Intelligent Edge Computing for IoT: Enhancing Security and Privacy

Lobna Osman[1], Olutosin Taiwo[2,*], Ahmed Elashry[3], Absalom E. Ezugwu[4]
[1]Delta Higher Institute for Engineering & Technology, Department of Electronics and Communications Engineering, Egypt.
[2]Department of Mathematical Sciences, Anchor University, Lagos, Nigeria.
[3]Department of Information Systems, Kafr El-Sheikh University, Kafr El-Sheikh 33511, Egypt
[4]Unit for Data Science and Computing, North-West University, 11 Hoffman Street, Potchefstroom 2520, South Africa
Email: lobna.aziz@dhiet.edu.eg ; otaiwo@aul.edu.ng ; ahmed_elashry@fci.kfs.edu.eg ; abiodun.ikotun@yabatech.edu.ng

Abstract

Edge computing is a distributed computing paradigm that involves processing data at or near the edge of the internet of things (IoT) network, instead of centralized server. This makes the cyber-attacks increasingly sophisticated, and traditional security measures become no longer sufficient to protect against them. Concurrently, privacy concerns arise when sensitive data is involved in Edge computing applications containing confidential information. In this paper, we propose a privacy-preserved federated learning (FL) approach for cyber-attack detection in edge based IoT ecosystem. A novel lightweight convolutional Transformer network (LCT) network is designed to precisely identify cyber-attacks though learning attack patterns from IoT traffics in local edge devices, where model is personalized though fine-tuning. The privacy of model and data is preserved in our system via incorporating differential privacy and secure aggregation during the cooperative training process on edge devices. We evaluate our proposed approach on a real-world dataset of network traffic (NSL-KDD) containing various types of attacks, and the experimental results show that our personalized FL approach outperforms traditional FL in terms of detection accuracy. We also show that our approach is effective in handling non-stationary data and adapting to changes in the network environment.

Keywords: Edge Computing; IoT; Intelligent Systems; Data Security; Privacy

1. Introduction

IoT stands for the Internet of Things, which refers to the network of physical objects or devices, vehicles, home appliances, and other items that are connected to the internet, enabling them to collect and exchange data. IoT technology allows these objects to be remotely controlled, monitored, and optimized, providing a wide range of benefits in various industries such as healthcare, transportation, manufacturing, and agriculture [1].

Edge computing is a distributed computing paradigm that brings computation and data storage closer to the source of data generation. This can be particularly useful in the context of the IoT, where large amounts of data are generated by a variety of sensors and devices. Traditionally, data generated by IoT devices is transmitted to a centralized cloud infrastructure for processing and analysis. However, this approach can be inefficient, as it requires a large amount of bandwidth and can lead to latency issues. Edge computing, on the other hand, processes data closer to the source, typically at the edge of the network, in order to reduce latency, improve reliability, and lower the cost of transmitting data to the cloud[2]–[4].

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

Despite benefits brought to IoT using edge computing, it also introduces several challenges. security and privacy issues are regarded as the most important interests of the research community and industrial communities. Both security and privacy are presenting a significant difficulty for various business associations and international corporations. Predominant cyberattacks have proved the exposures of edge computing based IoT. This vulnerability exists because the interconnectedness of edge devices in the IoT networks make them accessible from the anonymized and disreputable internet, which imply broader attack surface. None of the globally reported issues, have a bigger effect on IoT adaptation than security and privacy. It's too bad, though, that users often don't understand how security issues affect them until after a breach has happened and caused huge problems, like the loss of important data. With all the security vulnerabilities that have put people's privacy at risk, users are now less willing to put up with bad security. Overall, edge computing in IoT introduces many security challenges that must be addressed to ensure the safety and privacy of the data and devices. It is important to implement a comprehensive security strategy that includes device security, data security, communication security, physical security, and scalability [5], [6], [7].

In response to the above challenges, this work contributes to body of knowledge thru proposing a novel federated learning (FL) framework that enables personalized model training to identify and detect the cyber-attacks on IoT, while preserving user privacy. A novel lightweight convolutional Transformer network (LCT) network is presented to capture both short- and long-term dependencies of attacks in IoT traffics on resource-constrained edge devices. Our framework includes differential privacy to preserve the privacy of user data during the learning process thru incorporating a privacy budget that limits the amount of information that can be learned about client during the training process Overall, our proposed personalized FL approach offers a promising solution for improving cyber-attack detection while preserving user privacy. It has the potential to be applied in various other domains where personalized models are required.

The remaining part of this work is outlined as follow. Section 2 review and discuss the literature studies. A background on the security of edge computing is presented in Section 3. Section 4 discuss and explain the methodology of the proposed model. Section 5 describe the performed experiments, the results, and related analysis. Finally, the conclusion is made available in section 6.

2. Related Work

With the increased interest about the security and privacy issues of edge enabled IoT networks, the literature contains many studies that have tried to cover these challenges and provide acceptable solution to them. In [8], the authors reviewed the challenges of privacy and security in IoT devices and provide potential solutions to mitigate these issues. They discussed the main challenges surrounding IoT security in terms of data security, device security, and network security, and highlighted the privacy concerns associated with IoT devices, such as the collection and sharing of sensitive personal data. In [9], the authors reviewed and analyzed the security and privacy challenges associated with edge computing and its role in context of the IoT environments. They discussed the key threats and attack vectors that can compromise the security and privacy of edge computing in IoT. These threats include distributed denial of service (DDoS) attacks, man-in-the-middle attacks, and data breaches.

Deep learning (DL) has a notable role in developing intelligent IoT model with high level security and privacy. For instance, in [10], the authors developed an edge-based intrusion detection for social IoT using Generative Adversarial Networks (GANs) that composed of generator and a discriminator. The generator developed to creates fake data samples, while the discriminator was used identify real and fake samples. The authors use a modified GAN architecture to generate realistic network traffic data and train the discriminator to identify anomalous traffic patterns. In [11], the authors proposed a lightweight and optimized deep learning-based host-intrusion detection system for IoT, which was deployed on the edge to improve real-time detection and response. The proposed system addressed the challenges of IoT security and achieves high performance, making it suitable for practical deployment in IoT environments. In [12], the authors developed a novel approach for zero-day botnet attack detection in IoT-edge devices using federated DL. Their approach addressed he challenges of resource constraints and data privacy and achieves high performance for attack detection. The authors demonstrated the feasibility and effectiveness of the proposed approach through experimental evaluation and provide insights for future research in this area. In [13], the authors presented DL-based reliable routing attack detection mechanism for industrial IoT, which addresses the challenges of routing attacks and achieves high performance for attack detection. they demonstrated the feasibility and effectiveness of the proposed approach through experimental evaluation and provide insights for future research in this area. In [14], the authors proposed a low-complexity mechanism, named LocKedge, for detection cyberattack on IoT edge

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

computing. This mechanism was build based on combination between DL and signal processing techniques to analyze the network traffic data and detect anomalous patterns that indicate cyberattacks. They also introduce a feature selection method that reduces the complexity of the detection mechanism and improves its performance.

Other studies moved toward leveraging the blockchain technology to address the security and privacy of edge based IoT. For example, the paper [15] discussed how the integration of edge computing and blockchain technology, a can help address the challenges of IoT, such as security, privacy, scalability, and interoperability. It also presented several use cases of blockchain for edge computing, including supply chain management, smart homes, smart cities, and healthcare. it also discussed the technical challenges of integrating blockchain with edge computing, such as network latency, computational complexity, and energy consumption. In [16], the authors proposed a deep recurrent neural network (RNN) to analyze the time-series data from the medical IoT sensors, and a ML algorithm to classify the data as normal or anomalous based on its similarity to previously observed data. however, the performance of this method relies on the underlying feature engineering applied. In [17], the authors developed a hybrid metho that combine blockchain and deep learning-based approach for securing edge-envisaged green connected autonomous vehicles (CAVs), in which, the blockchain was used to securely store and manage the data generated by CAVs, and deep models was used to analyze the data and detect anomalous patterns that indicate cyberattacks. They also introduce a federated learning approach that allows multiple CAVs to collaboratively train the deep learning models without revealing their private data. In [18], the authors suggested a method for detecting cyberattacks in the industrial edge of things (IEoT) while preserving privacy through the use of blockchain-orchestrated federated learning. FL was applied to enables the training of models across multiple devices without sharing the underlying data. Blockchain in this approach adds an additional layer of security by creating a distributed ledger of transactions that provide a secure way to orchestrate the FL process and ensure that the data remains private and secure.

3. Securing Edge Computing environment

The integration of edge technologies into IoT systems bring many advantages to that facilitate the management of huge quantity of data propagating across IoT networks. This data varies in their level of sensitivity according to the nature of services and applications from which it is generated. As shown in Figure 1, the traditional installation of edge based IoT systems, the data is communicated between IoT layer and edge layer across local wired and/or wireless networks. Contrarywise, the data is communicated between edge layer and cloud layer via public wired and/or wireless network. Unfortuitously, there is no edge computing paradigm that is secured enough, which leaves them exposed to significant privacy and security risks as well as attacks on those fronts.

To this end, A security architecture for edge based IoT system should include measures to protect edge devices, networks, and applications from various types of cyber threats. These measures can be defined according to the type and the nature of cyberattacks threatening the system. the work [9] taxonomized the important conceivable security and privacy attacks, their categories, and their sources into different classes including Malicious Hardware/Software Injection, Jamming Attacks, Distributed Denial of Service (DDoS), Eavesdropping or Sniffing, Non-Network Side-Channel Attacks, Routing Information Attacks, Forgery Attacks, Unauthorized Control Access, Integrity Attacks Against Machine Learning, Replay Attack or Freshness Attacks, Inessential Logging Attacks, Security Threats from/on IoT Devices, Privacy Leakage, and unknown attacks.

To mitigate these security and privacy challenges, it is essential to implement robust security measures that span the entire edge computing architecture, from the devices themselves to the communication channels and cloud-based services. This includes implementing secure boot and firmware update mechanisms, deploying encryption and access controls, Security monitoring and logging, and using secure communication protocols. It is also important to perform regular security audits and vulnerability assessments to identify and address any potential security weaknesses. Network segmentation can be used to isolate edge devices and applications from the rest of the network, reducing the attack surface and preventing lateral movement by attackers. Blockchain technology can be used to securely manage and share data across distributed edge devices and ensure its integrity. More, deep learning can be used to detect and prevent cyberattacks, and to enhance the effectiveness of intrusion detection and prevention systems.

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

4. The proposed model

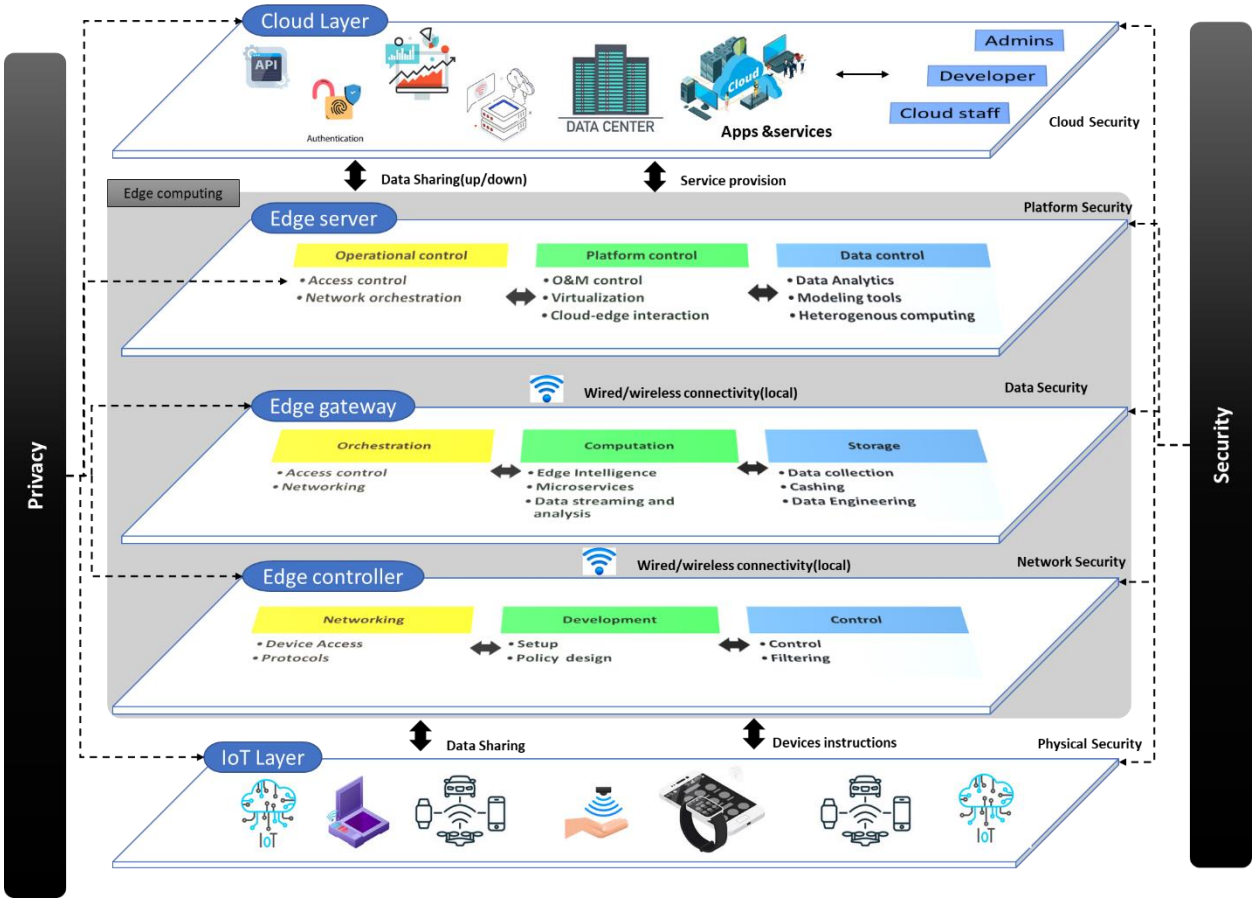

Figure 1: systematic diagram of security and privacy dimensions in edge computing based IoT ecosystem

Once the input of network traffics are fed into the proposed model, they are embedded to take the form of the vectorized representations of raw inputs. Since the IoT traffic samples include some categorical attributes (like protocol, ports, service, flag), the proposed LCT model add tabular positional embedding (PE) layer at the beginning of the network to enable exploiting the positional information of traffic feature during the learning process. To do so, the PE adopt the sine and cosine occupation with diverse rate of recurrence to encode the positional information in traffic data. Specially, the former function is used for even positions, while the latter is used to encode information at odd positions. This can be mathematically expressed as follows:

$$PE(pos, 2i) = sin\left(\frac{pos}{1000^{\frac{2i}{d_{model}}}}\right) \quad (1)$$

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

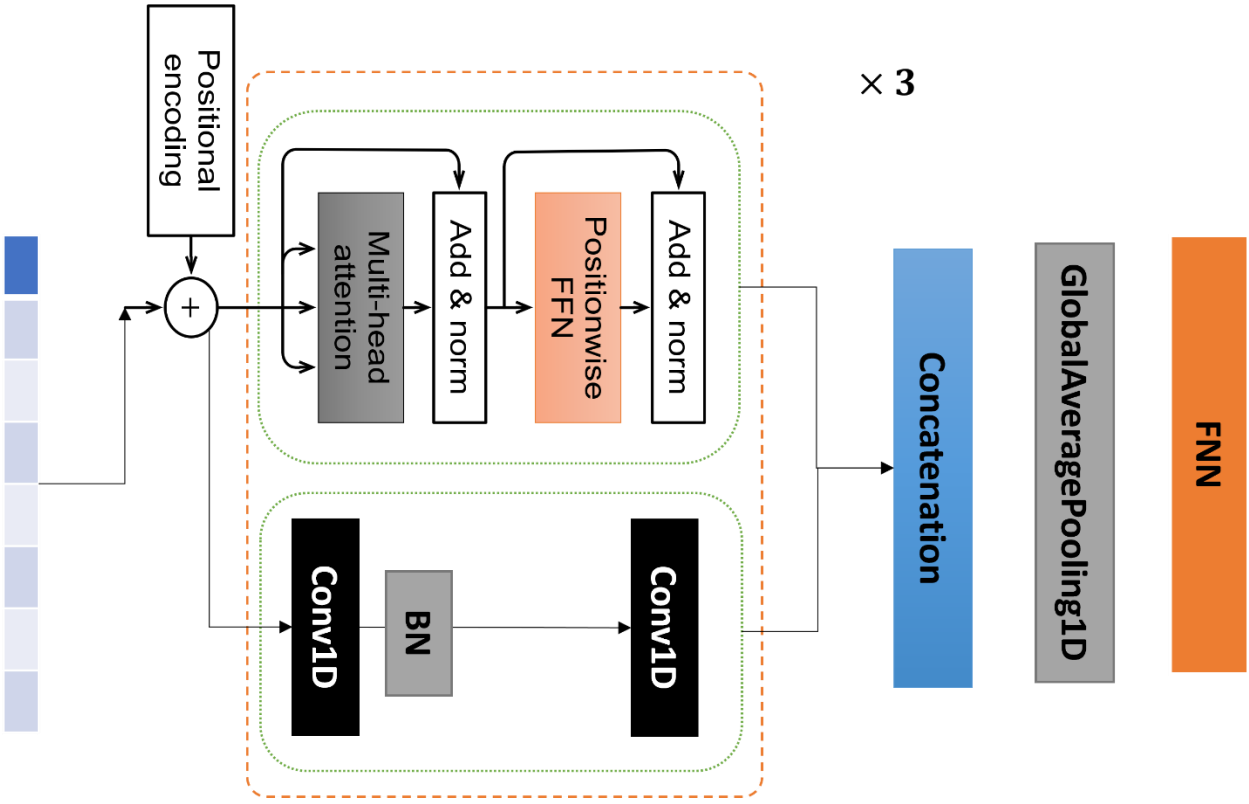

Figure 2: Illustration of the architecture of the proposed LCT network for privacy-preserved cyber-attack detection in edge-based IoT.

$$PE(pos, 2i+1) = cos\left(\frac{pos}{1000^{\frac{2i}{d_{model}}}}\right) \quad (2)$$

The embedded inputs are followingly passed to stack of three transformer blocks (See Figure 2). In each transformer block, the received embedding is projected into a set of queries (Q), keys (K) and values (V). These metrices are used followingly used to calculate scaled dot-product attention as follow:

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (3)$$

The term $\sqrt{d_k}$ is scaling variable used to soothes the gradients computation throughout the propagation training. Decisively, a new feature maps are generated from the dot product between the normalized matrix and value matrix V. To further boost the representational power, we implement multi-head SA (MHSA) by performing the above computation concurrently for different heads, whereas everyone individualistically learns distinct $Q/K/V$ vectors with parameters $W_i^Q \in \mathbb{R}^{d_{hidden} \times d_k}$, $W_i^K \in \mathbb{R}^{d_{hiddenl} \times d_k}$, and $W_i^V \in \mathbb{R}^{d_{hidden} \times d_v}$, correspondingly. This way, the outcome of head h_i represent the outcome of $i-th$ SA operation, whereas all heads' outcomes are concatenated to compute the final representation. This method grants the model the ability to concentrate on a variety of positions and supplies the attention layer with a number of distinct representational thread.

$$MHSA(Q, K, V) = Concat(h_1, \dots, h_h)W^O \quad (4)$$

$$h_i = Attention(QW_i^Q, KW_i^K, VW_i^V) \quad (5)$$

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

Beyond the SA layer, the transformer module is configured with feed-forward network (FFN) that is composed of two dense layers with Gaussian Error Linear Unit (GeLU) function. Besides, indistinguishable weights are optimized on every row of the attention matrices, which could be deemed as cross-correlation operation for elements of attention matrix. This can be mathematically expressed as follows:

$$FFN(x) = \sigma(max(0, xW_1 + b_1)W_2 + b_2) \quad (6)$$

Layer normalisation is performed on each sample so that training can be maintained consistently, and convergence can occur more quickly.

$$LN(x) = \frac{x - \mu}{\delta} \cdot \alpha + \beta \quad (7)$$

In parallel to transformer blocks, convolution block is built up with two convolutions one followed by batch normalize and other is standalone. This is expressed as follow:

$$O_C = conv_{3\times3}\left(BN\left(conv_{3\times3}(x)\right)\right) \quad (8)$$

After the thirds block, we combine the output of the transformer branch, O_T, with the output of convolutional branch, O_C as follow.

$$O_F = concat\ (O_T, O_C) \quad (9)$$

Finally, the model prediction is computed as a probability of each class with the SoftMax operation:

$$p_{o,c} = \frac{e^{o_k}}{\Sigma_j e^{o_j}} \quad (10)$$

The training process use the following categorical loss to update the parameters during the training.

$$loss = -\sum_{c=1}^{M} y_{o,c} \log(p_{o,c}) \quad (11)$$

4.2. Privacy-preserved Learning

Federated learning (FL) is a distributed machine learning paradigm that enables training of models on decentralized data sources without requiring data to be collected in a central location. In this paradigm, the models are trained on data that is distributed across multiple edge devices or nodes in a network, and the updates to the model are communicated between these nodes. The primary goal of FL is to improve privacy by allowing individual devices to retain their data and only share updates with the central model. This approach has become increasingly popular in applications such as mobile devices, where privacy concerns make it difficult to collect large amounts of data centrally. To this end, the LCT model is trained using improve federated training mechanism, described as follow.

Personalized FEDAVG (PFEDAVG) mechanism is presented as an extension to the FEDAVG algorithm [19] to allows for personalization of LCT network for edge devices during the distributed training. In the FEDAVG mechanism, each device is assigned a personalized the local LCT network that is trained using its own network traffic data. The personalized models are then aggregated to obtain the final model. The FEDAVG mechanism can be described mathematically as follows:

Assume that there are a set of N edge devices (known as clients) denoted by $C = \{C_1, C_2, \ldots, C_N\}$, where each edge device has its own IoT traffic data, D_i. Our objective is to train a personalized LCT network for each edge device making use of these distributed data in a privacy-preserving manner. Given W_i denote the parameters of LCT network for device C_i that need to be optimized to perfectly identify security attacks, without leaking the privacy of local data. Let $f(W_i, D_i)$ be the loss function representing the discrepancy between the predictions of the model and the original class labels, where D_i denote the local data on which the loss function is computed.

The FEDAVG mechanism is designed to achieve privacy-preserved training of LCT network according to the following steps:

1. Initialization: The central server initializes the personalized machine learning models $W = \{W_1, W_2, \ldots, W_N\}$ for all devices.

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

2. Client selection: A subset of devices (clients) is selected randomly from C to participate in the training process.
3. Local training: Each selected client C_i trains its personalized model W_i locally using its own dataset D_i. The local training involves computing the gradient of the loss function with respect to the model parameters. The gradient is denoted by $g_i = \nabla f(W_i, D_i)$.
4. Noise injection: Each selected client C_i adds noise to its local LCT network update to ensure differential privacy. The noise is generated from a Gaussian distribution with mean zero and variance σ^2, where σ is the privacy parameter. The noisy model update is denoted by g_i'.
5. Model update: Each selected client C_i upload its noisy version of local update g_i' to the central server for aggregation.
6. Personalization: The central server updates the personalized LCT network for each device C_i using the local updates from the selected clients. The updated personalized LCT network is computed as follows: $W_i' = W_i - \alpha \sum \frac{g_i'}{|S|}$, where S is the set of selected clients and α is the learning rate.
7. Aggregation: The central server aggregates the personalized LCT networks from all devices by computing the average model. The average model is computed as follows: $W' = \left(\frac{1}{N}\right) \sum W_i'$.
8. Global update: The central server updates the global LCT network W using the average model $W' = W + \beta(W' - W)$, where β is a weight decay parameter.
9. Repeat: Steps 2-8 are repeated for multiple rounds until convergence.

5. Results and Discussion

This section argues the experimental design of this work and the empirical findings obtained from each experiment.

5.1. Experimental setup

This subsection argues the specifications of the experiments conducted to evaluate and analyze the performance of the proposed model for intelligent IoT. This includes the materials, evaluation indicators, implementation, etc.

Materials: To experiment with proposed model, NSL-KDD [20] dataset is used for training and evaluation. The dataset contains three files one for training (**KDDTrain+**) and two for testing. Each consist of a total of 43 features. The data contain number of classes of traffics belonging to five main families namely Denial of service (DoS), Normal, Probe, Remote to User (U2R) Attacks, and Root to Local attacks (R2L) attacks. Table 1 summarize the class distribution of different sets of NSL-KDD data.

Table 1: Summary of class distribution in training and testing sets of NSL-KDD data.

Class label		Normal	Dos	Probing	R2L	U2R	Total
Training Set	**#Samples**	60,659	41,323	10,461	884	40	113,375
	Percentage (%)	53.5	36.45	9.23	0.78	0.04	100
Test Set	**#Samples**	6684	4604	1195	111	12	12,598
	Percentage (%)	53.05	36.55	9.49	0.88	0.03	100

Training: The training of the proposed model is conducted on a Lenovo workstation equipped with 64 GB memory, and CPU Intel® Core™ i9-12900K. Nvidia GeForce RTX 2080 is used for accelerating the training process. The model building and training are coded in TensorFlow 2.8. The training process uses the AdamW for parameter optimization over 60 epochs, with 0.001 as the initial learning rate, and a batch size of 1024. The number of communication rounds is set to 25 in our system.

Evaluation: For evaluating the performance of the proposed models, four common classification metrics are used in this work, which can be defined as follows:

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (12)$$

$$Precision = \frac{TP}{TP + FP} \quad (13)$$

$$Recall = \frac{TP}{TP + FN} \quad (14)$$

$$F1 - measure = 2 * \frac{Recall \times Precision}{Recall + Precision} \quad (15)$$

5.2. Experimental Results

This section argues the experimental results obtained from simulation experiments of the proposed model. Table 2 report the class level performance of the proposed FL framework against and centralized training. The numerical results show that LCT network can achieve precise detection of cyber-attacks under central training scenario, with 99% accuracy and 99% f1-score. More interestingly, the proposed FL approach can achieve high detection performance while maintaining the privacy of data at the edge devices. This, in turn reflect the importance of our personalization mechanism in reducing the privacy-accuracy trade-offs.

Table 2: Comparison of results of proposed method on the test set.

	Centralized			Proposed		
Methods	Precision	Recall	F1-score	Precision	Recall	F1-score
Normal	99.36	99.15	99.25	97.66	97.85	97.75
Dos	99.26	98.91	99.09	97.74	96.94	97.34
Probing	95.75	98.08	96.90	88.90	90.46	89.67
R2L	99.10	99.10	99.10	93.86	96.40	95.11
U2R	92.31	100.00	96.00	92.31	100.00	96.00

To further understand performance of the proposed model, Figure 3 displayed confusion matrix of the proposed model for test set. it worth noting that the proposed FL approach can identify different attacks with high precision. To ensure the training stability, we provide the training and loss curves of local LCT in Figure 4. To further identify the discriminative power of the proposed FL model, we compare its performance against FEDAVG baseline in Figure 5. It is notable that our FL model can achieve higher performance over FEDAVG with lesser performance drop from the centralized scenario.

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

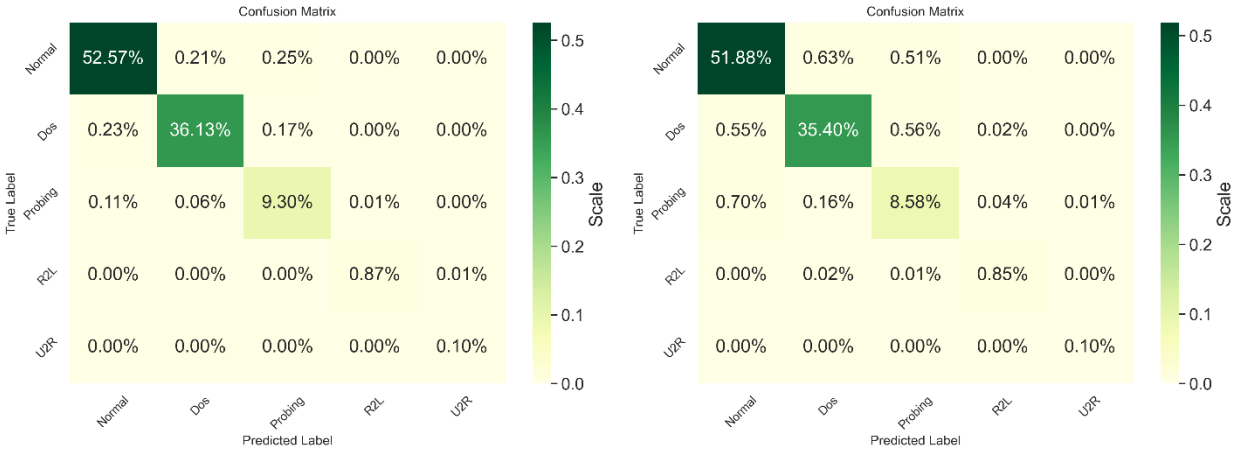

Figure 3: confusion matrix plot for the proposed model under centralized (left) and federated setting (right)

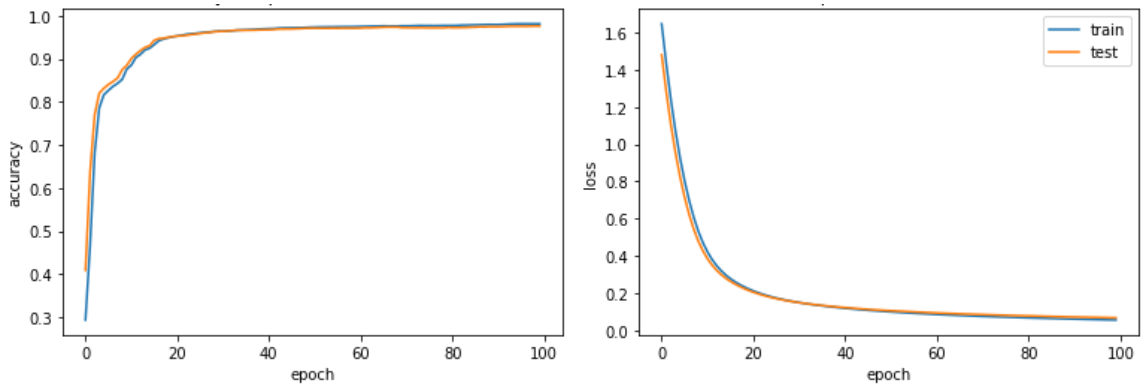

Figure 4 illustration of the accuracy and loss curves of the training of the LCT network.

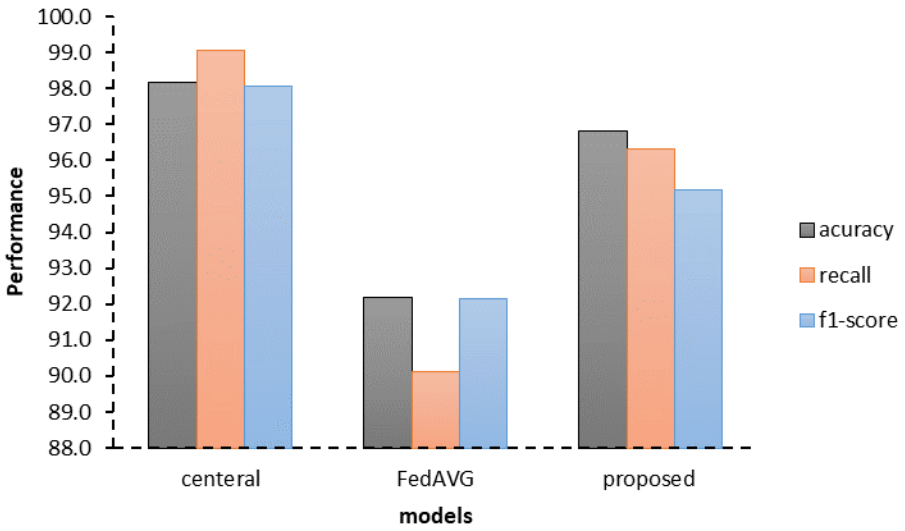

Figure 5: comparison of the performance of the proposed FL model against FEDAVG

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

6. Conclusion

This work presents a novel edge-based federated learning framework for precise detection of security attacks in a privacy-preserved manner. It introduces a lightweight convolutional Transformer (LCT) Network for detecting type of attacks exist in IoT traffics on local edge network. An intelligent privacy-preserved FL is introduced to train personalized LCT network under cooperation among edge devices. Experimental evaluation demonstrated that proposed system can effectively detect IoT security attack with high accuracy, and also without leaking the privacy of data at edge devices. Future work will extend the proposed solution to run under distributed blockchain orchestration aiming to achieve high-level of trust in edge based IoT.

References

[1] Mona Mohamed, A comparative study on Internet of Things (IoT): Frameworks, Tools, Applications and Future directions, Journal of Intelligent Systems and Internet of Things, Vol. 1, No. 1, 13-39, 2020

[2] Q. Luo, S. Hu, C. Li, G. Li, and W. Shi, "Resource Scheduling in Edge Computing: A Survey," *IEEE Commun. Surv. Tutorials*, 2021, doi: 10.1109/COMST.2021.3106401.

[3] Ahmed Abdelmonem , Shimaa S. Mohamed, Internet of Things risks, benefits, challenges in industrial application: Survey, American Journal of Business and Operations Research, Vol. 8, No. 1, 47-59, 2022, doi : https://doi.org/10.54216/AJBOR.080105)

[4] X. X. X. Wang *et al.*, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Commun. Surv. Tutorials*, 2020.

[5] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," *IEEE Communications Surveys and Tutorials*. 2021, doi: 10.1109/COMST.2021.3062546.

[6] S. Singh, R. Sulthana, T. Shewale, V. Chamola, A. Benslimane, and B. Sikdar, "Machine-Learning-Assisted Security and Privacy Provisioning for Edge Computing: A Survey," *IEEE Internet Things J.*, 2022, doi: 10.1109/JIOT.2021.3098051.

[7] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digit. Commun. Networks*, 2020, doi: 10.1016/j.dcan.2019.08.006.

[8] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Appl. Sci.*, 2020, doi: 10.3390/APP10124102.

[9] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things," *IEEE Internet of Things Journal*. 2021, doi: 10.1109/JIOT.2020.3015432.

[10] L. Nie *et al.*, "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," *IEEE Trans. Comput. Soc. Syst.*, 2022, doi: 10.1109/TCSS.2021.3063538.

[11] I. Idrissi, M. Azizi, and O. Moussaoui, "A Lightweight Optimized Deep Learning-based Host-Intrusion Detection System Deployed on the Edge for IoT," *Int. J. Comput. Digit. Syst.*, 2022, doi: 10.12785/ijcds/110117.

[12] Mohammad Hammoudeh , Saeed M. Aljaberi, Modeling of Deep Learning based Intrusion Detection System in Internet of Things Environment, Journal of Cybersecurity and Information Management, Vol. 8, No. 1, 17-25, 2021 doi : https://doi.org/10.54216/JCIM.080102.

[13] S. Nayak, N. Ahmed, and S. Misra, "Deep Learning-Based Reliable Routing Attack Detection Mechanism for Industrial Internet of Things," *Ad Hoc Networks*, 2021, doi: 10.1016/j.adhoc.2021.102661.

[14] T. T. Huong *et al.*, "LocKedge: Low-Complexity Cyberattack Detection in IoT Edge Computing," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3058528.

[15] T. R. Gadekallu *et al.*, "Blockchain for Edge of Things: Applications, Opportunities, and Challenges," *IEEE Internet Things J.*, 2022, doi: 10.1109/JIOT.2021.3119639.

[16] Navod Neranjan Thilakarathne , Rohan Samarasinghe , Mohan Krishna Kagita , Surekha Lanka , Hussain Ahmad, Smart Grid: A Survey of Architectural Elements, Machine Learning and Deep Learning Applications and Future Directions, Journal of Intelligent Systems and Internet of Things, Vol. 3, No. 1, 32-42, 2021 doi : https://doi.org/10.54216/JISIoT.030103

[17] P. Kumar, R. Kumar, G. P. Gupta, and R. Tripathi, "BDEdge: Blockchain and Deep-Learning for Secure Edge-Envisioned Green CAVs," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 3, pp. 1330–1339, Sep. 2022, doi: 10.1109/TGCN.2022.3165692.

[18] M. Abdel-Basset, N. Moustafa, and H. Hawash, "Privacy-Preserved Cyberattack Detection in Industrial

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023

Edge of Things (IEoT): A Blockchain-Orchestrated Federated Learning Approach," *IEEE Trans. Ind. Informatics*, vol. 18, no. 11, pp. 7920–7934, Nov. 2022, doi: 10.1109/TII.2022.3167663.

[19] Y. Ye, S. Li, F. Liu, Y. Tang, and W. Hu, "EdgeFed: Optimized Federated Learning Based on Edge Computing," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3038287.

[20] L. Dhanabal and S. P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms," *Int. J. Adv. Res. Comput. Commun. Eng.*, 2015.

DOI: https://doi.org/10.54216/JISIoT.080105
Received: December 22, 2022 Accepted: January 18, 2023