STE-PFL: Spatial-Temporal Enhanced Personalized Federated Learning for IoT Cross-Domain Access Decision-Making

1st Chunwen Liu
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China
liuchunwen@iie.ac.cn

2nd Hongchen Yu
School of Data Science and Technology
Heilongjiang University
Harbin, China
2212634@s.hlju.edu.cn

3rd Juxin Xiao
Institute of Information Engineering
Chinese Academy of Sciences
School of Cyber Security
University of Chinese Academy of Sciences
Beijing, China
xiaojuxin@iie.ac.cn

4th Feng Dai
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China
daifeng@iie.ac.cn

5th Jie Yin
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China
yinjie@iie.ac.cn

6th Qixu Liu
Institute of Information Engineering
Chinese Academy of Sciences
School of Cyber Security
University of Chinese Academy of Sciences
Beijing, China
liuqixu@iie.ac.cn

***Abstract*—Insufficient access control in the domain of cross-domain IoT (CD-IoT) can result in unauthorized access events and impede the seamless functioning of collaborative IoT applications. The introduction of federated learning facilitates the development of dynamic intelligent access decision-making models for CD-IoT systems. Nonetheless, existing research overlooks the necessity of protecting the privacy of devices and inadequately tackles local model performance and data heterogeneity issues on CD-IoT devices. In this paper, we propose a privacy-preserving access decision-making model for CD-IoT based on Spatial-Temporal Enhanced Personalized Federated Learning (STE-PFL) that enables the detection of fine-grained attack behaviors without the need for data to leave the devices. This approach also enhances the local training model by comprehensively extracting spatial and temporal features from the traffic data. Additionally, it employs the Per-FedAvg algorithm to provide each user with an appropriate initial model during the training phase, allowing the model to quickly adapt to local data and enhance its ability to handle not independent and identically distributed (Non-IID) data effectively. By leveraging the Dirichlet distribution, we construct two Non-IID data scenarios using the CICIDS2018 and UNSW-NB15 datasets, respectively, to thoroughly evaluate the effectiveness of the proposed access decision-making model. The results demonstrate that our model delivers commendable accuracy in CD-IoT access decision support, and surpasses other baseline models in terms of accuracy, recall, and F1-score.**

***Index Terms*—IoT, cross-domain, access decision-making models, personalized federated learning, spatial-temporal enhanced network**

This work was supported by the Climbing Program of the Institute of Information Engineering, Chinese Academy of Sciences (No. E3Z0071116), the Key Laboratory of Network Assessment Technology at Chinese Academy of Sciences and Beijing Key Laboratory of Network security and Protection Technology.

I. Introduction

The rapid advancement of Internet of Things (IoT) technology in recent years has given rise to an increasing number of applications, such as Industrial Internet of Things (IIoT) [1], smart healthcare [2], intelligent transportation [3], and smart cities [4]. The application of IoT technologies enables various heterogeneous devices to connect and communicate, fostering an increase in cross-domain IoT (CD-IoT) system interaction demands, which are crucial for enhancing efficiency and reducing costs. For instance, in the IIoT manufacturing sector, the entire manufacturing process involves multiple different IoT production domains, where devices from different domains can coordinate work according to task requirements and adjust production parameters and procedures in real-time [5]. Similarly, in the healthcare industry, the National Health Information Network has created a virtual alliance of IoT domains across multiple hospitals, ensuring seamless information flow between doctors and patients [6].

Access control plays a vital role in preventing unauthorized access. In dynamic access control methods, access logs serve as the input for a policy mining algorithm that is capable of automatically recognizing attack traffic and mining access control policies [7]. Traditional machine learning methods require centralized collection and processing of data. However, due to reasons such as data privacy, security, or regulatory constraints, cross-domain data sharing is limited. Therefore, data barriers have become one of the challenges in access control of CD-IoT.

To enable model training within domain-specific servers

without the need for cross-domain data exchange, researchers have introduced federated learning [5], [7]. This approach allows domains to locally train models and only share the updated gradients of the models. However, in order to enhance the protection of device privacy, it is imperative to enforce limitations on intra-domain data exchange for IoT devices [8]. Additionally, recognizing fine-grained attack behaviors contributes to the development of more secure strategies [9], but existing research on access decision-making for CD-IoT system based on federated learning overlooks this aspect. Furthermore, the CD-IoT ecosystem comprises numerous devices and cross-domain systems, where variations in device characteristics and system configurations can lead to disparate data distributions on each individual device. Consequently, the overall data across all devices may be highly heterogeneous and non-idd [10], leading to poor performance of federated learning participants [8], [11].

In this paper, we propose a privacy-preserving access decision-making model for CD-IoT based on Spatial-Temporal Enhanced Personalized Federated Learning (STE-PFL) to solve above problems. This model enables STE-PFL training on cross-domain devices without the need to share device data, thereby addressing privacy concerns associated with device data and avoiding the resource pressure of centralized training. In order to enhance the performance of federated local models and identify fine-grained attack behaviors, we construct a hybrid neural network multi-classification model named Spatial-Temporal Enhanced Network (STE-Net). STE-Net integrates CNN and BiLSTM to extract temporal and spatial features from data, and utilize self-attention mechanisms to focus more on relevant information. Furthermore, we combine Per-FedAvg with STE-Net to propose the Spatial-Temporal Enhanced Personalized Federated Learning (STE-PFL) method, which aims to provide each user with a suitable initial model. STE-PFL allows the training model to quickly adapt to local data and effectively handle Non-IID data. As a result, we obtain a personalized global cross-domain access decision-making model that can make decisions on cross-domain access requests.

Our contributions can be summarized as follows:

- We construct a hybrid neural network multi-classification model, STE-Net, to improve accuracy in local training models and identify fine-grained attack behaviors.
- By introducing Per-FedAvg into the access decision-making for CD-IoT systems, we alleviate the performance degradation issue of traditional federated learning caused by Non-IID data.
- We propose a privacy-preserving access decision-making model for CD-IoT based on STE-PFL. This model involves CD-IoT devices as participants and aims to determine whether to allow or deny access requests of CD-IoT without sharing the privacy information of the devices.
- By leveraging the Dirichlet distribution, we construct two Non-IID data scenarios using the CICIDS2018 and UNSW-NB15 datasets, respectively, to thoroughly evaluate the effectiveness of the proposed access decision-making model. The results demonstrate that our model delivers commendable accuracy in CD-IoT access decision support, and surpasses other baseline models in terms of accuracy, recall, and F1-score.

II. Related Work

Traditional access control methods for CD-IoT typically depend on trusted third parties to authenticate requests and make corresponding access control decisions. For example, the National Health Information Network establishes a virtual alliance of IoT domains in multiple hospitals by providing a trusted third-party platform [6]. Similarly, companies such as SmartThings and Google Home provide cross-platform access services. These IoT platforms make access decisions and translate user rules into requests across different domains. Bai L et al. [12] proposed a cross-domain access control method based on trusted third parties and attribute mapping centers, which achieves cross-domain collaboration by translating user rules into requests across different domains. While the cross-domain authorization and access control technology offered by trusted third-party organizations can help alleviate certain security risks [13], [14], these organizations are still susceptible to potential attacks [15] and often lack secure access control policies for cross-domain collaboration [7].

As a decentralized mechanism that does not require trusted third parties, blockchain can enable effective cross-domain transmission and usage of authentication certificates by introducing cross-chain technology into the authentication process of CD-IoT [16]. For example, Yu X et al. [17] proposed a cross-domain IIoT data sharing mechanism based on consortium blockchain, which introduces consortium chains to build trust between different domains in the IIoT. Scholars [18]–[20] have also developed cross-domain dynamic access control models based on blockchain, utilizing the decentralized and tamper-resistant properties of blockchain to record access policies and logs. However, these methods still necessitate expert participation in configuration and lack adaptive access control capabilities, which renders it challenging to dynamically adjust them based on users' actual needs and behavior.

To address these challenges, researchers have started researching more intelligent and adaptive access control methods for CD-IoT. Among these, federated learning is considered a key technology for breaking down data barriers between domains. It enables model training without sharing data across domains, while also helping to enhance the level of intelligence. For instance, Li C et al. [5] utilized LSTM combined with FedAvg methods to design cross-domain behavior recognition models, achieving unified anomaly recognition for devices. In another study [7], scholars proposed a cross-domain interactive decision approach using CNN and FedAvg methods, which can decide whether to allow or deny the cross-domain access requests without sharing privacy information of collaboration participants.

However, there are still some shortcomings in the research on intelligent dynamic access control in CD-IoT. Firstly, the potential risks of data sharing among devices within a domain,

have been overlooked and need to be further considered and addressed. Secondly, most of the current local machine learning models are based on a single model. However, in the context of access flow classification, it is essential to comprehensively consider the temporal and spatial features of data. Thirdly, current research mainly divides traffic into two categories of normal and abnormal, lacking analysis of more granular traffic features, which limits the development of effective security strategies. Finally, the problem of reduced federated learning performance in the context of Non-IID data has been overlooked. In practical applications, there is often highly heterogeneous data between different domains, which directly affects the performance and accuracy of traditional federated learning.

Therefore, this paper proposes a privacy-preserving access decision-making model for CD-IoT based on STE-PFL with devices as participants to avoid data sharing among them. This model enables the external server to obtain the decision-making model without sharing device data, whether in the domain or across domains. Furthermore, a multiclass model based on STE-Net is proposed to comprehensively extract temporal and spatial features, thus enhancing the accuracy and generalization ability of local models and identifying fine-grained attack behaviors. Moreover, Per-FedAvg is employed to enhance the accuracy and applicability of the global model in Non-IID scenarios. Finally, we obtain a personalized global access decision-making model for CD-IoT that can make decisions on cross-domain access requests.

III. Methodology

A. Operational Environment of access control in CD-IoT

The operational environment we are considering for our work involves diverse domains sharing STE-PFL model parameters to create a more efficient cross-domain access decision solution. These domains can be units within a single entity or different institutions. The transmission of model parameters can occur through various means, such as transferring them from the CD-IoT device to the external server or utilizing an internal server for relay. The specific transmission method can be tailored based on the requirements of the network environment and data security. In either case, the external server is responsible for executing the aggregation task and obtaining the decision-making model. Fig. 1 presents this operating environment. In the following experimental validation, we create a simulation involving 20 cross-domain devices functioning as participants. These devices are distributed across various IoT domains.

B. STE-Net

In this paper, we propose STE-Net, a hybrid network-based classifier designed to extract temporal and spatial features from network traffic data for accurate classification. The structure of STE-Net comprises five key components, as depicted in Fig. 2.

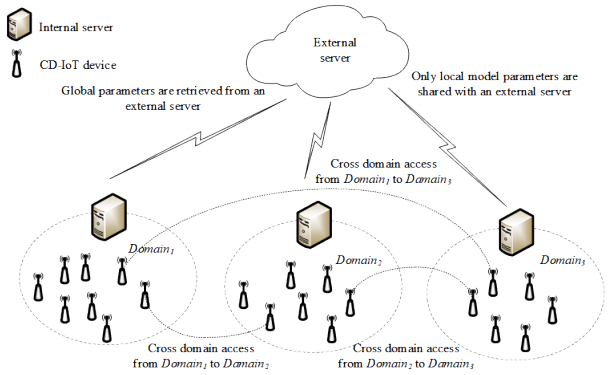

Fig. 1. An illustrative environment where cross-domain devices act as participants in STE-PFL setup.

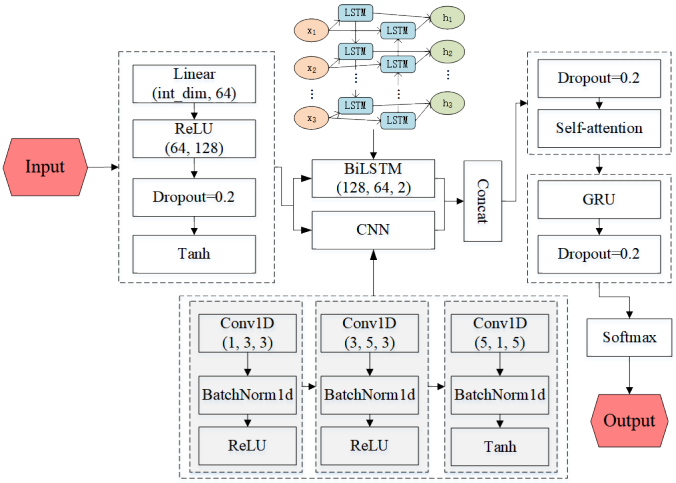

Fig. 2. Structure of the STE-Net.

The first layer consists of linear transformations and non-linear processing with the ReLU activation function. Its purpose is to modify the number of features and prepare for feature extraction in the subsequent layer. Dropout operations are introduced to prevent overfitting.

The second layer combines BiLSTM and CNN layers. BiLSTM captures temporal information, while CNN extracts spatial features. The outputs of both are concatenated to integrate information, enhancing the model's representation and generalization abilities. The inclusion of batch normalization in the process reduces the network's reliance on initial weights and helps alleviate issues such as gradient vanishing and exploding. Additionally, dropout is employed to enhance the model's ability to generalize and reduce overfitting. The primary goal of this layer is to extract more information regarding the spatial and temporal features of network traffic.

The third layer is a self-attention layer. It employs a self-attention mechanism to model the relationships between elements in the sequence. By adaptively focusing on important parts, the expressive power of the model is improved.

The fourth layer is a GRU classifier layer that captures long-term dependencies in the sequential data. Dropout operations

are used to prevent overfitting in this layer as well.

Finally, the model's output is transformed into probabilities for each class using the Softmax function, enabling fine-grained access control decisions for CD-IoT system.

C. Per-FedAvg

In the traditional federated learning framework, a basic aggregation function called FedAvg [21] is commonly used to combine local updates generated by each client in each training round. However, FedAvg only develops one shared model for all users without adapting it to individual users. This limitation becomes particularly problematic in scenarios with unbalanced data, potentially leading to reduced performance of FedAvg [8].

To address this issue, a personalized federated learning called Per-FedAvg was proposed by Fallah in 2020 [22]. Per-FedAvg is specifically developed to tackle the problem of 'client-drift' caused by variations in data across clients, which can result in unstable models and slow convergence. It facilitates the discovery of an initial shared model that can be easily fine-tuned by current or new users to fit their individual local datasets through only one or a few iterations of gradient descent. The objective function can be expressed using equation (1) as follows:

$$\min_{w \in \mathbb{R}^D} F(w) = \frac{1}{n} \sum_{i=1}^{N} f_i(w - a \cdot \nabla f_i(w)) \tag{1}$$

Here, a represents a scalar constant indicating the step size. In our research, we focus on the Per-FedAvg to effectively deal with scenarios consisting of heterogeneous data distributions.

D. Training Process for Our STE-PFL

STE-PFL is a combination of STE-Net and Per-FedAvg. In Fig. 3, we present the training process for our STE-PFL model. The six key steps involved in this training process are outlined below: 1) Initialization of the model parameters for the external server. 2) Random selection of a subset of CD-IoT devices by the external server, which is followed by the distribution of the model parameters to these selected devices. 3) Upon receiving the model parameters, the CD-IoT devices optimize the STE-Net models using their respective local datasets. 4) The CD-IoT devices perform personalized optimization, which helps to further improve the model's performance. 5) The updated model parameters obtained from personalization are uploaded by the CD-IoT devices. 6) The external server receives the updated model parameters from the CD-IoT devices and aggregates them to generate a new global model.

IV. Experiment Analysis

A. Experimental Environment

In this paper, the specific experimental environment is shown in TABLE I.

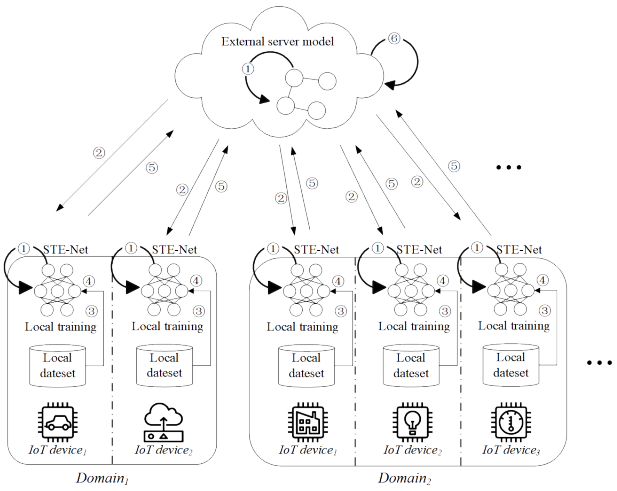

Fig. 3. Workflow of STE-PFL.

TABLE I
CONFIGURATION OF EXPERIMENTAL ENVIRONMENT

Name	Version
GPU	NVIDIA GeForce RTX 3090
CPU	Intel (R) Core (TM) i9-9900K CPU @ 3.6GHz
RAM	32G
Language	Python 3.10.13
Pytorch	2.0.1

B. Use of Datasets

In this paper, CICIDS2018 and UNSW-NB15 [23] datasets are used to evaluate the effectiveness of proposed method. Due to limitations in the experimental environment, we employ the SMOTE method to sample these two datasets. Additionally, we follow the approach described in [24] to randomly select data and allocate devices according to a Dirichlet distribution. This approach allows us to simulate Non-IID scenarios and enhances the reliability of our experiments. Taking into account existing research [25], we set the parameter to 0.1 to create a high Non-IID data condition. The Non-IID data distribution for the CICIDS2018 and UNSW-NB15 datasets can be observed in Fig. 4 and Fig. 5, respectively. The training set and testing set are divided in an 8:2 ratio.

1) CICIDS2018 Dataset

CICIDS2018 is an upgraded version of the CICIDS2017 dataset released by The Canadian Institute for Cybersecurity. This dataset comprises fourteen different types of attacking behaviors. The dataset includes network traffic and system logs for each machine captured, as well as 80 features extracted from the captured traffic using CICFlowMeter-V3.

2) UNSW-NB15 Dataset

The original network packets of the UNSW-NB15 dataset were created by the ACCS Network Scope Lab using the IXI PrimeSturf tool, and contain both real-world network normal activity and synthetic contemporary attacks. There are 9 categories of attacks present in the dataset, and a total of 49 features are utilized to describe each data instance.

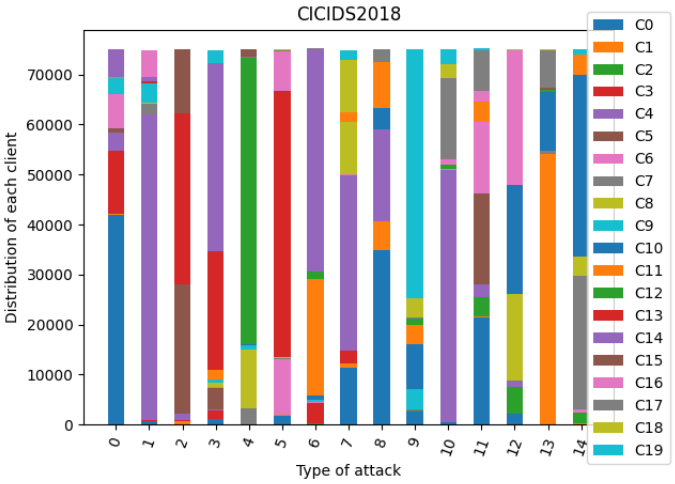

Fig. 4. Data distribution of CICIDS2018.

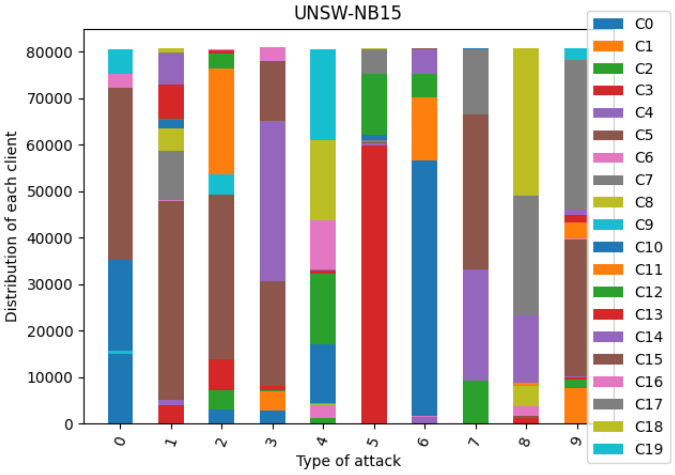

Fig. 5. Data distribution of UNSW-NB15.

C. Dataset Preprocessing Step

1) Label Encoding

The network traffic dataset contains certain feature columns that are represented using non-numeric data. However, machine learning algorithms typically require numeric data for processing. Therefore, this paper employs label encoding to convert the non-numeric features into numeric representations, enabling the STE-PFL models to effectively process and analyze these features.

2) Data Normalisation

Data normalization aids in accelerating model convergence and improving convergence accuracy. In this paper, the data is standardized using the minimum-maximum normalization, compressing it into the range of [0,1].

V. Experimental Results

A. The Analysis of STE-PFL Performance

1) STE-PFL Performance Analysis on the CICIDS2018 Dataset

We conduct experiments using the CICIDS2018 dataset and compare FedAvg (STE-Net) with STE-PFL. We also compare our proposed STE-PFL model with existing research to validate its effectiveness and generalization. Fig. 6 and TABLE II present the experimental results on the CICIDS2018 dataset, comparing our proposed STE-PFL model with FedAvg (STE-Net), Fed-ANIDS [26] and stacked-unsupervised-FL [27].

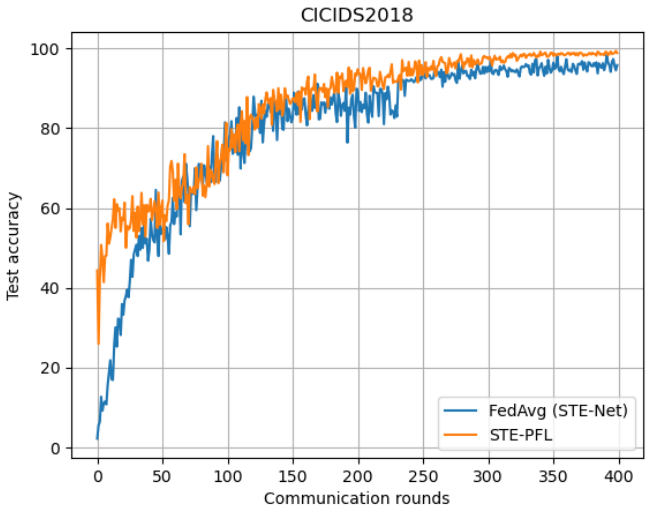

Fig. 6. STE-PFL performance analysis on CICIDS2018.

TABLE II
Comparison of STE-PFL performance on CICIDS2018

Model	ACC	F1-score	Recall
FedAvg (STE-Net)	98.4%	89.6%	90.8%
[26]	94.5%	90.6%	N/A
[27]	98%	90%	88%
STE-PFL	**99.4%**	**91.3%**	**91.3%**

Based on the experimental results (please see Fig. 6 and TABLE II), it can be observed that our proposed STE-PFL model achieves a stable state with the highest accuracy of 99.4% as the number of training rounds increases, demonstrating its effectiveness. Comparing with FedAvg (STE-Net), STE-PFL achieves faster convergence and higher accuracy, with an improvement of 1.0% in accuracy, 1.7% in F1-score, and 0.5% in recall. The STE-PFL model outperforms Fed-ANIDS [26] with an improvement of 4.9% in accuracy and 0.7% in F1-score, and stacked-unsupervised-FL [27] with improvements of 1.4% in accuracy, 1.3% in F1-score, and 3.3% in recall, further validating its effectiveness in access control of CD-IoT.

2) STE-PFL Performance Analysis on the UNSW-NB15 Dataset

Based on the UNSW-NB15 dataset, we conduct a comparison between FedAvg (STE-Net) and STE-PFL, and also compare STE-PFL with FL-SEResNet [28]. The results are presented in Fig. 7 and TABLE III.

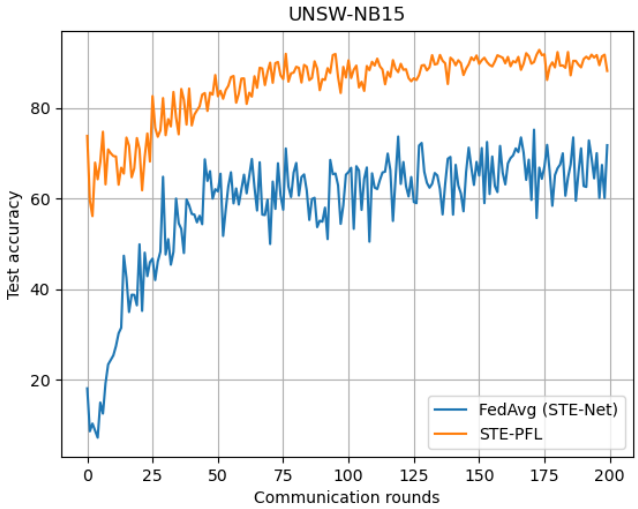

Fig. 7. STE-PFL performance analysis on UNSW-NB15.

TABLE III
COMPARISON OF STE-PFL PERFORMANCE ON UNSW-NB15

Model	ACC	F1-score	Recall
FedAvg (STE-Net)	75.2%	38.6%	44.5%
[28]	80.4%	N/A	N/A
STE-PFL	**92.9%**	**60.0%**	**60.6%**

From TABLE III and Fig. 7, it is evident that our STE-PFL model consistently improves its accuracy on the UNSW-NB15 dataset, reaching a stable state with a highest accuracy of 92.9%. It outperforms FedAvg (STE-Net) in terms of convergence speed and accuracy, achieving improvements of 17.7% in accuracy, 21.4% in F1-score, and 16.1% in recall. Additionally, when compare to the FL-SEResNet model, our STE-PFL model showes a 12.5% improvement in accuracy, further validating its effectiveness in CD-IoT access control in heterogeneous data scenarios.

B. The Analysis of STE-Net Performance

We validates the effectiveness of the STE-Net model through experimental results on the CICIDS2018 and UNSW-NB15 datasets. We compare the STE-Net model with BiLSTM and CNN under both FedAvg and Per-FedAvg frameworks.

1) STE-Net Performance Analysis on the CICIDS2018 Dataset

Based on the experimental results obtained from the CICIDS2018 dataset (please see Fig. 8, Fig. 9 and TABLE IV), it is evident that the STE-Net model proposed in this paper outperforms the CNN and BiLSTM models under the FedAvg framework. The STE-Net model achieves higher scores in performance indicators such as accuracy, F1-score, and recall.

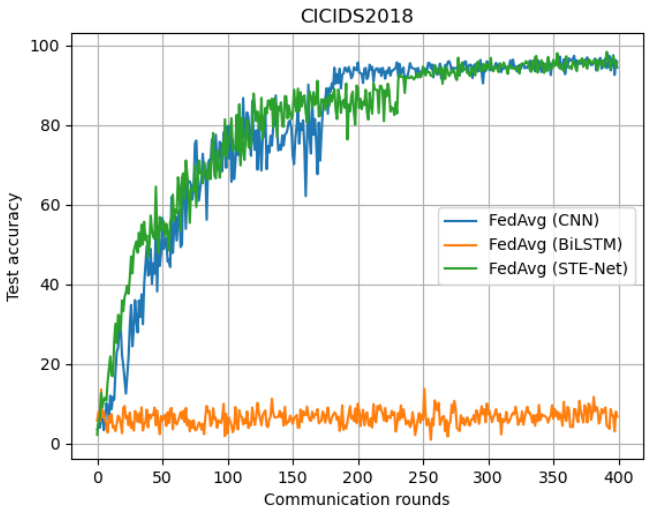

Fig. 8. The STE-Net performance under the FedAvg framework on CICIDS2018.

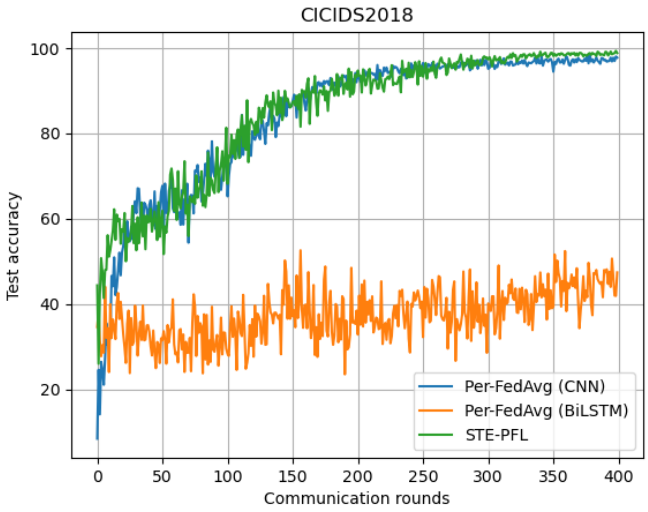

Fig. 9. STE-Net performance analysis under the Per-FedAvg framework on CICIDS2018.

TABLE IV
COMPARISON OF STE-NET PERFORMANCE ON CICIDS2018

Model	ACC	F1-score	Recall
FedAvg (BiLSTM)	13.8%	3.1%	11.3%
FedAvg (CNN)	97.6%	83.9%	86.1%
FedAvg (STE-Net)	**98.4%**	**89.6%**	**90.8%**
Per-FedAvg (BiLSTM)	52.6%	11.2%	16.6%
Per-FedAvg (CNN)	98.4%	88.2%	88.1%
STE-PFL	**99.4%**	**91.3%**	**91.3%**

For instance, the FedAvg (STE-Net) achieves 98.4% in accuracy, while FedAvg (BiLSTM) and FedAvg (CNN) achieve 13.8% and 97.6%, respectively. Similarly, under the Per-FedAvg framework, the STE-Net model also shows significant superiority over the CNN and BiLSTM models, with higher accuracy, F1-score, and recall. Notably, the STE-PFL model achieves an impressive 99.4% in ACC, whereas Per-FedAvg (BiLSTM) and Per-FedAvg (CNN) score 52.6% and 98.4%, respectively.

2) STE-Net Performance Analysis on the UNSW-NB15 Dataset

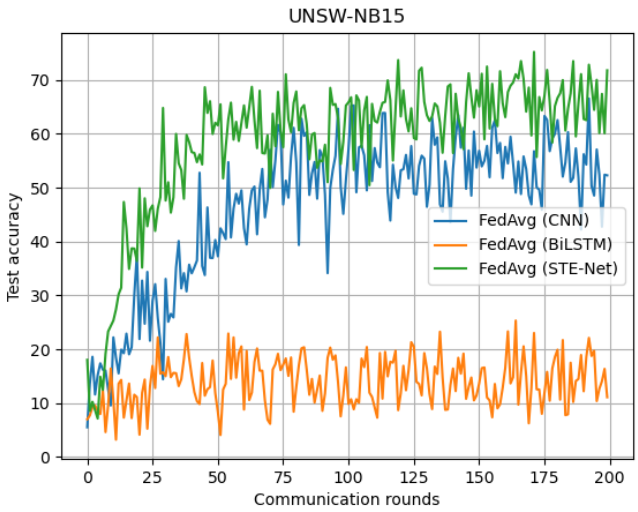

Fig. 10. STE-Net performance under the FedAvg framework on UNSW-NB15.

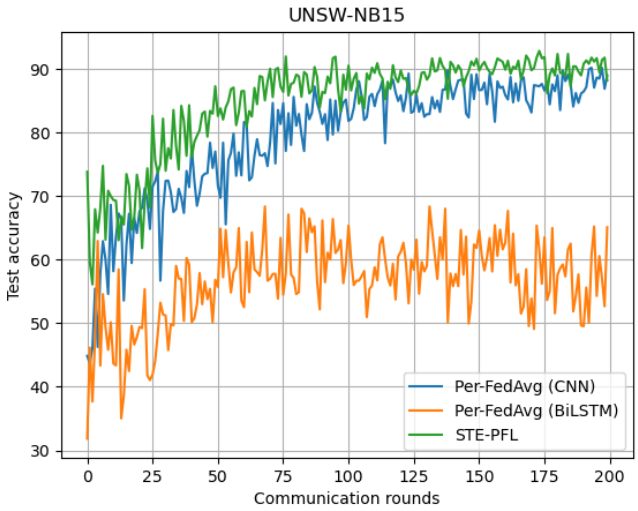

Fig. 11. STE-Net performance analysis under the Per-FedAvg framework on UNSW-NB15.

The experimental results on the UNSW-NB15 dataset (please see Fig. 10, Fig. 11 and TABLE V) show that under the FedAvg framework, STE-Net model shows obvious advantages over CNN and BiLSTM model. STE-Net model has higher scores on accuracy, F1-score and recall. For example, when using the FedAvg framework, the accuracy of the STE-Net model reaches 75.2%, while the accuracy of the CNN and BiLSTM models is 66.6% and 25.3%, respectively. Similarly, under the Per-FedAvg framework, STE-Net model is also significantly better than CNN and BiLSTM model, and its performance in accuracy, F1-score and recall is far superior to the other two models. Our experimental results clearly show the effectiveness and generalization of STE-Net model in CD-IoT access control.

TABLE V
COMPARISON OF STE-NET PERFORMANCE ON UNSW-NB15

Model	ACC	F1-score	Recall
FedAvg (BiLSTM)	25.3%	11.6%	17.2%
FedAvg (CNN)	66.6%	33.6%	40.0%
FedAVG (STE-Net)	**75.2%**	**38.6%**	**44.5%**
Per-FedAvg (BiLSTM)	68.4%	23.3%	27.8%
Per-FedAvg (CNN)	90.2%	59.8%	59.8%
STE-PFL	**92.9%**	**60.0%**	**60.6%**

VI. CONCLUSION

In this paper, we propose a novel privacy-preserving access decision-making model for CD-IoT based on federated learning with devices as participants to avoid data sharing among them. To enhance the applicability of federated learning models and improve the accuracy and generalization ability of local training models, we introduce the STE-PFL model. The STE-PFL model successfully achieves secure model training and robust attack behavior recognition by combining the advantages of Per-FedAvg and STE-Net.

This study utilizes the Dirichlet distribution to create two Non-IID data scenarios from the CICIDS2018 and UNSW-NB15 datasets, with the aim of comprehensively evaluating the effectiveness of STE-PFL in these scenarios. The results show that STE-PFL can extract highly correlated information related to access decisions from access traffic data. In terms of CD-IoT access decision support, it demonstrates considerable accuracy and outperforms other baseline models in metrics such as accuracy, recall, and F1-score. Additionally, the results indicate that using access information based on the application layer for access decisions is a feasible cross-domain collaboration method. Particularly in CD-IoT applications, STE-PFL has great potential as a complementary solution to access control policies.

REFERENCES

[1] Y. Wang and X. Xu, "An Industrial Internet of Things-oriented Malicious Traffic Detection Network with Neural Network Partial Architecture Search," 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, 2023, pp. 1820-1825.

[2] B. B. S., X. W., and A. I., "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," IEEE Access, vol. 5, pp. 26521-26544, 2017-01-01. 2017.

[3] G. B. and B. R. D., "Secure, Privacy Preserving, and Verifiable Federating Learning Using Blockchain for Internet of Vehicles," IEEE Consumer Electronics Magazine, vol. 11, no. 6, pp. 67-74, 2022-01-01. 2022.

[4] L. Silva, M. Calazans, L. Vasconcelos, R. Barcellos, D. Trevisan, and J. Viterbo, "Smart Cities in Focus: A Bicycle Transport Applications Analysis," 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, 2023, pp. 855-860.

[5] C. Li et al., "Federated hierarchical trust-based interaction scheme for cross-domain industrial IoT," IEEE Internet of Things Journal, vol. 10, no. 1, pp. 447-457. 2022.

[6] T. H. Payne, D. E. Detmer, J. C. Wyatt, and I. E. Buchan, "National-scale clinical information exchange in the United Kingdom: lessons for the United States," J. Am. Med. Inform. Assn., vol. 18, no. 1, pp. 91-98, 2011-01-01. 2011.

[7] C. Li, F. Li, Z. Hao, L. Yin, Z. Sun, and C. Wang, "An IoT Crossdomain Access Decision-Making Method Based on Federated Learning," Wireless Communications and Mobile Computing, vol. 2021, pp. 1-9. 2021.

[8] Q. Zhang, Y. Wang, T. Wei, J. Wen, J. Chen, and X. Qiu, "IoT Intrusion Detection Based on Personalized Federated Learning," 2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2023, pp. 326-329.

[9] N. L. Lincy and Midhunchakkaravarthy, "The Investigation of Network Security, Including Penetrating Threats and Potential Security Measures," Soft Computing for Security Applications: Proceedings of ICSCS 2022, pp. 107-117: Springer, 2022.

[10] X. Sáez-De-Cámara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks," Comput. Secur., vol. 131, p. 103299. 2023.

[11] P. Kairouz et al., "Advances and open problems in federated learning," Foundations and Trends® in Machine Learning, vol. 14, no. 1–2, pp. 1-210. 2021.

[12] L. Bai, K. Fan, Y. Bai, X. Cheng, H. Li, and Y. Yang, "Cross-domain access control based on trusted third-party and attribute mapping center," J. Syst. Architect., vol. 116, p. 101957, 2021-01-01. 2021.

[13] J. Sun and Y. M. Fang, "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems," IEEE T. Parall. Distr., vol. 21, no. 6, pp. 754-764. 2010.

[14] H. Anada, J. Kawamoto, J. Weng, and K. Sakurai, "Identity-Embedding Method for Decentralized Public-Key Infrastructure," Trusted Systems - 6th International Conference, M. Yung, L. Zhu, and Y. Yang, eds., Springer International Publishing, 2015, pp. 1-14.

[15] M. Alam, X. Zhang, K. Khan, and G. Ali, "xDAuth: a scalable and lightweight framework for cross domain access control and delegation," Proceedings of the 16th ACM symposium on Access control models and technologies, Association for Computing Machinery, 2011, pp. 31-40.

[16] D. Li, J. Yu, X. Gao, N. Al-Nabhan, and Z. Pan, "Research on Multidomain Authentication of IoT Based on Cross-Chain Technology," Secur. Commun. Netw., vol. 2020, p. 6679022, 2020-01-01. 2020.

[17] X. Yu, Y. Xie, Q. Xu, Z. Xu, and R. Xiong, "Secure Data Sharing for Cross-domain Industrial IoT Based on Consortium Blockchain," 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, 2023, pp. 1508-1513.

[18] S. Sun, S. Chen, R. Du, and C. Mateos, "Trusted and Efficient Cross-Domain Access Control System Based on Blockchain," Sci. Programming-Neth., vol. 2020, p. 8832568, 2020-01-01. 2020.

[19] C. Li, F. Li, L. Yin, T. Luo, B. Wang, and Y. Zhang, "A Blockchain-Based IoT Cross-Domain Delegation Access Control Method," Secur. Commun. Netw., vol. 2021, p. 3091104, 2021-01-01. 2021.

[20] X. Hao, W. Ren, Y. Fei, T. Zhu, and K. R. Choo, "A blockchain-based cross-domain and autonomous access control scheme for internet of things," IEEE T. Serv. Comput., vol. 16, no. 2, pp. 773-786. 2022.

[21] B. Mcmahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y Arcas, "Communication-efficient learning of deep networks from decentralized data," Artificial intelligence and statistics, PMLR, 2017, pp. 1273-1282.

[22] A. Fallah, A. Mokhtari, and A. Ozdaglar, "Personalized federated learning: A meta-learning approach," arXiv preprint arXiv:2002.07948. 2020.

[23] N. Moustafa and J. Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," Information Security Journal: A Global Perspective, vol. 25, no. 1-3, pp. 18-31. 2016.

[24] T. H. Hsu, H. Qi, and M. Brown, "Measuring the effects of non-identical data distribution for federated visual classification," arXiv preprint arXiv:1909.06335. 2019.

[25] H. Reguieg, M. E. Hanjri, M. E. Kamili, and A. Kobbane, "A Comparative Evaluation of FedAvg and Per-FedAvg Algorithms for Dirichlet Distributed Heterogeneous Data," arXiv preprint arXiv:2309.01275. 2023.

[26] M. J. Idrissi et al., "Fed-ANIDS: Federated learning for anomaly-based network intrusion detection systems," Expert Syst. Appl., vol. 234, p. 121000. 2023.

[27] G. de Carvalho Bertoli, L. A. P. Junior, O. Saotome, and A. L. Dos Santos, "Generalizing intrusion detection for heterogeneous networks: A stacked-unsupervised federated learning approach," Comput. Secur., vol. 127, p. 103106. 2023.

[28] C. Zheng, Y. Wu, and K. Xiao, "Intrusion detection based on federated learning and deep residual network," Journal of Computer Applications, vol. 43, no. S1, p. 133. 2023.