산업 IoT 전용 분산 연합 학습 기반 침입 탐지 시스템

Md Mamunur Rashid [1], 최필주 [1], 이석환 [2], 권기룡 [1]
[1] 부경대학교 인공지능융합학과
[2] 동아대학교 컴퓨터공학과

mamunrashid.ete88@gmail.com, pjchoi@pknu.ac.kr, skylee@dau.ac.kr, kiryongkwon@gmail.com

Distributed Federated Learning-based Intrusion Detection System for Industrial IoT Networks

Md Mamunur Rashid [1], Piljoo Choi [1], Suk-Hwan Lee [2], Ki-Ryong Kwon [1]
[1]Dept. of Artificial Intelligence Convergence, Pukyong National University
[2] Dept. of Computer Engineering, Donga University

Abstract

Federated learning (FL)-based network intrusion detection techniques have enormous potential for securing the Industrial Internet of Things (IIoT) cybersecurity. The openness and connection of systems in smart industrial facilities can be targeted and manipulated by malicious actors, which emphasizes the significance of cybersecurity. The conventional centralized technique's drawbacks, including excessive latency, a congested network, and privacy leaks, are all addressed by the FL method. In addition, the rich data enables the training of models while combining private data from numerous participants. This research aims to create an FL-based architecture to improve cybersecurity and intrusion detection in IoT networks. In order to assess the effectiveness of the suggested approach, we have utilized well-known cybersecurity datasets along with centralized and federated machine learning models.

1. Introduction

The Internet of Things (IoT) is one of the technologies that has been effectively adopted, in part because of its capacity to facilitate interconnection among densely packed heterogeneous things. A number of interactions between the various parts of industrial systems are made possible by the deployment of various intelligent devices (such as IoT devices) with heterogeneous specifications and capabilities. These devices also add a ubiquitous digital aspect by involving society and industries [1]. IoT is rapidly expanding, which necessitates the enforcement of appropriate security and privacy policies to guard against threats to the industrial system's security and privacy. Because some IoT-related threats can be more damaging in an IoT environment, conventional security measures may not always be adequate [2].

The development of intrusion detection systems, or IDSs, which are specialized security systems made to continuously monitor and evaluate incidents within computer networks and systems for indications of security breaches, is one of the hottest security research areas. IDS use two primary operating strategies: The disadvantage of a signature-based IDS is that it cannot identify new or unidentified assaults despite maintaining a preset signature of attack. In order to build a model that can distinguish between attack and normal behavior, anomaly-based IDSs use machine learning (ML). Although the latter can get around the issue of detecting new threats, it also creates additional issues. Federated Learning (FL) approach enables multiple parties to collaborate on the evolution of models without sharing sensitive information. Researchers have used different State-of-the-Art ML models as well as several modified methods in conjunction with federated learning to introduce intelligent intrusion detection by analyzing network traffic and identifying anomalies in IoT networks [3].

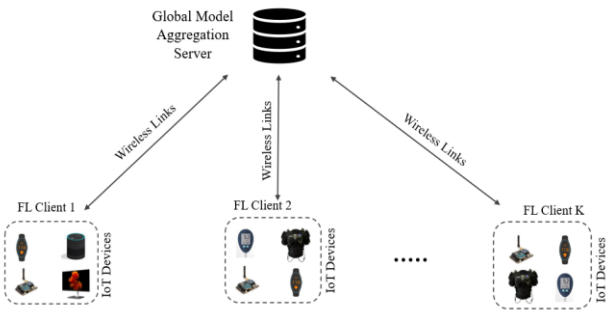

Figure 1. A generic representation of a Federated Learning Process.

In order to safeguard the security and privacy of IIoT data,

the approach for precisely identifying unwanted intrusions in wireless networks is presented in this study. We developed and tested an FL-based IIoT network that can identify network intrusions and boost security by using local machine learning (ML) on dispersed local clients rather than a centralized server.

2. Related Works

We have emphasized the benefits and drawbacks of previous research focused on the usage of FL and ML in IoT networks and intrusion detection.

Zarpelo et al. [4] gave an overview of IDS that are specific to the IoT and a taxonomy to organize them. Also, they presented a thorough comparison of the different IDS for IoT, taking things like installation strategy, detection mechanism, and validation strategy into account. Benkhelifa et al. [5] were more concerned with enhancing IoT intrusion detection processes. They investigated the current state of the art, with a focus on IoT architecture. It provided a more comprehensive and critical analysis.

A deep learning-based IDS for distributed DoS (DDoS) assaults that is based on three models—convolutional neural networks, deep neural networks, and recurrent neural networks—was examined by Ferrag et al. in a report published in 2014 [6]. Using two new real-world traffic datasets, CIC-DDoS2019 and TON_IoT, which feature different types of DDoS attacks, the performance of each model was examined across two categorization types (binary and multiclass). Khan et al.'s [7] main focus was on the use of decentralized ML technology to manage the enormous amounts of data from the expanding IoT devices, and they then talked about the difficulties of FL. In order to design a FL incentive mechanism to enhance communication between devices and edge servers, their team built a Stackelberg game-based methodology.

A system based on FL was described by Driss et al. [8] for detecting cyberattacks in vehicular sensor networks (VSNs). Utilizing gadgets for training and sharing computer resources is made possible by the suggested FL method. The suggested solution uses an ensemble unit based on Random Forest (RF) in conjunction with a collection of Gated Recurrent Units (GRU) to improve performance in attack detection. Vehicle IoT devices have sensors that generate device-specific information that, if released, could compromise device security, according to Du et al. [9]. Cooperative driving necessitates the sharing of GPS, cameras, radar, etc. The authors suggested employing FL to integrate vast IoT networks with numerous devices, hence enhancing system security and performance.

3. Proposed Method

We suggest a federated learning-based strategy for IoT network intrusion detection using ML. The layout of the suggested FL technique for IIoT intrusion detection is shown in Figure 2, where a number of devices are installed in various locations and connected to the network. Our proposed model is divided into three parts:

- Local-end Learnings and Intelligence
- Learnings Distribution
- Accumulated Global Learnings

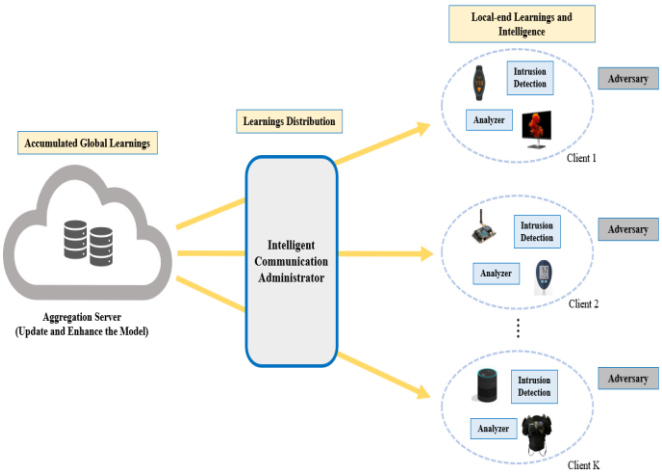

Figure 2. Proposed FL architecture for IoT intrusion detection.

3.1. Local-end Learnings and Intelligence

In this part of the framework, each k client (k ∈ [1, …, K]) at the local end trains the data acquired from their separate IIoT devices with the local models shared by the server, while the IDS at the client end detects any unwanted attacks. Also, an analyzer is employed to keep track of their network data for subsequent analysis. This kind of smart learning on the device protects the independence of local intrusion detection by requiring local training, tweaking of parameters, and improved inference procedures.

3.2. Learnings Distribution

With the aim of integrating the models and developing a better intrusion detection system with optimum parameters, the clients exchange their trained learning with a server-based system for aggregation. The intelligent communication administrator (e.g., security gateway) is in charge of all interactions between clients and the aggregation server.

3.3. Accumulated Global Learnings

In order to obtain the efficiency of centralized ML methods, which somewhat contain global data learning, the detection models are exchanged with the server-based aggregation platform. The aggregation server is responsible for the accumulation of local learning and making this into global learning. The distributed clients receive the optimized model through the communication platform, which allows for knowledge sharing. A client can detect intrusions learned using comparable behavior obtained from several participating devices thanks to this sharing mechanism, which gradually improves learning.

4. Experiments and Results

The appropriate data collection must be chosen because IoT networks need them for both training and testing IDS. Edge-IIoTset is a data set for industrial IoT (IIoT) and IoT applications that are frequently used in cybersecurity research.

Table 1 compares the accuracy outcomes of the global models, the best clients, and the worst clients after the 1st and 50th FL rounds. As can be observed, the performance for all classes increased as the round increased. Additionally, it can be seen that the detection accuracy is fairly competitive with the centralized learnings. We can therefore conclude that our FL model is extremely efficient and ensures increased privacy.

Table 1. Federated Learning Model's Evaluation for Intrusion Detection.

Classifier	Clients	1st Round			50th Round		
		Best	Worst	Global	Best	Worst	Global
CNN	*K=3*	**63.23**	52.84	62.19	**91.34**	90.62	91.27
	K=9	56.71	55.23	57.34	91.3	90.18	91.13
	K=15	56.51	57.23	57.78	90.77	89.65	90.56
RNN	*K=3*	**61.67**	54.87	61.28	**92.49**	92.08	92.37
	K=9	58.43	53.67	56.84	92.41	92.01	92.28
	K=15	59.65	52.69	58.92	92.19	91.98	92.02

5. Conclusion

In this research, we proposed a more secure and private FL-enabled federated IIoT intrusion detection system. We evaluated CNN and RNN, two well-known ML models, on both centralized and federated systems. These tests were based on the Edge-IIoTset dataset, a recent cybersecurity dataset. The experiments presented in this paper illustrate its applicability and usefulness and have significant effects on the use of federated learning in the context of IoT networks. In our future work, we intend to make the model more reliable when there might be malicious edge nodes on the network. Additionally, we will concentrate on a mechanism that uses an outlier detection filtering technique to prevent poisoning attempts that are injected gradually.

Acknowledgments: This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2023-2020-0-01797) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation) and the MSIT (Ministry of Science and ICT), Korea, under the ICT Consilience Creative program (IITP-2023-2016-0-00318) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation).

References

[1] Boyes, H., Hallaq, B., Cunningham, J. and Watson, T., 2018. The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, *101*, pp.1-12.

[2] Sengupta, J., Ruj, S. and Bit, S.D., 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications*, *149*, p.102481.

[3] McMahan, B., Moore, E., Ramage, D., Hampson, S. and y Arcas, B.A., 2017, April. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics* (pp. 1273-1282). PMLR.

[4] Zarpelão, B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C., 2017. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, pp.25-37.

[5] Benkhelifa, E., Welsh, T. and Hamouda, W., 2018. A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. *IEEE communications surveys & tutorials*, *20*(4), pp.3496-3509.

[6] Ferrag, M.A., Shu, L., Djallel, H. and Choo, K.K.R., 2021. Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. *Electronics*, *10*(11), p.1257.

[7] Khan, L.U., Pandey, S.R., Tran, N.H., Saad, W., Han, Z., Nguyen, M.N. and Hong, C.S., 2020. Federated learning for edge networks: Resource optimization and incentive mechanism. *IEEE Communications Magazine*, *58*(10), pp.88-93.

[8] Driss, M., Almomani, I., e Huma, Z. and Ahmad, J., 2022. A federated learning framework for cyberattack detection in vehicular sensor networks. *Complex & Intelligent Systems*, *8*(5), pp.4221-4235.

[9] Du, Z., Wu, C., Yoshinaga, T., Yau, K.L.A., Ji, Y. and Li, J., 2020. Federated learning for vehicular internet of things: Recent advances and open issues. *IEEE Open Journal of the Computer Society*, *1*, pp.45-61.