIoT and data security were protected by the advanced blockchain system. In traditional blockchain architecture, data is stored in Merkle trees. Verifying the accuracy and completeness of the data requires a considerable amount of proof. The model can dynamically combine multiple encryption techniques to ensure the confidentiality of IIoT data while reducing the size of evidence and increasing transmission efficiency. To reduce node storage requirements, the IASVC model uses the IIoT node data upload skill. To meet the above application requirements, an IASVC based on bilinear mapping was created. However, this approach only assessed the evidence aggregation of a single commitment.

For IIoT networks, Zhang et al. [19] offered a smart and secure 5G that goes beyond the frame. Using the recently described cross-domain sharing strategy and deep reinforcement learning (DRL) technique, an effective edge resource planning approach was created. A novel credit-differentiated transaction approval system was developed to secure IIoT network edge service transactions. However, the performance of this model is not particularly strong.

Khan et al. [20] presented a revolutionary collaborative federated learning system for smart industries. A decomposition and relaxation-based approach was used to solve a presented integer linear programming problem. Convex optimization solvers were used to solve the subproblems when their convexity was demonstrated.

Sater et al. [21] presented a federated stacked Long Short-Term Memory (LSTM) structure designed for anomaly detection in intelligent buildings through the use of federated learning for IoT sensor data. The FSLSTM network consists of two models: a local LSTM model that acquires data from individual sensors, and a global model that aggregates weights, adjusts parameters, and disseminates sensor results for each computation. Nevertheless, there are deficiencies in security and the overall performance is deemed unsatisfactory.

He et al. [22] integrate long short-term memory (LSTM) into CGAN training to enhance the performance of generative networks. Leveraging LSTM networks' ability for feature extraction, CGAN-generated data is employed as augmented data and utilized in malware detection and classification. Furthermore, distributed federated learning with differential privacy ensures data security and privacy by allowing collaborative training of CGAN models across multiple distributed datasets. To maintain security during the aggregation and updating of the global algorithm, blockchain is utilized for storing and disseminating the training models. Nevertheless, LSTMs may demand significant processing power, especially when handling large-scale IIoT datasets or deep architectures, which could hinder their deployment on IIoT devices with limited resources.

Hamouda et al. [23] propose a unique privacy-preserving secure architecture named PPSS, which is founded on blockchain-enabled FL providing enhanced transparency, reliability, and confidentiality. The PPSS architecture utilizes a permissioned-blockchain network to ensure multi-party computation and promote cross-silo FL through a lightweight and energy-efficient consensus mechanism called Proof-of-Federated Deep-Learning (PoFDL). Initially, client modifications are safeguarded from unauthorized access through the utilization of new model-containing blocks and differentially private training of stochastic gradient descent (DP-SGD) are verified and added to the blockchain using the PoFDL protocol in the second stage. Blockchain, while offering immutability and transparency, may jeopardize participants' privacy in federated learning. The blockchain's transaction logs can provide details on the contributions and model updates provided by certain IIoTs.

Yazdinejad et al. [24] have devised a threat hunting framework named Block Hunter utilizing federated learning to automatically seek out attacks within blockchain-based IIoT networks. The Block Hunter operates within a federated environment and integrates various machine learning algorithms within a cluster-oriented architecture to detect anomalies. It represents the primary endeavor in federated threat hunting within IIoT networks, ensuring privacy preservation while pinpointing aberrant activities. Nonetheless, due to the necessity of effective cross-device training and communication, lightweight models are commonly employed in federated learning, posing challenges in developing highly intricate models for advanced threat detection.

Friha et al. [25] introduce a secure, decentralized, Differentially Private (DP) Federated Learning (FL)-based intrusion detection system (2DF-IDS) designed to enhance the security of intelligent industrial structures. The 2DF-IDS consists of three fundamental elements: a decentralized FL strategy (which mitigates risks associated with assaults or single points of failure linked to a conventional FL analysis aggregation server), a key exchange protocol (ensuring the secure transmission of weights among all peers within the system), and a differentially private gradient exchange mechanism (enhancing the FL approach's privacy level).However with Federated Learning, updates to the models are exchanged through interaction between nearby devices and a central server. Enhanced communication overhead can affect real-time operations in smart industrial facilities with constrained network bandwidth.

A. Problem statement

A network of networked devices called the Internet of Things (IoT) uses computer resources like processors or sensors to store, gather, and transfer data through the Internet. The general objective or aim of the IoT ecosystem, such as smart homes, industry, or healthcare operations, is served by each device that carries out a particular activity. Most IoT models are associated with cloud devices, which are less secure and more vulnerable to attacks. Researchers around the world are conducting studies to improve security and identify intruders. However, most are incorrect and have difficulty preserving the collected data. Attackers are becoming more sophisticated and a traditional adversary model cannot prevent or detect them. As more IIoT devices and people engage in collaborative learning, there may be concerns about the scalability of blockchain networks. Performance difficulties can be caused by large transaction volumes and the requirement for consensus techniques. Proof-of-Work (PoW) is one of the blockchain's energy-intensive consensus algorithms. The energy consumption of blockchain processes could be a major disadvantage in IIoT scenarios where devices have limited resources. Furthermore, the combination of federated learning and blockchain technology presents novel possibilities for attacks. Potential security vulnerabilities could arise from adversarial attacks directed towards the consensus method, federated learning process or connectivity among IIoT devices. These issues inspire this research to start with the security of federated learning models and blockchain security.

III. Proposed methodology

Data acquisition, pre-processing and intrusion detection are the three main methods used in the proposed intrusion detection architecture. The input data is initially collected from publicly accessible sources. The initial pre-processing is performed to reduce the irrelevant information through data normalization, reduction, cleaning and transformation. The Blockchain Assisted Deep Federated Learning (BC_DFL) intrusion detection system uses this pre-processed data as input. The federated learning-based Capsule Auto-Encoder (FL_CAE) in this framework learns the characteristics from the inputs and then uses them to identify intruders. For storage purposes, blockchain technology (BCTech) is used to increase security as it eliminates the dangers associated with rogue nodes and the failure of individual servers. The proposed strategy will reduce intrusion as it leverages the best security, privacy and storage paradigm. Consequently, the proposed detection model is able to identify dangerous behaviours based on the input data. Figure 1 shows the basic block diagram of the proposed model.

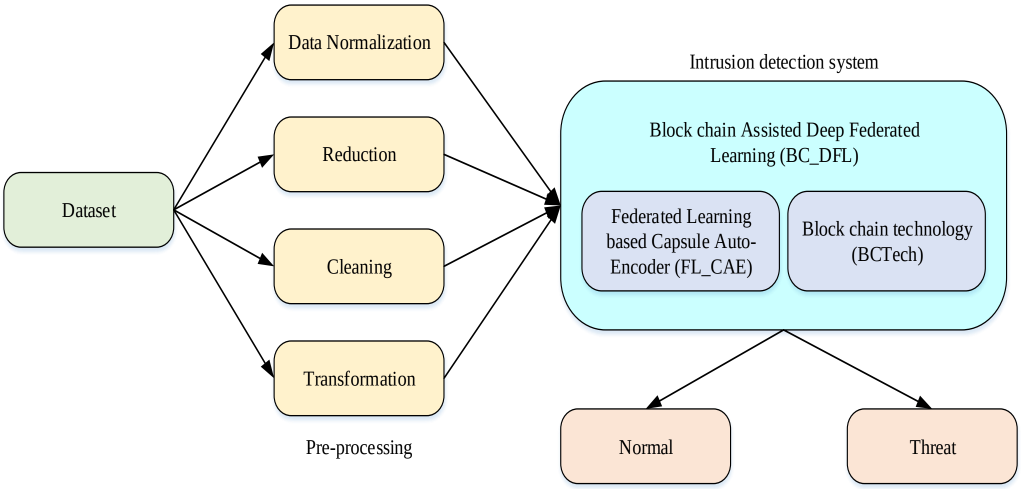

Data Normalization
Reduction
Cleaning
Transformation
Dataset
Pre-processing
Intrusion detection system
Block chain Assisted Deep Federated Learning (BC_DFL)
Federated Learning based Capsule Auto-Encoder (FL_CAE)
Block chain technology (BCTech)
Normal
Threat

Figure 1: Basic block diagram of the proposed model

A. Pre-processing

Data pre-processing is crucial as it cleans, reduces and normalizes the data to prepare it for processing in the next phase. Pre-processing in this research includes data normalization, cleaning, reduction and transformation. These steps help reduce the risk of error and increase the accuracy of subsequent algorithms.

Data cleaning- Data preparation that involves changing missing, inaccurate, irrelevant, redundant, or incorrectly provided data is known as data cleaning. In data analysis, the data is not strictly necessary as it would make it difficult to provide correct results. Data cleaning is not just limited to deleting errors, this includes the elimination of information. The process of data cleaning includes removing unwanted information, correcting inaccurate information and deleting unwanted information without losing important data. The main goal was to clean the data in datasets that standardized data analysis and were easily accessible to find the appropriate data for the query.

Data transformation - All category data has been summarized in this numeric format. The UNSW-NB15 and ToN_IoT dataset spans a variety of data types and ranges. Therefore, data normalization is a part of data transformation. Data normalization reduces the value range of the attribute data to an acceptable level.

Min-Max normalization- Due to missing or unclear data, the missing data needs to be modified by removing unnecessary data to improve quality. Both integration and data normalization benefit from the min-max normalization technique. Any feature value that has a minimum value is converted to 0, and any feature value that has a maximum value is converted to 1. Each value is translated from decimal values between 0 and 1. The normalization procedure is described in equation (1),

$$Norm_X = \frac{D_X - Min_x}{Max_X - Min_x} \tag{1}$$

Where represents the data point, represents the data point's minimum value and indicates the data point's maximum value or the batch instances. Using structured data, these variables calculate a normalized value to fill the gaps. Once the unstructured information has undergone min-max normalization, traffic data contamination will further increase the level of uncertainty in the data.

Data reduction- Reduction of dimensions is the method used in data reduction. The risk of detecting false data patterns is to be reduced and the chosen features require the removal of all unnecessary elements and features of the fraud domain. The well-known PCA or principal component analysis is a common transformation technique. The problem of feature selection is solved with this approach from the point of view of numerical analysis. PCA effectively performed feature selection by determining the appropriate number of key components.

B. System model

The proposed approach is based on a blockchain-based federated learning technique that leverages capsule autoencoder support to build various learning models to enable accurate and timely support for critical infrastructure at the edge. This approach will enable a trustworthy cooperative network to deliver services precisely and quickly. Most distributed and decentralized learning systems are assumed to be either erroneous or raise security issues. Accuracy and trustworthiness are ensured by integrating the capsule autoencoder with blockchain-assisted composite learning.

The proposed strategy considers the fact that all distributed learning or federated learning, is carried out assistance of a capsule network. Without using the central server, data collection and training occur exclusively on the end device. A global model is then built on the central server using the federated averaging technique. To ensure a secure and reliable discussion of device model updates, nodes that score above a certain threshold are included in the offered public blockchain. The blockchain stores the information with high security while the information is being received. The answer implies that sensitive data nodes must use blockchain to validate the locally trained models. Normally there are no time restrictions in such situations. While non-critical infrastructure applications may bypass the blockchain certification process, meeting the applications' deadline requirements. Figure 2 represents the system model of the proposed model.

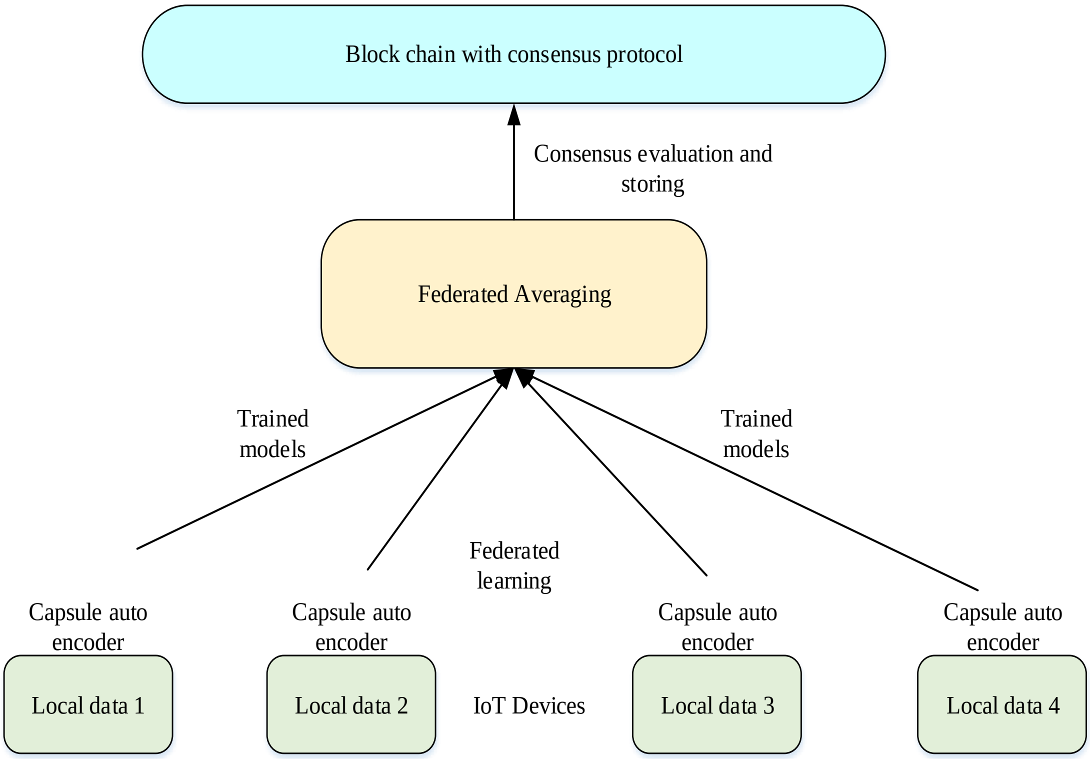


Figure 2: System model of the proposed model

C. Block chain Assisted Deep Federated Learning (BC_DFL)

The proposed framework consists of three algorithms: blockchain structure, federated learning model and capsule auto-encoder, each described below.

D. 3.3.1 Federated Learning based Capsule Auto-Encoder (FL_CAE)

The federated learning-based Capsule Auto-Encoder (FL_CAE) in this framework learns the characteristics from the inputs and then uses them to identify intruders. The Capsule Auto-Encoder is used as a component of several privacy and security systems, including Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). The location and orientation of a feature can be precisely described by the vectors that the capsule network uses to transmit information. The capsule-based network design has a particular advantage over other deep learning structures in that it uses a local feature for classification that is ideally suited to the NIDS position. The encoder is used with input variables $I_j \in \alpha, \beta$ in conjunction with the capsule network to enhance the learning procedure.

Input is provided by the low-level capsule C_i which represents the initial data fusion vector and iterates to create the output O_j of the high-level capsule. It repeats the calculation of linear weights but additionally includes a weight coefficient E_{ij}, which stands for the low-level capsule. The input I_j for the capsule auto encoder is obtained using equation (2).

$$I_j = \sum_i E_{ij} \hat{C}_{j|i} = \|O_j\| \qquad where, \hat{C}_{j|i} = wC_{ij}C_i \tag{2}$$

Softmax is employed to ensure that all the weights are E_{ij} where the expression is given as:

$$E_{ij} = Soft\max(v_{ij}) \cdot I_j \tag{3}$$

Where v_{ij} is a transient variable having a value of 0 and E_{ij} changes its value throughout the process of iteration.

The basic structure of a capsule network consists of an encoder indicated EN_X, a decoder is denoted as DE_X and a detection layer. One of the aims of finding a program for each input attribute is to minimize the loss between input and result across all information characteristics. Equation (4) yields the following results for the reconstruction loss:

$$REC_{loss} = \min \frac{1}{A} \sum_{a=1}^{A} \left\| DE_X \left(EN_X \left(F_a \right) \right) - F_a \right\|_2^2 \tag{4}$$

In equations (5) and (6), the $EN_X(a_1)$ and $DE_X(a_2)$ are represented by

$$EN_X(a_1) = \lambda(F * W1) \tag{5}$$

$$DE_X(a_2) = \lambda(G * W2) \tag{6}$$

The weight criteria of both the decoder and the encoder are $W1$ and $W2$, while a_1 and a_2 are the input criteria. The convolutional operator is represented by the $*$ and $\lambda(\cdot)$ stands for convolution and activation function, respectively. The CAE's detection layer can be achieved by equation (7):

$$P_{ij} = \frac{\left(1 + \left\| u_i - O_j \right\|^2\right)^{-1}}{\sum_j \left(1 + \left\| u_i - O_j \right\|^2\right)^{-1}} \tag{7}$$

Where O_j denotes the output criteria. The P_{ij} is the expected probability that u_i will occur when the given characteristic j. The detection loss is specified by equation (8) as follows:

$$DET_{loss} = \sum_i \sum_j D_{ij} \log \frac{D_{ij}}{P_{ij}} \tag{8}$$

Where D_{ij} is the pre-determined target in this case, and data intrusion is identified by applying equation (7). In equations (5) and (6), the loss criteria DET_{loss} and the weight criterion $W1$ and $W2$ are optimized.Detection layer in equation (8) is minimized by employing an adaptive transient search optimization approach. A capsule auto-encoder can be used to identify the intrusion.

Data is gathered locally and delivered to the end devices in a collaborative learning system known as federated learning (FL). A global model is then developed by combining the training models. End devices only exchange the parameters of their local models with the server and do not pass on the local training/test data sets. In the proposed method, the FL-Averaging algorithm (Avg_{FL}) is used to control how the end-device training architecture are handled on the centralized server, resulting in the creation of a common global model.

The capsule auto-encoder training on the terminals is done using the SGD (Stochastic Gradient Decent) method and the gradient descent optimization approximation. After randomly selecting a portion of the main dataset, swap the dataset features for the estimated values. Avg_{FL} takes into account three variables: the volume of the mini-batch, the amount of training performed on the dataset's end-devices and the percentage of end-device computations. These elements make it easier for end devices to share the gradient decrease. The server then receipts the average of the trained models produced, makes a broadcasts and adjustment chosen Avg_{FL} device is given in Algorithm 1.

```
Algorithm 1: $Avg_{FL}$
Input: Pre-processed data
Process: $Avg_{FL}$ (End device side)
Output: Gets $n_p$ from main server
Initialization: If $n^l_{p,0} = n_p$ :        $n_0$ is the initialization of the server model
        For $k = 0,1,2,\cdots$ do
        Sample $\phi$ is selected from $H_{in}$ :     $H_{in}$ is the local end device
        Dataset Update $n^l_{p,k+1} = n^l_{p,k} - (n^l_{p,k}, \phi)$
        End for
Set $n^l_{p+1} = n^l_{p,Kk}$
Transmit $n^l_{p+1}$ to main server
Process: $Avg_{FL}$ (main server)
Initialize $n_0$ (initializing the server model)
        For each iteration $p = 0,1,2,\cdots$ do
        $|Z_p| = Z \cdot L \geq 1;$
                For each user $l \in |z_p|$ do $n^l_{p+1}$        end device update
                $n_{p+1} = \sum_{l \in z_p} \frac{m_l}{m_\alpha} n^l_{p+1}$        where $m_\alpha = \sum_{l \in z_p} m_l$
                End for
        End for
```

Initially the input is obtained by the output of the pre-processing stage. Both the edge devices and the server are targeted by the Avg_{FL}. The server's GM is designated as n_0, which is randomly adjusted. The first round then starts with the central server chooses a subsection of the end devices (z_p such that $|z_p| = Z \cdot L \geq 1;$) and dispersing its present global model n_p among all of the end devices in z_p. When the server's shared model n_p is updated, the end devices update their models (n^l_p). After grouping their local datasets according to size, the end devices execute SGD iterations. After receiving the individually trained models from all end devices (n^l_{p+1}) and uploading them, the centralized server then generates the newly updated global model n_{p+1}.In terms $Z, \beta, \lambda, \Gamma \, and \, iter$ stand for iterations before updating the global model. The term $iter, \Gamma, \lambda \, and \, \beta$ are accepted by SGD for employing in training. The data of the proposed Federated Learning based Capsule Auto-Encoder is stored in Blockchain technology.

E. Blockchain technology

Blockchain technology enables federated learning to ensure the validity of locally derived data and learned models. Since decentralized tasks often rely on untrusted endpoints to work together, a consensus method must be considered to ensure the accuracy and reliability of the service, task, or data provided. Blockchain technology creates a decentralized, impenetrable record to build trust without a central authority. To confirm blockchain content, sequence, and hash pointers, users compare locally stored versions of the blockchain using a consensus process. Numerous consensus algorithms, including Practical Byzantine Fault Tolerance (pBFT), Proof-of-Stake (PoS), Proof-of-Work (PoW), and others, are proposed in research. Each protocol can work well under specific circumstances and in a specific network environment.

In terms of crucial IoT structures, blockchain technology has the potential to provide helpful solutions to a wide range of problems, especially in terms of security and reliability. For example, blockchain technology can instantly provide IoT end devices with a unique identifier without needing a central server. Furthermore, the end devices, possessing a unique identity and specific key, cryptographically sign the directed communication between the end devices to blockchain. It enables a protected and reliable exchange of device model updates by merging blockchain technology with the crucial infrastructure provided by federated learning. This proposed strategy incorporates blockchain technology as an additional layer of security to guarantee devices reliability. Untrusted devices can be removed from the blockchain as it is expanded to include trusted devices. Any consensus algorithm can be used with the proposed blockchain-backed FL model. However, the pBFT is very effective against defects since terminals can be portable. The system is not affected by terminals that do not provide a consensus response or do so in a flawed or erroneous manner, and unanimity can be guaranteed. Miners, which can be trusted endpoints or edge devices, perform the model verification process.

The locally learnt model is sent from each end device to the linked miner that the fog has selected. Miners do cross-check by comparing and exchanging local model changes with the global model. A block is then created that keeps track of all modifications once the local model changes are verified using a consensus mechanism (pBFT) used to determine the overall value. Figure 3 shows the structure of the proposed model.

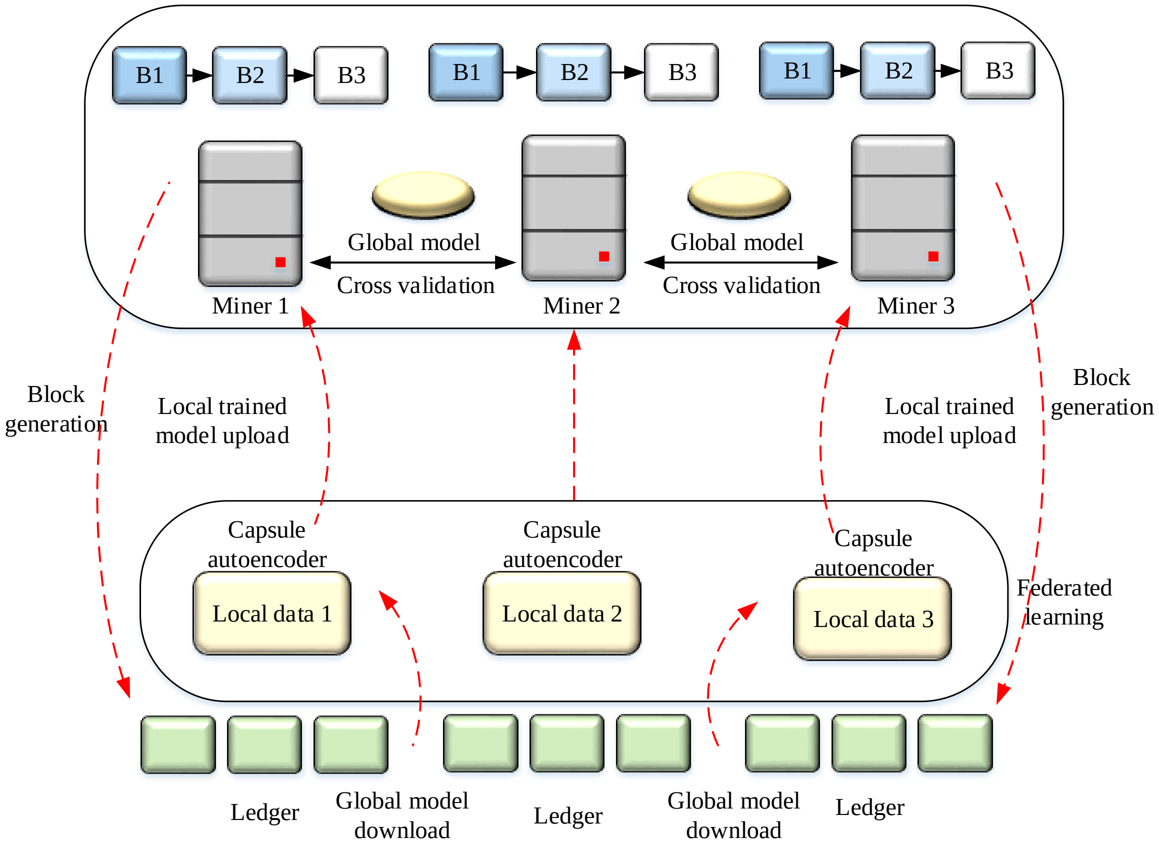


Figure 3: proposed model

IV. Results and discussion

The PYTHON platform has been utilized for the execution, incorporating system specifications featuring an Intel(R) Core (TM) i7-3770 CPU @ 3.40GHz, along with 16 GB of installed memory. The operating system employed is 64-bit, devoid of pen or touch input. The assessment of effectiveness encompasses parameters such as accuracy, f1-score, recall, precision, and execution time, evaluating established methods like Integrated CNN with Long Short Term Memory (LSTM)-based Fog Computing Intrusion Detection (ICNN-FCID), Cholesky Factorization based Online Sequential Extreme Learning Machines with Persistent Regularization (CF-OSELM-PRFF), Enhanced Hybrid Intrusion Detection System (EHIDS), and Anomaly Behaviour Analysis Intrusion Detection System (ABA-IDS), using the UNSW-NB15 and ToN_IoT dataset.

The renowned UNSW-NB15 dataset, made available in 2015 by the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS), comprises artificial attack scenarios and benign network activity. These were created using the IXIA PerfectStorm tool, with 100 GB of pcap files recorded via the tcpdump utility. Initial dataset characteristics, extracted using Argus and Bro-IDS (now Zeek), as well as twelve additional SQL techniques, resulted in a total of 2,540,044 flows. Among these, 2,218,761 (87.35%) are benign flows, while 321,283 (12.65%) represent attack streams.

The ToN-IoT dataset, a recently published heterogeneous compilation from 2019, integrates operating system logs, IoT network traffic, and telemetry data from IoT services. This article focuses on the segment displaying network traffic flows within the dataset. It includes various attack scenarios executed by ACCS at the Cyber Range Lab, simulating a real large-scale network environment. The dataset encompasses attacks such as DoS, DDoS, ransomware, etc., comprising a total of 22,339,021 flows. Within these flows, there are 796,380 (3.56%) benign instances and 21,542,641 (96.44%) attack samples.

A. Performance evaluation

For the evaluation, the proposed model is compared to existing models in terms of accuracy, precision, recall, and f1-score with a basic evaluation matrix such as true negative (tn), true positive (tp), false negative (fn) , and false positive (fp). More details of the evaluation matrix is given below:

True Positive (tp)- The proportion of samples that are properly identified as normal in the normal portion and as a threat in the threat portion.

True Negative (tn)- The proportion of samples that are properly identified as posing a threat to the normal portion or the threat to the normal portion.

False positive (fp)- The number of samples incorrectly identified as threats in the threat portion and as normal in the normal portion.

False Negative (fn)- The percentage of samples incorrectly identified as normal in the threat and threat in the normal portions.

Using the evaluation matrix, the performance of the proposed model can be defined by:

Accuracy- The percentage of samples that can be successfully located in the entire data set is referred to as accuracy. This statistic is not useful for comparing methods because the data set used is imbalanced. The accuracy can be represented as follows:

$$Accuracy = \frac{tn + tp}{tn + tp + fp + fn} \tag{9}$$

Precision- Precision is the ratio of the number of samples correctly identified as normal in the normal portion or as a threat in the threat portion compared to the total number of samples correctly identified as normal/threatening.

$$precision = \frac{tp}{tp + fp} \tag{10}$$

Recall- Recall is the proportion of samples properly identified as normal in the normal component or as a threat in the threat portion relative to the total number of samples that are correctly classified as normal/threat in the dataset.

$$recall = \frac{tp}{tp + fn} \tag{11}$$

F1-score- F1-Score represents the harmonic mean of precision and recall.

$$F1 - score = \frac{2 \times recall \times precision}{recall + precision} \tag{12}$$

B. Performance evaluation using UNSW-NB15 dataset

The performance evaluation of the proposed and existing model in terms of accuracy is shown in Figure 4. The accuracy is taken by varying the data size from 10000 to 60000. The existing models like EHIDS, ABA-IDS, CF-OSELM-PRFF and ICNN-FCID are used to compare with the proposed model. EHIDS model achieved an average accuracy of 96.45%, while CF-OSELM-PRFF achieved an average accuracy of 92.27%. ABA-IDS and ICNN-FCID models achieved an average accuracy of 90.74% and 94.61%, respectively. The proposed model achieved an average accuracy of 97.26% which is the best among all other existing methods. Table 1 represents the accuracy values of the proposed and existing models.

Table 1: Accuracy of proposed and existing models

Methods	Data size					
	10000	20000	30000	40000	50000	60000
EHIDS	92.08	94.48	94.68	99.03	98.57	99.87
CF-OSELM-PRFF	92.34	92.73	91.69	91.75	93.25	91.88
ABA-IDS	90.71	90.58	90.71	90.78	90.84	90.84
ICNN-FCID	91.88	94.16	93.9	95.45	96.04	96.23
PROPOSED	93.38	95.45	95.78	99.61	99.42	99.97

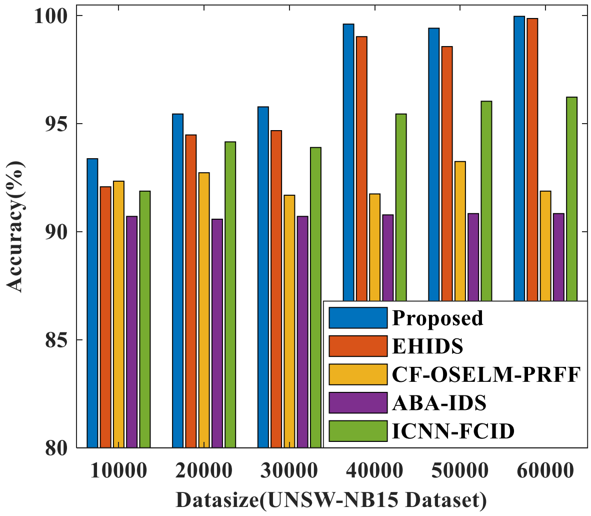


Figure 4: performance evaluation using the UNSW-NB15 dataset in terms of accuracy.

Figure 5 represents the precision of the proposed and existing models using the UNSW-NB15 dataset. The EHIDS model has a precision of 96.45%, and CF-OSELM-PRFF has a precision of 94.94%. The ABA-IDS model has a precision of 82.42%, while the ICNN-FCID model has a precision value of 94.42%, respectively. The suggested model demonstrates. a precision value of 97.28%, surpassing all other current models. In Table 2, the precision values of both the proposed model and the current models are depicted across various data sizes.

Table 2: Precision value of existing and proposed model

Models	Data size					
	10000	20000	30000	40000	50000	60000
EHIDS	92.33	94.56	94.8	98.67	98.61	99.76
CF-OSELM-PRFF	93.47	93.53	94.74	95.29	95.83	96.8
ABA-IDS	80.97	82.9	82.05	82.78	82.9	82.96
ICNN-FCID	93.6	95.23	94.44	94.14	94.5	94.62
PROPOSED	94.02	95.77	95.65	99.21	99.21	99.82

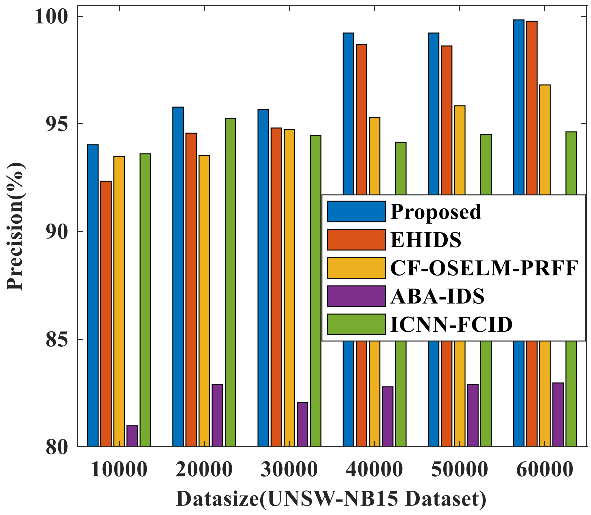


Figure 5: Precision of the proposed and existing models

Figure 6 represents the recall value of the existing and proposed model while using the UNSW-NB15 dataset.EHIDS model have an average recall value of 92.17%, and CF-OSELM-PRFF have a recall value of 90.52%. TheABA-IDS model has a recall value of 90.15%, while the ICNN-FCID model have a recall value of 89.11%,respectively.

The proposed model has a precision value of 92.97% which have a clear edge over all other models. Table 3 represents the recall value of the existing and proposed model.

Table 3: Recall value of existing and proposed models

Model	Data size					
	10000	20000	30000	40000	50000	60000
EHIDS	92.17	94.43	94.56	98.47	98.41	99.57
CF-OSELM-PRFF	90.52	91.25	92.48	93.09	94.86	95.84
ABA-IDS	90.15	90.76	91.31	91.44	91.74	91.74
ICNN-FCID	89.11	88.26	87.16	87.4	90.03	87.95
PROPOSED	92.97	95.11	95.35	99.08	98.96	99.88

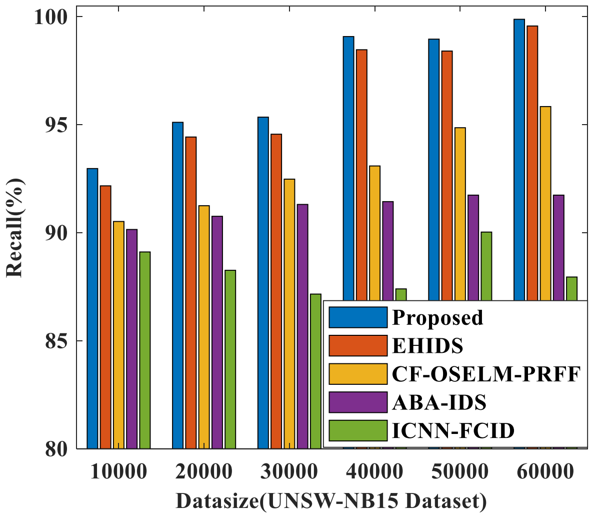


Figure 6: Recall of existing and proposed model

Figure 7 represents the F1-score of the proposed and existing model using the UNSW-NB15 dataset. The F1-score of the EHIDS model is 96.26%, and the CF-OSELM-PRFF model has an F1-score of 93%. The ABA-IDS model has the F1-score of 86.69%, while the ICNN-FCID model have a value of 90.56%, respectively. The proposed model has an F1-score of 96.96% which is the best compared to other existing models. Table 4 represents the F1-score of the proposed and existing models.

Table 4: F1-score of the proposed and existing model

Model	Data size					
	10000	20000	30000	40000	50000	60000
EHIDS	92.16	94.35	94.63	98.8	98.45	99.79
CF-OSELM-PRFF	91.59	92.23	93	93.85	94.7	95.12
ABA-IDS	86.78	85.65	86.86	86.86	86.86	87.14
ICNN-FCID	90.88	91.1	89.75	89.89	91.8	89.96
PROPOSED	92.93	95.27	95.41	99.15	99.15	99.86

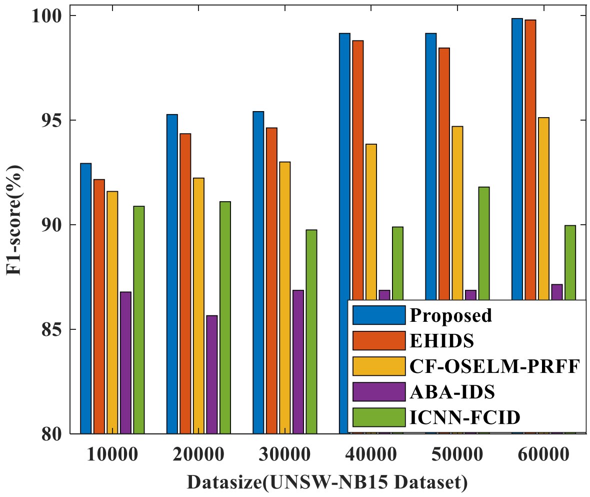


Figure 7: F1-score of proposed and existing model

C. Performance evaluation using ToN_IoT dataset

Figure 8 represents an evaluation of the accuracy of the proposed and existing designs. Variations in data size between 10000 and 60000 are used to determine accuracy. To compare the proposed model with existing methods, the models like EHIDS, CF-OSELM-PRFF, ABA-IDS, and ICNN-FCID are employed. The EHIDS model has an accuracy of 95.24%, while the CF-OSELM-PRFF model have an accuracy of 91.23%. The accuracy rates for the ABA-IDS and ICNN-FCID models have the value of 89.84% and 92.03%, respectively. The proposed approach surpassed all other existing methods in terms of accuracy, with an average of 95.74%. The values for the proposed and previous models' accuracy are shown in Table 5.

Table 5: Accuracy value of the proposed and existing model

	Data size					
Model	10000	20000	30000	40000	50000	60000
EHIDS	88.01	91.8	94.84	98.01	99.25	99.57
CF-OSELM-PRFF	82.86	87.39	90.68	94.22	95.71	96.52
ABA-IDS	81.74	84.91	90.25	93.11	94.04	95.03
ICNN-FCID	84.91	87.95	91.43	94.29	96.65	96.96
PROPOSED	88.45	92.48	95.53	98.57	99.63	99.81

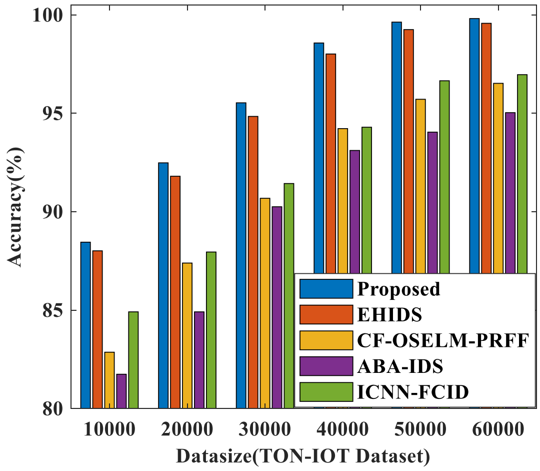


Figure 8: Accuracy of the proposed and existing model

The precision of the proposed and existing ones utilizing the ToN_IoT dataset is shown in Figure 9. The precision of the EHIDS model is 98.99%, whereas the CF-OSELM-PRFF model has a precision of 95.27%. The precision for the ABA-IDS model is 94%, whereas the precision for the ICNN-FCID model is 95.48%. The proposed approach has the highest precision among the existing model at 99.54%. The precision value for the proposed and existing models for each data size is shown in Table 6.

Table 6: precision of the proposed and existing models

	Data size					
Models	10000	20000	30000	40000	50000	60000
EHIDS	98.08	98.65	99.22	99.29	99.15	99.57
CF-OSELM-PRFF	94.38	94.16	94.8	95.44	95.94	96.94
ABA-IDS	88.54	91.96	94.52	95.8	96.01	97.22
ICNN-FCID	94.66	95.02	95.37	95.66	96.65	95.52
PROPOSED	98.65	99.43	99.72	99.72	99.79	99.93

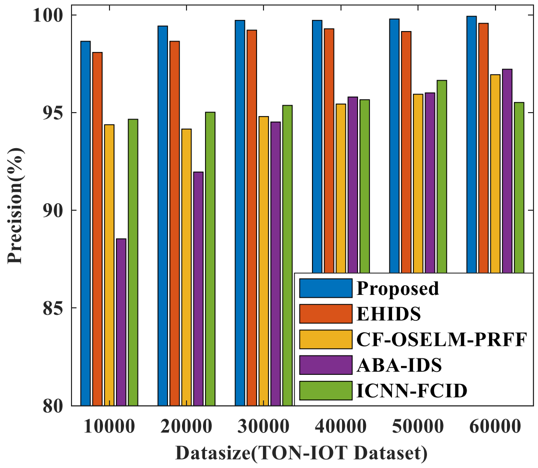


Figure 9: precision of the proposed and existing models

Using the ToN_IoT dataset, Figure 10 shows the recall value of the existing and proposed models. The recall rate for the EHIDS model is 98.97%, whereas the recall rate for the CF-OSELM-PRFF is 93.08%. The recall for the ABA-IDS model is 94.01%, whereas the recall for the ICNN-FCID model is 94.44%. The proposed model outperforms all other models with a recall value of 99.49%. The recall value of the existing and proposed models is shown in Table 7.

Table 7: Recall of the proposed and existing model

	Data size					
Model	10000	20000	30000	40000	50000	60000
EHIDS	98.01	98.91	98.99	98.95	99.53	99.43
CF-OSELM-PRFF	90.57	91.27	92.72	93.24	95.07	95.65
ABA-IDS	88.77	91.9	94.4	95.85	96.25	96.89
ICNN-FCID	93.31	93.64	94.22	94.37	95.32	95.78
PROPOSED	98.45	99.47	99.55	99.57	99.91	99.99

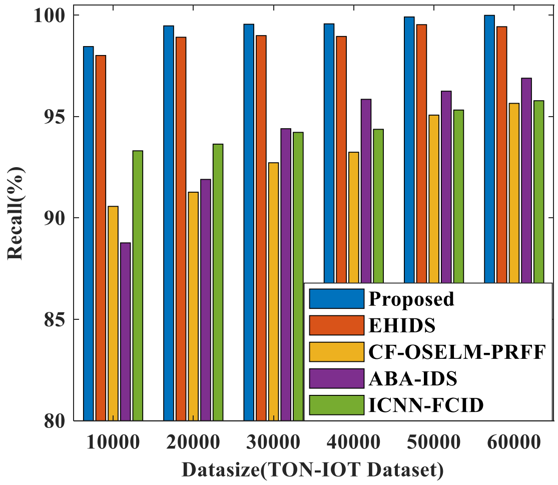


Figure 10: Recall of the proposed and existing model

On the basis of the ToN_IoT dataset, Figure 11 shows the F1-score for the proposed and existing models. The F1-score of the CF-OSELM-PRFF model is 93.4%, and 98.75% for the EHIDS model. The F1-score for the ICNN-FCID model is 91.73%, whereas the ABA-IDS model has a value of 93.91%. The proposed model has the highest F1-score of 99.24% compared to other existing models. The F1-score of the proposed and existing models is shown in Table 8.

Table 8: F1-score of the proposed and existing model

Model	Data size					
	10000	20000	30000	40000	50000	60000
EHIDS	97.6	98.77	98.89	98.83	99.42	99.02
CF-OSELM-PRFF	91.7	92.34	93.16	93.68	94.68	94.84
ABA-IDS	88.89	92.16	94.27	95.44	96.08	96.67
ICNN-FCID	91.17	91.11	91.81	91.93	92.34	92.03
PROPOSED	98.13	99.53	99.36	99.36	99.59	99.48

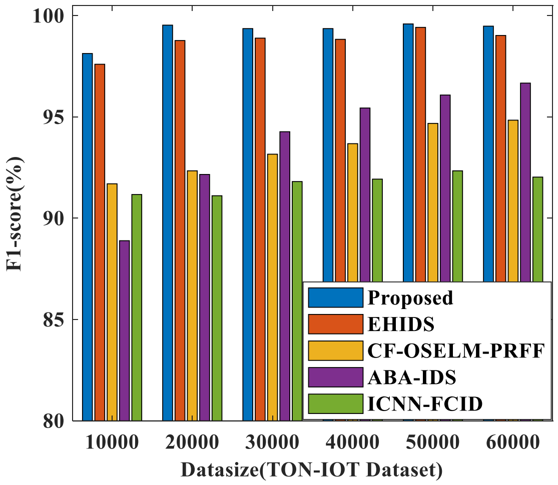


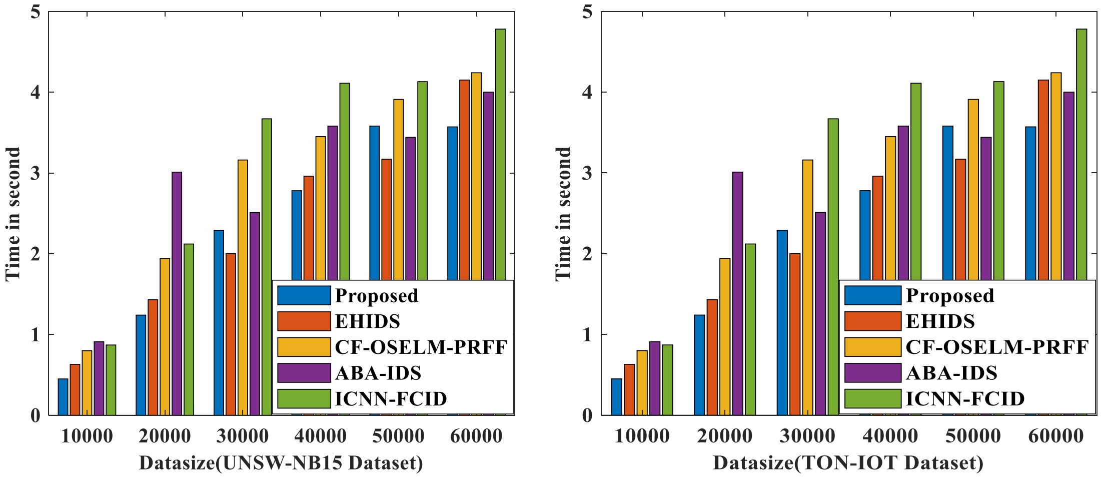
Figure11: F1-score of the proposed and existing model

Figure 12 represents the execution time of the proposed and existing models in terms of the UNSW-NB15 and ToN_IoT datasets. Figure 12 (a) represents the execution time in the UNSW-NB15 dataset. The EHIDS model has an execution time of 2.39 seconds, and the CF-OSELM-PRFF model has a time of 2.91 seconds. The models like ABA-IDS and ICNN-FCID have an execution time of 2.9 and 3.28 seconds, respectively. Figure 12 (b) denotes the execution time in the ToN_IoT dataset. The CF-OSELM-PRFF model has an execution time of 2.91 seconds, and the EHIDS model has a time of 1.87 seconds. The ABA-IDS model has a time of 2.94 seconds, while ICNN-FCID has an execution time of 3.24 seconds. The proposed model has an execution time of 2.31 seconds in the UNSW-NB15 dataset and 1.66 seconds for the ToN_IoT dataset, respectively. Table 9 represents the execution time of the proposed and existing model in both datasets.

Table 9: Execution time (Time in seconds) in UNSW-NB15 and ToN_IoT dataset

UNSW-NB15						
	Data size					
Models	10000	20000	30000	40000	50000	60000
EHIDS	0.63	1.43	2	2.96	3.17	4.15
CF-OSELM-PRFF	0.8	1.94	3.16	3.45	3.91	4.24
ABA-IDS	0.91	3.01	2.51	3.58	3.44	4
ICNN-FCID	0.87	2.12	3.67	4.11	4.13	4.78

PROPOSED	0.45	1.24	2.29	2.78	3.58	3.57
TON-IOT dataset						
Models	Data size					
	10000	20000	30000	40000	50000	60000
EHIDS	0.73	1.05	1.65	2	2.57	3.25
CF-OSELM-PRFF	0.86	2.01	3.18	3.5	3.95	4
ABA-IDS	0.97	2.53	3.07	3.51	3.6	3.96
ICNN-FCID	0.97	2.15	3.66	4.02	4.14	4.54
PROPOSED	0.59	0.81	1.46	1.82	2.34	2.99



(a) (b)

Figure 12: Execution time comparison in UNSW-NB15 and ToN_IoT dataset

In terms of accuracy, precision, recall, F1-score, and execution time, the proposed model has a clear advantage over existing models in both UNSW-NB15 and ToN_IoT datasets.

V. CONCLUSION

In the proposed intrusion detection architecture of this study, the three primary techniques are collecting data, pre-processing and intrusion detection. Pre-processing is performed to reduce unnecessary information and improve quality through data normalization, reduction, cleaning and transformation. The Blockchain Assisted Deep Federated Learning (BC_DFL) intrusion detection system uses this pre-processed data as input. The federated learning-based Capsule Auto-Encoder (FL_CAE) framework learns the characteristics from the inputs and then uses them to identify intruders. Blockchain technology (BCTech) is used for storage purposes and also increases security as it eliminates the risk of adversarial nodes and individual server failure. This research uses UNSW-NB15 and ToN_IoT datasets for implementation and performance evaluation. In the results section, the proposed model is juxtaposed with existing models regarding metrics such as accuracy, precision, recall, F1 score, and execution time. The proposed model demonstrated an F1 score, recall, accuracy, and precision of 96.96%, 96.89%, 97.26%, and 97.28% respectively in the UNSW-NB15 dataset, and 95.74%, 99.54%, 99.49%, and 99.24% in the ToN_IoT dataset. The execution time of the proposed model amounts to 2.31 seconds in the UNSW-NB15 dataset and 1.66 seconds in the UNSW-NB15 dataset.

However, this research requires more storage space and hence the computational complexity issue is slightly enhanced. Thus, in the future, lightweight approaches will be used to solve the complexity issues. In addition, the research aims to develop an effective intrusion detection model to support compound learning models as well as a trust model to improve blockchain algorithms. Subsequent advancements may focus on combining BDFL with self-governing security reaction methods. This could lessen the need for human participation in cyber-security incident response by enabling systems to react automatically and in real-time to threats that are detected. Furthermore, there will be additional security issues when 5G networks are implemented in industrial environments. With its ability to adjust to the unique needs of 5G networks, BDFL can solve problems with edge computing, low-latency communication and a large number of linked devices.

REFERENCES

[1] Almaiah, Mohammed Amin, Aitizaz Ali, Fahima Hajjej, Muhammad Fermi Pasha, and Manal Abdullah Alohali. "A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things." Sensors 22, no. 6 (2022): 2112.

[2] Yazdinejad, Abbas, Ali Dehghantanha, Reza M. Parizi, Mohammad Hammoudeh, Hadis Karimipour, and Gautam Srivastava. "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks." IEEE Transactions on Industrial Informatics 18, no. 11 (2022): 8356-8366.

[3] Abdel-Basset, Mohamed, Nour Moustafa, and Hossam Hawash. "Privacy-preserved cyberattack detection in industrial edge of things (IEOT): a blockchain-orchestrated federated learning approach." IEEE Transactions on Industrial Informatics 18, no. 11 (2022): 7920-7934.

[4] Zahoor, Nadia, Ismail Golgeci, Lauri Haapanen, Imran Ali, and Ahmad Arslan. "The role of dynamic capabilities and strategic agility of B2B high-tech small and medium-sized enterprises during COVID-19 pandemic: Exploratory case studies from Finland." Industrial Marketing Management 105 (2022): 502-514.

[5] Liu, Hong, Shuaipeng Zhang, Pengfei Zhang, Xinqiang Zhou, Xuebin Shao, Geguang Pu, and Yan Zhang. "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing." IEEE Transactions on Vehicular Technology 70, no. 6 (2021): 6073-6084.

[6] Alkadi, Osama, Nour Moustafa, Benjamin Turnbull, and Kim-Kwang Raymond Choo. "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks." IEEE Internet of Things Journal 8, no. 12 (2020): 9463-9472.

[7] Cui, Lei, Youyang Qu, Gang Xie, Deze Zeng, Ruidong Li, Shigen Shen, and Shui Yu. "Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures." IEEE Transactions on Industrial Informatics 18, no. 5 (2021): 3492-3500.

[8] Sahut, Jean-Michel, Denis Schweizer, and Marta Peris-Ortiz. "Technological forecasting and social change introduction to the VSI technological innovations to ensure confidence in the digital world." Technological Forecasting and Social Change 179 (2022): 121680.

[9] Bugshan, Neda, Ibrahim Khalil, Mohammad Saidur Rahman, Mohammed Atiquzzaman, Xun Yi, and Shahriar Badsha. "Toward trustworthy and privacy-preserving federated deep learning service framework for industrial internet of things." IEEE Transactions on Industrial Informatics 19, no. 2 (2022): 1535-1547.

[10] Wei, Jiannan, Qinchuan Zhu, Qianmu Li, Laisen Nie, Zhangyi Shen, Kim-Kwang Raymond Choo, and Keping Yu. "A redactable blockchain framework for secure federated learning in industrial Internet of Things." IEEE Internet of Things Journal 9, no. 18 (2022): 17901-17911..

[11] Abdel-Basset, Mohamed, Nour Moustafa, Hossam Hawash, Imran Razzak, Karam M. Sallam, and Osama M. Elkomy. "Federated intrusion detection in blockchain-based smart transportation systems." IEEE Transactions on Intelligent Transportation Systems 23, no. 3 (2021): 2523-2537..

[12] Tahir, Bushra, Alireza Jolfaei, and Muhammad Tariq. "Experience-driven attack design and federated-learning-based intrusion detection in industry 4.0." IEEE Transactions on Industrial Informatics 18, no. 9 (2021): 6398-6405.

[13] Fu, Xiuhua, Rongqun Peng, Wenhao Yuan, Tian Ding, Zhe Zhang, Peng Yu, and Michel Kadoch. "Federated learning-based resource management with blockchain trust assurance in smart IoT." Electronics 12, no. 4 (2023): 1034.

[14] Ruzafa-Alcázar, Pedro, Pablo Fernández-Saura, Enrique Mármol-Campos, Aurora González-Vidal, José L. Hernández-Ramos, Jorge Bernal-Bernabe, and Antonio F. Skarmeta. "Intrusion detection based on privacy-preserving federated learning for the industrial IoT." IEEE Transactions on Industrial Informatics 19, no. 2 (2021): 1145-1154.

[15] Otoum, Safa, Ismaeel Al Ridhawi, and Hussein Mouftah. "A federated learning and blockchain-enabled sustainable energy-trade at the edge: A framework for industry 4.0." IEEE Internet of Things Journal (2022).

[16] Kumar, Randhir, and Rakesh Tripathi. "DBTP2SF: a deep blockchain-based trustworthy privacy-preserving secured framework in industrial internet of things systems." Transactions on Emerging Telecommunications Technologies 32, no. 4 (2021): e4222.

[17] Latif, Shahid, Zeba Idrees, Jawad Ahmad, Lirong Zheng, and Zhuo Zou. "A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things." Journal of Industrial Information Integration 21 (2021): 100190.

[18] Wang, Jin, Jiahao Chen, Yongjun Ren, Pradip Kumar Sharma, Osama Alfarraj, and Amr Tolba. "Data security storage mechanism based on blockchain industrial Internet of Things." Computers & Industrial Engineering 164 (2022): 107903.

[19] Zhang, Ke, Yongxu Zhu, Sabita Maharjan, and Yan Zhang. "Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things." IEEE network 33, no. 5 (2019): 12-19.

[20] Khan, Latif U., Madyan Alsenwi, Ibrar Yaqoob, Muhammad Imran, Zhu Han, and Choong Seon Hong. "Resource optimized federated learning-enabled cognitive internet of things for smart industries." IEEE Access 8 (2020): 168854-168864.

[21] Sater, Raed Abdel, and A. Ben Hamza. "A federated learning approach to anomaly detection in smart buildings." ACM Transactions on Internet of Things 2, no. 4 (2021): 1-23.

[22] He, Xiaoqiang, Qianbin Chen, Lun Tang, Weili Wang, and Tong Liu. "Cgan-based collaborative intrusion detection for uav networks: A blockchain-empowered distributed federated learning approach." IEEE Internet of Things Journal 10, no. 1 (2022): 120-132.

[23] Hamouda, Djallel, Mohamed Amine Ferrag, Nadjette Benhamida, and Hamid Seridi. "PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for Industrial IoTs." Pervasive and Mobile Computing 88 (2022): 101738.

[24] Yazdinejad, Abbas, Ali Dehghantanha, Reza M. Parizi, Mohammad Hammoudeh, Hadis Karimipour, and Gautam Srivastava. "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks." IEEE Transactions on Industrial Informatics 18, no. 11 (2022): 8356-8366.

[25] Friha, Othmane, Mohamed Amine Ferrag, Mohamed Benbouzid, Tarek Berghout, Burak Kantarci, and Kim-Kwang Raymond Choo. "2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT." Computers & Security 127 (2023): 103097.