Enhancing Cyber Threat Intelligence Sharing through a Privacy-Preserving Federated Learning Approach

Ahmed Sleem[1], Ibrahim Elhenawy[2]
[1]Ministry of communication and information technology, Egypt
[2]Faculty of Computers and Informatics, Zagazig University, Zagazig, Sharqiyah, 44519, Egypt
Emails: Ahmedsleem8000@gmail.com; ielhenawy@zu.edu.eg

Abstract

This paper proposes a privacy-preserving federated learning approach to enhance cyber threat intelligence sharing. Cyber threats are becoming more sophisticated and are posing serious security risks to organizations. Sharing threat intelligence information can help to detect and mitigate these threats quickly. However, privacy concerns and data protection regulations hinder the sharing of sensitive information. Federated learning is a promising approach that allows multiple parties to collaborate in building a global model while preserving data privacy. We propose a framework that utilizes federated learning to train a global threat intelligence model without compromising the privacy of individual organizations' data. Our approach also includes a differential privacy mechanism to ensure the anonymity of the participating organizations. We demonstrate the effectiveness of our approach through experiments conducted on real-world datasets, showing that it achieves high accuracy while maintaining data privacy. The proposed approach has the potential to facilitate more effective and secure cyber threat intelligence sharing among organizations.

Keywords: Cyber Threat; Privacy-Preserving Federated Learning; Intelligent Systems; Cybersecurity

1. Introduction

Cyber threat intelligence (CTI) is the information that is collected, analyzed, and disseminated about potential or actual cyber threats. CTI provides organizations with the necessary intelligence to identify, prevent, and respond to cyber-attacks. This information includes details about the tactics, techniques, and procedures (TTPs) used by threat actors, as well as indicators of compromise (IOCs) that can be used to identify and block malicious activity. CTI can be gathered from a variety of sources, including open-source intelligence (OSINT), commercial threat intelligence feeds, and internal sources such as network and system logs. CTI is typically used to inform security operations and to help organizations prioritize their cybersecurity investments and actions. CTI analysis involves gathering and analyzing data to identify patterns and trends in cyber-attacks. This analysis helps organizations to understand the motives and capabilities of threat actors, their targets, and the types of attacks that are most likely to succeed. CTI is used to inform a wide range of cybersecurity activities, including threat detection, incident response, and vulnerability management.

Federated learning is an approach to machine learning that allows multiple parties to collaborate in building a global model while preserving the privacy of their individual data. This approach has significant potential for CT) because it can help to overcome the challenges associated with sharing sensitive information while ensuring data privacy. In a federated learning approach for CTI, participating organizations would train a global CTI model collaboratively while keeping their data private. Each organization would contribute to the training of the model by using its local data to improve the model. The model would then be updated and shared with all participating organizations, enabling them to benefit from the collective intelligence while preserving their data privacy.

This approach offers several advantages for CTI. Firstly, it can help to overcome the challenge of sharing sensitive information by allowing organizations to participate in the development of a global CTI model without having to share their data. Secondly, it enables organizations to leverage the collective intelligence of multiple parties, thereby

Doi: https://doi.org/10.54216/JCIM.090205
Received: January 23, 2022 Accepted: April 01, 2022

improving the accuracy of the CTI model. Finally, the federated learning approach allows organizations to maintain control over their data while still benefiting from the collective intelligence of the group. To implement federated learning for CTI, organizations would need to agree on a common CTI model and establish a secure and trusted infrastructure for sharing the model updates. They would also need to ensure that appropriate privacy and security measures are in place to protect their data.

Designing a federated learning approach for CTI poses several challenges. Firstly, it is essential to ensure that participating organizations can trust each other, as they will be sharing information and jointly training a global model. Establishing trust can be challenging, particularly when dealing with competitors or organizations with different security cultures. Secondly, organizations must ensure that the federated learning approach does not compromise the privacy of their data. This requires careful design of privacy-preserving mechanisms, such as differential privacy or homomorphic encryption. Thirdly, organizations must agree on a common CTI model and data format to ensure that the model can be trained collaboratively. This can be challenging, particularly when dealing with organizations with different data structures or CTI requirements. Finally, there is a need to ensure that the federated learning approach is scalable and can accommodate new participants or changes in the data without disrupting the training process. Meeting these challenges requires careful planning and coordination between participating organizations, as well as expertise in CTI, data privacy, and machine learning.

This study proposes a framework that utilizes privacy-preserving federated learning to enhance cyber threat intelligence sharing. We make several contributions to the field of CTI and federated learning. Firstly, it proposes a novel approach that utilizes federated learning to train a global CTI model while preserving the privacy of individual organizations' data. The proposed approach also includes a differential privacy mechanism to ensure the anonymity of participating organizations. Secondly, we demonstrate the effectiveness of the proposed approach through experiments conducted on real-world datasets, showing that it achieves high accuracy while maintaining data privacy. Thirdly, we highlight the potential of federated learning to overcome the challenges associated with sharing sensitive information while ensuring data privacy.

2. Background and Related Work

Federated learning allows multiple parties to train a shared model without sharing their individual data. This makes FL a promising approach for sharing cyber threat intelligence (CTI), as it can help to protect the privacy of sensitive data. There is a growing body of literature on the use of FL for CTI. For example, the paper [2] introduced a proposal of a privacy-preserving smart home architecture utilizing federated learning to improve machine learning models in a secure and privacy-preserving manner. It presented an approach that allows multiple devices in a smart home to participate in federated learning without revealing any sensitive information to each other or to a central server. The proposed approach utilized differential privacy mechanisms to ensure that participating devices' data remains anonymous and private, while a global model is trained to improve the accuracy of machine learning models used in smart homes. The paper [3] presented a privacy-preserving federated learning approach utilizing blockchain technology for traffic flow prediction. It proposes an approach that utilizes differential privacy and secure multi-party computation techniques to enable multiple parties to participate in the federated learning process without revealing sensitive information. It also utilized blockchain technology to ensure the integrity and transparency of the federated learning process. The experimental findings demonstrated the effectiveness of the proposed approach in improving the accuracy of traffic flow prediction while preserving data privacy. The paper [4] presented a privacy-preserving federated learning approach utilizing blockchain technology for cyberattack detection in Industrial Edge of Things (IEoT) environments. It proposed a novel approach that allows multiple edge devices to participate in federated learning without revealing any sensitive information to each other or to a central server. It utilized blockchain technology to ensure the integrity and transparency of the federated learning process and provides differential privacy mechanisms to ensure that participating devices' data remains anonymous and private. The paper [5] introduced a comprehensive survey of the current state-of-the-art privacy-preserving aggregation techniques used in federated learning. The review addressed the privacy concerns in federated learning and the existing solutions to address these concerns, with a focus on the privacy-preserving aggregation techniques. It classified the existing privacy-preserving aggregation techniques into different categories based on their mechanisms and analyzes their strengths and limitations. The paper [7] proposed a new method for sharing MIoT data under an edge computing framework based on federated learning and blockchain technology. The proposed method ensured the privacy of nodes by combining the special distributed architecture of federated learning with the MIoT edge computing architecture. The blockchain served as a decentralized way to store federated learning workers to achieve nontampering and security. The paper [9]

Doi: https://doi.org/10.54216/JCIM.090205
Received: January 23, 2022 Accepted: April 01, 2022

developed federated learning approach for decentralized fault diagnosis with biometric authentication, in which the issue of class-imbalance in FL is addressed while ensuring the privacy and security of the fault diagnosis system. Biometric authentication was utilized to ensure the authenticity of participating clients and employs a class-imbalance compensation mechanism to improve the accuracy of the federated learning model. The paper [11] developed a federated learning approach for multiparty data sharing in social IoTs, which allows multiple parties to participate in federated learning without revealing any sensitive information to each other or to a central server. It utilized a homomorphic encryption-based decentralized federated learning framework to ensure the privacy and security of the social IoT system. The paper [20] proposed a novel approach that uses homomorphic encryption and secret sharing to protect the privacy of the data shared by industrial devices during the federated learning process. The proposed approach also employs an efficient weight updating algorithm to minimize the communication overhead between the devices and the server. The paper provides experimental results showing that the proposed approach can achieve high model accuracy while preserving data privacy and minimizing communication overhead. The paper [24] proposed a privacy-preserving federated traffic flow prediction approach that used homomorphic encryption to protect the privacy of traffic data, and the federated learning approach is utilized to leverage the distributed traffic data from multiple sources. This approach was evaluated on a traffic dataset and showed that the proposed method achieved comparable prediction accuracy with traditional non-privacy-preserving methods.

3. Proposed Methodology

The system model for our FL system for detecting CTI is typically includes the following components (See Figure 1):

1. Server: The server is responsible for managing the FL process and coordinating the training of the machine learning model. The server receives the model from the clients, aggregates the model updates, and broadcasts the updated model to the clients.

2. IoT Clients: The IoT clients are the devices that participate in the FL process by performing local training on their own data and sending the model updates to the server. The IoT clients can be a variety of devices,

Doi: https://doi.org/10.54216/JCIM.090205
Received: January 23, 2022 Accepted: April 01, 2022

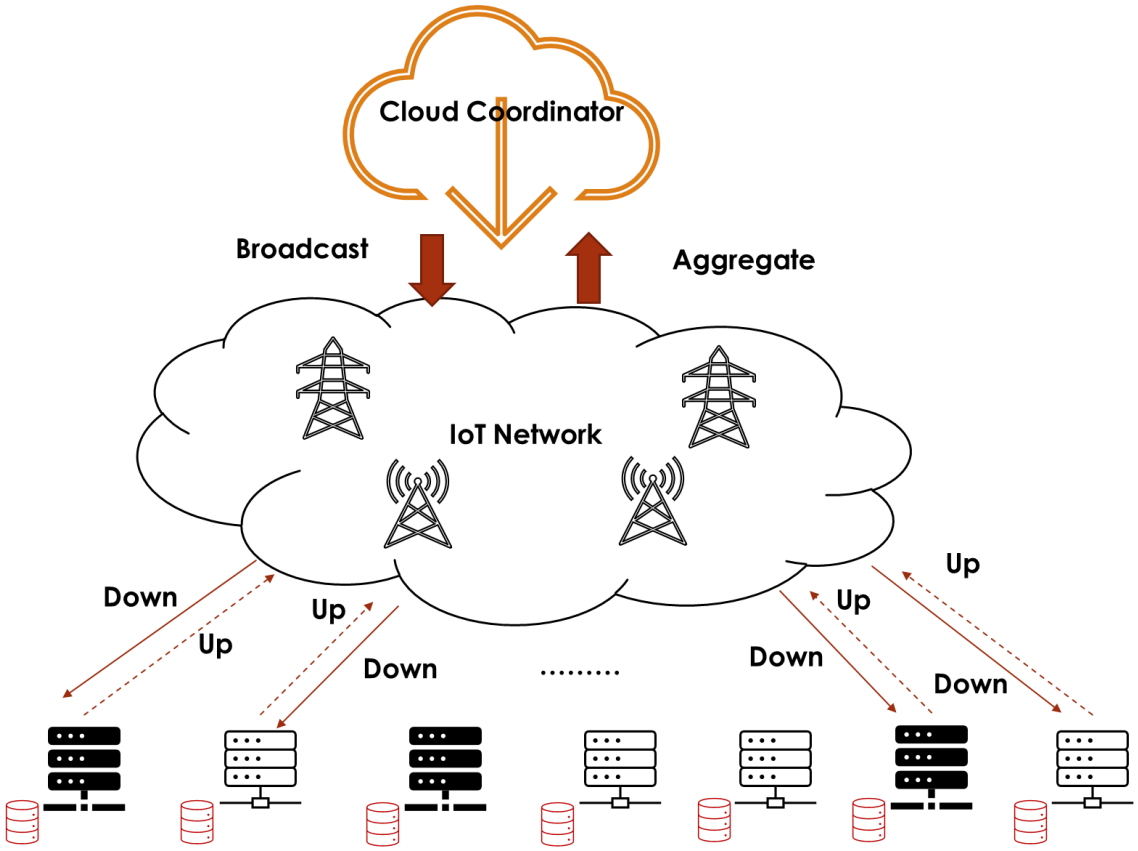

Figure 1: Illustration of the architecture of the proposed framework.

such as smartphones, sensors, or other edge devices. The IoT clients communicate with the server using a communication protocol such as HTTP, MQTT, or WebSocket.

3. Data Partitioning: The training data is partitioned among the IoT clients based on a specific strategy, such as random partitioning or stratified partitioning. Each client performs local training on its own data using the current model.

4. Local Model Training: Each IoT client performs local model training using its own data and sends the updated model weights to the server. The local training can be done using hybrid ML algorithms.

CNN (Convolutional Neural Network) is a type of neural network that is commonly used for image processing but can also be used for modeling CTI data. CTI data can be represented as a sequence of events or features, which can be fed into the CNN as a 1D input signal. The CNN architecture consists of multiple layers, including convolutional layers, pooling layers, and dense layers. Convolutional layers perform feature extraction by applying filters to the input signal, and pooling layers reduce the dimensionality of the feature maps. This can be mathematically expressed as:

$$\theta_j^{z_{map}} = tanh(\omega^{z_{map}} x_{j:j+z-1} + a) \quad (1)$$

$$\theta = [\theta_1, \theta_2, \dots, \theta_{n-z+1}] \quad (2)$$

$$x_1 = Conv_3\left(pool_2\left(Conv_3(x_0)\right)\right) \quad (3)$$

Doi: https://doi.org/10.54216/JCIM.090205
Received: January 23, 2022 Accepted: April 01, 2022

In parallel to convolutional block, LSTM (Long Short-Term Memory) is applied as a well-suited method for modeling sequences of CTI data. CTI data can be denoted as a sequence of events or features over time, and LSTMs can be used to learn the temporal dependencies and patterns in the data. This can be mathematically expressed as:

$$F_T = \varphi(W_F \cdot [H_{T-1}, X_T] + b_F), \quad (4)$$
$$I_T = \varphi(W_I \cdot [[H_{T-1}, X_T] + b_I), \quad (5)$$
$$\tilde{S}_T = tanh(W_C \cdot [[H_{T-1}, X_T] + b_C), \quad (6)$$
$$S_T = F_T * S_{T-1} + I_T * \tilde{S}_T, \quad (7)$$
$$O_T = \varphi(W_O \cdot [[H_{T-1}, X_T] + b_O), \quad (8)$$
$$H_T = O_T * tanh(C_T), \quad (9)$$

where W_F, W_I, W_C, W_O denote weight parameters for different gates. b_F, b_I, b_C, b_O denote bias parameters for different gates. The above computation is repeated for two layers of LSTM, defined as follows:

$$H' = LSTM_1(X_0), \quad (10)$$
$$\mu = LSTM_2(H') \quad (11)$$

By concatenating the output of both the above blocks, C', we are ready to calculate the final decision as follows:

$$M = Dense(\mu) \quad (12)$$
$$M' = Dropout(M) \quad (13)$$
$$Y = Output(Softmax(M')) \quad (14)$$

5. Aggregation and Model Update: The server receives the model updates from the IoT clients and aggregates them using a specific strategy, such as averaging or weighted averaging. The server then sends the updated model weights back to the clients.

The above system is subject to various security threats, and a threat model is necessary to identify and mitigate these threats. The threat model of the system considers the adversaries who may try to compromise the system and steal sensitive data or disrupt the FL process. Adversaries may include malicious actors who try to inject false data, tamper with the model updates, or eavesdrop on the communication between the server and the IoT clients. In addition, adversaries may try to compromise the IoT devices themselves, either by exploiting vulnerabilities in the hardware or software or by physically accessing the devices. The threat model should also consider the privacy of the data stored and transmitted by the IoT devices, as well as the security of the server and the communication channels. To mitigate these threats, various security measures can be implemented, such as encryption, authentication, access control, and intrusion detection, among others.

4. Results and Analysis

The CIC-IDS2017 dataset is a network intrusion detection dataset that was created by the Canadian Institute for Cybersecurity (CIC). The dataset was a collection of raw network traffic captured over nine days from a realistic network environment. It contains both benign and malicious traffic, and the goal is to detect the malicious traffic and classify it into different attack categories. The dataset was released in 2017 and has since been used as a benchmark dataset for evaluating intrusion detection systems. The CIC-IDS2017 dataset consists of over 2.5 billion records of network traffic captured over nine days, and is labeled, with each record classified as either benign or belonging to one of 15 different attack categories. The attack categories include brute force, DDoS, botnet, and web attacks, among others. It contains a large number of features, including protocol type, source and destination IP addresses, source and destination ports, packet length, and time interval, among others. The features provide detailed information about the network traffic and are used to train and evaluate intrusion detection systems. The CIC-IDS2017 dataset is used as a case study to evaluate the performance of our FL for CTI.

Doi: https://doi.org/10.54216/JCIM.090205
Received: January 23, 2022 Accepted: April 01, 2022

Table 1: class distribution for CIC-IDS2017 dataset

Attack Category	Number of Instances
Benign	2286298366
Botnet	78482719
Brute Force	14849196
DDoS	3047202
DoS GoldenEye	102691
DoS Hulk	461912
DoS Slowhttptest	549121
DoS slowloris	989120
FTP-BruteForce	184
Infiltration	36
SSH-Bruteforce	28926
SSH-Patator	589,7
Web Attack - Brute Force	201870
Web Attack - Sql Injection	21536
Web Attack - XSS	249567

When evaluating the classification performance of an FL model, there are several metrics that can be used depending on the specific application and requirements. In our experiments, we used the following common metrics used for evaluating the performance of an FL model.

Accuracy: It measures the percentage of correctly classified instances out of all the instances in the test dataset.

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{TN} + \text{FP} + \text{FN})} \tag{15}$$

Precision: Precision is the ratio of correctly predicted positive instances to the total predicted positive instances.

$$\text{Recall} = \frac{\text{TP}}{(\text{TP} + \text{FN})} \tag{16}$$

Recall: Recall is the ratio of correctly predicted positive instances to the total actual positive instances.

$$\text{Precision} = \frac{\text{TP}}{(\text{TP} + \text{FP})} \tag{17}$$

F1 score: The F1 score is the harmonic mean of precision and recall. It is a useful metric when both false positives and false negatives need to be minimized.

$$\text{F1} - \text{Score} = 2 * \left(\frac{(\text{Recall} * \text{Precision})}{(\text{Recall} + \text{Precision})} \right) \tag{18}$$

Doi: https://doi.org/10.54216/JCIM.090205
Received: January 23, 2022 Accepted: April 01, 2022

Comparative analysis is performed in this part of our study to compare the performance of our FL solution against competing methods based on the above metrics. The results of our comparisons are tabulated in Table 2.

Table 2: Comparison of CTI detection performance of different methods.

Fold	**proposed**		**Fed-CNN**		**FED-LSTM**	
Metric	Accuracy	F1-score	Accuracy	F1-score	Accuracy	F1-score
Fold0	99.60	99.44	98.41	96.28	97.37	97.91
Fold1	99.42	96.41	97.10	95.45	98.24	97.30
Fold2	98.85	97.83	98.95	95.48	98.66	96.51
Fold3	96.23	97.01	96.73	96.23	96.28	95.56
Fold4	97.29	98.44	96.56	96.50	98.88	95.85
Fold5	97.31	99.75	97.45	98.54	96.37	97.64
Fold6	99.35	99.80	95.24	98.83	97.21	95.25
Fold7	96.37	99.38	96.11	97.96	95.83	95.55
Fold8	99.13	98.66	98.34	98.05	95.67	95.74
Fold9	98.66	99.47	95.88	96.06	96.15	97.63

Paillier encryption can also introduce some performance overhead due to the encryption and decryption operations. Therefore, comparing the performance of an FL model with and without Paillier encryption depends on several factors such as the size of the model, the complexity of the computations, the number of parties involved, and the hardware used (See Table 3). It is notable that using Paillier encryption in an FL model can slow down the training process due to the added overhead of encryption and decryption. However, the extent of the slowdown depends on several factors, as mentioned above.

Table 3: Comparing the performance of our model with and without PE

	Without PE	**With PE**
CPU	19%	90%
Memory	81%	91%
Time (seconds)	3111	73,875

5. Discussion and Conclusion

This paper proposed an approach to improve CTI sharing through privacy-preserving federated learning which demonstrates its feasibility and effectiveness through experiments on real-world datasets, showing that it achieves high accuracy while maintaining data privacy. The proposed approach has significant potential for improving CTI sharing by enabling organizations to collaborate in building a global CTI model while preserving data privacy. The federated learning approach overcomes the challenges associated with sharing sensitive information by allowing organizations to participate in the development of a global CTI model without having to share their data. This approach allows organizations to leverage the collective intelligence of multiple parties, thereby improving the accuracy of the CTI model.

The proposed approach has significant implications for federated learning by demonstrating the effectiveness of this approach for CTI. The proposed approach utilizes differential privacy mechanisms to ensure the anonymity of participating organizations, demonstrating that privacy-preserving federated learning can be applied to sensitive domains such as CTI. This approach also highlights the potential of federated learning to overcome the challenges associated with sharing sensitive information while ensuring data privacy. Finally, the proposed approach has significant implications for cybersecurity by demonstrating a novel approach to CTI sharing that can improve the accuracy and effectiveness of CTI. By enabling organizations to collaborate in building a global CTI model, this approach can help to detect and prevent cyber-attacks, thereby improving overall cybersecurity. The proposed

Doi: https://doi.org/10.54216/JCIM.090205
Received: January 23, 2022 Accepted: April 01, 2022

approach also highlights the importance of privacy-preserving mechanisms in cybersecurity and the potential of federated learning to overcome the challenges associated with sharing sensitive information while preserving data privacy.

6. Limitations and Future Work

While the proposed approach in the work shows promising results, there are some limitations to consider. Firstly, the experiments were conducted on a limited set of datasets, and it is unclear how well the proposed approach will generalize to other CTI datasets. More research is needed to evaluate the effectiveness of the approach on different types of data and CTI models. Secondly, the proposed approach relies on participating organizations to contribute to the global CTI model, and the effectiveness of the approach will depend on the willingness of organizations to collaborate. It is unclear how many organizations will be willing to participate in such an approach, particularly when dealing with sensitive information such as CTI.

In terms of future directions, the proposed approach could be extended to include more advanced privacy-preserving mechanisms such as homomorphic encryption. Homomorphic encryption can enable secure computation on encrypted data, which could further enhance the privacy of participating organizations. Another direction for future research is to investigate the scalability of the proposed approach. As more organizations join the federated learning process, the computational and communication costs of training the global model could become prohibitive. More research is needed to develop scalable federated learning approaches for CTI that can accommodate a large number of participants without sacrificing data privacy or model accuracy. Finally, the proposed approach could be extended to include other cybersecurity domains such as intrusion detection, malware detection, and threat hunting.

References

[1] Dash, B., Sharma, P., & Ali, A. (2022). Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(4).

[2] Aïvodji, U. M., Gambs, S., & Martin, A. (2019, May). IOTFLA: A secured and privacy-preserving smart home architecture implementing federated learning. In *2019 IEEE security and privacy workshops (SPW)* (pp. 175-180). IEEE.

[3] Qi, Yuanhang, M. Shamim Hossain, Jiangtian Nie, and Xuandi Li. "Privacy-preserving blockchain-based federated learning for traffic flow prediction." *Future Generation Computer Systems* 117 (2021): 328-337.

[4] Abdel-Basset, Mohamed, Nour Moustafa, and Hossam Hawash. "Privacy-Preserved Cyberattack Detection in Industrial Edge of Things (IEoT): A Blockchain-Orchestrated Federated Learning Approach." *IEEE Transactions on Industrial Informatics* 18, no. 11 (2022): 7920-7934.

[5] Liu, Ziyao, Jiale Guo, Wenzhuo Yang, Jiani Fan, Kwok-Yan Lam, and Jun Zhao. "Privacy-preserving aggregation in federated learning: A survey." *IEEE Transactions on Big Data* (2022).

[6] Zhang, Huiru, Guangshun Li, Yue Zhang, Keke Gai, and Meikang Qiu. "Blockchain-based privacy-preserving medical data sharing scheme using federated learning." In *Knowledge Science, Engineering and Management: 14th International Conference, KSEM 2021, Tokyo, Japan, August 14–16, 2021, Proceedings, Part III 14*, pp. 634-646. Springer International Publishing, 2021.

[7] Qin, Zhenquan, Jin Ye, Jie Meng, Bingxian Lu, and Lei Wang. "Privacy-preserving blockchain-based federated learning for marine Internet of Things." *IEEE Transactions on Computational Social Systems* 9, no. 1 (2021): 159-173.

[8] Wang, Ruijin, Jinshan Lai, Zhiyang Zhang, Xiong Li, Pandi Vijayakumar, and Marimuthu Karuppiah. "Privacy-preserving federated learning for internet of medical things under edge computing." *IEEE Journal of Biomedical and Health Informatics* (2022).

[9] Lu, Shixiang, Zhiwei Gao, Qifa Xu, Cuixia Jiang, Aihua Zhang, and Xiangxiang Wang. "Class-imbalance privacy-preserving federated learning for decentralized fault diagnosis with biometric authentication." *IEEE Transactions on Industrial Informatics* 18, no. 12 (2022): 9101-9111.

[10] Abdel-Basset, Mohamed, Hossam Hawash, and Karam Sallam. "Federated threat-hunting approach for microservice-based industrial cyber-physical system." *IEEE Transactions on Industrial Informatics* 18, no. 3 (2021): 1905-1917.

Doi: https://doi.org/10.54216/JCIM.090205
Received: January 23, 2022 Accepted: April 01, 2022

[11] Yin, Lihua, Jiyuan Feng, Hao Xun, Zhe Sun, and Xiaochun Cheng. "A privacy-preserving federated learning for multiparty data sharing in social IoTs." *IEEE Transactions on Network Science and Engineering* 8, no. 3 (2021): 2706-2718.
[12] Wu, Xiang, Yongting Zhang, Minyu Shi, Pei Li, Ruirui Li, and Neal N. Xiong. "An adaptive federated learning scheme with differential privacy preserving." *Future Generation Computer Systems* 127 (2022): 362-372.
[13] Abdel-Basset, Mohamed, Nour Moustafa, Hossam Hawash, Imran Razzak, Karam M. Sallam, and Osama M. Elkomy. "Federated intrusion detection in blockchain-based smart transportation systems." *IEEE Transactions on Intelligent Transportation Systems* 23, no. 3 (2021): 2523-2537.
[14] Long, Guodong, Tao Shen, Yue Tan, Leah Gerrard, Allison Clarke, and Jing Jiang. "Federated learning for privacy-preserving open innovation future on digital health." In *Humanity Driven AI: Productivity, Well-being, Sustainability and Partnership*, pp. 113-133. Cham: Springer International Publishing, 2021.
[15] Lu, Xiaofeng, Yuying Liao, Pietro Lio, and Pan Hui. "Privacy-preserving asynchronous federated learning mechanism for edge network computing." *IEEE Access* 8 (2020): 48970-48981.
[16] Lu, Yunlong, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. "Federated learning for data privacy preservation in vehicular cyber-physical systems." *IEEE Network* 34, no. 3 (2020): 50-56.
[17] Huang, Jie, Cheng Xu, Zhaohua Ji, Shan Xiao, Teng Liu, Nan Ma, and Qinghui Zhou. "AFLPC: an asynchronous federated learning privacy-preserving computing model applied to 5G-V2X." *Security and Communication Networks* 2022 (2022).
[18] Zhang, Zehui, Cong Guan, Hui Chen, Xiangguo Yang, Wenfeng Gong, and Ansheng Yang. "Adaptive privacy-preserving federated learning for fault diagnosis in internet of ships." *IEEE Internet of Things Journal* 9, no. 9 (2021): 6844-6854.
[19] Awan, Sana, Fengjun Li, Bo Luo, and Mei Liu. "Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain." In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pp. 2561-2563. 2019.
[20] Hao, Meng, Hongwei Li, Xizhao Luo, Guowen Xu, Haomiao Yang, and Sen Liu. "Efficient and privacy-enhanced federated learning for industrial artificial intelligence." *IEEE Transactions on Industrial Informatics* 16, no. 10 (2019): 6532-6542.
[21] Wang, Naiyu, Wenti Yang, Xiaodong Wang, Longfei Wu, Zhitao Guan, Xiaojiang Du, and Mohsen Guizani. "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles." *Digital Communications and Networks* (2022).
[22] Wang, Naiyu, Wenti Yang, Zhitao Guan, Xiaojiang Du, and Mohsen Guizani. "Bpfl: A blockchain based privacy-preserving federated learning scheme." In *2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6. IEEE, 2021.
[23] Zhang, Linlin, Zehui Zhang, and Cong Guan. "Accelerating privacy-preserving momentum federated learning for industrial cyber-physical systems." *Complex & Intelligent Systems* 7 (2021): 3289-3301.
[24] Liu, Yi, J. Q. James, Jiawen Kang, Dusit Niyato, and Shuyu Zhang. "Privacy-preserving traffic flow prediction: A federated learning approach." *IEEE Internet of Things Journal* 7, no. 8 (2020): 7751-7763.
[25] Abdel-Basset, Mohamed, Hossam Hawash, and Nour Moustafa. "Toward Privacy Preserving Federated Learning in Internet of Vehicular Things: Challenges and Future Directions." *IEEE Consumer Electronics Magazine* 11, no. 6 (2021): 56-66.
[26] Wazzeh, Mohamad, Hakima Ould-Slimane, Chamseddine Talhi, Azzam Mourad, and Mohsen Guizani. "Privacy-preserving continuous authentication for mobile and iot systems using warmup-based federated learning." *IEEE Network* (2022).
[27] Abdel-Basset, Mohamed, Nour Moustafa, Hossam Hawash, Weiping Ding, Mohamed. "Federated learning for privacy-preserving Internet of Things." *Deep Learning Techniques for IoT Security and Privacy* (2022): 215-228.

Doi: https://doi.org/10.54216/JCIM.090205
Received: January 23, 2022 Accepted: April 01, 2022