

Contract-based federated learning framework for intrusion detection system in internet of things networks

Yuris Mulya Saputra¹, Divi Galih Prasetyo Putri¹, Jimmy Trio Putra¹, Budi Bayu Murti¹, Wahyono²

¹Department of Electrical Engineering and Informatics, Vocational College, Universitas Gadjah Mada, Yogyakarta, Indonesia

²Department of Computer Science and Electronics, Faculty of Mathematics and Natural Sciences, Universitas Gadjah Mada, Yogyakarta, Indonesia

Article Info

Article history:

Received Nov 7, 2024

Revised Jun 12, 2025

Accepted Jul 10, 2025

Keywords:

Contract theory

Federated learning

Incentive mechanism

Internet of things

Network security

ABSTRACT

A plethora of national vital infrastructures connected to internet of things (IoT) networks may trigger serious data security vulnerabilities. To address the issue, intrusion detection systems (IDS) were investigated where the behavior and traffic of IoT networks are monitored to determine whether malicious attacks or not occur through centralized learning on a cloud. Nonetheless, such a method requires IoT devices to transmit their local network traffic data to the cloud, thereby leading to data breaches. This paper proposes a federated learning (FL)-based IDS on IoT networks aiming at improving the intrusion detection accuracy without privacy leakage from the IoT devices. Specifically, an IoT service provider can first motivate IoT devices to participate in the FL process via a contract-based incentive mechanism according to their local data. Then, the FL process is executed to predict IoT network traffic types without sending IoT devices' local data to the cloud. Here, each IoT device performs the learning process locally and only sends the trained model to the cloud for the model update. The proposed FL-based system achieves a higher utility (up to 44%) than that of a non-contract-based incentive mechanism and a higher prediction accuracy (up to 3%) than that of the local learning method using a real-world IoT network traffic dataset.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Wahyono

Department of Computer Science and Electronics, Faculty of Mathematics and Natural Sciences

Universitas Gadjah Mada

Yogyakarta, Indonesia

Email: wahyo@ugm.ac.id

1. INTRODUCTION

The growing popularity of internet of things (IoT) networks pose new challenges to data security and privacy. Specifically, national vital infrastructures linked to the IoT networks, such as transportation, energy, and healthcare systems, can be vulnerable to cyber-attacks that may lead to damaging consequences for national security and the well-being of society. For that, the IoT network security enhancement is crucial for national vital infrastructures through protective measures such as the adoption of intrusion detection systems (IDS), data encryption, and regular security updates to reduce risks and boost infrastructure resilience [1], [2].

One solution to improve the IoT network security for vital infrastructure protection is the development of automatic IDS at the centralized cloud server deployed by IoT service providers (ISPs) [3]. Here, the use of machine learning (ML) using deep learning (DL) approaches for IDS implementation in the cloud server has been widely investigated. For example, the works in [4]–[10] propose network attack classification based on

deep neural networks (DNN) utilizing various network traffic information datasets with different capture times. Specifically, the authors in [4], [5] discuss a DNN-based IDS to classify malware to notify users about potential attacks. Using Apache Spark, Mighan and Kahani [6] investigates the comparison of IDS between the proposed DL method and several linear ML methods. Then, an adaptive DNN-based IDS framework is proposed in [7], aiming at classifying network attacks. To tackle the unsupervised feature learning, a non-symmetric deep auto-encoder for network IDS is studied in [8], [9]. Moreover, Zhong *et al.* [10] introduces a hierarchical DL leveraging behavior and content features to recognize the network traffic attacks.

The use of DL approach for IDS scenario is then extended to IoT network-based applications. For example, a DL-based IDS using feed-forward neural networks (FNN) for binary and multi-class traffic flow classification in packet level of IoT devices is investigated in [11]. Otoum *et al.* [12] proposes a DL-based IDS utilizing stacked-deep polynomial network to obtain optimal security risk detection. Then, an IoT-based IDS to reveal distributed denial-of-service botnet attacks using DNN approach is investigated in [13]. Furthermore, an anomaly-based IDS to classify attacks using convolutional neural networks (CNN)-based approach for IoT networks is studied in [14]. Elnakib *et al.* [15] extends the previous work to cover the multi-class categorization using anomaly-based attack datasets for the IoT networks. Nonetheless, all of these studies are using the centralized learning process at the cloud server. In this case, sending network traffic data from IoT devices to the cloud server for the centralized learning may trigger to other issues such as data traffic breaches and privacy leakage of the IoT devices. As the alternative solution, each IoT device can process the network traffic data locally, however, this IDS approach will not achieve high intrusion detection accuracy due to limited local data and computational constraints on IoT devices [16].

The development of edge computing and distributed ML [17], [18] can be used to automatically detect intrusions from IoT devices without compromising privacy. For that, a federated learning (FL) approach has emerged as one of the most potential solutions to achieve that goal. Specifically, each IoT device executes the learning process locally and only sends the trained model to the cloud for the model update without sharing the IoT device's local data. The use of FL has been investigated in [19]–[24]. Particularly, the work in [19], [20] propose an IDS using FL with attention gated recurrent unit (through eliminating insignificant trained model to the cloud) and conventional DL method, respectively. Then, an FL-based IDS to tackle cyberattacks using DNN, CNN, and recurrent neural networks (RNN) for agricultural IoT environment is discussed in [21]. Using non-independent and identically distributed security attacks data, Alcazar *et al.* [22] incorporates FL via FedAvg and Fed+ approaches for IDS in an industrial IoT setting. Another performance comparison between FedProx and FedAvg methods for distributed network IDS is investigated in [23]. According to Oliveira *et al.* [24], an FL-enabled IDS with asynchronous learning using binary and multi-class classification is also introduced. Nevertheless, these studies utilize outdated network traffic datasets. They also do not consider the economic aspect of the system participating in the learning process (due to the selfishness characteristic of IoT devices). In other words, the above system will not work unless IoT devices are motivated to join in the FL processes. Therefore, the use of incentives as a reward for IoT device participation is required.

To address the aforementioned problem, in this paper, an integrated FL-based IDS framework with contract-based incentive mechanism for an IoT network is proposed. This aims to predict network traffic types (i.e., normal patterns or attack patterns) with high accuracy while maximizing utility for the whole IoT network in the FL processes. Specifically, an ISP can first motivate a set of IoT devices in the considered area to join the FL processes. Here, the ISP can provide incentive mechanism for the IoT devices by solving a contract optimization problem that maximizes the utility for the ISP and the IoT devices. This optimization will produce a set of optimal contracts containing performance and reward for the IoT devices. The ISP then offers the optimal contracts to the IoT devices in which they can receive or reject the offered contracts according to their decisions. In this way, the IoT devices that receive the contracts can participate in the FL processes. For the FL process, each participating IoT device can first execute the training process locally using its local network traffic data. Then, the trained model from the training process can be shared to the ISP's cloud for the global network traffic model update without revealing any private information of the IoT devices. Through experimental results using a real-world IoT network traffic dataset, the proposed contract-based FL framework can obtain a higher utility (up to 44%) than that of non-contract-based incentive mechanism and a higher prediction accuracy (up to 3%) than that of the local learning method. In the following, the details of contract-based incentive mechanism and FL approach between the ISP and IoT devices are discussed. Then, extensive comparisons in terms of utility, validation accuracy, validation loss, and learning performances are presented.

2. METHOD

Let $\mathcal{N} = \{1, \dots, n, \dots, N\}$ is the set of IoT devices and assume that a cloud-based ISP is connected to N IoT devices via Wi-Fi or cellular networks in the considered IoT network for a certain period. Here, the ISP utilizes a huge computing resource while the IoT devices have limited computing resources. To predict

network traffic types of IDS with high accuracy while maximizing utility for the whole IoT network in the FL processes, two approaches are investigated. Particularly, an incentive mechanism based on a contract theory approach between the ISP and participating IoT devices is first designed. This is carried out by formulating a contract optimization problem to find the optimal contracts containing performance in terms of quantity and quality of IoT network traffic data from each IoT device. This optimal IoT network traffic data is then used as the input data for the learning processes through using the FL approach without sharing any sensitive data of the IoT devices. The whole model architecture is shown in Figure 1.

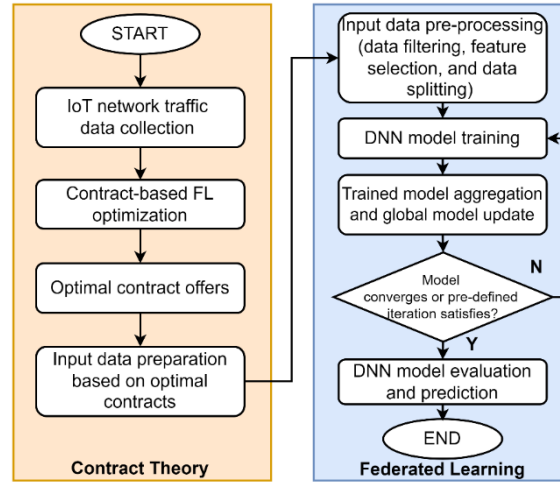


Figure 1. The model architecture of the proposed IDS in the IoT network

2.1. Contract-based incentive approach

Figure 2 shows the procedures for contract-based incentive and FL approach for the IDS in the IoT network. In this context, contract-based incentive mechanism is implemented to motivate IoT devices with high quantity and quality local network traffic data in joining the FL process, aiming at producing high-accuracy IDS. This incentive mechanism is based on the contract theory, an economic approach that balances the utilities of the ISP and IoT devices in the FL process under information asymmetry [25]. To this end, the ISP works as a principal which offers the contracts to the IoT devices as observed in Figure 2(a). Meanwhile, the participating IoT devices act as agents that have rights to receive or reject the offered contracts. As the principal, the ISP will provide incentives to the IoT devices as part of the contracts in return for their participation in the FL process. An IoT device that participates more in the FL process will receive more incentives from the ISP. Nonetheless, due to the information asymmetry between the ISP and IoT devices (i.e., the ISP does not know the preferences as well as network traffic data quality and quantity of the IoT devices due to their privacy), the ISP will only obtain the general information from the IoT devices, e.g., IoT device specification and resource information [26].

After the general information is collected from the IoT devices, the ISP can perform the FL contract optimization that maximizes utilities of the ISP and IoT devices. Specifically, the ISP first divides the IoT devices into N types. This type represents the willingness of an IoT device to participate in the FL process considering its network traffic data quality and quantity. Let β_n denote an IoT device with type- n , in which $\beta_1 < \dots < \beta_n < \dots < \beta_N$, $n \in \{1, \dots, N\}$. The larger β_n reflects the higher willingness to participate in the FL process due to the higher incentive (at the expense of higher data quantity and quality) [26], [27]. In this case, the ISP does not have any knowledge of the true type of each participating IoT device in the FL process. However, the ISP knows the likelihood that an IoT device belongs to a type- n from prior activities of the IoT devices [26] such that $\sum_{n=1}^N \rho_n = 1$, where ρ_n is the probability of IoT device with type- n .

Next, the FL contract optimization problem can be formulated with the aim to maximize the utility of the ISP in the FL process, in addition to the utility of IoT devices. First, the utility of the ISP that employs an IoT device with type- n can be expressed as the combination between the benefit and cost functions in executing the FL process as (1):

$$\mu_n^{ISP} = \alpha X_n - \sigma Y_n \quad (1)$$

Where αX_n indicates the benefit function for the ISP with $\alpha > 0$ is a conversion variable that implies the monetary unit of the IoT network traffic data quantity and quality X_n [28]. Meanwhile, Y_n is the incentive for the participating IoT devices and σ represents unit cost of the incentive. Since there exists N types of the participating IoT devices with probability $\rho_n, \forall n \in \mathcal{N}$, then the expected utility of the ISP can be formulated in (2).

$$\mu^{ISP} = \sum_{n=1}^N \mu_n^{ISP} \rho_n \quad (2)$$

Second, the utility of an IoT device with type- n that also contains the benefit and costs functions can be defined as (3).

$$\mu_n^{IoT} = \beta_n \gamma(Y_n) - \eta X_n \quad (3)$$

Where $\gamma(Y_n) = \sqrt{Y_n}$ is a strictly increasing concave benefit function with $\gamma(0) = 0, \gamma'(Y_n) < 0, \gamma''(Y_n) < 0, \forall Y_n$ [27]. Additionally, η corresponds to the computation and memory costs for the IoT device with type- n in training its local network traffic data in the FL process.

To obtain the contract feasibility, each offered contract package, i.e., $(X_n, Y_n), \forall n \in \mathcal{N}$, must meet individual rationality (IR) and incentive compatibility (IC) constraints [25], [27]. The IR constraints guarantee that an IoT device with type- n will obtain the utility that is greater than or equal to zero as described as (4).

$$\mu_n^{IoT} = \beta_n \gamma(Y_n) - \eta X_n \geq 0, \forall n \in \mathcal{N} \quad (4)$$

Meanwhile, the IC constraints ensure that all IoT devices only accept contract packages designed for their respective types under the presence of information asymmetry, as given in (5).

$$\beta_n \gamma(Y_n) - \eta X_n \geq \beta_m \gamma(Y_m) - \eta X_m, m \neq n, \forall m, n \in \mathcal{N} \quad (5)$$

To this end, the FL contract optimization problem that maximizes the expected utility of the ISP under the IR and IC constraints of the IoT devices can be formulated by (6).

$$\max_{(X,Y)} \sum_{n=1}^N \mu_n^{ISP} \rho_n \quad (6)$$

Subject to the IR, IC, and monotonicity constraints as shown in (7) to (9).

$$\beta_n \gamma(Y_n) - \eta X_n \geq 0, \forall n \in \mathcal{N} \quad (7)$$

$$\beta_n \gamma(Y_n) - \eta X_n \geq \beta_m \gamma(Y_m) - \eta X_m, m \neq n, \forall m, n \in \mathcal{N} \quad (8)$$

$$\beta_1 < \dots < \beta_n < \dots < \beta_N, n \in \{1, \dots, N\} \quad (9)$$

Where $X = [X_1, \dots, X_n, \dots, X_N]$ and $Y = [Y_1, \dots, Y_n, \dots, Y_N]$. Using the same method as in [26]–[28], the optimal contracts (X^*, Y^*) can be found through simplifying the IR and IC constraints such that the problem becomes (10).

$$\max_{(X,Y)} \sum_{n=1}^N \mu_n^{ISP} \rho_n \quad (10)$$

Subject to the monotonicity condition in (9), and the simplified IR and IC constraints as given in (11) to (12).

$$\beta_1 \gamma(Y_1) - \eta X_1 = 0 \quad (11)$$

$$\beta_n \gamma(Y_n) - \eta X_n = \beta_{n-1} \gamma(Y_{n-1}) - \eta X_{n-1}, \forall n \in \mathcal{N} \quad (12)$$

2.2. Federated learning approach

Upon obtaining the optimal contract packages (X^*, Y^*) for all participating IoT devices, the learning process using FL between the ISP and the participating IoT devices in \mathcal{N} that accept the offered optimal contracts can be executed and illustrated in Figure 2(b). Specifically, for each learning round, IoT devices first train their individual network traffic data locally and then only send the trained IDS models to the ISP's cloud

within a pre-defined limited period, ensuring the data privacy of the IoT devices. To obtain the global IDS model, the ISP's cloud can aggregate all the received trained IDS models and use this aggregated IDS model to update the current global IDS model. Here, the current global IDS model is used for the next learning FL iteration process by the cloud and the IoT devices. This process repeats until the global IDS model converges or the learning duration reaches the specified deadline time. Hence, using a such FL approach, the accuracy of IDS in the IoT network can be improved while preserving private information and reducing communication overhead (since IoT network traffic data is typically much larger than the training model) in the FL process.

To implement the DL process in the FL process, a DNN approach [29] is employed. Particularly, input data containing tabular data with many samples and training features (such as packet type, service, protocol, and other relevant network traffic features) along with training labels, i.e., network traffic pattern, is first collected from the real network traffic activity on each IoT device. To reduce the complexity of the learning process, the feature selection process using the correlation between features and label is then executed. In this case, the features with the correlation value less than 0.1 can be dropped from the training process. Upon selecting the relevant features, the input data is fed into the DNN on each IoT device. Here, the DNN model includes an input layer, several hidden layers with activation functions, some dropout layers, and the output layer with an output activation function for the network traffic pattern classification. Once the DNN model is created on each IoT device, the IoT device can perform the learning process locally to generate a trained model γ_n^t , where n is the index of IoT device and t is the iteration of FL process. The aggregation of trained models then leads to the global IDS model G_t that can be expressed as (13).

$$G_t = \frac{1}{N} \sum_{n=1}^N \gamma_n^t \quad (13)$$

Using the global model G_t , each IoT device can perform the next iteration's training process to obtain $G_{t+1}, G_{t+2}, \dots, G^*$. The final G^* , which is the final global IDS model, is then used to validate the accuracy of IDS using new network traffic data generated by the IoT devices for other periods.

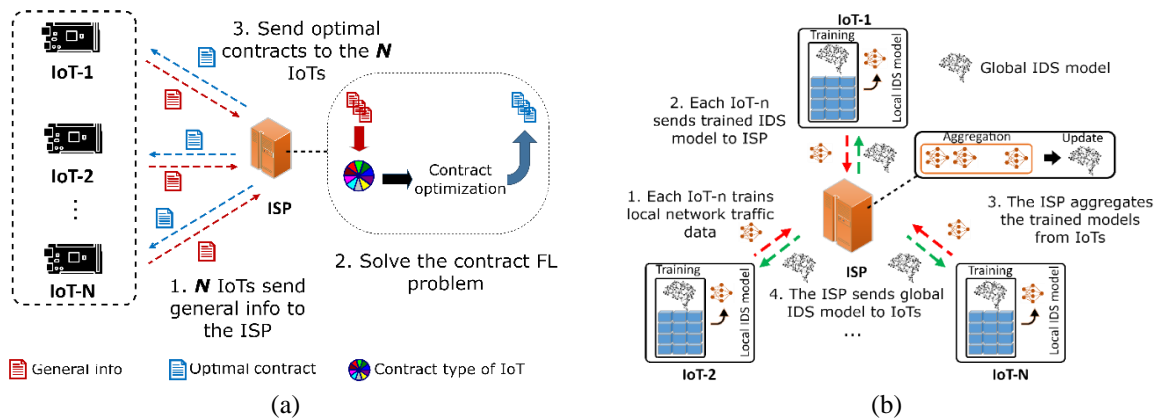


Figure 2. The procedures for (a) contract-based incentive and (b) FL approach for the IDS in the IoT network

3. RESULTS AND DISCUSSION

To evaluate the superiority of the proposed contract-based FL framework, a real-time IoT network traffic dataset from UCI Machine Learning Repository [30] that contains 83 features and 100K samples with normal and attack network activities. These samples are divided into subsamples according to the number of participating IoT devices. For the incentive mechanism, the proposed contract-based FL system is compared with the information symmetry (i.e., the ISP completely knows the true type of IoT devices) and the baseline method (i.e., the ISP provides the proportional incentive for the participating IoT devices). In this case, 10 participating IoT devices are considered to receive the optimal contracts that corresponds to 10 types of IoT devices.

Next, the FL process is then implemented using the DNN model with TensorFlow NVIDIA T4 Tensor Core GPU. Particularly, three hidden layers with rectified linear unit (ReLU) activation function, two dropout layers, and an output layer with SoftMax activation function are employed. To further show the FL performance, the proposed framework is compared with the centralized learning (i.e., DNN global) and the local learning (i.e., DNN local). Additionally, 2-label and 12-label scenarios are used. Specifically,

2-label scenario includes the 2 types of normal and attack patterns. Meanwhile, 12-label scenario contains the real network traffic patterns such as DOS_SYN_Hping, ARP_poisoning, NMAP_UDP_SCAN, NMAP_XMAS_TREE_SCAN, NMAP_OS_DETECTION, NMAP_TCP_scan, DDOS_Slowloris, Metasploit_Brute_Force_SSH, NMAP_FIN_SCAN, MQTT, Thing_speak, Wipro_bulb_Dataset, Amazon-Alexa. Additionally, a different number of participating IoT devices is also considered.

3.1. Utility performance

Prior to evaluating the FL performance, the utility performances of the ISP and participating IoT devices based on the contract theory are first demonstrated as shown in Figure 3. Particularly, as shown in Figure 3(a), the ISP always obtains positive utility for IoT device with type 1 to 10. This proves that the IR constraints are satisfied for all types of the IoT devices. Additionally, the utility of the ISP follows an increasing function regarding the types of IoT devices. This is because the IoT device with a higher type has more willingness to join the FL process, thereby leading to higher utility of the ISP in terms of the global IDS model accuracy.

Moreover, the ISP's normalized utility of proposed contract-based system is between the information-symmetry and baseline mechanisms, i.e., at 0.28 when IoT device has type 10. In this case, the information-symmetry mechanism acts as the upper-bound solution since the ISP completely knows the types of all IoT devices. As a result, the ISP can maximize its utility at the expense of zero utilities for all the participating IoT devices, as illustrated in Figure 3(b). Next, it can be observed in Figures 3(a) and 3(b) that the proposed contract-based system can achieve utility of the ISP and utility of IoT devices up to 44 and 572% higher than those of the baseline mechanism, respectively. This is due to the non-contract mechanism in which the participating IoT devices will receive linear/proportional incentives for their contributions in the FL process. From Figure 3, it can be summarized that the total utility of the ISP and IoT devices for the proposed framework is close to that of the ISP and IoT devices for the information-symmetry scheme as the upper bound solution. This indicates that the proposed contract-based framework is suitable for the FL process through balancing the utility performance of the ISP and participating IoT devices effectively [31].

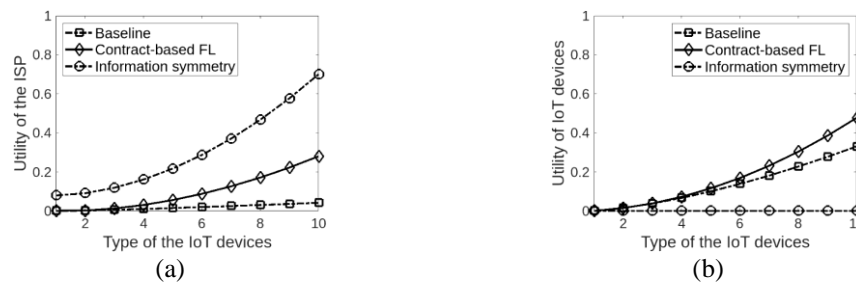


Figure 3. Normalized utility performance for (a) the ISP and (b) participating IoT devices

3.2. Learning performance

According to the optimal contracts that maximize utility of the ISP and IoT devices in section 3.1, the accuracy and loss performance comparisons can then be evaluated when 10 IoT devices participate in the FL process. Specifically, when various numbers of labels are used as shown in Table 1, the 2-label scenario outperforms all the performances of the 12-label scenario. Here, both training and validation accuracy of 2-label scenario achieves more than 2% better than those of 12-label scenario. This is because the 12-label scenario may suffer from misclassification due to many classes. This result also aligns with the loss performance where the training and validation losses of the 2-label scenario reach 7 times and 3 times better than those of the 12-label scenario, respectively.

When different approaches are used as observed in Table 2, the accuracy performance of the proposed FL framework, i.e., DNN FL, are between the DNN global and DNN local. In particular, the DNN global can achieve the accuracy that is slightly higher than that of the DNN FL by 1%. The reason is that the DNN global acts as the upper bound where all the network traffic data is trained at the cloud of the ISP. Nonetheless, this method may lead to the privacy leakage of the IoT devices when the cloud collects their local network traffic data. In contrast, the DNN FL can outperform the accuracy performance of the local learning or DNN local by approximately 3%. This is due to the insufficient network traffic data which is trained at the IoT device locally without any collaboration with the other IoT devices.

To further show a more practical scenario, different number of participating IoT devices is executed. In this case, the number of IoT devices varies from 5 to 20 devices. As shown in Table 3, the proposed FL can slightly produce a higher validation accuracy and a lower loss when 10, 15, and 20 number of IoT

devices are deployed. This implies that more participating IoT devices with more network traffic data and sufficient data quality can improve the accuracy and loss performances.

Table 1. The FL performances for different number of labels with 10 IoT devices

Number of labels	Training accuracy (%)	Validation accuracy (%)	Training loss	Validation loss
2	98.6	98.4	0.043	0.039
12	97.13	97.5	0.091	0.125

Table 2. The FL performances for proposed and other approaches with 2 labels and 10 IoT devices

Method	Training accuracy (%)	Validation accuracy (%)	Training loss	Validation loss
DNN global	99.61	99.64	0.011	0.016
DNN FL	98.6	98.4	0.043	0.039
DNN local	98.4	95.4	0.067	0.372

Table 3. The FL performances for various number of IoT devices with 2 labels

Number of IoT devices	Training accuracy (%)	Validation accuracy (%)	Training loss	Validation loss
5	98.5	98.37	0.043	0.038
10	98.6	98.4	0.043	0.039
15	98.6	98.4	0.042	0.038
20	98.43	98.42	0.045	0.043

To show the performances of the above scenarios in more detail, the validation accuracy and loss for 50 learning rounds are studied. This can be observed clearly in Figures 4 to 6 that although the accuracy and loss gaps are high at the beginning of the FL process, the difference gets lower when more learning rounds are conducted. Particularly, both 2-label and 12-label scenarios in Figure 4 and various number of IoT devices scenarios in Figure 6 can achieve the accuracy convergence after 30 and 25 learning rounds, respectively. Additionally, there exists a performance anomaly for the DNN local in Figure 5 where its validation loss suffers from overfitting, i.e., the validation loss keeps increasing. This is because the training process generates a simple trained model (with limited local network traffic data due to inherent restricted storage and resources at the IoT device), thereby leading to the overfitting for the testing/validation process.

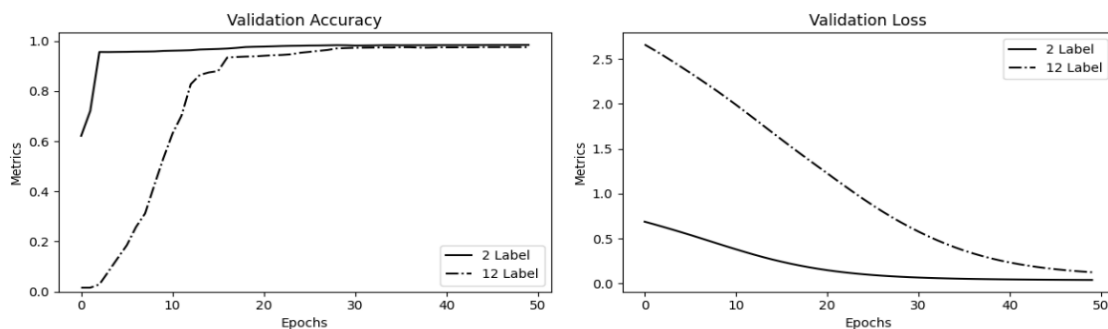


Figure 4. The validation accuracy and loss performances for various number of labels

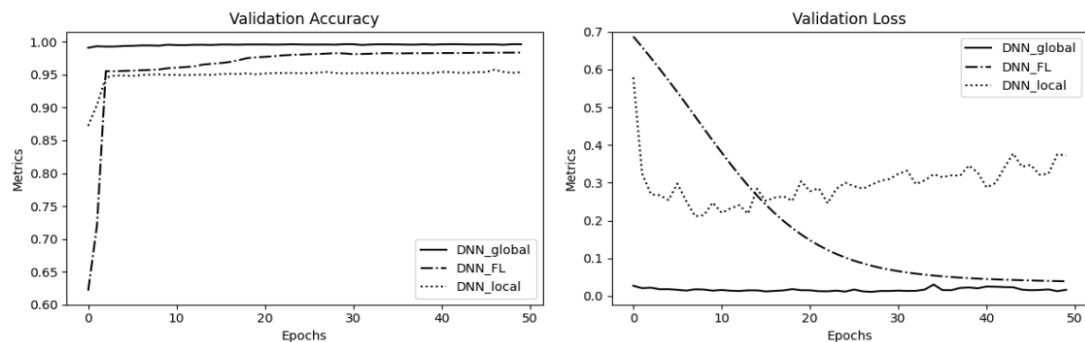


Figure 5. The validation accuracy and loss performances for various learning methods

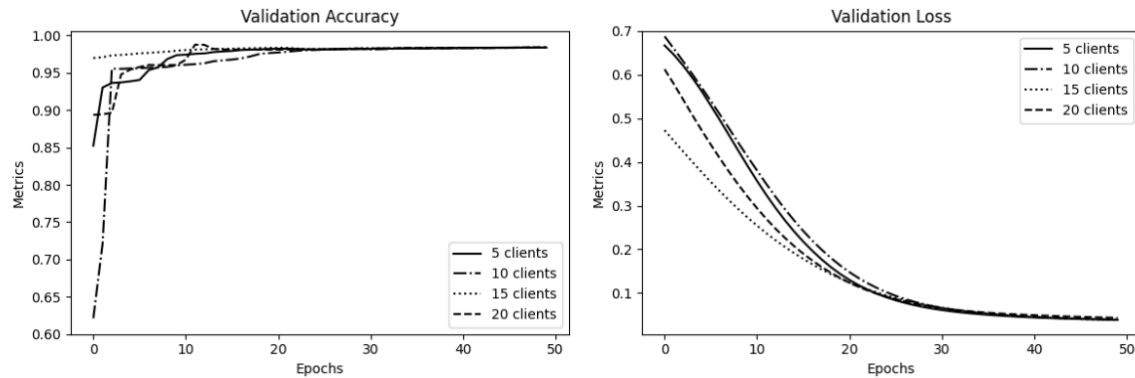


Figure 6. The validation accuracy and loss performances for different numbers of IoT devices

4. CONCLUSION

This paper presents a contract-based FL framework for IDS in the IoT network to improve the intrusion detection accuracy without privacy leakage from the IoT devices. Particularly, the ISP can first drive the IoT devices in the considered network to join the FL process through employing the contract-based incentive mechanism based on their local data quality and quantity. In this case, the ISP is required to address the contract optimization problem aiming at obtaining the optimal contracts. Using the optimal contracts for joining IoT devices, the FL process is then implemented to predict IoT network traffic types. Here, each IoT device conducts the learning process locally and only sends the trained model to the cloud for the model update. Through experimental results using the real-world IoT network traffic dataset, the proposed FL-based system can produce 44% higher utility than that of the baseline method and prediction accuracy by 98.4%, a 3% higher than that of the local learning method.

FUNDING INFORMATION

The authors thank the Program Peningkatan Academic Excellence Skema B Universitas Gadjah Mada 2024 that provides sponsor and financial support under grant number 6529/UN1.P1/PT.01.03/2024.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Yuris Mulya Saputra	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓
Divi Galih Prasetyo Putri	✓		✓			✓	✓		✓		✓			
Jimmy Trio Putra		✓		✓	✓					✓			✓	
Budi Bayu Murti		✓				✓				✓			✓	
Wahyono	✓			✓						✓	✓			✓

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nvestigation

R : **R**esources

D : **D**ata Curation

O : Writing - **O**riginal Draft

E : Writing - Review & **E**diting

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY




The data that support the findings of this study are openly available in [UCI Machine Learning Repository] at <http://doi.org/10.24432/C5P338>, reference [30].

REFERENCES




- [1] M. Aboubakar, M. Kellil, and P. Roux, "A review of IoT network management: current status and perspectives," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 7, pp. 4163–4176, 2022, doi: 10.1016/j.jksuci.2021.03.006.
- [2] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: requirements, challenges, and solutions," *Internet of Things*, vol. 14, Jun. 2021, doi: 10.1016/j.iot.2019.100129.
- [3] I. H. Sarker, M. M. Hoque, M. K. Uddin, and T. Alsanoosy, "Mobile data science and intelligent apps: concepts, AI-based modeling and research directions," *Mobile Networks and Applications*, vol. 26, no. 1, pp. 285–303, 2021, doi: 10.1007/s11036-020-01650-z.
- [4] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.
- [5] S. Gurung, M. K. Ghose, and A. Subedi, "Deep learning approach on network intrusion detection system using NSL-KDD dataset," *International Journal of Computer Network and Information Security*, vol. 11, no. 3, pp. 8–14, 2019, doi: 10.5815/ijcnis.2019.03.02.
- [6] S. N. Mighan and M. Kahani, "A novel scalable intrusion detection system based on deep learning," *International Journal of Information Security*, vol. 20, no. 3, pp. 387–403, 2021, doi: 10.1007/s10207-020-00508-5.
- [7] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Procedia Computer Science*, vol. 185, pp. 239–247, 2021, doi: 10.1016/j.procs.2021.05.025.
- [8] E. U. Qazi, M. Imran, N. Haider, M. Shoaib, and I. Razzak, "An intelligent and efficient network intrusion detection system using deep learning," *Computers and Electrical Engineering*, vol. 99, 2022, doi: 10.1016/j.compeleceng.2022.107764.
- [9] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018, doi: 10.1109/TETCI.2017.2772792.
- [10] W. Zhong, N. Yu, and C. Ai, "Applying big data based deep learning system to intrusion detection," *Big Data Mining and Analytics*, vol. 3, no. 3, pp. 181–195, 2020, doi: 10.26599/BDMA.2020.9020003.
- [11] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," in *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*, 2019, pp. 256–25609, doi: 10.1109/PRDC47002.2019.00056.
- [12] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: a deep learning-based intrusion detection framework for securing IoT," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, 2022, doi: 10.1002/ett.3803.
- [13] P. Jithu, J. Shareena, A. Ramdas, and A. P. Haripriya, "Intrusion detection system for IoT Botnet attacks using deep learning," *SN Computer Science*, vol. 2, no. 3, 2021, doi: 10.1007/s42979-021-00516-9.
- [14] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, 2022, doi: 10.1016/j.compeleceng.2022.107810.
- [15] O. Elnakib, E. Shaaban, M. Mahmoud, and K. Emara, "EIDM: deep learning model for IoT intrusion detection systems," *Journal of Supercomputing*, vol. 79, no. 12, pp. 13241–13261, 2023, doi: 10.1007/s11227-023-05197-0.
- [16] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, "Application of machine learning in wireless networks: key techniques and open issues," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4, pp. 302–3108, 2019, doi: 10.1109/COMST.2019.2924243.
- [17] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: a survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2224–2287, 2019, doi: 10.1109/COMST.2019.2904897.
- [18] W. Y. B. Lim *et al.*, "Federated learning in mobile edge networks: a comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020, doi: 10.1109/COMST.2020.2986024.
- [19] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, and W. Pan, "Intrusion detection for wireless edge networks based on federated learning," *IEEE Access*, vol. 8, pp. 217463–217472, 2020, doi: 10.1109/ACCESS.2020.3041793.
- [20] Z. Tang, H. Hu, and C. Xu, "A federated learning method for network intrusion detection," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 10, 2022, doi: 10.1002/cpe.6812.
- [21] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, K. K. R. Choo, and M. Nafaa, "FELIDS: Federated learning-based intrusion detection system for agricultural internet of things," *Journal of Parallel and Distributed Computing*, vol. 165, pp. 17–31, 2022, doi: 10.1016/j.jpdc.2022.03.003.
- [22] P. R. -Alcazar *et al.*, "Intrusion detection based on privacy-preserving federated learning for the industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1145–1154, 2023, doi: 10.1109/TII.2021.3126728.
- [23] M. J. Idrissi *et al.*, "Fed-ANIDS: federated learning for anomaly-based network intrusion detection systems," *Expert Systems with Applications*, vol. 234, 2023, doi: 10.1016/j.eswa.2023.121000.
- [24] J. A. D. Oliveira *et al.*, "F-NIDS — A network intrusion detection system based on federated learning," *Computer Networks*, vol. 236, 2023, doi: 10.1016/j.comnet.2023.110010.
- [25] P. Bolton and M. Dewatripont, *Contract theory*. Cambridge, Massachusetts: MIT Press, 2005.
- [26] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10700–10714, 2019, doi: 10.1109/IIOT.2019.2940820.
- [27] Y. Zhang, L. Song, W. Saad, Z. Dawy, and Z. Han, "Contract-based incentive mechanisms for device-to-device communications in cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 10, pp. 2144–2155, 2015, doi: 10.1109/JSAC.2015.2435356.
- [28] Y. M. Saputra, D. T. Hoang, D. N. Nguyen, L. N. Tran, S. Gong, and E. Dutkiewicz, "Dynamic federated learning-based economic framework for internet-of-vehicles," *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 2100–2115, 2023, doi: 10.1109/TMC.2021.3122436.
- [29] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F.E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11–26, 2017.
- [30] B. Sharmi and R. Nagapadma, "RT-IoT2022," *UCI Machine Learning Repository*, 2023, doi: 10.24432/C5P338.
- [31] Y. M. Saputra, D. N. Nguyen, D. T. Hoang, Q. V. Pham, E. Dutkiewicz, and W. J. Hwang, "Federated learning framework with straggling mitigation and privacy-awareness for AI-based mobile application services," *IEEE Transactions on Mobile Computing*, vol. 22, no. 9, pp. 5296–5312, 2023, doi: 10.1109/TMC.2022.3178949.

BIOGRAPHIES OF AUTHORS






Yuris Mulya Saputra    is currently an Assistant Professor as well as the Deputy Head at Department of Electrical Engineering and Informatics, Vocational College, Universitas Gadjah Mada, Indonesia and an Adjunct Fellow at School of Electrical and Data Engineering, University of Technology Sydney. He obtained Ph.D. in Electrical and Data Engineering from the University of Technology Sydney (Australia) in 2022. His research interests include mobile computing, energy and economic efficiency, machine learning, IoT, and optimization problems for wireless communication networks. He is affiliated with IEEE as a senior member. He is currently an active reviewer for various Q1 journals including IEEE TMC, IEEE WCM, IEEE IoT Journal, IEEE TNNLS, IEEE TBD, IEEE TCCN, and IEEE TCE. He can be contacted at email: ym.saputra@ugm.ac.id.






Divi Galih Prasetyo Putri    received her bachelor degree and master's degree in Informatics Engineering from Institut Teknologi Sepuluh Nopember, Indonesia in 2014 and 2016 respectively. She obtained her Ph.D. of Informatics in 2021 from University of Milano Bicocca. Currently, she is an Assistant Professor at the Department of Electrical Engineering and Informatics, Universitas Gadjah Mada. Her research interests include several topics in information retrieval, sentiment analysis, data science, and software engineering. She can be contacted at email: divi.galih@ugm.ac.id.






Jimmy Trio Putra    received his bachelor degree in Electrical Engineering from Universitas Bengkulu, Indonesia, in 2013. He graduated with a Master of Engineering at Universitas Gadjah Mada in 2015. He is an Assistant Professor in the Department of Electrical Engineering and Informatics, Vocational College, Universitas Gadjah Mada. He is pursuing his Doctoral Degree in the Department of Electrical and Information Engineering, Faculty of Engineering, Universitas Gadjah Mada, Indonesia. His research interests are power systems, distributed generation, and vehicle to grid. He can be contacted at email: jimmytrioputra@ugm.ac.id.



Budi Bayu Murti    received the B.S. degree in Electrical Engineering from Universitas Gadjah Mada, Yogyakarta, Indonesia, in 1996 and the M.Eng. degree from the same university in 2005. Currently, he is a lecturer, researcher in the Department of Electrical Engineering and Informatics, Vocational College, Universitas Gadjah Mada, and pursuing a doctoral degree in Electrical Engineering at Universitas Gadjah Mada. His research interests include wireless communication, signal processing, optical communication, cognitive radio, and biomedical instrumentation. He can be contacted at email: budibm@ugm.ac.id.



Wahyono    received the B.Sc. degree in Computer Science from Universitas Gadjah Mada, Indonesia, and the Ph.D. degree from The University of Ulsan, South Korea. He is an Associate Professor at the Department of Computer Science and Electronics, Universitas Gadjah Mada, Indonesia. His research interests include machine learning, computer vision, and pattern recognition. He actively participates as a member of the societies, a reviewer in reputable international journals, and an editor in several journals. He can be contacted at email: wahyo@ugm.ac.id.