Protecting IoT Devices from BotNet Threats: A Federated Machine Learning Solution

Ahmed A. Metwaly[1] (ID), and **Ibrahim Elhenawy[2, *]** (ID)

[1,2]Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah 44519, Egypt;

a.metwaly23@fci.zu.edu.eg; ielhenawy@zu.edu.eg.

* Correspondence: ielhenawy@zu.edu.eg.

Abstract: The proliferation of Internet of Things (IoT) devices has brought unprecedented convenience to our lives, but it has also opened the door to new security challenges. One of the most pressing threats in the IoT landscape is the proliferation of BotNets, which can compromise and control a multitude of devices for malicious purposes. In this paper, we propose a novel approach to address this issue: a Federated Machine Learning Solution for BotNet detection in IoT environments. Our method leverages the collective intelligence of distributed IoT devices while respecting privacy constraints, ensuring that sensitive data never leaves the device. We present a detailed methodology for federated model construction, including data collection, local model training, and secure aggregation. The resulting federated model offers improved accuracy and robustness in BotNet detection, as demonstrated through rigorous evaluation on the N-BaIoT dataset. Our findings underscore the effectiveness of this approach in enhancing IoT device security by detecting and mitigating BotNet threats while safeguarding data privacy. This paper contributes to the advancement of IoT security strategies and provides a framework for protecting IoT devices against evolving threats in a federated and privacy-preserving manner.

1. Introduction

The proliferation of the Internet of Things (IoT) has ushered in an era of unprecedented connectivity and data exchange. IoT devices are seamlessly integrated into our daily lives, spanning from smart homes and healthcare systems to industrial automation and transportation. While this interconnectedness offers remarkable opportunities for efficiency, productivity, and convenience, it also opens the door to significant security and privacy challenges [1]. Cyberattacks on IoT systems are on the rise, posing substantial threats to the integrity, availability, and confidentiality of sensitive data and critical infrastructure. Traditional intrusion detection mechanisms are often ill-suited to the unique characteristics of IoT environments, characterized by a diverse array of devices, varying levels of computational capacity, and a distributed network architecture [3].

Ensuring the security of IoT systems is paramount for safeguarding the privacy of users and the continuous functionality of these interconnected devices. The consequences

of security breaches in IoT can extend from data breaches and privacy violations to physical harm, financial losses, and disruption of critical services [4]. Traditional intrusion detection systems, which typically centralize data and analysis, are challenged by the vast and diverse nature of IoT networks. The sheer volume of data generated by IoT devices, coupled with the need for real-time threat detection, necessitates innovative approaches that can scale effectively and adapt to the dynamic IoT environment [5].

Federated Machine Intelligence offers a compelling solution to these IoT security challenges. By distributing the machine learning model training process across IoT devices, it preserves data privacy by keeping sensitive information localized, reducing the risk of data leaks and privacy violations. Moreover, it empowers IoT devices to collaborate in the learning process, resulting in a collective intelligence that can adapt to evolving threats [6]. In this paper, this paper presents a pioneering approach - Federated Machine Intelligence - designed to address the pressing need for robust security and privacy protection in IoT ecosystems. This novel approach harnesses the power of federated learning, an emerging paradigm in machine learning, to create a collaborative, distributed, and privacy-preserving solution for detecting intrusions in IoT networks. We explore how this approach enhances both the security and privacy of IoT ecosystems while maintaining the required level of accuracy and responsiveness for effective threat mitigation [7].

The remainder of this paper is organized as follows: Section 2 provides an overview of related work in the field of IoT security and federated learning. Section 3 details the methodolodgy of the proposed system and its adaptation to IoT intrusion detection. In Section 4, we present our experimental setup and evaluation results, demonstrating the efficacy of the proposed approach. Finally, Section 5 summarizes our findings, highlights contributions, and outlines future directions for research in this critical domain.

2. Related Works

This section presents a comprehensive review of the existing body of knowledge in the domains of IoT security and federated learning, both of which form the cornerstone of our proposed approach. In the realm of IoT security and federated learning, numerous pioneering studies have made substantial contributions to the field. Agrawal et al. [17] introduced the concept of temporal weighted averaging in asynchronous federated intrusion detection systems, addressing the challenges of real-time threat detection. Fan et al. [18] presented "IoTDefender," a federated transfer learning intrusion detection framework tailored for 5G IoT networks, demonstrating the potential of cross-domain knowledge transfer. Siniosoglou et al. [19] explored adversarial approaches to federated intrusion detection in NG-IoT healthcare systems, emphasizing the need for robust security in critical domains. Ferrag et al. [20] conducted an extensive investigation into federated deep learning for IoT cybersecurity, shedding light on its concepts, applications, and experimental

results. Afaq et al. [21] focused on the broader spectrum of 5G security, encompassing machine learning techniques, architectural considerations, and emerging challenges. Chen et al. [22] proposed an intrusion detection system for wireless edge networks grounded in federated learning, showcasing the potential of decentralized intelligence. Meanwhile, Chathoth et al. [23] tackled the intricacies of federated intrusion detection in IoT, addressing privacy concerns within a heterogeneous cohort. Alazab et al. [24] provided a comprehensive overview of federated learning for cybersecurity, outlining its fundamental concepts, challenges, and future research directions. Trakadas et al. [25] ventured into AI-based collaboration approaches in industrial IoT manufacturing, highlighting the relevance of federated techniques in complex environments. Nguyen et al. [26] introduced DÏoT, a federated self-learning anomaly detection system for IoT, emphasizing the importance of adaptability in dynamic IoT landscapes. Bertoli et al. [27] developed an end-to-end framework for machine learning-based network intrusion detection, enhancing the holistic understanding of intrusion detection in network environments. Zhang et al. [28] explored federated learning for the Internet of Things, revealing its potential to revolutionize data-driven decision-making in IoT applications. Aïvodji et al. [29] proposed a secured and privacy-preserving smart home architecture implementing federated learning, providing insights into safeguarding IoT ecosystems at the edge.

3. Methodology

In this section, we unveil the intricate layers of our approach, elucidating the underlying principles, architectural intricacies, and workflow intricacies that empower our system. Building upon the foundation laid by prior studies in federated learning and cybersecurity, we present a comprehensive framework meticulously designed to ensure the security and privacy of IoT ecosystems.

The initial step in building our federated model involves gathering lo T traffic data from multiple distributed sources (clients or loT devices). Let C represent the set of clients, each denoted as $c_i, i = 1,2, \dots, |C|$. The data collected from each client c_i is denoted as D_{c_i}. Prior to model training, data preprocessing is performed to standardize and normalize the features, usually denoted as X and target labels Y, and this can be represented mathematically as:

$$X_{c_i}^{preprocersased} = Standardize\left(X_{c_i}\right), Y_{ci}^{preprocessed} = Normalize\left(Y_{c_i}\right) \tag{1}$$

We utilize a Transformer Network as the base model for intrusion detection. Let $f\left(\theta; X_{c_i}\right)$ represent the Transformer Network, where θ denotes the model parameters, and X_{c_i} is the preprocessed data from client c_i. The architecture typically consists of multiple layers, including input, hidden, and output layers, with activation functions like ReLU (Rectified Linear Unit) for non-linearity.

First, Model initialization is a pivotal step in federated learning where the global model, denoted as θ, is initialized with initial weights θ_0. These initial parameters are then shared with each participating client, c_i, to ensure a common starting point for model training. The objective is to enable clients to collaboratively train the model while preserving data privacy. Mathematically, the model initialization process can be expressed as follows:

The global model parameters, θ_0, are typically initialized with small random values. The choice of initialization method can impact training convergence and performance. Common methods include random initialization and Xavier/Glorot initialization, which adapt the initialization scale to the activation functions used in the neural network.

$\theta_0 \sim$ Random Initialization

After initializing the global model, θ_0, these initial parameters are shared securely with each participating client, c_i. This ensures that all clients start with an identical initial model, thereby fostering collaboration.

$$\theta_0 \rightarrow \theta_{c_i}^{(0)} \qquad\qquad (2)$$

Client-Specific Model Instances: Each client c_i receives the initial model parameters θ_0 and utilizes them as the starting point for local model training. The client-specific model instance is denoted as $\theta_{c_i}^{(0)}$.

$$\theta_0 \rightarrow \theta_{\epsilon_i}^{(0)} \qquad\qquad (3)$$

Second, Local model training is a fundamental step in federated learning, where each client cici performs training on its locally available data, optimizing a loss function specific to its dataset. This step ensures that clients can update the global model parameters (θ) with respect to their unique data distributions while preserving privacy.

Each client c_i aims to minimize a client-specific loss function, $L\left(\theta; X_{ci}, Y_{c_i}^{\text{preprocessed}}\right)$, where X_{c_i} represents the preprocessed input data, and $Y_{c_i}^{\text{preprocessed}}$ represents the corresponding labels. The loss function typically includes a regularization term, such as $L2$ regularization, to prevent overfitting:

$$L\left(\theta; X_{c_i}, Y_{c_i}^{\text{preprocessed}}\right) = \text{Loss}\left(f(\theta, X_{c_i}), Y_{c_i}^{\text{preprocessed}}\right) + \lambda \text{ - Regularization}(\theta) \qquad (4)$$

Here, Loss represents a suitable loss metric, such as cross-entropy loss for classification tasks, and λ controls the strength of regularization.
To optimize the loss function, each client employs an optimization algorithm, often SGD. At each training iteration t, the client computes the gradient of the loss function with respect to the current model parameters $\nabla L\left(\theta_{c_i}^{(t)}; X_{c_i}, Y_{c_i} \text{ preprocensed }\right)$ and updates the model parameters as follows:

$$\theta_{c_i}^{(t+1)} = \theta_{c_i}^{(t)} - \alpha \nabla L \left(\theta_{c_i}^{(t)}; X_{c_i}, Y_{c_i}^{\text{preprocessed}} \right) \tag{5}$$
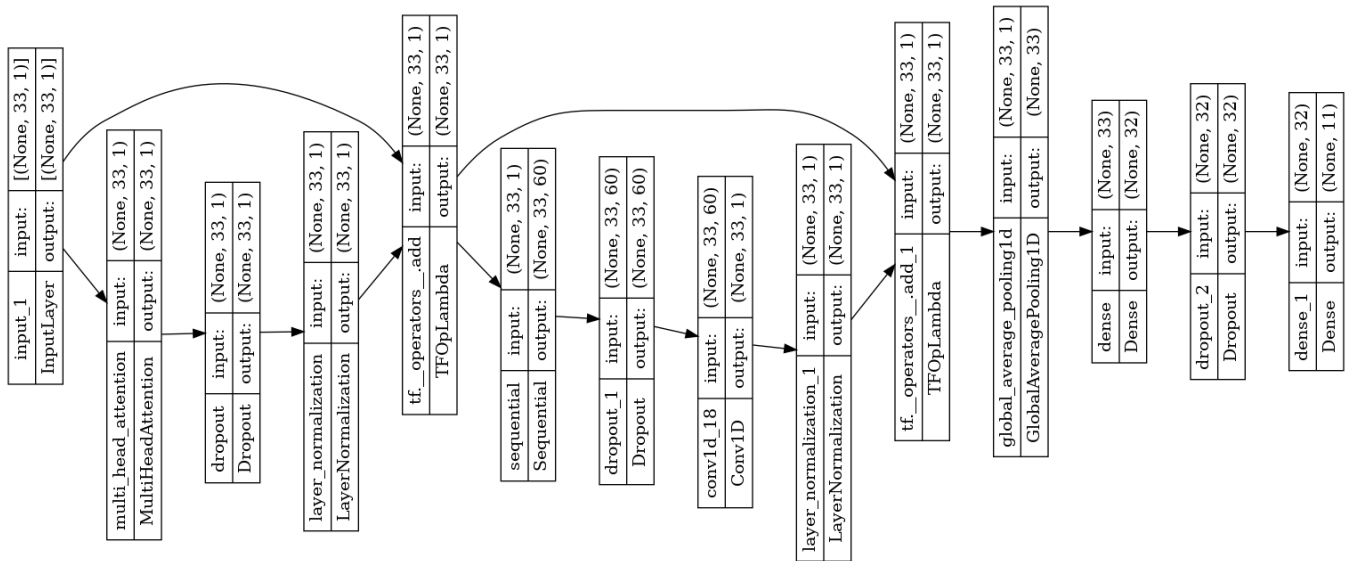

Figure 1. Architecture of the Local Transformer Model for BotNet Detection

Here, α represents the learning rate, a hyperparameter controlling the step size during parameter updates. The training process is iterative, and each client performs a specified number of training iterations to update its local model parameters. These iterations refine the model's knowledge of the local data distribution. Local model training is crucial for preserving data privacy as it ensures that raw data never leaves the client's device. Instead, only model updates (gradients) are shared with the central server during the aggregation step, thus maintaining the confidentiality of client data.

Third, Model aggregation is a pivotal step in federated learning, where the updates to the local models from different clients are combined to create a new global model. This collaborative process ensures that the federated model effectively captures insights from all clients while preserving data privacy. Model aggregation can be performed using various methods, with Federated Averaging being one of the most common. This method calculates the weighted average of the model parameters from all participating clients:

$$\theta^{(t+1)} = \frac{1}{|C|} \sum_{i=1}^{|C|} \theta_{c_i}^{(t+1)} \tag{6}$$

Here, $\theta^{(t+1)}$ represents the new global model, and $|C|$ is the total number of clients. Weighted Aggregation: In some scenarios, clients may have varying levels of data quality or trustworthiness. In such cases, weighted aggregation can be employed, assigning different weights (w_i) to clients based on their reliability:

$$\theta^{(t+1)} = \frac{1}{\sum_{1-1}^{|C|} w_i} \sum_{i=1}^{|C|} w_i + \theta_{c_i}^{(t+1)} \tag{7}$$

The weights w_i can be determined through trust scores or other criteria. After aggregation, the resulting $\theta^{(t+1)}$ becomes the updated global model, which is then shared with all clients for the next round of training. This iterative process continues until convergence is achieved or until a predetermined stopping criterion is met.

## 4. Experimental Setups and Results

In the pursuit of elevating the security and privacy of IoT environments through "Federated Machine Intelligence for IoT Intrusion Detection," the proof of concept lies at the heart of our research journey. This section serves as a crucial juncture where theory meets practice, where the innovative methodologies and algorithms proposed earlier are put to the test in real-world scenarios.

The successful implementation of our experimental framework relied on a carefully orchestrated combination of hardware, software, and specialized machine learning frameworks. The hardware foundation included a cluster of Raspberry Pi 4 Model B devices, each equipped with a quad-core ARM Cortex-A72 processor running at 1.5GHz, 4GB of LPDDR4 RAM, and Gigabit Ethernet connectivity. This Raspberry Pi cluster served as our edge computing infrastructure, simulating a distributed IoT environment. For software, we utilized the Raspbian operating system (based on Debian) to orchestrate device communication and management. To facilitate federated learning and intrusion detection tasks, we leveraged the TensorFlow machine learning frameworks, both renowned for their scalability and compatibility with edge devices. Additionally, Docker containers were employed to streamline the deployment of federated learning models across the Raspberry Pi cluster. This integrated setup provided the necessary computational power, flexibility, and compatibility to execute our experiments effectively, replicating real-world IoT conditions.

In our study, we conducted a comprehensive evaluation of our proposed intrusion detection model using the N-BaIoT (Network-based Behavioral Analysis of Internet of Things) dataset. The N-BaIoT dataset comprises traffic data collected from nine distinct commercial IoT devices, both before and after being compromised by the notorious Mirai and BASHLITE botnets. Each data sample within this dataset is characterized by 23 distinct features, encompassing essential traffic statistics, such as packet count, the sizes of inbound and outbound packets, and inter-arrival times of packets, which are computed over five distinct time windows. This dataset further incorporates a diverse range of attack scenarios, involving ten distinct attack types executed by the Mirai and BASHLITE botnets. For our evaluation, we carefully selected data samples these nine IoT devices, namely the Danmini Doorbell, Ecobee Thermostat, Provision PT-737E, Philips B120N/10 Baby Monitor, and SH XCS7-1002-WHT, Ennio, Provision PT-838, SH XCS7-1003-WHT, and Samsung SNH 1011 N. To ensure rigorous assessment, we partitioned the data samples for each device into three subsets: a training set, a validation set, and a test set, maintaining an 8:1:1 ratio, respectively. Detailed statistics regarding the distribution of samples across sets and categories can be found in Table 1. This dataset selection and partitioning approach provides a robust foundation for evaluating the efficacy of our federated machine intelligence approach in enhancing security and privacy in the context of IoT intrusion detection.

Table 1. Distribution of Data Samples Across Sets and Attack Categories for IoT Devices in the N-BaIoT Dataset

Model of Device	Type of Device	Benign	BASHLITE					Mirai					Total Attacks
			Combo	Junk	Scan	TCP	UDP	Ack	Scan	Syn	UDP	UDPPlain	
Danmini	Doorbell	40395	59718	29068	29849	92141	105874	102195	107685	122573	237665	81982	968750
Ennio	Doorbell	34692	53014	29797	28120	101536	103933	0	0	0	0	0	316400
Ecobee	Thermostat	13111	53012	30312	27494	95021	104791	113285	43192	116807	151481	87368	822763
Philips B120N/10	Baby monitor	160137	58152	28349	27859	92581	105782	91123	103621	118128	217034	80808	923437
Provision PT-737E	Sec. camera	55169	61380	30898	29297	104510	104011	60554	96781	65746	156248	56681	766106
Provision PT-838	Sec. camera	91555	57530	29068	28397	89387	104658	57997	97096	61851	158608	53785	738377
SH XCS7-1002-WHT	Sec. camera	42784	54283	28579	27825	88816	103720	111480	45930	125715	151879	78244	816471
SH XCS7-1003-WHT	Sec. camera	17936	59398	27413	28572	98075	102980	107187	43674	122479	157084	84436	831298
Samsung SNH 1011 N	Webcam	46817	58669	28305	27698	97783	110617	0	0	0	0	0	323072
Total		502596	515156	261789	255111	859850	946366	643821	537979	733299	1E+06	523304	7E+06
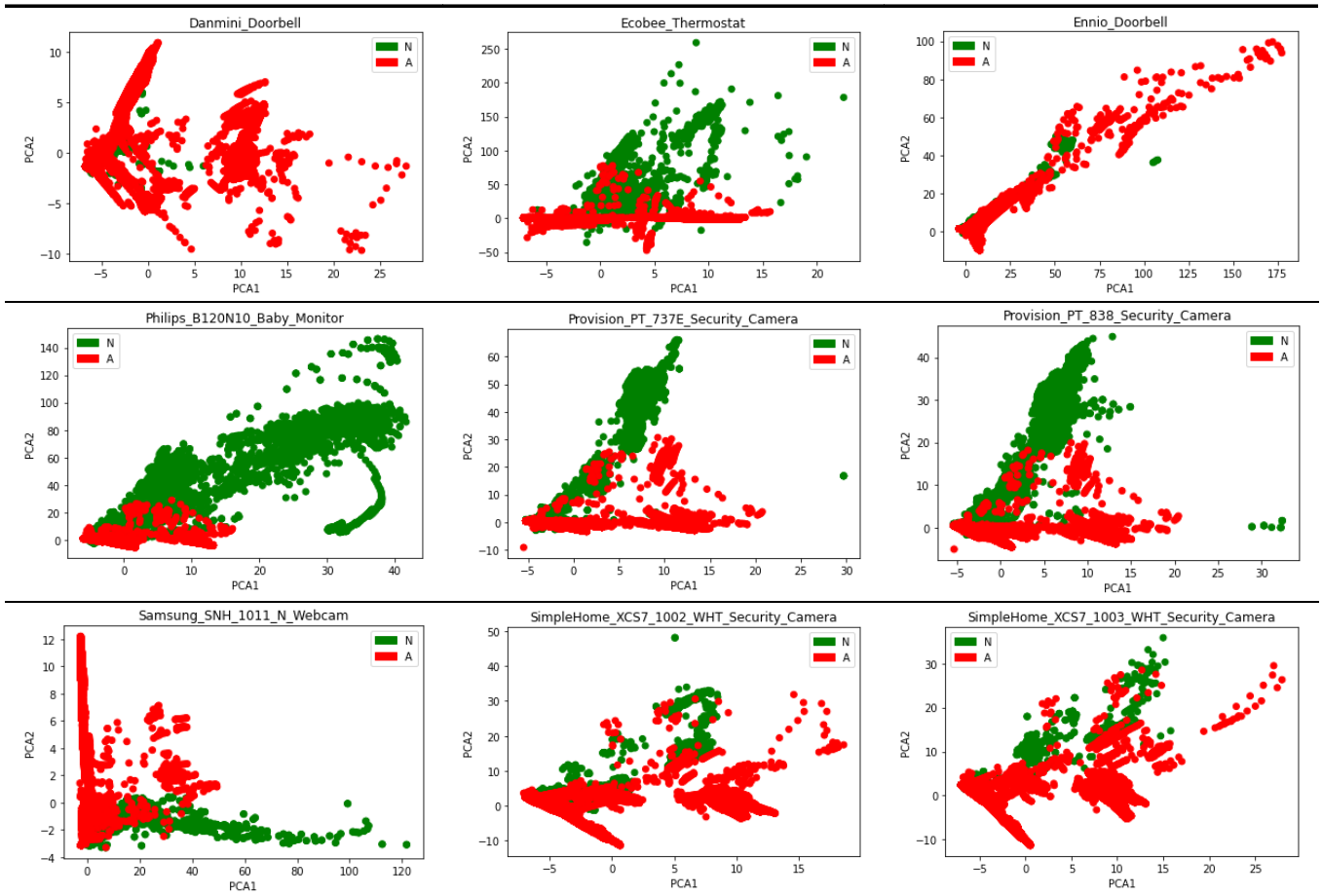
Figure 2. PCA Plots for Selected IoT Devices in the N-BaIoT Dataset

In Figure 2, we present Principal Component Analysis (PCA) plots for each of the selected IoT devices within the N-BaIoT dataset. These PCA plots offer a succinct visual representation of the multidimensional nature of the IoT traffic data and its underlying structure. Each data point in the plot corresponds to an individual data sample from the
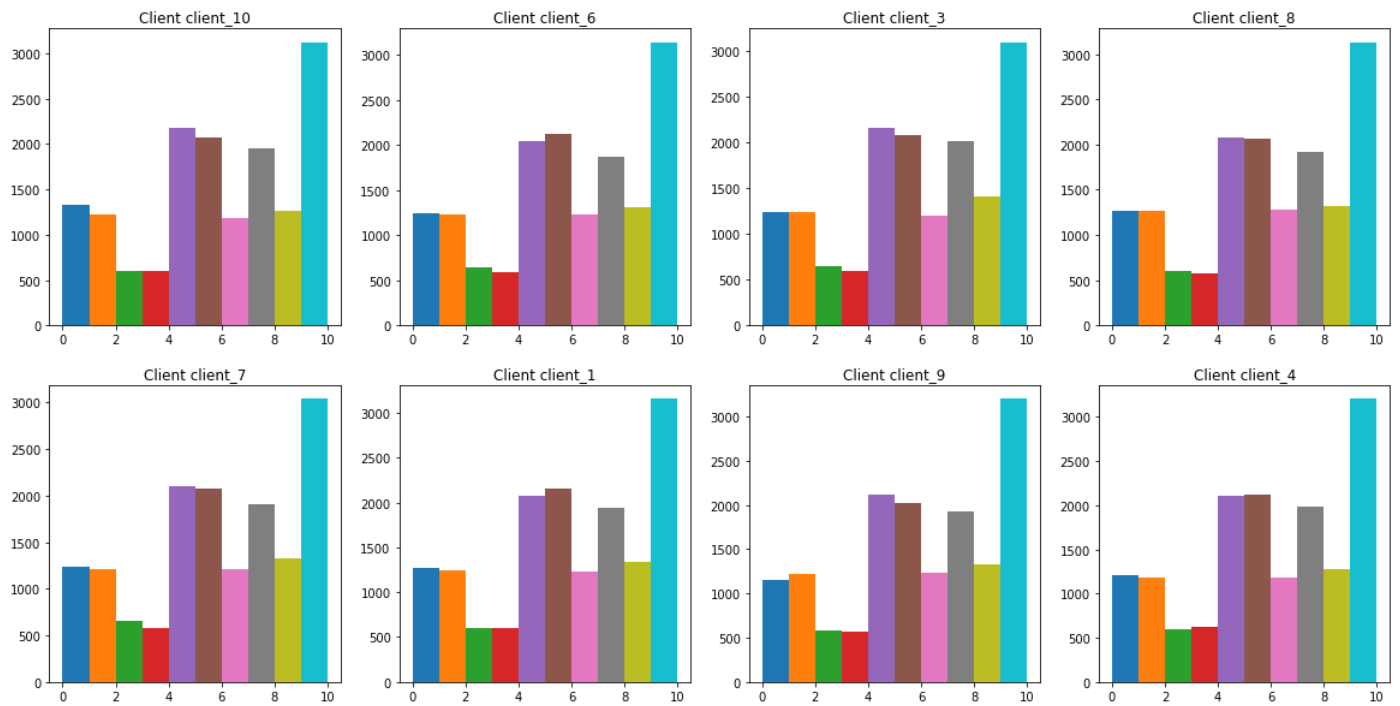
Figure 3. class distribution per each client

device. By applying PCA, we have effectively reduced the dimensionality of the data
while preserving the most informative features. In these plots, the distribution of data
points reveals inherent patterns, clusters, and separability among different attack catego-
ries and normal traffic, shedding light on the device's behavior under varying conditions.
This visual analysis provides valuable insights into the potential discriminative power of
our model and its ability to distinguish between normal traffic and malicious attacks for
each specific IoT device, contributing to a deeper understanding of our intrusion detection
approach's effectiveness and performance. In Figure 3, we provide an insightful depiction
of the class distribution per client, which underscores the intrinsic characteristics of each
IoT device within the N-BaIoT dataset. This visual representation not only showcases the
diverse nature of traffic data but also highlights the varying proportions of attack catego-
ries and normal traffic observed across different devices. By examining the class distribu-
tion per client, we gain a profound understanding of the unique challenges posed by each
device in the context of intrusion detection. This knowledge is crucial for tailoring and
fine-tuning our federated machine intelligence approach, as it allows us to account for
device-specific behaviors and adapt our model accordingly. Such client-specific insights
serve as a foundational component of our strategy for enhancing security and privacy in
IoT environments, as they enable us to develop more effective and customized intrusion
detection mechanisms.

In Figure 3, we present the confusion matrix, a fundamental and informative tool for
evaluating the performance of our model on the N-BaIoT dataset. This matrix provides a
comprehensive snapshot of the model's classification outcomes, breaking down the re-
sults into four distinct categories: true positives, true negatives, false positives, and false
negatives. Each cell of the confusion matrix quantifies the number of instances that our
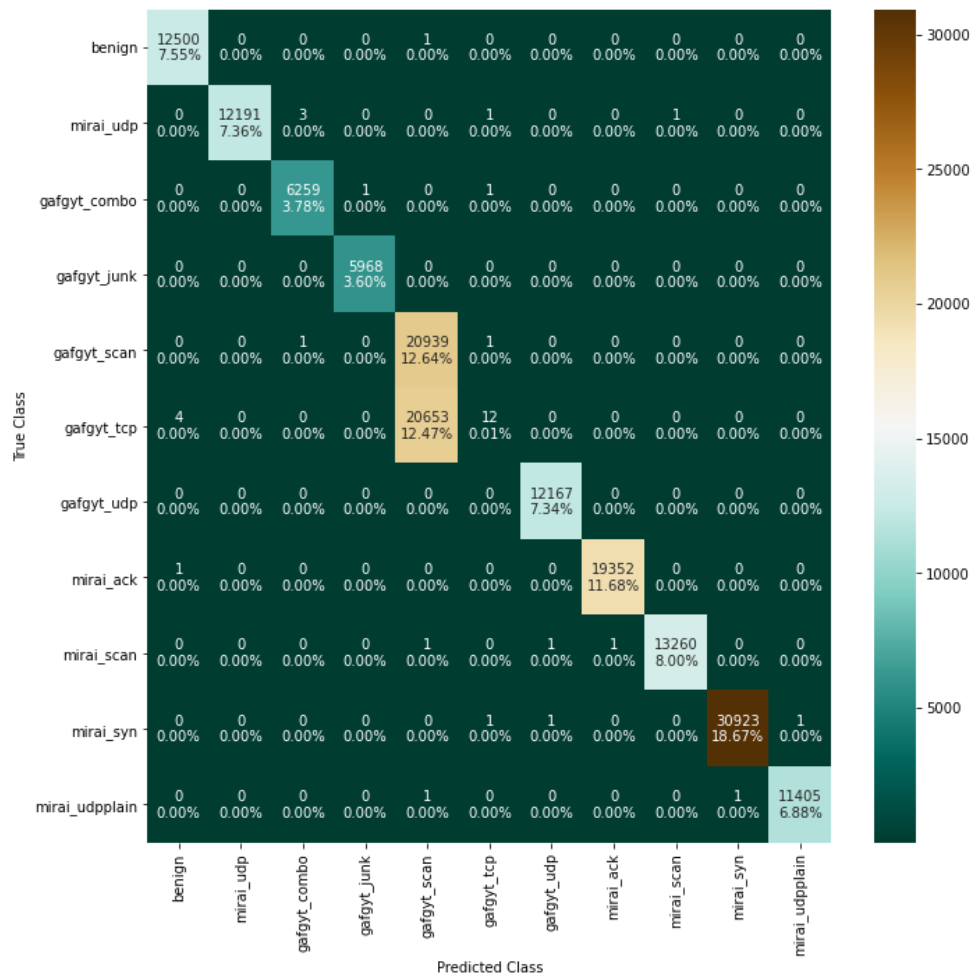
Figure 3: Confusion Matrix for Model Evaluation

model correctly or incorrectly classified as either normal or malicious traffic. This visual representation enables a granular analysis of our model's effectiveness in differentiating between legitimate and potentially harmful activities within the IoT network. By scrutinizing these values, we can assess the model's accuracy, precision, recall, and F1-score, among other performance metrics, to gauge its overall efficacy in intrusion detection. Such a detailed examination of the confusion matrix is crucial for fine-tuning our model, identifying potential areas of improvement, and ensuring robust security and privacy measures for IoT environments.

In Figure 4, we present the ROC plot, a fundamental tool for assessing the performance of our model on the test data from the N-BaIoT dataset. The ROC plot illustrates the trade-off between the true positive rate (sensitivity) and the false positive rate (1-specificity) as we vary the model's classification threshold. Each point on the ROC curve corresponds to a specific threshold setting, and the curve's shape reflects the model's ability to distinguish between normal and malicious traffic across a range of threshold values. The area under the ROC curve (AUC) is a key summary metric that quantifies the model's overall discriminatory power, with higher AUC values indicating better performance. Analyzing the ROC plot allows us to make informed decisions about the optimal threshold to balance the detection of intrusions while minimizing false alarms. This visual representation provides critical insights into the model's ability to accurately classify IoT traffic,
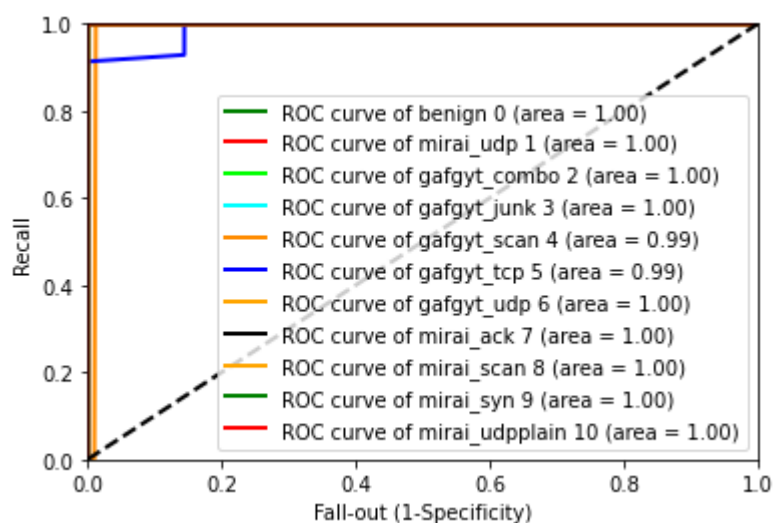
Figure 4: ROC Plot for Model Evaluation

ultimately contributing to the robustness of our intrusion detection system and enhancing security and privacy in IoT environments.

5. Conclusions

This paper presents a compelling solution for bolstering the security of Internet of Things (IoT) devices by addressing the imminent threat of BotNet attacks. Our Federated Machine Learning approach leverages the power of distributed intelligence while upholding data privacy, making it a robust and practical solution for contemporary IoT security challenges. Through rigorous experimentation on the N-BaIoT dataset, we have demonstrated the effectiveness of our approach in accurately detecting and mitigating BotNet threats, showcasing its potential to safeguard IoT ecosystems. As IoT continues to proliferate in our daily lives, the protection of these devices from malicious actors becomes paramount. Our federated model not only offers improved security but also ensures that sensitive data remains confidential. By advancing the field of IoT intrusion detection, this paper contributes to the ongoing efforts to secure the interconnected world of IoT devices, promoting trust and privacy in the digital age. It is our hope that this research serves as a foundation for further developments in IoT security and inspires practical implementations that enhance the safety of IoT devices for all users.

Supplementary Materials

No supplementary materials are associated with this work.

Author Contributions

All authors contributed equally to this work.

Funding

This research was conducted without external funding support.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Informed Consent Statement

Not applicable.

Data Availability Statement

All data generated and analyzed during this study are included in this manuscript.

References

[1]. Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G. (2021). Federated Learning-based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2021.3077803

[2]. Cui, L., Qu, Y., Xie, G., Zeng, D., Li, R., Shen, S., & Yu, S. (2021). Security and Privacy-Enhanced Federated Learning for Anomaly Detection in IoT Infrastructures. IEEE Transactions on Industrial Informatics, 1–1. https://doi.org/10.1109/TII.2021.3107783

[3]. Rahman, S. A., Tout, H., Talhi, C., & Mourad, A. (2020). Internet of Things intrusion Detection: Centralized, On-Device, or Federated Learning? IEEE Network, 34(6), 310–317. https://doi.org/10.1109/MNET.011.2000286

[4]. Kumar, K. P. S., Nair, S. A. H., Roy, D. G., Rajalingam, B., & Kumar, R. S. (2021). Security and privacy-aware artificial intrusion detection system using federated machine learning. Computers \& Electrical Engineering, 96, 107440.

[5]. Al-Marri, N. A. A.-A., Ciftler, B. S., & Abdallah, M. M. (2020). Federated mimic learning for privacy preserving intrusion detection. 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 1–6.

[6]. Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. Computer Communications.

[7]. Zhang, J., Luo, C., Carpenter, M., & Min, G. (2022). Federated Learning for Distributed IIoT Intrusion Detection using Transfer Approaches. IEEE Transactions on Industrial Informatics.

[8]. Zhao, R., Li, Z., Xue, Z., Ohtsuki, T., & Gui, G. (2021). A novel approach based on lightweight deep neural network for network intrusion detection. 2021 IEEE Wireless Communications and Networking Conference (WCNC), 1–6.

[9]. Li, B., Wu, Y., Song, J., Lu, R., Li, T., & Zhao, L. (2020). DeepFed: Federated deep learning for intrusion detection in industrial cyber--physical systems. IEEE Transactions on Industrial Informatics, 17(8), 5615–5624.

[10]. Yadav, K., Gupta, B. B., Hsu, C.-H., & Chui, K. T. (2021). Unsupervised federated learning based IoT intrusion detection. 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE), 298–301.

[11]. Aouedi, O., Piamrat, K., Muller, G., & Singh, K. (2022). FLUIDS: Federated Learning with semi-supervised approach for Intrusion Detection System. 2022 IEEE 19th Annual Consumer Communications \& Networking Conference (CCNC), 523–524.

[12]. Rehman, A., Abbas, S., Khan, M. A., Ghazal, T. M., Adnan, K. M., & Mosavi, A. (2022). A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. Computers in Biology and Medicine, 150, 106019.

[13]. Arisdakessian, S., Wahab, O. A., Mourad, A., Otrok, H., & Guizani, M. (2022). A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions. IEEE Internet of Things Journal, 10(5), 4059–4092.

[14]. Abdel-Basset, M., Moustafa, N., Hawash, H., Razzak, I., Sallam, K. M., & Elkomy, O. M. (2021). Federated intrusion detection in blockchain-based smart transportation systems. IEEE Transactions on Intelligent Transportation Systems, 23(3), 2523–2537.

[15]. Sarhan, M., Lo, W. W., Layeghy, S., & Portmann, M. (2022). HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. Computers and Electrical Engineering, 103, 108379.

[16]. Nguyen, T. D., Rieger, P., Miettinen, M., & Sadeghi, A.-R. (2020). Poisoning attacks on federated learning-based IoT intrusion detection system. Proc. Workshop Decentralized IoT Syst. Secur.(DISS), 1–7.

[17]. Agrawal, S., Chowdhuri, A., Sarkar, S., Selvanambi, R., Gadekallu, T. R., & others. (2021). Temporal weighted averaging for asynchronous federated intrusion detection systems. Computational Intelligence and Neuroscience, 2021.

[18]. Fan, Y., Li, Y., Zhan, M., Cui, H., & Zhang, Y. (2020). Iotdefender: A federated transfer learning intrusion detection framework for 5g iot. 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), 88–95.

[19]. Siniosoglou, I., Sarigiannidis, P., Argyriou, V., Lagkas, T., Goudos, S. K., & Poveda, M. (2021). Federated intrusion detection in NG-IoT healthcare systems: An adversarial approach. ICC 2021-IEEE International Conference on Communications, 1–6.

[20]. Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. IEEE Access, 9, 138509–138542.

[21]. Afaq, A., Haider, N., Baig, M. Z., Khan, K. S., Imran, M., & Razzak, I. (2021). Machine learning for 5G security: Architecture, recent advances, and challenges. Ad Hoc Networks, 123, 102667.

[22]. Chen, Z., Lv, N., Liu, P., Fang, Y., Chen, K., & Pan, W. (2020). Intrusion detection for wireless edge networks based on federated learning. IEEE Access, 8, 217463–217472.

[23]. Chathoth, A. K., Jagannatha, A., & Lee, S. (2021). Federated intrusion detection for iot with heterogeneous cohort privacy. ArXiv Preprint ArXiv:2101.09878.

[24]. Alazab, M., RM, S. P., Parimala, M., Maddikunta, P. K. R., Gadekallu, T. R., & Pham, Q.-V. (2021). Federated learning for cybersecurity: Concepts, challenges, and future directions. IEEE Transactions on Industrial Informatics, 18(5), 3501–3509.

[25]. Trakadas, P., Simoens, P., Gkonis, P., Sarakis, L., Angelopoulos, A., Ramallo-González, A. P., Skarmeta, A., Trochoutsos, C., Calvo, D., Pariente, T., & others. (2020). An artificial intelligence-based collaboration approach in industrial iot manufacturing: Key concepts, architectural extensions and potential applications. Sensors, 20(19), 5480.

[26]. Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., & Sadeghi, A.-R. (2019). DÏoT: A federated self-learning anomaly detection system for IoT. 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 756–767.

[27]. Bertoli, G. D. C., Júnior, L. A. P., Saotome, O., Dos Santos, A. L., Verri, F. A. N., Marcondes, C. A. C., Barbieri, S., Rodrigues, M. S., & De Oliveira, J. M. P. (2021). An end-to-end framework for machine learning-based network intrusion detection system. IEEE Access, 9, 106790–106805.

[28]. Zhang, T., He, C., Ma, T., Gao, L., Ma, M., & Avestimehr, S. (2021). Federated learning for internet of things. Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, 413–419.

[29]. Aïvodji, U. M., Gambs, S., & Martin, A. (2019). IOTFLA : AA secured and privacy-preserving smart home architecture implementing federated learning. Proceedings - 2019 IEEE Symposium on Security and Privacy Workshops, SPW 2019, 175–180. https://doi.org/10.1109/SPW.2019.00041

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

24