Journal of Intelligent Systems and Internet of Things
Vol. 12, No. 02, PP. 89-98, 2024
DOI: https://doi.org/10.54216/JISIoT.120207

An IoT Device-Level Vulnerability Control Model Through Federated Detection

Umar Audi Isma'ila[1, 4, *], Kamaluddeen Usman Danyaro [1, 4], Mohd Fadzil Hassan[1, 4], Aminu Aminu Muazu[1, 2], M. S. Liew[3]

[1] Computer and Information Sciences Department, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak, Malaysia
[2] Computer Sciences Department, Faculty of Natural and Applied Science, Umaru Musa Yar'adua University Katsina, Nigeria
[3] Civil and Environmental Engineering, Faculty of Engineering, Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak, Malaysia
[4] Centre for Research in Data Science (CeRDaS), Computer Information Science Department, Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak, Malaysia
Emails: umar_22005104@utp.edu.my; kamaluddeen.usman@utp.edu.my, mfadzil_hassan@utp.edu.my; aminu.aminu@umyu.edu.ng; shahir_liew@utp.edu.my
* Correspondence: umar_22005104@utp.edu.my

Abstract

In the rapidly expanding Internet of Things (IoT) landscape, the security of IoT devices is a major concern. The challenge lies in the lack of intrusion detection systems (IDS) models for these devices. This is due to resource limitations, resulting in, single point of failure, delayed threat detection and privacy issues when centralizing IDS processing. To address this, a LiteDLVC model is proposed in this paper, employing a multi-layer perceptron (MLP) in a federated learning (FL) approach to minimize the vulnerabilities in IoT system. This model manages smaller datasets from individual devices, reducing processing time and optimizing computing resources. Importantly, in the event of an attack, the LiteDLVC model targets only the compromised device, protecting the FL aggregator and other IoT devices. The model's evaluation using the BoT-IoT dataset on TensorFlow Federated (TFF) demonstrates higher accuracy and better performance with full features subset of 99.99% accuracy on test set and achieved average of 1.11sec in detecting bot attacks through federated detection. While on 10-best subset achieved 99.99 on test with 1.14sec as average detection time. Notably, this highlights that LiteDLVC model can potential secure IoT device from device level very efficiently. To improve the global model convergence, we are currently exploring the use genetic algorithm. This could lead to better performance on diverse IoT data distributions, and increased overall efficiency in FL scenes with non-IID data.

Received: August 18, 2023 Revised: November 21, 2023 Accepted: April: 17, 2024

Keywords: IoT device-level vulnerability; Federated detection; Intrusion detection model; Bot-IoT dataset evaluation

1. Introduction

IoT (Internet of Things) devices have become an integral part of our connected world, revolutionizing the way we interact with technology and the environment. These devices come in various forms, ranging from simple sensors such of temperature and humidity sensors to complex devices like smart thermostats, wearables, and industrial machinery [1, 2] as illustrated in Figure 1. However, the rapid proliferation of IoT devices has introduced significant security challenges. As the number of IoT devices continues to grow, so does the potential attack surface for malicious actors seeking to compromise these devices [3]. Frequently, IoT devices are expected to increase to 25.1 billion by 2025 from their current number [4]. According to Jaidka et al [4] the majority of businesses and individuals nowadays seek to collaborate with IoT development firms, in order to integrate IoT into their activities. For instance, in smart electricity, IoT sensors that were placed at various points in the power grid are continuously collecting data on voltage, current, line losses, and other parameters [5]. In contemporary healthcare systems, IoT-enabled infusion pumps can adjust medication dosage based on real-time patient data [6]. In the coming years, the sixth generation (6G) wireless communication technology is expected to greatly enhance the implementation of various emerging IoT applications [7]. However, this growing interconnectivity and widespread adoption of IoT devices make the intelligent processes of IoT susceptible to cyber-attacks. Meanwhile, botnets have had a deep impact on the security of IoT devices by dramatically increasing the attack vulnerability scene [8]. One of the most alarming consequences of IoT botnets is the capacity for launching massive DDoS attacks [3]. By enlisting thousands or even millions of compromised IoT devices, attackers can overload and paralyze targeted devices, initiating severe disruptions.

Meanwhile, Machine learning (ML) have become an effective intelligent tool for defending networks from intrusions. Intrusion detection systems (IDS) which aim to protect and preserve networks from cyber threats [9]. Though IDS model employed for securing IoT devices often face significant challenges due to centralizing the model on single cloud server that includes lengthy detection of threats and single point of failure [10]. Additionally, centralizing the processing of IDS model on a single server raises privacy concerns [11]. This makes it challenging to deploy AIDS model directly on these devices. Addressing these constraints is crucial for enhancing the security of IoT devices. Therefore, in this paper, we propose LiteDLVC (Lite Device-Level Vulnerability Control) model.

Figure 1: IoT Devices over Internet

The LiteDLVC model leverages a multi-layer perceptron (MLP) within the framework of FL[12]. Thus, FL enables multiple distributed devices to collaboratively create a robust ML model for detecting botnet attacks in IoT. Typically, clients involved in the process ask for and obtain the global model parameters from a centralized cloud server. Each of these clients then trains a local ML model using its private network traffic data, utilizing the global model parameters. The resulting model updates are then transmitted back to the central cloud server for aggregation. The FL approach necessitates reduced latency, power, and memory requirements as there is no necessity to transmit network data to a central cloud server [13].

One of the distinctive features of our LiteDLVC model is its adept management of smaller datasets from individual IoT devices. This approach results in a substantial reduction in processing time, which, in turn, leads to a more

efficient utilization of computing resources. The use of the MLP within the LiteDLVC model plays a pivotal role in achieving efficiency. MLP allows for intricate data processing and pattern recognition, improving the model's ability to make informed decisions on data from individual devices [14]. Furthermore, in the unfortunate event of a security breach or attack, our model's intelligence comes to the forefront. It selectively targets and isolates only the compromised device, ensuring that the rest of the IoT ecosystem remains attack-less. This focused response not only boosts security but also minimizes disruption to the FL aggregator and other interconnected devices, thus reducing the single point of failure of the IoT system. Through the propose LiteDLVC model, we aim to significantly improve the privacy and security of IoT devices while concurrently enhancing the operational efficiency of IoT devices. The subsequent sections of this paper will provide, an exploration of our model, its architectural design, experimental results, and the broader implications of our model in the context of IoT device security.

1.1 Related Works

Although Zhuotao L. et.al. [15] Presented a decentralized FL approach for anomaly detection using Convolutional Neural Networks (CNN) sets the stage for innovative decentralized solutions in IoT security. Secondly, Osama S. et al. [16] Explores on network attack detection through FL with Logistic Regression (LR) that yields a robust 94% accuracy, while emphasizing the need for continued research to fully harness FL's potential. Another work of Mohamed et al. [17] Which focus on efficient and lightweight CNNs for IoT malware detection with a transparency-driven approach is a notable contribution. Additional work of Sánchez S. et al. [18] Achieved a remarkable 99.79% accuracy in malware detection and plans to evaluate adversarial attacks in unsupervised scenarios showcasing the robustness of FL in countering threats. Aliya et al [19] introduces privacy-preserving intrusion detection, recognizing the critical role of privacy in FL for IoT security. Also Jingyi et al [20] advances multi-class classification of DDoS attacks, which an essential aspect of IoT device security by utilizing LSTM algorithm. R. Zhao [21] achieves an impressive 99.21% accuracy in IDS and on LSTM algorithm. Lastly, Pedro R. et al [22] work emphasizes personalized FL approaches for privacy-preserving intrusion detection in the industrial IoT sector, underscoring the need for tailored solutions. Table 1 analyzed these existing works. These works collectively showcase FL's potential for achieving high accuracy in IoT security, underlining ongoing research directions and the vital importance of minimizing vulnerabilities and privacy considerations. However, none of these work consider the average time efficiency for detection while they consider the classification performance. Additionally, the evaluation dataset on the existing works lacks diversity to IoT network traces. Hence, in this paper, we propose LiteDLVC model, which represents a significant step forward in the realm of IoT security.

Table 1: Analysis of Related Works for Iot through Federated Detection

Authors	Dataset	Modelling Algorithm	Accuracy
Zhuotao L., 2022 [15]	IoT23	CNN	84.63
Osama S., 2021 [16]	NSL-KDD	LR	94
Mohamed A., 2022 [17]	Virus-MNIST	CNN	91.33
Sánchez S., 2022 [18]	N-BaIoT	MLP	99.79
Aliya T., 2021 [19]	UNSW-NB15	DNN	98
Jingyi L., 2021 [20]	CICDDoS2019	LSTM	97
R. Zhao., 2022 [21]	SEA	LSTM	99.21
Pedro R., 2023 [22]	ToN_IoT	LR	>80

2. Methods and Materials

This section presents the propose LiteDLVC model, details on evaluation dataset, as well as data preprocessing task. Additionally, it provides insights into model evaluation metrics.

2.1 Proposed IoT LiteDevice-Level Vulnerability Control (LiteDLVC) Model

The term "LiteDLVC" is created to highlight two key features of our proposed model. Initially, the influence of the proposed architectural design (depicts in Figure 2) and the lightweight nature of the FedAvg algorithm[12]. Besides, the term highlights the model's ability to weight the strengths of FedAvg using MLP in our design while addressing the unique challenge posed by IoT devices of limited computation resources, model training mode and

distributed data, specifically minimizing the computational resources of IoT devices. The provided phases below outlines the steps for developing the LiteDLVC model:

- Phase 1: Setting up a TFF (TensorFlow Federated) environment that represents the LiteDLVC model.
- Phase 2: Defining the LiteDLVC model architecture for simulation. This include defining the MLP classifier architecture. Table 2 provides a comprehensive overview of the MLP architecture in LiteDLVC model. The architecture consists of five layers: an input layer and four dense layers. The input layer has two branches with 13 and 27 nodes independently (for 10-best features subset and full feature subset of Bot-IoT dataset). The subsequent dense layers each have 100 nodes and utilize the ReLU activation function, presenting non-linearity to the model. The final dense layer, with 2 nodes, employs the SoftMax activation function, commonly for binary classes (normal: 0 and attack: 1), to produce probability distributions over the target classes.

Table 2: Configuration Structure of MLP architecture

Keras layer	**Number of nodes**	**Activation**
Input	13 and 27 independently	--
Dense	100	ReLU
Dense	100	ReLU
Dense	100	ReLU
Dense	2	SoftMax

- Phase 3: Constructing the TFF model by defining the federated plan that make up the model. This includes specifying the FedAvg algorithm as our aggregation function using eq. 1, then loss function, epochs, and any other necessary parameter.

$$g_w = {}^{1}/_{k} * \sum_{k}^{k=1} g_k \qquad (1)$$

- Phase 4: Performing the federated training by distributing the data and model across the simulated IoT devices and server. This by use of TFF's federated training process which involves the following sub-phases.
- Sub-phase 4.1: The FL aggregator generates the developed FL plan.
- Sub-phase 4.2: Devices that intend to utilize the model, regardless of their participation in the FL process, download the model from FL aggregator.
- Sub-phase 4.3: These devices keep their local data private and utilize it on their devices to enhance the learned model.
- Sub-phase 4.4: Instead of transmitting sensitive data to FL aggregator, then only the model parameters of the updated LiteDLVC model are shared with the FL aggregator.
- Sub-phase 4.5: Once all the updates are received, the FL aggregator aggregates the weights from the different device models and creates a new global LiteDLVC model.
- Sub-phase 4.6: The server sends the global model parameters back to the devices.
- Sub-phase 4.7: Each device utilizes the global model parameters and further improves them based on the newly generated data. However, from sub-phase 4.4 to sub-phase 4.7 are repeated to enable continuous learning and improvement of the model over time.
- Phase 5: Evaluating the trained model using appropriate metrics and analyze it is result. This may involve measuring accuracy, precision, recall and FAR.

Various IoT architectures have existed [23] based on the functionality needed by relevant disciplines. In our proposed model architecture, we propose having an input layer, edge-classification layer, transport layer, aggregator layer and application layer as depicts in Figure 2. Our contribution lies in edge-Classification Layer which enables rapid attack detection at the source, enhancing efficiency. Secondly, the Aggregation Layer which efficiently manages model weights, fostering secure and collaborative detection across IoT devices.

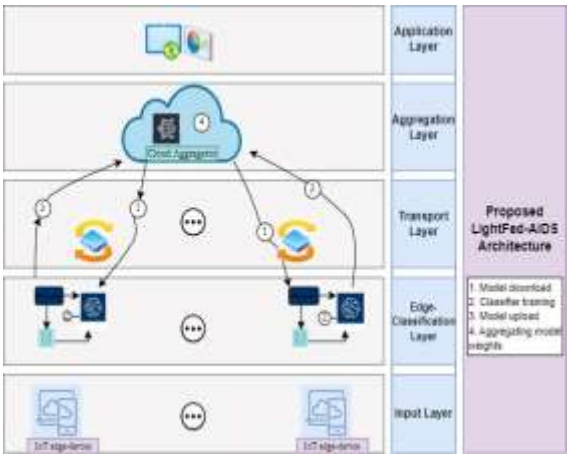

Figure 2: High Level View of Proposed LiteDLVC Architecture

2.2 Benchmark Dataset

In order to evaluate the proposed LiteDLVC model, Bot-IoT dataset [24] were selected among the datasets reviewed in literature. This dataset is large and features diverse for training A-IDS model. With approximately 73 million instances compared to TON_IoT that comprises 22 million instances. It is important to note that each instance is representative of a network session. The features of a session represent an aggregation of all the bytes and packets related to a single communication session between two hosts. Moreover, the dataset comprises IoT network traces, showcasing the unique tasks of securing IoT devices compared to UNSWNB15 with no IoT network traces. It additionally encompasses a wide range of attack diversity, including different types of DoS and DDoS attacks across various transactional protocols. Hence, Bot-IoT dataset serves as a motivating resource to explore and address this research problem of IoT device security. With this overview in mind, and the fact that it remains up recent with limited FL works makes it relevant for this the experiments. Table 3 outlines the description of the dataset, its features, and the preprocessing tasks.

Table 3: Evaluation Dataset

	Bot-IoT Dataset[24]
Description	The Bot-IoT dataset [24] is a publicly available dataset that simulates IoT-based botnet attacks. Moreover, it contains network traffic data generated from a simulated IoT environment that is infected with the Mirai botnet, which is a malware that targets IoT devices. According to [25], the dataset consists of two sets and two subsets that have distinct file format, dimension, and features. Thus, raw set and full set, then 5 percent subset and 10-best subset, respectively. All the subsets are extracted from the full set which contains roughly 73 million counts of instances [25]. Overall, it includes traffic data captured from both the botnet infected devices and the network traffic that the devices generate [24]. It also includes a variety of transactional network protocols, such as HTTP, TCP, and UDP, where each comprises certain attacks count.
Features	The features in this dataset can be categorized into three main groups: dependent, independent standard, and independent calculated. Dependent features include Category, Subcategory, and Attack. Independent standard features consist of attributes such as flgs, proto, state, sport, dport, and others. Independent calculated features involve more complex metrics like TnBP_Src_IP, TnBP_Dst_IP, Pkts_P_State_P_Protocol_P_DestIP, and many more. In addition to these categories, there are a few miscellaneous features like pkSeqID, seq, stime, saddr, and daddr, which are also present within the dataset. These feature groups collectively play a crucial role in IDS model for IoT scene [25].
Preprocessing	It is worth highlighting that the initial four preprocessing steps mainly involve exploratory data analysis (EDA), data cleaning (removing the redundant feature), dataset version selection (i.e. full feature subset or 10-best feature subset) for the classification, and lastly, the split of data from the federated data into training and validation data for each participating device in the experiment. In this phase, we deliberately creating non-IID data for the FL setting because the Bot-IoT dataset was originally intended for centralized ML. We split the dataset such that each device in the experiment has its own independent training and validation sets. To achieve this, we calculated the number of rows in the dataset and divided it by the number of participating IoT devices (2 in this case). Using Python slicing, we then created "Devices_1"

by selecting rows from the beginning of the **full dataframe** up to the calculated split point. "Device_2" contains the remaining rows. This mimics the real-world FL scenario where data distributions differ across individual devices, resulting in non-IID data. These preprocessing steps are performed prior to conducting any experiments in this study.

2.3 Validation Metrics

Confusion matrix is used in this work to determine evaluation metrics such accuracy, precision, recall, and F1 score. Hence, the metrics for amount of True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN) predictions built by the classifier are computed using equations in Table 4.

Table 4: Validation Metrics

Metrics	Formula
Accuracy	$(TP + TN)/(TP + TN + FP + FN)$
Precision (Detection rate)	$TP/(TP + FP)$
Recall	$TP/(TP + FN)$
F1-score	$2 * (Precision * Recall)/Precision + Recall$

3. Result and Discussion

We conducted our experiment using the TensorFlow Federated (TFF) framework within the Google Colab integrated development environment (IDE). The experiments were executed on a system equipped with a Pentium Dual-core CPU, a 32-bit operating system, and 3GB of RAM. In our experiments, we employed two IoT devices as clients, each responsible for training their own MLP classifier locally utilizing binary class (normal: 0 and attack:1). We utilized the FedAvg algorithm [22] for the aggregation of model weights. It is important to note that the clients worked with non-iid datasets of equal size but with differing feature distributions. These datasets did not share the same types of attacks, and the number of samples for each attack varied between them. Lastly, Table 5 provides the training hyperparameters used in LiteDLVC experiment.

Table 5: LiteDLVC Training Hyperparameters

Parameter	Value
Participating Devices	2
Client Optimizer	SGD
Server Optimizer	SGD
Learning rate	0.01
batch size	32
Epochs	100

3.1 LiteDLVC Model Performance

Table 6: Performance Analysis for LiteDLVC Model

Bot-IoT Dataset Version	Full Features		10-Best Features	
Metrics	**Train**	**Test**	**Train**	**Test**
Accuracy	0.9998	0.9999	0.9999	0.9999
Precision	0.9988	0.9999	0.9848	0.9999
Recall	1.0	0.9999	0.9924	0.9999
F1-score	0.9999	0.9999	0.9999	0.9999
AvgTime(sec)	2.81	1.11	2.94	1.14

Table 6 shows the validation metrics assessed in federated scenario, employing FedAvg Algorithm. It's worth noting that participating devices achieve higher accuracy of around 99.99% on test set for both Bot-IoT dataset versions. This distinction can be rationalized by the fact that devices with fewer classes (Target feature) and less balance tend to excel in classifying samples from dominant classes. However, within a federated framework, the weights of these devices with fewer classes can be negatively influenced by the weights of other clients encompassing a wider range of classes, as these parties identify varying and additional types of bot attacks.

Additionally from Table 6, the Accuracy for both training and testing sets exhibit extremely high values, ranging from 0.9998 to 0.9999, indicating a near-perfect classification of instances. In terms of Precision, which measures the accuracy of positive predictions, is also notably high, with values exceeding 0.9988 in most cases. Recall, reflecting the model's ability to capture all relevant instances, shows consistently high performance, especially for the full features set. The F1-score, a harmonic mean of precision and recall, maintains exceptionally high values across all scenarios with 0.9999, suggesting a balanced performance between precision and recall. The AvgTime metric, representing the average time taken for predictions in seconds, is generally low, indicating efficient model inference.

Figure 3 and 4 depict the training accuracy for the global model on the BoT-IoT dataset for LiteDLVC. Notably, for full features subset, the accuracy values show unsteadiness until reaching around 30th epochs, after which they stabilize. While the evolution of accuracy values for 10-best features demonstrate unsteadiness until reaching around the 30th epochs, after which they stabilize. Meanwhile, the confusion matrix for these experiment are illustrated in Figure 5 and Figure 6.

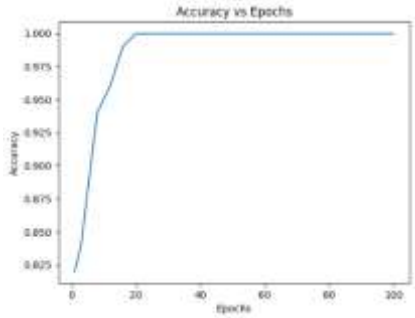

Figure 3: Training accuracy for global model on full features subset

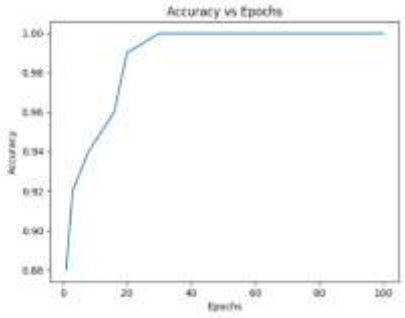

Figure 4: Training accuracy for global model on 10-best features subset

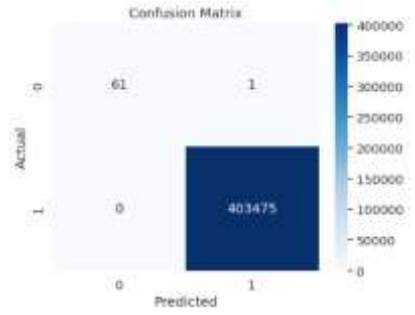

Figure 5: Confusion matrix on full features subset

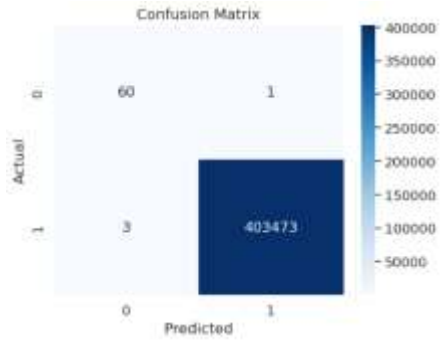

Figure 6: Confusion matrix on 10-best features subset

Figure 7 and 8 depict the average testing accuracy for the participating IoT devices (clients) on the BoT-IoT dataset for LiteDLVC. Remarkably, the accuracy values of 99.99% demonstrate consistency around the 100th epoch, showcasing LiteDLVC model stabilization. It should be noted that these results are quite good; moreover, the full feature subset exhibits more stability than the 10-best features subset since it achieved 1.11sec as average detection time.

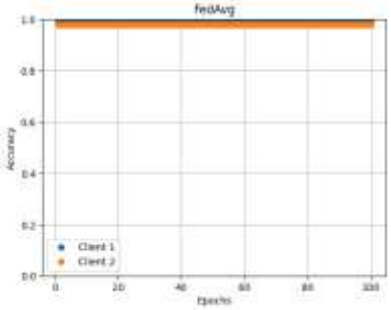

Figure 7: Testing accuracy for each client on full features subset

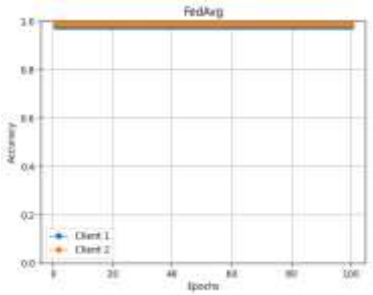

Figure 8: Testing accuracy for each client on 10-best features subset

Table 7: Performance comparison with existing works

Authors	Dataset	Modelling Algorithm	Accuracy	AvgTime
Zhuotao L. 2022 [15]	IoT23	CNN	84.63	--
Mohame A. 2022 [17]	Virus-MNIST	CNN	91.33	--
Sánchez S. 2022 [18]	N-BaIoT	MLP	99.79	--
Jingyi L 2021 [20]	CICDDoS2019	LSTM	97	--
Pedro R 2023 [22]	ToN_IoT	LR	>80	--
LiteDLVC model	Bot-IoT dataset (full subset)	MLP	99.99	1.11

Table 7 shows the comparison of LiteDLVC model with other existing works. Notably, LiteDLVC model applied to the Bot-IoT dataset, achieved an impressive accuracy of 99.99% with average detection time of 1.11sec. Although these related works did not provide the exact AvgTime value they obtained, but it does not undermine their model but highlights the gap of not prioritizing average detection time of their model which very essential in deploying the IDS model.

3.2 Discussion

This study address the specific challenges of securing IoT devices while reducing the single point of failure, delayed threat detection and privacy issues. Additionally, the primary contributions of our architectural framework are twofold. Firstly, the Edge-Classification Layer enables rapid attack detection at the source, enhancing efficiency. Secondly, the Aggregation Layer efficiently manages model weights, fostering secure and collaborative detection across IoT devices. Upon inspecting the results, it becomes evident that the proposed LiteDLVC model through federated detection on Bot-IoT dataset outperforms other methods such of FEDGAN-IDS[19].

Meanwhile, reducing high single point of failure, delayed threat detection and privacy issues in IoT is challenging especially when assessing the classifier performance. Despite the success of our LiteDLVC model on Bot-IoT dataset, it is observed that it requires a deep understanding of the underlying concepts. For Instance, the individual IoT device data for IDS model in FL scenes. Thus, could brought issues like redundant or compromised data in local clients which can lead to model failure, this is significant concerns in real-time IDS scenarios for IoT device in FL, knowingly as non-Independently and Identically Distributed (non-IID data). Therefore, there is highly need to address these challenges of non-IDD data. This can potentially affect the accuracy of attacks detection in the IoT devices, specifically those with limited resources. Aiming at this problem, we are currently working in addressing non-IID data in FL by exploring the use of genetic algorithms.

4. Conclusion

This article introduces LiteDLVC (an IoT device-level vulnerability control) model, a significant step forward in the realm of IoT device security. Our model addresses the centralized IDS problem considering the resource limitations of IoT devices. Our model is structured to incorporate several key elements. Firstly, it aims to achieve a strong bot attack detection rate. Secondly, it prioritizes rapid processing of incoming network traffic. Thirdly, it is proficient at aggregating and updating models from various devices efficiently. Finally, it maintains the privacy of sensitive data from IoT devices during the learning process. Our finding show that the full features of Bot-IoT dataset achieved lesser bot attack detection time of 1.11sec, while 10-best features set achieved 99.99% accuracy. This highlights that LiteDLVC model can potential secure IoT device from device level by efficiently utilizing the IoT devices resources through federated attack detection. In future research, challenges of non-IDD data can potentially affect the accuracy of attacks detection in the IoT devices, specifically those with limited computational resources.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

ACKNOWLEDGMENT: The authors wish to acknowledge the support in part by Universiti Teknologi PETRONAS (UTP) and the Yayasan Universiti Teknologi PETRONAS-Fundamental Research Grant (YUTP-FRG) for the funding of project titled: Fundamental study of supervised machine learning techniques for autonomous defect mapping of offshore structures (cost centre: 015LC0-373).

References

[1] Bansal, S. and D. Kumar, *IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication.* International Journal of Wireless Information Networks, 2020. **27**(3): p. 340-364.
[2] Alhandi, S.A., H. Kamaludin, and N.A.M. Alduais, *Trust Evaluation Model in IoT Environment: A Comprehensive Survey.* IEEE Access, 2023.
[3] Kumari, P. and A.K. Jain, *A comprehensive study of DDoS attacks over IoT network and their countermeasures.* Computers & Security, 2023: p. 103096.
[4] Jaidka, H., N. Sharma, and R. Singh. *Evolution of iot to iiot: Applications & challenges*. in *Proceedings of the international conference on innovative computing & communications (ICICC)*. 2020.
[5] Alduais, N.A.M., J. Abdullah, and A. Jamil, *RDCM: An efficient real-time data collection model for IoT/WSN edge with multivariate sensors.* IEEE Access, 2019. **7**: p. 89063-89082.
[6] Farivar, F., et al., *Application of fuzzy learning in IoT-enabled remote healthcare monitoring and control of anesthetic depth during surgery.* Information Sciences, 2023. **626**: p. 262-274.
[7] Nguyen, D.C., et al., *6G Internet of Things: A comprehensive survey.* IEEE Internet of Things Journal, 2021. **9**(1): p. 359-383.
[8] Koroniotis, N., N. Moustafa, and E. Sitnikova, *Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions.* IEEE Access, 2019. **7**: p. 61764-61785.
[9] Sarhan, M., S. Layeghy, and M. Portmann, *Evaluating Standard Feature Sets Towards Increased Generalisability and Explainability of ML-based Network Intrusion Detection.* arXiv preprint arXiv:2104.07183, 2021.
[10] Ahmad, R. and I. Alsmadi, *Machine learning approaches to IoT security: A systematic literature review.* Internet of Things, 2021. **14**: p. 100365.
[11] Rahman, S.A., et al., *Internet of things intrusion detection: Centralized, on-device, or federated learning?* IEEE Network, 2020. **34**(6): p. 310-317.
[12] McMahan, B., et al. *Communication-efficient learning of deep networks from decentralized data*. in *Artificial intelligence and statistics*. 2017. PMLR.
[13] Nguyen, D.C., et al., *Federated Learning for Internet of Things: A Comprehensive Survey.* IEEE Communications Surveys & Tutorials, 2021. **23**(3): p. 1622-1658.
[14] Cook, A.A., G. Mısırlı, and Z. Fan, *Anomaly detection for IoT time-series data: A survey.* IEEE Internet of Things Journal, 2019. **7**(7): p. 6481-6494.
[15] Lian, Z. and C. Su. *Decentralized Federated Learning for Internet of Things Anomaly Detection*. in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*. 2022.
[16] Shahid, O., et al. *Detecting Network Attacks using Federated Learning for IoT Devices*. in *2021 IEEE 29th International Conference on Network Protocols (ICNP)*. 2021. IEEE.
[17] Abdelbasset, M., et al., *Efficient and Lightweight Convolutional Networks for IoT Malware Detection: A Federated Learning Approach.* IEEE Internet of Things Journal, 2022.
[18] Rey, V., et al., *Federated learning for malware detection in iot devices.* Computer Networks, 2022. **204**: p. 108693.
[19] Tabassum, A., et al., *Fedgan-ids: Privacy-preserving ids using gan and federated learning.* Computer Communications, 2022. **192**: p. 299-310.
[20] Li, J., et al. *FIDS: Detecting DDoS Through Federated Learning Based Method*. in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 2021. IEEE.
[21] Zhao, R., et al., *Intelligent intrusion detection based on federated learning aided long short-term memory.* Physical Communication, 2020. **42**: p. 101157.
[22] Ruzafa-Alcazar, P., et al., *Intrusion Detection based on Privacy-preserving Federated Learning for the Industrial IoT.* IEEE Transactions on Industrial Informatics, 2021.
[23] Man, D., et al., *Intelligent intrusion detection based on federated learning for edge-assisted Internet of Things.* Security and Communication Networks, 2021. **2021**.
[24] Koroniotis, N., et al., *Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset.* Future Generation Computer Systems, 2019. **100**: p. 779-796.
[25] Peterson, J.M., J.L. Leevy, and T.M. Khoshgoftaar. *A review and analysis of the bot-iot dataset.* in *2021 IEEE International Conference on Service-Oriented System Engineering (SOSE)*. 2021. IEEE.