Federated Deep Learning for Intrusion Detection in Consumer-Centric Internet of Things

Segun I. Popoola, Agbotiname L. Imoize, *Senior Member*, *IEEE*, Mohammad Hammoudeh, *Senior Member*, *IEEE*, Bamidele Adebisi, *Senior Member*, *IEEE*, Olamide Jogunola, *Member*, *IEEE*, Abiodun M. Aibinu

***Abstract*—Consumer-centric Internet of Things (CIoT) will play a pivotal role in the fifth industrial revolution (Industry 5.0) but it exhibits vulnerabilities that can render it susceptible to various cyberattacks. Recent studies have explored the potential of Federated Learning (FL) for privacy-preserving intrusion detection in IoT. However, the development of the FL models relied on unrealistic and irrelevant network traffic data, while also exhibiting limitations in terms of covered attack types and classification scenarios. In this paper, we develop Federated Deep Learning (FDL) models using three recent and highly relevant datasets, covering a wide range of attack types as well as binary and multi-class classification scenarios. Our findings demonstrate that the FDL models not only achieve high classification performance, comparable to traditional Centralized Deep Learning (CDL) models, in terms of accuracy** ($99.60 \pm 0.46\%$)**, precision** ($92.50 \pm 8.40\%$)**, recall** ($95.42 \pm 6.24\%$)**, and F1 score** ($93.51 \pm 7.76\%$) **but also exhibit superior computational efficiency compared to their CDL counterparts. The FDL approach reduces the training time by** $30.52 - 75.87\%$**. These classification performance and computational efficiency were achieved through multiple rounds of distributed local training in FDL. Therefore, the proposed FDL framework presents a robust security solution for designing and deploying a resilient CIoT.**

***Index Terms*—Federated learning, intrusion detection, cyber security, deep learning, industrial internet of things.**

I. Introduction

THE fifth industrial revolution, commonly referred to as Industry 5.0, has garnered significant attention and recognition within the industrial sector, owing to its extensive advantages. This is still an open and evolving concept with no generally acceptable definition or standard yet. However, according to the European Commission report [1], "Industry 5.0 recognizes the power of industry to achieve societal goals beyond jobs and growth to become a resilient provider of prosperity, by making production respect the boundaries of our planet and placing the well-being of the industry worker at the center of the production process." The vision of Industry 5.0 revolves around sustainability, human-centricity, and resiliency, embodying a forward-thinking approach to industrial development [2].

Consumer-centric Internet of Things (CIoT) will play a pivotal role in the fifth industrial revolution (Industry 5.0) but it exhibits vulnerabilities that can render it susceptible to various cyberattacks. Moreover, the unlawful exploitation of critical user information within the CIoT poses significant risks to trust, security, and can potentially lead to the collapse of the system. Consequently, CIoT must be resilient to cyberattacks to ensure the confidentiality, integrity, and availability of data and infrastructure.

Artificial Intelligence (AI) can simulate human intelligence, and this is crucial in building resilient CIoT. In particular, Machine Learning (ML) and Deep Learning (DL) models can be developed to automatically detect cyber-attacks in IIoT systems. In Centralized ML (CML) and Centralized DL (CDL), distributed data from multiple sources are transmitted to a central location, such as a cloud server, for storage, processing, and model training. However, these centralized approaches face critical privacy concerns, high communication overhead, and computational complexity [3].

Federated Learning (FL) is a decentralized and privacy-preserving approach for ML and DL [4]. It offers lower communication overhead and computational complexity compared to the conventional centralized approach. Distributed network traffic data may contain private and sensitive information about users and this poses a high risk of privacy leakage in CDL [5]. Furthermore, the current strict data privacy protection laws, such as the European Union's General Data Protection Regulation (GDPR)[1] and the Consumer Privacy Bill of Rights in the United States of America, necessitates the adoption of a privacy-preserving DL approach.

In this paper, we propose FDL approach for network intrusion detection in CIoT to address the limitations of CDL method. Our objective is to develop FDL models for collaborative and privacy-preserving network intrusion detection in CIoT while ensuring high classification performance and computational efficiency. Although there are some related works in the literature, previous studies used outdated and irrelevant data sets to develop FL models. Furthermore, the coverage of attack types and classification scenarios was limited in those

Manuscript received May xx, 2023; revised August xx, 2023.

This work was supported by the Engineering and Physical Sciences Research Council [grant number EP/X039021/1]; and the European Research Executive Agency (REA) Project 101086387- REMARKABLE

S. I. Popoola, and O. Jogunola are with the Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M1 5GD, United Kingdom. *Corresponding Author*: s.popoola@mmu.ac.uk

A. L. Imoize is with the Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria, and the Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany

M. Hammoudeh is with the Department of Information and Computer Science, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

B. Adebisi is with the Department of Engineering, Manchester Metropolitan University, Manchester M1 5GD, United Kingdom.

A. M. Aibinu is with the Department of Mechatronics, Federal University of Technology, Minna, Nigeria

[1] https://gdpr.eu/

studies. Later in Section II, we will go into a comprehensive review of the relevant literature. The main contributions of this paper can be summarized as follows.

1) We propose an FDL method that utilizes a Deep Neural Network (DNN) model architecture for local training at the network edge. This method is designed for privacy-preserving, network-based intrusion detection in CIoT.
2) We train and evaluate multiple FDL models using three most relevant and recent datasets (i.e., X-IIoTID, Edge-IIoTset, and WUSTL-IoT-2021) to assess the classification performance and computational efficiency of the proposed method. The evaluation metrics include accuracy, recall, precision, F1 score, training time, and testing time.
3) We conduct a comprehensive investigation to validate the effectiveness of the FDL models in both binary and multiclass classification scenarios. We then compare the classification performance and computational efficiency of the FDL models with traditional CDL models.

The remaining parts of the paper are organized as follows: Section II provides a review of the related work. Section III presents the security threats and data distribution in CIoT datasets. Section IV discusses the centralized and federated deep learning processes for intrusion detection in CIoT. Section V analyzes and discusses the results of our experiments. Finally, in Section VI, we summarize our findings and provide directions for future research.

II. Review of Related Work

In the literature, researchers used different datasets to develop and evaluate the effectiveness of FL models for intrusion detection in IoT systems. The list of these datasets is presented in Table I. However, these datasets are not suitable for efficient network-based intrusion detection in CIoT systems [6], [7]. For instance, the Bitcoin Transactions and Ethereum Classic (ETC) BigQuery datasets contain benign and malicious cryptocurrency transaction information, which are largely irrelevant to intrusion detection detection in CIoT. These datasets are more suitable for anomaly and fraud detection in a blockchain network.

The Power System dataset contains normal operation activities, natural events (short-circuit fault and line maintenance), and attack events (remote tripping command injection, relay setting change, and data injection). The features in the dataset are electrical parameters collected from phasor measurement units within an electricity grid network. However, the requirements and the operational patterns of CIoT are different compared to power systems. Therefore, the relevant application of this dataset is limited to fault and attack detection in power systems.

The Secure Water Treatment (SWaT), Water Distribution (WADI), Gas Pipeline, and Water Storage Tank datasets are popularly used for attack detection in specific industrial process within the context of Industrial Control System (ICS). These datasets depend highly on features related to sensor measurements, actuators' statuses, and specific parameters of industrial packets, which limited their use for diverse industrial systems.

TABLE I
Datasets used for FL models in related work

Dataset	Related FL Paper(s)
Bitcoin Transactions	[8]
ETC BigQuery	[8]
Power System	[9]
SWaT	[8], [10], [11]
WADI	[11]
Gas Pipeline	[8], [12], [13]
Water Storage Tank	[12]
NSL-KDD	[11]
UNSW-NB15	[14], [15]
CIC-IDS-2017	[16]
CIC-IDS-2018	[16]
ToN_IoT	[17], [18]
CIC-DDoS2019	[19], [20]
LITNET-2020	[17]

Furthermore, the NSL-KDD, UNSW-NB15, CIC-IDS-2017, CIC-IDS-2018, CIC-DDoS2019, and LITNET-2020 are mostly relevant to intrusion detection in traditional computer networks. These datasets provide the network traffic characteristics of attacks against traditional IT services but they do not contain realistic CIoT systems' activities, connection protocols and services, diverse communication patterns, and CIoT-specific attack behaviours. For instance, the data samples in the NSL-KDD dataset were collected more than 20 years ago. The testbed did not include any CIoT device because the dataset was created before the widespread adoption of CIoT. In fact, the samples in the NSL-KDD dataset were simulated to represent a typical United States Air Force's local area network.

The benign traffic samples in the CIC-DDoS2019 were generated by four traditional Personal Computers (PCs) using the Hypertext Transfer Protocol (HTTP), HTTP Secure (HTTPS), File Transfer Protocol (FTP), Secure Socket Shell (SSH), and email communication protocols. An effective dataset should cover a wide range of attacks that could be launched against IIoT systems. However, some of the datasets have limited attack types. For example, the CIC-DDoS2019 dataset contains only Distributed Denial of Service (DDoS) attacks.

In recent research, the development of datasets such as the X-IIoTID [7], Edge-IIoTset [6], and WUSTL-2021-IIoT [21] datasets has been specifically tailored for intrusion detection within the CIoT context. These datasets were created with an emphasis on multi-platform connectivity protocols and incorporate devices from a range of vendors. They exhibit both connectivity and device agnosticism. This means that they maintain compatibility with CIoT systems regardless of the specific connectivity protocols, platforms, configurations, or the particular hardware and software deployed. This characteristic aptly mirrors the heterogeneity of network traffic and system activities generated by various CIoT devices, connectivity protocols, and communication patterns, thus ensuring the interoperability of CIoT systems. These datasets encapsulate the behaviours associated with novel CIoT connectivity protocols, the activities of contemporary IIoT devices, and a diverse array of attack types and scenarios. They comprise of multi-view features, including network traffic, host resources, logs, and alerts.

TABLE II
REVIEW OF RELATED WORK

Ref	CL	FL	No. of classes in datasets							
			X-IIoTID			Edge-IIoTset			WUSTL-IIoT	
			2	10	19	2	6	15	2	5
[7]	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗
[22]	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗
[23]	✓	✗	✓	✗	✓	✗	✗	✗	✗	✗
[24]	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗
[25]	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗
[26]	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗
[27]	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗
[28]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓
[29]	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗
[30]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓
[6]	✓	✓	✗	✗	✗	✓	✓	✓	✗	✗
[31]	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
[32]	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
[33]	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
[34]	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗
[35]	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗
[36]	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗
[37]	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗
[38]	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗
[39]	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗
Ours	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

The taxonomy of related work that has utilized X-IIoTID, Edge-IIoTset, and WUSTL-IIoT-2021 datasets for intrusion detection in IIoT is presented in Table II. In previous work [7], [25]–[30], researchers have proposed different ML and DL frameworks for intrusion detection in IIoT based on the CL approach. However, none of these studies explored the FL approach. Furthermore, none of the authors evaluated their CL models using all three datasets.

Al-Hawawreh et al [7] explored all classification scenarios in the X-IIoTID dataset, but they did not cover the other two datasets. On the other hand, authors in [25]–[30] focused on the WUSTL-IIoT-2021 dataset only. However, some of them explored only binary classification [25]–[27], [29], while others focused on 5-class classification [28], [30]. Thus, no study has covered all classification scenarios in all three datasets. Similarly, the authors in [6], [14], [31]–[37] explored the FL approach for intrusion detection in IIoT, but none of them developed and evaluated their FL models using all three datasets.

In addition, Makkar et al [32], Hamouda et al [36], and El Houda et al [14] did not consider the CL approach. Therefore, the performance and computation efficiency of their FL models could not be compared with those of corresponding CL models. Some studies [6], [14], [34]–[37] focused on the Edge-IIoTset dataset only. Among them, Ferrag et al [6] explored all classification scenarios in the dataset, Aouedi et al [35] considered only two scenarios, i.e., 6-class and 15-class, and El Houda [14], Friha et al [34], Hamouda et al [36], and Rashid et al [37] explored binary, 6-class, and 15-class scenarios, respectively.

To address these gaps in the literature, we propose to develop and evaluate CDL and FDL models using all three datasets and cover all classification scenarios in each dataset. To the best of our knowledge, our study is the first to use the WUSTL-IIoT-2021 dataset for FL-based intrusion detection in CIoT. The proposed study is expected to contribute to the development of more accurate and efficient intrusion detection systems for CIoT.

III. CENTRALIZED AND FEDERATED DEEP LEARNING

A. Deep Neural Network

A DNN architecture is used to learn the hierarchical features, complex patterns, and non-linear relationships in the network traffic data, $X \in \mathbb{R}^{M \times D_{\text{in}}}$, where M is the total number of samples and D_{in} is the number of input features. The feedforward neural network is made up of an input layer, three hidden layers, and an output layer. The first hidden layer transforms a batch of the input data, $X_{\text{batch}} \in \mathbb{R}^{N \times D_{\text{in}}}$ and produces:

$$Z_1 = \sigma_1\big(X_{\text{batch}} \cdot W_1 + B_1\big), \tag{1}$$

where $N = M/N_{\text{batch}}$, N is the number of samples in a batch, N_{batch} is the number of batches in the entire dataset, $Z_1 \in \mathbb{R}^{N \times H_1}$ is the output of the first hidden layer, $W_1 \in \mathbb{R}^{D_{\text{in}} \times H_1}$ is the weight, H_1 is the number of hidden neurons, $B_1 \in \mathbb{R}^{N \times H_1}$ is the bias, and $(\cdot)$ is a matrix dot multiplication. σ_1 is a ReLU activation function defined as:

$$f(a) = \max(0, a). \tag{2}$$

The second hidden layer transforms Z_1 and produces:

$$Z_2 = \sigma_1\big(Z_1 \cdot W_2 + B_2\big), \tag{3}$$

where $Z_2 \in \mathbb{R}^{N \times H_2}$ is the output of the second hidden layer, $W_2 \in \mathbb{R}^{H_1 \times H_2}$ is the weight, H_2 is the number of hidden neurons, and $B_2 \in \mathbb{R}^{N \times H_2}$ is the bias.

The third hidden layer transforms Z_2 and produces:

$$Z_3 = \sigma_1\big(Z_2 \cdot W_3 + B_3\big), \tag{4}$$

where $Z_3 \in \mathbb{R}^{N \times H_3}$ is the output of the third hidden layer, $W_3 \in \mathbb{R}^{H_2 \times H_3}$ is the weight, H_3 is the number of hidden neurons, and $B_3 \in \mathbb{R}^{N \times H_3}$ is the bias.

Finally, the output layer transforms Z_4 and produces:

$$Y_{\text{pred}} = \sigma_2\big(Z_3 \cdot W_{\text{out}} + B_{\text{out}}\big), \tag{5}$$

where $Y_{\text{pred}} \in \mathbb{R}^{N \times D_{\text{out}}}$ is the final output which represents the predicted class probabilities, $W_{\text{out}} \in \mathbb{R}^{H_3 \times D_{\text{out}}}$ is the weight, D_{out} is the number of output neurons, and $B_{\text{out}} \in \mathbb{R}^{N \times D_{\text{out}}}$ is the bias. σ_2 is a softmax activation function defined as:

$$\sigma_2(z)_j = \frac{e^{z_j}}{\sum_{k=1}^{D_{\text{out}}} e^{z_k}}, \tag{6}$$

where $j = \{1, \ldots, D_{\text{out}}\}$, e is the base of natural logarithm, z_j is the j^{th} element of the input vector z, and $\sigma_2(z)_j$ represents the j^{th} component of the output of the softmax function applied to z.

B. Centralized Deep Learning

In CDL, all the participating CIoT nodes are expected to send their private network traffic data to a cloud server for aggregation and global model training. In this case, the DNN model is trained centrally with all the data in the training sets of each of the three datasets. The predicted probabilities of the DNN model, Y_{pred}, is compared with the one-hot encoded labels, Y_{true}. The categorical cross-entropy loss function (ϕ) is used to measure the differences between Y_{pred} and Y_{true} as follows:

$$L = \phi\left(Y_{\text{pred}}, Y_{\text{true}}\right) = -\sum_{n=1}^{N} Y_{\text{true (i)}} \log\left(Y_{\text{pred (i)}}\right) \tag{7}$$

To reduce the training losses, the weights and biases of the DNN model are adjusted over E epochs using the Adam [40] and RMSprop optimizers (Φ), as recommended in [6], [7], [21]. The learning rate (η) was set to 0.001 to ensure model convergence.

C. Federated Deep Learning

The FDL is modeled as a collaborative learning process which involves a cloud server and K distributed edge nodes in an CIoT network. Due to the resource-constraints in some CIoT devices, the local training is performed at the edge nodes close to the devices based on the concept of edge computing. The integration of edge computing with federated learning in the CIoT domain offers a powerful solution to the challenges of privacy, network efficiency, latency, and resource limitations. It empowers edge devices to contribute meaningfully to model training while staying within their operational constraints. Thus, a global DNN model (also known as FDL model) and K local DNN models are created using the same hyperparameters. Similarly, the weights of the local DNN models are set to be the same as those of the FDL model. The local DNN models are trained with their respective private training data for a single epoch. At the end of the training, the weights of the local DNN models are sent to the cloud server for aggregation using the FedAvg algorithm [4].

Algorithm 1: Model Aggregation for FDL

```
Initialize K = 10
Initialize R = 10
Initialize server model parameters W^(0)
for r = 1 to R do
    for k = 1 to K do
        Set the client model parameters
        W_k^(r) = W^(r)
        Train the client model on its local data D_k
        W_k^(r+1) = W_k^(r) − η∇φ_k(W_k^(r), D_k)
    end for
    Aggregate the local models' parameters
    W^(r+1) = (1/K) Σ_{k=1}^{K} W_k^(r+1)
end for
```

The model aggregation process for FDL is described in Algorithm 1. Each CIoT edge node, $k \in \{1, \ldots, K\}$, sets its local DNN model to the initial weights of the global DNN model, $W^{(r=0)}$. The CIoT edge node then trains its local DNN model on its private data, $D_k \in \{D_1, \ldots, D_K\}$. The updated local model parameters, W_k^{r+1}, are computed as:

$$W_k^{(r+1)} = W_k^{(r)} - \eta \nabla \phi_k(W_k^{(r)}, D_k), \tag{8}$$

where, ϕ_k is the categorical loss function for the local DNN model on CIoT edge node k's private data, η is the rate at which the learning moves towards a minimum of the loss function, and $\nabla(\cdot)$ is the gradient of the categorical loss function with respect to the model parameters. After all the CIoT edge nodes have updated their respective local DNN models, they send their parameters to the cloud server. Then, the server aggregates the local model updates to improve the classification performance of the FDL model. The updated FDL model parameters, W^{r+1}, are calculated as the average of the parameters of all the local DNN models:

$$W^{(r+1)} = \frac{1}{K} \sum_{k=1}^{K} W_k^{(r+1)} \tag{9}$$

The averaging method ensures that each IIoT edge node's model contributes equally to the global model, regardless of the size or distribution of its private data.

D. Experiments

We conducted several experiments to train and test the proposed CDL and FDL models for network intrusion detection in CIoT environment using the X-IIoTID, Edge-IIoTset, and WUSTL-IIoT-2021 datasets. The experimental setup for the development of the models involves both computer hardware and software, as presented in Table III.

The computation involves the use of Central Processing Unit (CPU), Random Access Memory (RAM), and Graphical Processing Unit (GPU). A special software framework, known as Compute Unified Device Architecture (CUDA)[2], was used to gain direct access to the GPU's virtual instruction set and parallel computational elements. The computer program was written using the Python programming language. Scikit-learn[3], Pandas[4], and Numpy[5] libraries were used for data preprocessing, while TensorFlow and Keras frameworks were used for the development of the CDL and FDL models.

1) Data Pre-Processing: The effectiveness of CDL and FDL models can be influenced by a range of factors. These factors encompass the quality of the training data, the relevance of network traffic features, the dataset's size and representativeness, and the complexity of the classification problem at hand. These considerations guided the selection of the most pertinent datasets, namely X-IIoTID, Edge-IIoTset, and WUSTL-IIoT-2021, while also highlighting the necessity of data preprocessing.

X-IIoTID dataset comprises 65 network traffic features and 820,834 network traffic samples. These samples can be classified into three distinct scenarios: binary, 10-class, and 19-class, as presented in Table IV.

[2]https://developer.nvidia.com/cuda-toolkit
[3]https://scikit-learn.org/stable/
[4]https://pandas.pydata.org/
[5]https://numpy.org/

TABLE III
HARDWARE AND SOFTWARE SPECIFICATIONS

Hardware/Software	Specification
CPU	12th Gen Intel(R) Core (TM) i9-12900K
RAM	128 GB
GPU	NVIDIA GeForce RTX 3090
CUDA	Version 11.4
IDE	Spyder version 5.3.3
Python	Version 3.9.13
TensorFlow	Version 2.11.1
Keras	Version 2.11.0
Sklearn	Version 1.2.2
Pandas	Version 1.5.3
Numpy	Version 1.22.4

TABLE IV
CENTRALIZED DATA DISTRIBUTION FOR X-IIOTID DATASET

Binary	**10-class**	**19-class**	**Samples**
Normal	Normal	Normal	421417
Attack	Reconnaissance	Generic scanning	50277
		Scanning vulnerabilities	52852
		Fuzzing	1313
		Discovering resources	23148
	Weaponization	Brute force attack	47241
		Dictionary attack	2572
		Malicious insider	17447
	Exploitation	Reverse shell	1016
		MITM attack	117
	Lateral Movement	MQTT cloud broker sub.	23524
		Modbus register reading	5953
		TCP relay attack	2119
	C&C	C&C	2863
	Exfiltration	Exfiltration	22134
	Tampering	False data injection	5094
		Fake notification	28
	Crypto ransomware	Crypto ransomware	458
	RDoS	RDoS	141261

Edge-IIoTset dataset encompasses 61 network traffic features and 1,909,671 network traffic samples. These samples are categorized into three distinct scenarios: binary, 6-class, and 15-class, as presented in Table V.

TABLE V
CENTRALIZED DATA DISTRIBUTION FOR EDGE-IIOTSET DATASET

Binary	**6-class**	**15-class**	**Samples**
Normal	Normal	Normal	1363998
Attack	DoS/DDoS attack	TCP SYN flood DDoS attack	50062
		UDP flood DDoS attack	121567
		HTTP flood DDoS attack	48544
		ICMP flood DDoS attack	67939
	Information gathering	Port scanning	19977
		OS fingerprinting	853
		Vulnerability scanning attack	50026
	MITM attack	MITM attack	358
	Injection attack	XSS attack	15066
		SQL injection	50826
		Uploading attack	36807
	Malware attack	Backdoor attack	24026
		Password cracking attack	49933
		Ransomware attack	9689

WUSTL-IIoT-2021 dataset comprises 1,194,464 network traffic samples characterized by 47 distinct features. These samples are grouped into two primary scenarios: binary and 5-class, as presented in Table VI.

In preparation for the model development phase, the three datasets were transformed to ensure they were in suitable for effective learning. This process of data preprocessing encompassed several key steps, including data cleaning, feature scaling, and data partitioning. In the data cleaning stage, efforts were made to remove duplicate samples, redundant features, and instances with missing values. To enhance model convergence, the features of the datasets were normalized using the min-max normalization method.

TABLE VI
CENTRALIZED DATA DISTRIBUTION FOR WUSTL-IIOT-2021 DATASET

Binary	**5-class**	**Samples**
Normal	Normal	1107448
Attack	Command injection	259
	DoS	78305
	Reconnaissance	8240
	Backdoor	212

From the X-IIoTID dataset, we removed six features: date, timestamp, source IP, destination IP, source port, and destination port. This action decreased the feature count from 65 to 59. Fifteen features, including time, source host, destination host, sender IP address, target IP address, file data, full request URI, transmit timestamp, request URI query, TCP options, TCP payload, TCP source port, TCP destination port, UDP port, and message, were removed from the Edge-IIoTset dataset, reducing the feature count from 61 to 46.

For the WUSTL-IIoT-2021 dataset, we eliminated six features: start time, last time, source address, destination address, source IP identifier, and destination IP identifier, thereby reducing the feature count from 47 to 41. The datasets' categorical features and labels were converted into numerical data through the application of one-hot encoding. The Edge-IIoTset dataset contained seven categorical features that were transformed into 49 numerical inputs, increasing the overall feature count from 46 to 95.

Subsequently, each dataset was divided into a training set comprising 70% of the data and a testing set comprising the remaining 30%. This division aimed to facilitate thorough model training and robust testing to evaluate the models' performance.

TABLE VII
HYPERPARAMETERS FOR CDL AND FDL MODELS

	X-IIoTID	Edge-IIoTset	WUSTL-IIoT-2021
D_{in}	59	95	41
H_1	200	90	200
H_2	200	90	200
H_3	200	-	neurons
D_{out}	2/10/19	2/6/15	2/5
σ_1	ReLU	ReLU	ReLU
σ_2	Softmax	Softmax	Softmax
ϕ	Cross entropy	Cross entropy	Cross entropy
Φ	RMSprop	Adam	RMSprop
η	0.001	0.001	0.001
N	250	250	250
E_{CDL}	10	25	10
E_{FDL}	1	1	1
R	10	25	10

2) Centralized and Federated Deep Learning: The classification performance of the CDL models depends on the choice of the hyperparameters and regularization techniques. Therefore, we employed the settings that were used in the previous related studies [6], [7], [41] because they yielded good classification performance. The hyperparameters of the

DNN model are presented in Table VII. The regularization technique helped mitigate overfitting and improved generalization by adding a penalty term to the loss function. The careful selection of hyperparameters led to optimal performance and better convergence during training. These combined efforts contributed to enhancing the overall effectiveness of the FDL model in capturing complex patterns within the data.

For the FDL, each of the training sets for the X-IIoTID, Edge-IIoTset, and WUSTL-IIoT-2021 datasets was divided among $K(= 10)$ CIoT edge nodes as shown in Tables VIII - X, respectively. The entire process was repeated for $R(= 10)$ communication rounds. This approach ensures that the FDL model is trained on all the CIoT edge nodes' private data without needing to send them to the cloud server.

E. Performance Evaluation

In recent related studies [6], [32]–[38], the classification performance of the CL and FL models were evaluated based on accuracy, recall, precision, and F1 score. There are other performance metrics, such as Receiver Operating Characteristic (ROC) curve. However, these four metrics (accuracy, recall, precision, and F1 score) are popularly used and they have proved to be sufficient and reliable in assessing the classification performance of ML, DL, and FL models in different application scenarios. So, for the sake of consistency and ease of result comparison, we decided to evaluate the classification performance of the CDL and FDL models in this study using the same metrics.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}, \tag{10}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \tag{11}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \tag{12}$$

$$\text{F1 score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}, \tag{13}$$

where True Positive (TP) is the number of malicious samples in the testing set that were correctly classified. True Negative (TN) is the number of benign samples that were correctly classified. False Positive (FP) is the number of benign samples that were misclassified as malicious. False Negative (FN) is the number of malicious samples that were misclassified as benign. Also, the computation efficiency of the models are evaluated based on training time and testing time.

IV. Results and Discussion

In this section, we analyze and discuss the classification performance and the computational efficiency of the CDL and FDL models in both binary and multi-class classification scenarios for each of the three datasets in this study.

A. Centralized Deep Learning

1) X-IIoTID: Table XI presents the classification performance of the CDL model on the X-IIoTID dataset. The model correctly identified 99.55% of benign and 98.48% of malicious samples in the binary scenario, signifying efficient detection with very few false alarms. In the 10-class scenario, the model correctly classified over 97% of samples in six categories but misclassified 14.15% of C&C, 5.66% of crypto ransomware, 15.64% of exploitation, and 5.78% of reconnaissance samples due to class imbalance in the training set. In the 19-class scenario, the CDL model accurately classified over 92% of samples for most classes. However, the false negative rates were 21.7% for C&C, 12.92% for CoAP scanning, 40.91% for fuzzing, 23.81% for MITM, 15.82% for shell, and 39.44% for TCP relay attacks, attributed to class imbalance in the training set.

The model effectively detects many types of attacks, yet exhibits higher false negative rates for C&C, CoAP scan, fuzzing, MITM, shell, and TCP relay attacks. These results show that while the CDL model is generally effective in network intrusion detection, its classification performance varies across different types of attacks. The higher false negative rates for specific attack categories will potentially make CIoT systems more vulnerable to these types of intrusions. Therefore, there is a need to generate and include more samples of these attack classes in the training set. Alternatively, data-level techniques (e.g., oversampling, undersampling, hybrid) and algorithmic solutions (e.g., cost-sensitive learning, re-weighting, threshold moving) may be explored to improve the training set balance.

2) Edge-IIoTset: Table XII presents the classification performance of the CDL models trained and tested on the Edge-IIoTset dataset. In the binary scenario, the CDL model correctly classified all the benign and malicious samples, demonstrating its ability to distinguish between benign and malicious network traffic without any errors.

In the 6-class scenario, the CDL model correctly identified over 98% of samples in each of three classes, namely benign, DoS/DDoS, and MITM. However, due to class imbalance in the training set, the model misclassified 24.6% of information gathering samples, 11.66% of injection samples, and 51.09% of malware samples. Thus, the model effectively detects benign traffic and DoS/DDoS and MITM attacks, but struggles with identifying information gathering, injection, and malware attacks.

In the 15-class scenario, the CDL model correctly classified over 93% of the samples across benign, backdoor, DDoS, and MITM classes. Yet, the model misclassified 15.58% to 66.71% of samples in the fingerprinting, password, port scanning, ransomware, SQL injection, uploading, vulnerability scanning, and XSS classes, primarily due to the class imbalance in the training set. Consequently, while the model excels at detecting benign traffic, backdoor, DDoS, and MITM attacks, it has a higher false negative rate when identifying attacks within the aforementioned classes.

3) WUSTL-IIoT-2021: Table XIII presents the accuracy, recall, precision, and F1 score of the CDL models trained and tested on the WUSTL-IIoT-2021 dataset. In binary classification, the CDL model correctly identified all benign

TABLE VIII
FEDERATED DATA DISTRIBUTION FOR X-IIOTID DATASET

Scenario	Class	Label	IIoT edge nodes									
			1	2	3	4	5	6	7	8	9	10
Binary	Normal	0	29533	29661	29439	29428	29609	29674	29569	29353	29196	29321
	Attack	1	27967	27839	28061	28072	27891	27826	27931	28147	28137	27929
10-class	C&C	0	198	177	209	193	191	217	195	202	214	233
	Crypto ransom	1	28	26	30	30	33	34	24	31	35	28
	Exfiltration	2	1576	1504	1580	1504	1478	1540	1559	1567	1576	1621
	Exploitation	3	77	86	73	72	85	72	67	72	87	84
	Lateral movt.	4	2282	2099	2182	2296	2291	2196	2217	2222	2246	2164
	Normal	5	29533	29661	29439	29428	29609	29674	29569	29353	29196	29321
	RDoS	6	9854	10019	9926	9919	9877	9853	9957	9852	9996	9803
	Reconnaissance	7	8932	8853	8993	9079	8821	8808	8883	9022	8981	8925
	Tampering	8	348	350	327	380	360	351	361	365	346	365
	Weaponization	9	4672	4725	4741	4599	4755	4755	4668	4814	4656	4706
19-class	Brute-force	0	3260	3349	3324	3180	3313	3352	3276	3410	3288	3299
	C&C	1	198	177	209	193	191	217	195	202	214	233
	CoAP scan	2	1619	1573	1640	1602	1598	1590	1646	1693	1638	1582
	Crypto ransom	3	28	26	30	30	33	34	24	31	35	28
	Data injection	4	348	346	327	379	359	350	360	361	344	364
	Dictionary	5	140	193	175	191	179	159	181	219	151	192
	Exfiltration	6	1576	1504	1580	1504	1478	1540	1559	1567	1576	1621
	Fake notification	7	0	4	0	1	1	1	1	4	2	1
	Fuzzing	8	96	104	95	86	100	104	83	90	80	101
	Insider	9	1272	1183	1242	1228	1263	1244	1211	1185	1217	1215
	MQTT	10	1684	1568	1642	1741	1689	1668	1658	1611	1639	1643
	MITM	11	4	9	4	13	7	6	10	6	6	10
	Modbus	12	465	389	391	397	444	395	420	434	447	390
	Normal	13	29533	29661	29439	29428	29609	29674	29569	29353	29196	29321
	OS scanning	14	3463	3480	3531	3634	3441	3452	3423	3540	3628	3538
	RDoS	15	9854	10019	9926	9919	9877	9853	9957	9852	9996	9803
	Shell	16	73	77	69	59	78	66	57	66	81	74
	TCP relay	17	133	142	149	158	158	133	139	177	160	131
	Vuln. scanning	18	3754	3696	3727	3757	3682	3662	3731	3699	3635	3704

TABLE IX
FEDERATED DATA DISTRIBUTION FOR EDGE-IIOTSET DATASET

Scenario	Class	Label	IIoT edge nodes									
			1	2	3	4	5	6	7	8	9	10
Binary	Attack	0	42351	41921	42475	42153	42433	42244	42208	41884	42213	42234
	Normal	1	113149	113449	112775	113097	112817	113006	113042	113366	113037	113016
6-class	DoS/DDoS	0	23761	23903	23678	23430	23671	23738	23600	23912	23682	23666
	Info. gathering	1	5107	5018	5127	5261	5180	5149	5066	5219	5088	5116
	Injection	2	7324	7205	7508	7432	7477	7292	7304	7269	7233	7320
	MITM	3	31	32	28	31	29	18	30	24	25	35
	Malware	4	6149	6011	5996	6127	5956	5881	6107	6122	6015	5884
	Normal	5	113128	113201	112913	112969	112937	113172	113143	112704	113207	113229
15-class	Backdoor	0	1695	1655	1826	1743	1783	1775	1690	1726	1749	1712
	DDoS-HTTP	1	3542	3483	3429	3440	3634	3571	3475	3407	3435	3598
	DDoS-ICMP	2	8210	8068	8259	8095	8142	8259	8120	7999	8056	8086
	DDoS-TCP	3	3395	3532	3543	3547	3542	3445	3557	3475	3460	3541
	DDoS-UDP	4	8597	8428	8457	8591	8548	8547	8477	8509	8430	8516
	Fingerprinting	5	72	61	67	57	68	70	58	66	82	74
	MITM	6	19	30	26	31	31	36	39	37	18	23
	Normal	7	113117	113430	112956	113120	112921	112958	113176	113461	113009	113068
	Password	8	3551	3502	3548	3491	3464	3613	3444	3527	3537	3511
	Port scanning	9	1616	1621	1535	1516	1606	1558	1575	1537	1651	1588
	Ransomware	10	765	796	748	749	756	767	798	781	806	771
	SQL injection	11	3657	3729	3550	3578	3554	3451	3523	3573	3678	3622
	Uploading	12	2732	2539	2716	2590	2640	2533	2608	2630	2637	2565
	Vuln. scanning	13	3472	3396	3463	3568	3449	3536	3576	3419	3545	3507
	XSS	14	1060	1100	1127	1134	1112	1131	1134	1103	1157	1068

TABLE X
FEDERATED DATA DISTRIBUTION FOR WUSTL-IIOT-2021 DATASET

Scenario	Class	Class	IIoT edge nodes									
			1	2	3	4	5	6	7	8	9	10
Binary	Normal	0	77576	77579	77693	77555	77563	77501	77499	77433	77465	77403
	Attack	1	6174	6171	6057	6195	6061	5999	6001	6067	6035	6097
5-class	Backdoor	0	18	16	14	12	14	21	14	12	12	14
	Injection	1	17	19	10	18	15	22	17	21	22	20
	DoS	2	5537	5538	5467	5598	5458	5377	5375	5453	5447	5498
	Reconn.	3	602	598	566	567	574	579	595	581	554	565
	Normal	4	77576	77579	77693	77555	77563	77501	77499	77433	77465	77403

instances and 99.87% of malicious instances, confirming its effectiveness in distinguishing network traffic types with vir-

TABLE XI
PERFORMANCE OF CENTRALIZED DEEP LEARNING MODELS BASED ON X-IIOTID DATASET

Scenario	Class	Accuracy	Recall	Precision	F1 Score
Binary	0	99.03	99.55	98.58	99.06
	1	99.03	98.48	99.52	99.00
	Avg	**99.03**	**99.02**	**99.05**	**99.03**
10-class	0	99.92	85.85	90.29	88.01
	1	99.99	94.34	88.76	91.46
	2	100.00	99.92	99.98	99.95
	3	99.98	84.36	98.69	90.96
	4	99.88	97.59	99.33	98.45
	5	98.69	99.50	97.99	98.74
	6	99.98	99.95	99.96	99.96
	7	98.89	94.22	98.57	96.35
	8	99.98	98.02	98.91	98.46
	9	99.99	99.95	99.95	99.95
	Avg	**99.73**	**95.37**	**97.24**	**96.23**
19-class	0	100.00	99.99	99.94	99.96
	1	99.91	78.30	93.55	85.25
	2	99.42	87.08	91.83	89.39
	3	100.00	94.97	97.42	96.18
	4	99.98	98.39	99.09	98.74
	5	99.99	98.23	100.00	99.11
	6	100.00	99.86	100.00	99.93
	7	100.00	92.31	100.00	96.00
	8	99.93	59.09	96.51	73.30
	9	100.00	99.98	99.92	99.95
	10	99.99	99.84	99.64	99.74
	11	99.99	76.19	86.49	81.01
	12	100.00	99.66	99.72	99.69
	13	99.07	99.48	98.73	99.10
	14	99.96	99.55	99.86	99.71
	15	99.98	99.97	99.94	99.96
	16	99.96	84.18	85.53	84.85
	17	99.89	60.56	96.51	74.42
	18	99.98	99.73	99.89	99.81
	Avg	**99.90**	**90.91**	**97.08**	**93.48**

TABLE XII
PERFORMANCE OF CENTRALIZED DEEP LEARNING MODELS BASED ON EDGE-IIOTSET DATASET

Scenario	Class	Accuracy	Recall	Precision	F1 Score
Binary	0	100.00	100.00	100.00	100.00
	1	100.00	100.00	100.00	100.00
	Avg	**100.00**	**100.00**	**100.00**	**100.00**
6-class	0	98.64	98.98	92.61	95.69
	1	98.95	75.40	91.66	82.74
	2	97.43	88.34	67.42	76.48
	3	100.00	100.00	100.00	100.00
	4	97.99	48.91	97.77	65.20
	5	100.00	100.00	100.00	100.00
	Avg	**98.83**	**85.27**	**91.58**	**86.68**
15-class	0	99.90	94.66	96.06	95.35
	1	99.16	93.99	74.89	83.36
	2	99.98	99.78	99.85	99.81
	3	99.50	99.99	81.97	90.09
	4	100.00	99.97	100.00	99.99
	5	99.96	41.18	63.64	50.00
	6	100.00	100.00	100.00	100.00
	7	100.00	100.00	100.00	100.00
	8	97.80	47.67	51.89	49.69
	9	99.44	54.57	84.67	66.37
	10	99.90	79.02	99.92	88.25
	11	97.63	62.38	48.35	54.48
	12	98.72	47.61	66.47	55.48
	13	99.56	84.42	95.77	89.74
	14	99.36	33.29	58.38	42.40
	Avg	**99.39**	**75.90**	**81.46**	**77.67**

tually no false positives and minimal false negatives. For the 5-class classification, it correctly identified over 99% of samples in benign, DoS, and reconnaissance classes. However, it misclassified 21.54% of backdoor and 10.26% of command injection instances due to the class imbalance in the training set. Despite its excellence in detecting benign, DoS, and reconnaissance traffic, the model shows higher false negative rates for backdoor and command injection attacks.

TABLE XIII
PERFORMANCE OF CENTRALIZED DEEP LEARNING MODELS BASED ON WUSTL-IIOT-2021 DATASET

Scenario	Class	Accuracy	Recall	Precision	F1 Score
Binary	0	99.99	100.00	99.99	99.99
	1	99.99	99.87	99.97	99.92
	Avg	**99.99**	**99.94**	**99.98**	**99.96**
5-class	0	100.00	78.46	100.00	87.93
	1	100.00	89.74	88.61	89.17
	2	99.76	99.98	96.47	98.19
	3	100.00	100.00	99.68	99.84
	4	99.75	99.74	100.00	99.87
	Avg	**99.90**	**93.58**	**96.95**	**95.00**

4) Computation Efficiency: Table XIV presents the duration required to train and test the CDL models utilizing the X-IIoTID, Edge-IIoTset, and WUSTL-IIoT-2021 datasets, in the context of both binary and multi-class classification scenarios. The average training times for the models, using the three datasets, were 215.36, 378.87, and 301.75 seconds, respectively. The training duration exhibited variation depending on the number of samples present in the training set of the employed dataset. A larger training set size correlated with a more extended training period.

Conversely, the trained models required an average of 3.14, 7.17, and 4.30 seconds to categorize samples in the testing sets for each of the three datasets, respectively. Similar to the training duration, the testing time was also directly proportional to the size of the samples in the testing set.

TABLE XIV
COMPUTATION EFFICIENCY OF CENTRALIZED DEEP LEARNING MODELS

Dataset	Scenario	Train time (s)	Test time (s)
X-IIoTID	Binary	216.43	3.50
	10-class	220.13	3.07
	19-class	209.51	2.85
Edge-IIoTset	Binary	384.82	8.10
	6-class	363.55	6.68
	15-class	388.24	6.74
WUSTL-IIoT-2021	Binary	298.06	3.90
	5-class	305.45	4.70

B. Federated Deep Learning

1) X-IIoTID Dataset: Figure 1 shows the FDL model's performance in a binary classification scenario using the X-IIoTID dataset. The model's classification accuracy improved with increasing communication rounds between clients and the aggregation server. After ten rounds, the model reached an accuracy of 98.56%, a recall of 98.53%, a precision of 98.60%, and an F1 score of 98.55%, closely aligning with that of the CDL model with a marginal difference of $0.45-0.49\%$.

Within the context of a 10-class classification scenario, Figure 2 shows the performance of the FDL model that was

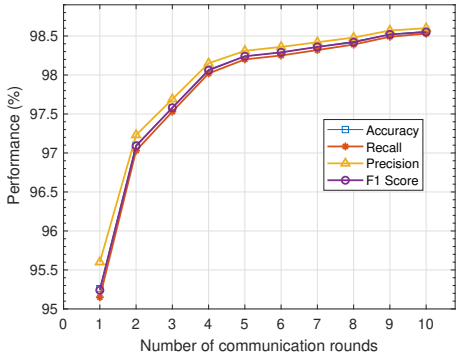

Fig. 1. Performance of FDL model in binary scenario based on X-IIoTID dataset

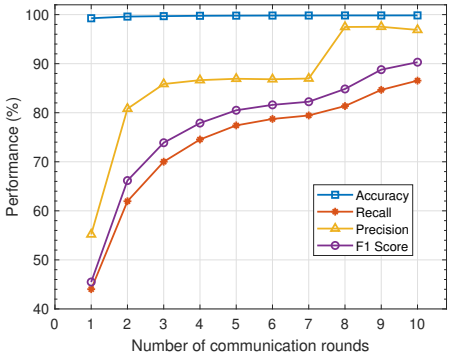

Fig. 3. Performance of FDL model in 19-class scenario based on X-IIoTID dataset

trained and tested with the X-IIoTID dataset. The model's classification accuracy improved as the number of communication rounds between clients and the aggregation server increased. At the end of the tenth communication round, the model attained an optimal performance with an accuracy of 99.71%, recall of 94.55%, precision of 96.47%, and an F1 score of 95.47%. The performance is comparable to that of the CDL model, with only a negligible difference of 0.02 – 0.82%.

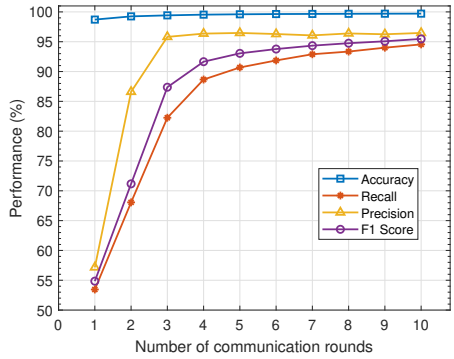

Fig. 2. Performance of FDL model in 10-class scenario based on X-IIoTID dataset

The performance of the FDL model in a 19-class classification scenario, trained and tested with the X-IIoTID dataset, is illustrated in Figure 3. The model's classification performance improved with an increase in the number of communication rounds between clients and the aggregation server. Notably, the model achieved optimal performance with an accuracy of 99.35%, recall of 74.98%, precision of 79.83%, and an F1 score of 75.24% after the 25th communication round. These results are comparable to those obtained with the CDL model, with a difference of only 0.2 – 4.37%.

2) Edge-IIoTset Dataset: Figure 4 shows the performance of the FDL model which was trained and tested with the Edge-IIoTset dataset within the context of binary classification scenario. Impressively, the model achieved a perfect classification performance with an accuracy, recall, precision, and F1 score of 100%. Of particular interest, the FDL model's performance was identical to that of the CDL model. These results indicate the suitability and effectiveness of the FDL model for binary classification tasks, while also highlighting its parity with the CDL model in terms of performance outcomes.

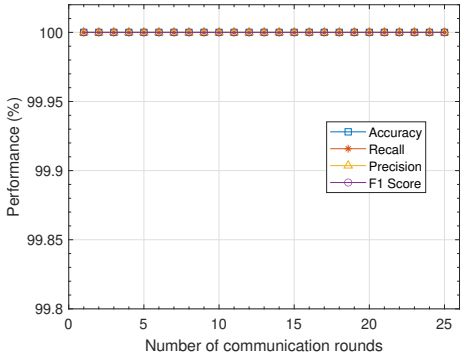

Fig. 4. Performance of FDL model in binary scenario based on Edge-IIoTset dataset

Figure 5 illustrates the performance of the FDL model trained and tested using the Edge-IIoTset dataset within the context of a 6-class classification scenario. The classification performance of the model exhibited an improvement with increasing rounds of communication between clients and the aggregation server. The optimal performance was achieved at the end of the twenty-first communication round with an accuracy of 98.80%, recall of 84.57%, precision of 90.85%, and an F1 score of 86.23%. These results demonstrate that the FDL model's performance is comparable to that of the CDL model, with a negligible difference of 0.03 – 0.73%.

Figure 6 shows the effectiveness of the FDL model when subjected to the Edge-IIoTset dataset under a 15-class classification setting. The FDL model's classification capability showed a marked improvement as the number of communication rounds between the clients and the aggregation server increased. The optimal classification performance was attained after the 25th round of communication, with the model achieving an accuracy of 98.80%, recall of 84.57%, precision of 90.85%, and an F1 score of 86.23%. These results prove that the FDL model can perform comparably to the CDL model, with a negligible deviation of 0.04 – 2.43%.

3) WUSTL-IIoT-2021 Dataset: The performance of the FDL model, trained and tested with the WUSTL-IIoT-2021

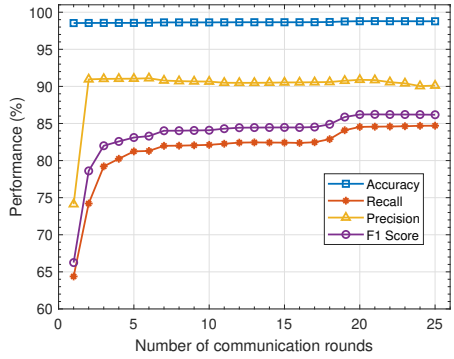

Fig. 5. Performance of FDL model in 6-class scenario based on Edge-IIoTset dataset

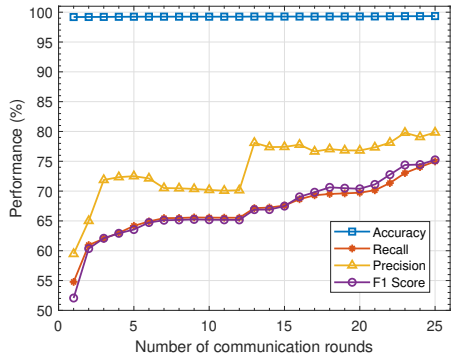

Fig. 6. Performance of FDL model in 15-class scenario based on Edge-IIoTset dataset

dataset in a binary classification scenario, is depicted in Figure 7. The classification performance of the model increased with an increase in the number of communication rounds between the clients and the aggregation server. The model achieved a remarkable accuracy of 99.39%, a recall of 99.86%, a precision of 99.95%, and an F1 score of 99.90%. This performance is comparable to that of the CDL model, with only a marginal difference of 0.02 – 0.08%.

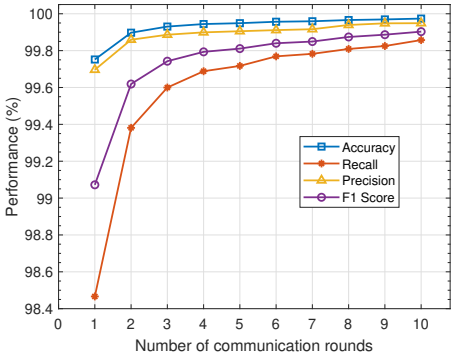

Fig. 7. Performance of FDL model in binary scenario based on WUSTL-IIoT-2021 dataset

Figure 8 illustrates the performance of the FDL model, which was both trained and tested using the WUSTL-IIoT-2021 dataset for a 5-class classification scenario. The model's classification performance improved as the number of communication rounds between clients and the aggregation server increased. The FDL model achieved an accuracy of 99.99%, a recall of 94.60%, a precision of 96.27%, and an F1 score of 95.38%. This level of performance is comparable to that of the CDL model, with only a slight difference of 0 – 0.68%.

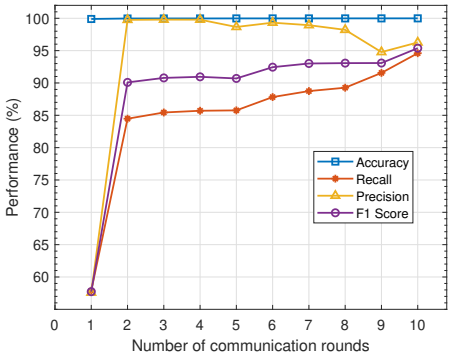

Fig. 8. Performance of FDL model in 5-class scenario based on WUSTL-IIoT-2021 dataset

4) Computation Complexity: Table XV presents the training and testing duration for FDL models utilizing three different datasets, namely X-IIoTID, Edge-IIoTset, and WUSTL-IIoT-2021, in both binary and multi-class classification settings. The average duration of training the models using the three datasets was 52.73, 263.22, and 72.80 seconds, respectively. The training time was observed to vary based on the size of the training set used in each dataset, with larger sets requiring a longer duration for training. Our findings indicate that FDL models have significantly faster training times, with 30.52 – 75.87% lower training times than CDL models.

TABLE XV
COMPUTATION EFFICIENCY OF FEDERATED DEEP LEARNING MODELS

Dataset	Scenario	Train time (s)	Test time (s)
X-IIoTID	Binary	52.41	3.09
	10-class	52.70	3.04
	19-class	53.08	3.02
Edge-IIoTset	Binary	258.03	7.00
	6-class	261.98	7.16
	15-class	269.66	6.88
WUSTL-IIoT-2021	Binary	72.60	3.90
	5-class	73.74	4.41

By contrast, the average time required by the trained models to classify the testing set samples for the corresponding datasets was 3.05, 7.01, and 4.16 seconds, respectively. The duration of testing was found to be directly proportional to the size of the testing set employed in each dataset, mirroring the trend observed in training. Notably, our findings indicate that the FDL model exhibited similar testing times to those of the CDL model.

C. Discussion

In this study, we considered three distinct threat models that are relevant to CIoT environment. A high classification performance when the X-IIoTID dataset was used implies

that the CDL and FDL models can effectively detect and prevent the nine attack scenarios: reconnaissance, weaponization, exploitation, lateral movement, C&C, exfiltration, tampering, crypto ransomware, and RDoS.

Reconnaissance involves several potential actions for attackers including: (i) scanning the target machine to gather general information, such as listening ports, operating system details, and available services; (ii) identifying known vulnerabilities and misconfigurations; (iii) discovering system or software errors and exceptions; and (iv) detecting available resources within the target environment. Weaponization enables attackers to gain entry into the target environment. This could occur through methods like brute force attacks, dictionary attacks, or exploits by malicious insiders.

Exploitation entails attackers capitalizing on known vulnerabilities within the target to establish a reverse TCP shell or initiate a Man-in-the-Middle (MITM) attack. Lateral movement empowers attackers to navigate further within the target environment, establishing a stronger foothold and compromising additional systems and networks. This could involve accessing MQTT cloud broker subscriptions and Modbus register readings, as well as infiltrating the mail server through TCP relay attacks. C&C allows attackers to establish communication channels between compromised machines and their servers. This facilitates the transmission of commands, enabling the attackers to gain control over compromised systems.

Exfiltration encompasses the theft of private and sensitive data from compromised machines using techniques such as compression and obfuscation. Tampering involves intentional manipulation, destruction, or alteration of information on compromised machines, often through methods like false data injection or counterfeit notifications. Crypto ransomware revolves around attackers encrypting critical data on compromised machines and subsequently demanding cryptocurrency payments in exchange for providing the decryption key. RDoS involves attackers threatening to launch DDoS attacks against the target's machines unless a ransom is paid.

For the Edge-IIoTset dataset [6], a high classification performance implies that the CDL and FDL models can effectively detect and prevent the following attack vectors: information gathering, DoS/DDoS attack, MITM attack, injection attack, and malware attack. DoS/DDoS attacks can be executed using methods like TCP SYN, UDP, HTTP, or ICMP flooding, causing a target system to become overwhelmed and unavailable.

Information gathering can acquire crucial information about target machines through techniques such as port scanning, OS fingerprinting, and vulnerability scanning. MITM attacks - the adversaries aim to compromise and manipulate the communication flow between two endpoints that assume they are communicating directly. Spoofing the Domain Name System (DNS) or the Address Resolution Protocol (ARP) are common methods. Injection attacks seek to compromise the confidentiality and integrity of a target machine by injecting malicious scripts into websites, altering a running Structured Query Language (SQL) query, or uploading malware onto web servers.

Malware attacks take forms such as backdoors, password cracking, or ransomware, all of which can lead to unauthorized access, data breaches, or system disruption. Finally, a high classification performance when the WUSTL-IIoT-2021 dataset was used implies that the CDL and FDL models can effectively detect and prevent reconnaissance, command injection attacks, DoS attacks, and backdoor attacks in IIoT environment.

V. Conclusion

In this paper, we developed FDL models for privacy-preserving network intrusion detection in CIoT networks using three recent and relevant datasets (X-IIoTID, Edge-IIoTset, and WUSTL-IIoT-2021), and covered all the binary and multi-class classification scenarios in the datasets. The results of this study show that, across all classification scenarios, the FDL models consistently achieved high performance in terms of accuracy, recall, precision, and F1 score. This performance was found to be comparable with that of the corresponding CDL models.

In assessing the computational efficiency, we observed that the training and testing times for the models were dependent on the size of the respective training and testing sets for each dataset. As expected, larger datasets required longer duration for training and testing. Importantly, our findings indicate that the FDL models exhibited significantly faster training times compared to the CDL models, while maintaining comparable testing times. The findings of this research demonstrate that the FDL framework exhibits superior efficacy in achieving timely and privacy-preserving intrusion detection in CIoT settings. Moreover, this enhanced performance is attained without any significant degradation in classification performance.

It is also important to note that the present study does not address security and privacy concerns in FL framework, which include issues like membership inference, model poisoning, and data poisoning. In future research, a combination of cryptographic techniques and adversarial defenses, such as differential privacy, homomorphic encryption, multi-party computation, and blockchain, will be taken into consideration. These measures aim to establish a secure and privacy-preserving FL methodology for intrusion detection in the IIoT.

References

[1] E. Commission, D.-G. for Research, Innovation, M. Breque, L. De Nul, and A. Petridis, *Industry 5.0 : towards a sustainable, human-centric and resilient European industry*. Publications Office of the European Union, 2021.

[2] L. Zong, F. H. Memon, X. Li, H. Wang, and K. Dev, "End-to-end transmission control for cross-regional industrial internet of things in industry 5.0," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4215–4223, 2021.

[3] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated deep learning for zero-day botnet attack detection in iot-edge devices," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3930–3944, 2021.

[4] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[5] S. I. Popoola, G. Gui, B. Adebisi, M. Hammoudeh, and H. Gacanin, "Federated deep learning for collaborative intrusion detection in heterogeneous networks," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 2021, pp. 1–6.

[6] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40 281–40 306, 2022.

[7] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "X-iiotid: A connectivity-agnostic and device-agnostic intrusion data set for industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3962–3977, 2021.

[8] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8356–8366, 2022.

[9] M. Abdel-Basset, N. Moustafa, and H. Hawash, "Privacy-preserved generative network for trustworthy anomaly detection in smart grids: A federated semisupervised approach," *IEEE transactions on industrial informatics*, vol. 19, no. 1, pp. 995–1005, 2022.

[10] A. N. Jahromi, H. Karimipour, and A. Dehghantanha, "Deep federated learning-based cyber-attack detection in industrial control systems," in *2021 18th International Conference on Privacy, Security and Trust (PST)*. IEEE, 2021, pp. 1–6.

[11] 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 Transactions on Information Forensics and Security*, vol. 18, pp. 41–56, 2022.

[12] O. Aouedi, K. Piamrat, G. Muller, and K. Singh, "Federated semisupervised learning for attack detection in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 286–295, 2022.

[13] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "Deepfed: Federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5615–5624, 2020.

[14] Z. Abou El Houda, B. Brik, A. Ksentini, L. Khoukhi, and M. Guizani, "When federated learning meets game theory: A cooperative framework to secure iiot applications on edge computing," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7988–7997, 2022.

[15] S. Islam, S. Badsha, S. Sengupta, I. Khalil, and M. Atiquzzaman, "An intelligent privacy preservation scheme for ev charging infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1238–1247, 2022.

[16] J. Zhang, C. Luo, M. Carpenter, and G. Min, "Federated learning for distributed iiot intrusion detection using transfer approaches," *IEEE Transactions on Industrial Informatics*, 2022.

[17] M. Abdel-Basset, N. Moustafa, and H. Hawash, "Privacy-preserved cyberattack detection in industrial edge of things (ieot): A blockchain-orchestrated federated learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7920–7934, 2022.

[18] P. Ruzafa-Alcázar, P. Fernández-Saura, E. Mármol-Campos, A. González-Vidal, J. L. Hernández-Ramos, J. Bernal-Bernabe, and A. F. Skarmeta, "Intrusion detection based on privacy-preserving federated learning for the industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1145–1154, 2021.

[19] P. T. Duy, T. Van Hung, N. H. Ha, H. Do Hoang, and V.-H. Pham, "Federated learning-based intrusion detection in sdn-enabled iiot networks," in *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*. IEEE, 2021, pp. 424–429.

[20] A. Zainudin, R. Akter, D.-S. Kim, and J.-M. Lee, "Fedddos: An efficient federated learning-based ddos attacks classification in sdn-enabled iiot networks," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2022, pp. 1279–1283.

[21] M. Zolanvari, M. A. Teixeira, L. Gupta, K. K. M, and R. Jain, "Wustl-iiot-2021 dataset for iiot cybersecurity research," *Washington University in St. Louis, USA*, 2021. [Online]. Available: http://www.cse.wustl.edu/ jain/iiot2/index.html

[22] H. Zhao, G. Liu, H. Sun, G. Zhong, S. Pang, S. Qiao, and Z. Lv, "An enhanced intrusion detection method for aim of smart grid," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2023.

[23] H. C. Altunay and Z. Albayrak, "A hybrid cnn+ lstmbased intrusion detection system for industrial iot networks," *Engineering Science and Technology, an International Journal*, vol. 38, p. 101322, 2023.

[24] P. Jayalaxmi, R. Saha, G. Kumar, M. Alazab, M. Conti, and X. Cheng, "Pignus: A deep learning model for ids in industrial internet-of-things," *Computers & Security*, p. 103315, 2023.

[25] M. Zolanvari, Z. Yang, K. Khan, R. Jain, and N. Meskin, "Trust xai: Model-agnostic explanations for ai with a case study on iiot security," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 2967–2978, 2023.

[26] M. M. Alani, E. Damiani, and U. Ghosh, "Deepiiot: An explainable deep learning based intrusion detection system for industrial iot," in *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*. IEEE, 2022, pp. 169–174.

[27] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "An effective intrusion detection approach based on ensemble learning for iiot edge computing," *Journal of Computer Virology and Hacking Techniques*, pp. 1–13, 2022.

[28] A. S. Dina, A. Siddique, and D. Manivannan, "A deep learning approach for intrusion detection in internet of things using focal loss function," *Internet of Things*, p. 100699, 2023.

[29] M. M. Alani, "An explainable efficient flow-based industrial iot intrusion detection system," *Computers and Electrical Engineering*, vol. 108, p. 108732, 2023.

[30] T. Gaber, J. B. Awotunde, S. O. Folorunso, S. A. Ajagbe, E. Eldesouky *et al.*, "Industrial internet of things intrusion detection method using machine learning and optimization techniques," *Wireless Communications and Mobile Computing*, vol. 2023, 2023.

[31] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "Asynchronous peer-to-peer federated capability-based targeted ransomware detection model for industrial iot," *IEEE Access*, vol. 9, pp. 148 738–148 755, 2021.

[32] A. Makkar, T. W. Kim, A. K. Singh, J. Kang, and J. H. Park, "Secureiiot environment: Federated learning empowered approach for securing iiot from data breach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6406–6414, 2022.

[33] P. Verma, J. G. Breslin, and D. O Shea, "Fldid: Federated learning enabled deep intrusion detection in smart manufacturing industries," *Sensors*, vol. 22, no. 22, p. 8974, 2022.

[34] O. Friha, M. A. Ferrag, M. Benbouzid, T. Berghout, B. Kantarci, and K.-K. R. Choo, "2df-ids: Decentralized and differentially private federated learning-based intrusion detection system for industrial iot," *Computers & Security*, p. 103097, 2023.

[35] O. Aouedi and K. Piamrat, "F-bids: Federated-blending based intrusion detection system," *Pervasive and Mobile Computing*, p. 101750, 2023.

[36] D. Hamouda, M. A. Ferrag, N. Benhamida, and H. Seridi, "Ppss: A privacy-preserving secure framework using blockchain-enabled federated deep learning for industrial iots," *Pervasive and Mobile Computing*, p. 101738, 2022.

[37] 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, 2023.

[38] Z. Abou El Houda, B. Brik, A. Ksentini, and L. Khoukhi, "A mec-based architecture to secure iot applications using federated deep learning," *IEEE Internet of Things Magazine*, vol. 6, no. 1, pp. 60–63, 2023.

[39] M. Al-Hawawreh and M. S. Hossain, "Federated learning-assisted distributed intrusion detection using mesh satellite nets for autonomous vehicle protection," *IEEE Transactions on Consumer Electronics*, 2023.

[40] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.

[41] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.

Segun I. Popoola received the B.Tech. degree in electronic and electrical engineering from the Ladoke Akintola University of Technology, Ogbomoso, Nigeria in 2014, the M.Eng. degree in information and communication engineering from the Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria in 2018, and the Ph.D. degree in cyber security and artificial intelligence from the Department of Engineering, Faculty of Science and Engineering, Manchester Metropolitan University, Manchester, U.K in 2022. His PhD thesis on federated deep learning for botnet attack detection in IoT networks was a product of an academic-industry partnership project jointly funded by the department of engineering at Manchester Metropolitan University and a cyber security company, Cyraatek Ltd UK. He is a Lecturer in the Department of Computing and Mathematics at Manchester Metropolitan University, U.K. In June 2022, he was endorsed as a Global Exceptional Talent by The Royal Society. His research interests include wireless communications, machine/deep learning, cybersecurity, and the Internet of Things. He is a Registered Engineer with the Council for the Regulation of Engineering in Nigeria (COREN). He has published more than 100 research papers in reputable journals and conference proceedings, including IEEE Internet of Things Journal, IEEE Access, and IEEE Vehicular Technology Conference.

Agbotiname L. Imoize (Senior Member, IEEE) is a lecturer in the Department of Electrical and Electronics Engineering at the University of Lagos, Nigeria. Before joining the University of Lagos, he was a Lecturer at Bells University of Technology, Nigeria. He also worked as a core network products manager at ZTE, Nigeria, and as a Network Switching Subsystem Engineer at Globacom, Nigeria. He was awarded the Fulbright fellowship as a visiting research scholar at the Wireless@VT Laboratory, Bradley Department of Electrical and Computer Engineering, Virginia Tech., USA, from 2017 to 2018. He is a research scholar at the Ruhr University Bochum, Germany, under the sponsorship of the Nigerian Petroleum Technology Development Fund (PTDF) and the German Academic Exchange Service (DAAD) through the Nigerian-German Postgraduate Program. He is the vice chair of the IEEE Communication Society, Nigeria chapter, and a registered engineer with the Council for the Regulation of Engineering in Nigeria (COREN). He is a senior member of the IEEE. His research interests cover the fields of 6G wireless communication systems, wireless security systems, and artificial intelligence.

Mohammad Hammoudeh (Senior Member, IEEE) received the B.Sc. degree in computer communications from Arts Sciences and Technology University, in 2004, the M.Sc. degree in advanced distributed systems from the University of Leicester, in 2006, and the Ph.D. degree in computer science from the University of Wolverhampton, in 2008. He is the Saudi Aramco Chair Professor of cyber security with the King Fahd University of Petroleum and Minerals. His research interests include the applications of zero trust security to internet-connected critical national infrastructures, blockchains, and other complex highly decentralized systems.

Bamidele Adebisi (Senior Member, IEEE) received the B.S. degree in electrical engineering from Ahmadu Bello University, Zaria, Nigeria, in 1999, the M.S. degree in advanced mobile communication engineering, and the Ph.D. degree in communication systems from Lancaster University, Lancaster, U.K., in 2003 and 2009, respectively. He was a Senior Research Associate with the School of Computing and Communication, Lancaster University, from 2005 to 2012. He joined Manchester Metropolitan University, Manchester, U.K., in 2012, where he is currently a Professor in electrical and electronic engineering. He has been involving in several commercial and government projects focusing on various aspects of wireline and wireless communications. He is particularly interested in the research and development of communication technologies for electrical energy monitoring/management, transport, water, critical infrastructures protection, home automation, the IoTs, and cyber physical systems. He has several publications and a patent in the research area of data communications over power line networks and smart grid. He is a member of the IET.

Olamide Jogunola (Member, IEEE) received the M.Sc. degree in networking and data communication from Kingston University, London, U.K., in 2015, and the Ph.D. degree in energy transactions in smart grid from Manchester Metropolitan University, Manchester, U.K., in 2019. She is currently a Research Associate with the Department of Engineering, Manchester Metropolitan University, working on Energy-IQ, a U.K.-Canada power forward smart grid demonstrator project. Her research interests include SG, P2P communication technology, the IoT, peer-to-peer energy trading, network optimization, and artificial intelligence for energy market.,Dr. Jogunola was a recipient of the School of Engineering, Manchester Metropolitan University Ph.D. Studentship on an EPSRC U.K.-Korea-funded project: P2P-ETS system. She was previously involved in an Horizon 2020 Smart Cities and Communities programme; Triangulum, funded by the European Commission.

Abiodun M. Aibinu received the Ph.D. degree from International Islamic University Malaysia, in 2010. He is currently a Professor with the Department of Mechatronics Engineering, Federal University of Technology, Minna, Nigeria. His research interests include digital signal and image processing, instrumentation and measurement, intelligent system design, and artificial intelligence with an emphasis on artificial neural networks and genetic algorithm. He has participated and won several awards at various international and national exhibitions and was nominated for 2012 promising researcher award and best teacher award at IIUM Malaysia. He has also won several research grant awards in and outside Nigeria and has authored/co-authored several publications in both local and international journals and conferences. He is presently, the Head of Department, Mechatronics Engineering Department, Federal University of Technology, Minna and the Director, Center for Open Distance and e-Learning (CODeL), Federal University of Technology, Minna.