IoT 네트워크에서 침입 탐지를 위한 블록체인 기반 연합 학습

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@tu.ac.kr, kiryongkwon@gmail.com

Blockchain-based Federated Learning for Intrusion Detection in IoT Networks

Md Mamunur Rashid [1], Philjoo Choi, [1] Suk-Hwan Lee [2], Ki-Ryong Kwon [3]
[1]Dept. of Artificial Intelligence Convergence, Pukyong National University
[2] Dept. of Computer Engineering, Donga University

Abstract

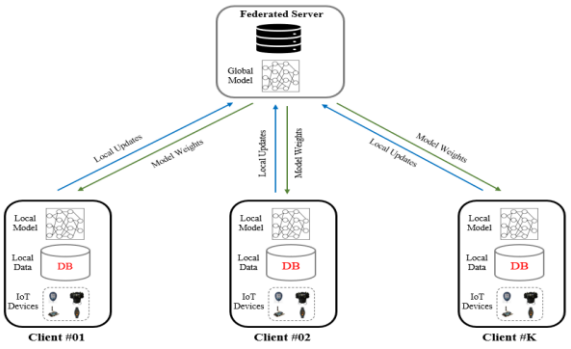
Internet of Things (IoT) networks currently employ an increased number of users and applications, raising their susceptibility to cyberattacks and data breaches, and endangering our security and privacy. Intrusion detection, which includes monitoring and analyzing incoming and outgoing traffic to detect and prohibit the hostile activity, is critical to ensure cybersecurity. Conventional intrusion detection systems (IDS) are centralized, making them susceptible to cyberattacks and other relevant privacy issues because all the data is gathered and processed inside a single entity. This research aims to create a blockchain-based architecture to support federated learning and 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 development of the Internet of Things (IoT) over the past few years has increased the level of comfort in people's lives by incorporating computers, gadgets, businesses, vehicles, and neighborhoods. Security and privacy are the top priorities for these real-time IoT systems because of the risk of unwanted intrusions, fatal attacks, or errors. An intrusion detection system (IDS) can be defined as a surveillance system that detects any abnormal activity by analyzing the metadata contained in network packets and sending out alarms when it finds one [1].

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 [2].

On cloud and IoT networks, Intrusion Detection Systems (IDS) and blockchain can be combined to identify cyberattacks and protect sensitive data. There has been a number of research to utilize blockchain technology in combination with ML methods as a means to combat unwanted intrusions in IoT networks and improve cybersecurity as a whole [3].



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

An effective solution to massive data storage issues is provided by the InterPlanetary File System (IPFS), which allows for the storing of a significant amount of data and is comparable to those of a blockchain. There is also Hyperledger Fabric, a blockchain infrastructure where all participating nodes are authorized, and distributed

applications can be developed. This research proposal aims to take the privilege of utilizing a decentralized storage system made up of combining IPFS and Hyperledger Fabric for intrusion detection [4].

2. Related Works

This section emphasizes the contributions and limitations of the related works that are pertinent to this research topic.

Using decentralized on-device data, Mothukuri et al. [5] introduced a federated-learning (FL)-based anomaly detection system to proactively identify infiltration in IoT networks. This method uses gated recurrent units (GRUs) algorithms with federated training rounds to protect the data on local IoT devices and communicates just the learnt weights with FL's main server.

According to Du et al. [6], sensors used in Vehicle IoT devices produce data that is unique to the device and could compromise the security of the device if it were to become public. To secure the system's overall efficacy and security, the authors propose adding FL as a remedy to that issue. To solve the aforementioned issue, the research proposes a Multi-access Edge Computing (MEC) method based on FL.

In order to detect DDoS assaults against mining pools on a network with a blockchain, Kumar et al. [7] develop a unique decentralized intrusion detection system (IDS) that makes use of fog computing. Training Random Forest (RF) and an improved gradient tree boosting system (XGBoost) on dispersed fog nodes are used to evaluate performance. An IoT-based distributed and collaborative anomaly detection platform called CIoTA was introduced by Golomb et al. [8]. Each device has an internal model that it uses to identify malicious activities. By adding new blocks to the chain, which are then broadcast to all neighboring nodes, new detection frameworks are traded. According to test results, CIoTA enhances network and device security by detecting different network intrusions.

3. Proposed Method

We suggest a federated learning-based strategy for IoT network intrusion detection using ML and blockchain technology. The framework of the suggested approach for IoT intrusion detection is shown in Figure 2, where several devices are placed in various locations and connected to the network. Three layers make up our suggested FL-model, and they are as follows:

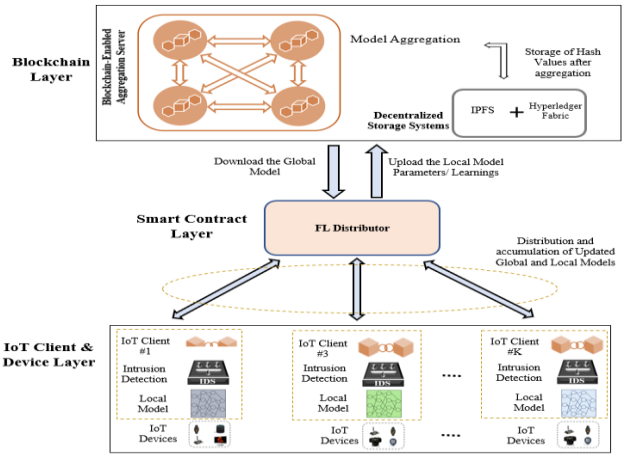
Three layers make up our suggested FL-model, and they are as follows:

- IoT clients and devices layer,
- Smart contracts layer, and
- Blockchain layer

The following are the functions of the layers.

- IoT Client and Device Layer for Local Training
- Smart Contract Layer for FL-Distribution
- Blockchain Layer for FL Aggregation and Storage

Recurrent neural networks (RNN) and convolutional neural networks (CNN) based on both centralized and FL methods are the ML classifiers we used in our method.



(Figure 2) Proposed BC-enabled FL architecture for IoT intrusion detection

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.

In order to examine two types of data for the FL Method, we employed client sets of 4, 8, and 12 and looked at Independent and Identically Distributed (IID) and Non-Independent Identically Distributed (Non-IID) data. Our model was trained for 20 FL training rounds. Even while all classes' performances increased as the round went on, IID normally has a smaller performance gap than the lowest and top clients do. The difference, however, is always quite noticeable with Non-IID because some clients only have a few classes. When K=12 in the first FL round, the difference between the best and worst customers is very considerable for CNN, however, it becomes less important for IID as we get closer to the 20th round. However, the differential for Non-IID is still significant.

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

Classifier	Clients	1st FL Round			20th FL Round		
		B	W	G	B	W	G
CNN	*K=4*	62.51	47.94	61.29	90.31	87.72	88.87
	K=8	56.29	44.86	55.44	90.37	87.46	88.73
	K=12	55.86	42.43	53.28	89.92	86.97	88.16
RNN	*K=4*	60.99	54.42	60.38	90.24	87.68	88.97
	K=8	57.72	50.27	55.94	**90.46**	**87.91**	89.05
	K=12	58.95	52.19	58.02	90.04	87.53	**89.62**

As shown in Figure 3, FL-Distributor provides the updated and aggregated global model to authorized clients so they can use it to train their local data.

(Figure 3) Successful deployment of global learning distribution smart contract

5. Conclusion

In this research, we proposed a more secure and private Blockchain-enabled federated ML-based IoT 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 experiment's findings showed that, when combined with our recommended FL approach, we can provide reasonably competitive results in intrusion detection. The smart contract-controlled distributor ensures that all transactions and activities taking place in the IoT intrusion detection system are continuously tracked and properly authenticated. The decentralized storage provided by the combination of IPFS and Hyperledger Fabric guarantees the privacy and security of the content and consequences of learning.

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] "Intrusion Detection System (IDS)," checkpoint.com, [Online]. Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/. [Accessed 13 09 2022].

[2] R. Zhao, Y. Yin, Y. Shi and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," *Physical Communication*, vol. 42, p. 101157, 2020.

[3] N. Alexopoulos, E. Vasilomanolakis, N. Réka Ivánkó and M. Mühlhäuser, "Towards blockchain-based collaborative intrusion detection systems," in *International Conference on Critical Information Infrastructures Security*, Lucca, Italy, pp. 107--118, 2017.

[4] M. M. Rashid, P. Choi, S.-H. Lee and K.-R. Kwon, "Block-HPCT: Blockchain Enabled Digital Health Passports and Contact Tracing of Infectious Diseases like COVID-19," *Sensors*, vol. 22, no. 11, p. 4256, 2022

[5] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-Learning-Based Anomaly Detection for IoT Security Attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545-2554, 2022.

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

[7] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," Journal of Parallel and Distributed Computing, vol. 164, pp. 55-68, 2022.

[8] T. Golomb, Y. Mirsky, and Y. Elovici, "CIoTA: Collaborative IoT anomaly detection via blockchain," arXiv preprint arXiv:1803.03807, 2018.