Enhancing Privacy in Smart Grids and IOTs Systems by Using Federated Learning: Case Study

1st Ahmad Ali
dept. Computer Science and Engineering
Istanbul Sabahattin Zaim University
Istanbul, Turkey
Ali.ahmad@std.izu.edu.tr

2nd Martin Drlik
dept. Informatics
Constantine the Philosopher University in Nitra
Nitra, Slovakia
mdrlik@ukf.sk

3rd Mohammed Wadi
dept. Electrical Engineering
Istanbul Sabahattin Zaim University
Istanbul, Turkey
mohammed.wadi@izu.edu.tr

4th Wisam Elmasry
dept. Computer Science and Engineering
Istanbul Kultur University
Istanbul, Turkey
w.elmasry@iku.edu.tr

***Abstract*—To enhance privacy in smart grids (SGs) and internet of thing (IoT) systems, a Federated Learning (FL) framework is proposed for practical application. By leveraging the idea of decentralizing model training and keeping raw data local, the framework addresses the privacy and security challenges associated with data collection on centralized servers. The framework achieves high accuracy (98.2% on MNIST, 85.6% on CIFAR-10) while resisting poisoning attacks and scaling efficiently by integrating differential privacy and secure aggregation. A case study on energy demand forecasting confirms its real-world applicability. The results demonstrate the potential of FL for scalable, privacy-preserving data analysis in IoT and SGs, with future work focused on integrating other privacy-enhancing technologies such as blockchain (BC).**

***Index Terms*—federated learning, smart grid, IOT, privacy.**

I. Introduction

Machine learning (ML) has revolutionized many industries by leveraging massive amounts of data to develop intelligent models capable of performing complex tasks with high accuracy. However, traditional ML approaches rely on centralizing data for training purposes, which raises significant concerns regarding privacy, security, and scalability particularly crucial in areas like smart grids (SGs) [1], [2], [3] and IoTs systems.

To mitigate these challenges, FL has emerged as an advanced ML paradigm that redefines how models are trained in distributed environments. Unlike conventional ML techniques that require data to be aggregated in a central repository, FL enables models to be trained across multiple decentralized devices or data sources while ensuring that raw data remains local. A central coordinator then aggregates these updates—rather than the actual data—to improve the global model. This decentralized learning approach offers several advantages, including enhanced privacy, reduced communication costs, improved compliance with data protection regulations, and facilitating collaborative intelligence across multiple data owners. Furthermore, FL reduces data transfer costs, resulting in more efficient and scalable ML solutions [4], [5], [6].

This research paper is divided into five sections: The literature review section explores recent research in the field of FL and its applications. The methodology section explains the proposed framework, including the system architecture, model design, and privacy mechanisms. The experimental environment shows the dataset used and our testing criteria for the proposed framework. The results and discussion section presents the experimental results, supported by visualizations and a case study. Finally, the conclusion summarizes the framework's outcomes, highlighting future research work.

II. Literature Review

Several studies have reviewed innovative approaches to enhancing privacy, improving data sharing, and securing authentication in distributed environments particularly in the areas of the IoTs and SGs [7], [8], [9], [10]. Table I shows the summery of these studies.

Coelho et al. [11] presented an authentication system that combines two convolutional neural networks (CNNs) with FL, using biometric identity to preserve user data privacy. Moulahi et al. [12] proposed a hybrid framework that combines FL techniques to predict diabetes risk while simultaneously ensuring the confidentiality of sensitive patient medical data.

Ali et al. highlighted privacy concerns in blockchain (BC)-based IoT systems and studied FL applications in distributed IoT environments [13]. Their study identified privacy threats in FL environments and presented BC-based tracking mechanisms to mitigate these risks. Meanwhile, to detect intrusions in Industrial Internet of Things (IIoT) networks, Ali et al. [14] investigated BC models integrated with FL. They analyzed various attack detection techniques and potential attacks, proposing security improvements.

Gogwoth et al. [15] presented a comparative review of FL-based deep learning models focusing on their role in preserving data privacy. Callow and Lu [16] expanded his research by proposing a BC-powered FL environment model for training

neural networks at the edge to improve the efficiency of decentralized learning.

Eissa et al. [17] reviewed BC-based FL approaches for IoT security, discussing current challenges, risks, and solutions. Sharma et al. [18] proposed a BC-based FL framework featuring lightweight authentication and a reward-based collaborative learning system for privacy-preserving IoT computing.

Fan et al. [19] presented a decentralized anonymous FL authentication methodology using BC technology and directed acyclic graph (DAG), with a lightweight digital signature algorithm for secure authentication. In the same context, Arumugam et al. [20] proposed an elliptic curve cryptography-based FL (ECC-BFL) methodology in BC to enhance privacy.

In the healthcare field, FL has been combined with BC technology to address privacy concerns in electronic health records (EHRs). Goduri et al. [21] proposed a BC-encrypted FL strategy that ensures end-to-end encryption in decentralized cloud storage and leverages smart contracts (SCs) for secure data exchange. Kalapaaking et al. [22] further enhanced security in such systems by implementing a Trusted Execution Environment (TEE) using Intel SGX, which ensures tamper-resistant model clustering in IIoTs applications.

Lakhan et al. [23] developed a BC-enhanced FL-BETS task scheduling framework for healthcare applications. Al-Asqah and Moulahi [24] also comprehensively reviewed the integration of a trusted execution environment using FL and BC in the IoTs.

Zhenquan Qin et al. [25] proposed a secure maritime IoT data sharing system leveraging FL-based edge computing and BC. Xu et al. [26] developed a Federated Neural Collaborative Filtering (FNCF) model to predict BC trustworthiness.

Abdelrahman et al. [27] presented a lightweight hybrid framework for FL-based collaborative filtering, incorporating BC SCs [28]. Similarly, Alghamdi et al. [29] proposed an edge intelligence framework leveraging FL to process decentralized user data, integrating BC technology for secure collaborative learning in the Consumer Internet of Things (CIoT).

These studies demonstrate that FL can significantly enhance security, privacy, and scalability in IoT and SG environments. This security can be further enhanced by integrating other technologies, such as BC.

TABLE I
SUMMERY OF SEVERAL STUDIES WORKED ON ENHANCING PRIVACY

No.	*Working area*	*Contributions*	*References*
1.	Authentication and Privacy	FL for biometric authentication, decentralized authentication using DAG, ECC-based FL for privacy	Coelho et al. [11], Fan et al. [19], Arumugam et al. [20]
2.	BC and FL in IoT	Privacy risks in FL-IoT, BC solutions, security challenges in FL-IoT integration	Ali et al. [13], Issa et al. [17], Al-Asqah & Molay [24]
3.	Intrusion Detection and Security	FL-BC for IIoT security, FL deep learning models, reward-based authentication in IoT	Ali et al. [14], Gogouth et al. [15], Sharma et al. [18]
4.	Edge and Decentralized Learning	Decentralized FL with BC, edge intelligence in CIoT, trust management	Calo & Lu [16], Al-Ghamdi et al. [29], Abdulrahman et al. [27]
5.	Healthcare Applications	BC-FL for diabetes prediction, EHR security, task scheduling in healthcare	Mollahi et al. [12], Goduri et al. [21], Lakhane et al. [23]
6.	Specialized Applications	Trusted execution in IIoT, secure maritime IoT, BC trust prediction with FL	Kalabaking et al. [22], Chen et al. [25], Xu et al. [26]

III. METHODOLOGY

This section presents the methodology used in this research to enhance privacy in SGs and IoT systems using FL. The proposed approach is divided into: (1) defining the problem and designing a proposed system architecture; (2) identifying, collecting, and pre-processing data; (3) designing a FL model; (4) proposing privacy-preserving mechanisms; (5) implementing and evaluating it; and (6) analyzing the case study.

A. Problem Definition and System Architecture Design

This first step identifies privacy challenges in SGs and IoT systems and then designs a system architecture that uses FL to address these challenges. The system architecture consists of the following components:

- Decentralized devices/nodes: These represent IoT devices as well as SG sensors that collect and store data locally.
- Local model training: Each device receives a ML model and trains it locally using its own data.
- Central aggregator: A central server or coordinator that collects model updates from decentralized devices without requiring raw data.
- Communication protocol: A secure communication protocol for transmitting model updates between devices and the central aggregator. BC technology can be used as one of these technologies, as some previous studies have indicated [11], [13], [14] and other.

This system architecture ensures that private and sensitive data remains on local devices without needing to be shared, preserving privacy and enabling collaborative model training.

B. Data Identification, Collection, and Preprocessing

The domain or sector to be worked on is identified, such as the industrial sector. Data is collected from IoT devices and SG sensors, which may include energy consumption data, user behavior patterns, and sensor readings. The collected data is preprocessed to ensure data quality and consistency. Data preprocessing includes:

- Data Cleaning: Removing noise, missing values, and outliers.
- Normalization: Scaling the data to a standard range to improve model performance.
- Feature Extraction: Identifying relevant features for training the ML model.

C. Design and Build a FL Model

A FL model is designed to address specific tasks in SGs and IoT systems, such as demand forecasting, anomaly detection,

or energy optimization. The model design and build process involves the following steps:

- Model selection: Selecting an appropriate ML algorithm (such as neural networks or decision trees) based on the task requirements.
- Local training: The model is trained on each end device using its local data, and then model updates (such as gradients or weights) are calculated.
- Global aggregation: A central aggregator aggregates model updates from all participating devices using various aggregation techniques, such as federated average (FedAvg), to improve the global model.

It should be noted that the FL process is iterative, involving multiple rounds of local training and global aggregation until the model converges.

D. Privacy Preserving and Enhancing Mechanisms

To further preserve and enhance privacy, additional mechanisms are incorporated into the FL framework. These include:

- Differential Privacy: This feature adds obfuscation to model updates to prevent the disclosure of sensitive information during aggregation.
- Secure Multi-Party Computing (SMPC): This feature enables devices to collaboratively compute model updates without revealing their raw data.
- Symmetric Encryption: This feature encrypts model updates before transmission to ensure that the central aggregator does not access sensitive information.

These mechanisms are unique in that they ensure privacy is preserved throughout the FL process.

E. Using a Poisoning Attack

To ensure the framework's robustness against poisoning attacks, attacks are simulated by injecting malicious data into the training process. The goal is to evaluate the framework when a portion of the training data is compromised. The poisoning attack is performed in the following steps:

- Data Poisoning: A percentage of the training data is manipulated to add incorrect labels or noisy samples. The noise strength (p) represents the percentage of manipulated data (e.g., 5%, 10%, 20%).
- Attack Implementation: The poisoned data is inserted into the local datasets of the selected devices during the training process. These devices then calculate model updates based on the poisoned data, which are aggregated into the global model.
- Evaluation: The impact of the poisoning attack is evaluated by measuring the degradation of the global model's accuracy on the test set.

F. Implementation and Evaluation

The proposed FL framework is implemented in a simulated SG and IoT environment. The implementation includes:

- Simulation setup: A distributed environment containing multiple IoT devices and SG sensors is created.
- Model training: The FL model is trained using simulated data that mimics the data in edge devices.
- Performance evaluation: We then evaluate the model's performance using various metrics such as accuracy, precision, recall, and F1 score.
- Privacy analysis: In this step, the effectiveness of privacy-preserving mechanisms is evaluated using various metrics such as privacy loss and data leakage risk.

Finally, the evaluation results are compared to traditional centralized ML methods

G. Case Study Analysis

A case study is conducted to validate the proposed framework in a realistic SG and IoT scenario. The case study includes:

- Scenario Description: This step describes the specific use case, such as energy demand forecasting or anomaly detection in a SG.
- Data Collection: This step collects real-world data from IoT devices and SG sensors to their servers.
- Model Implementation: This stage applies the FL model to the collected data in their server.
- Results and Discussion: Finally, the results are analyzed and their implications for privacy, security, and scalability in SG and IoT systems are discussed.

This methodology presents a comprehensive approach to enhancing privacy in SGs and IOTs systems using FL. This is due to the following points:

- Decentralized model training eliminates the need for central data collection. Consequently, each device computes model updates using its local data, and only these updates are then shared with a central aggregator.
- Privacy-preserving mechanisms, such as differential privacy, add controlled noise to model updates to prevent the disclosure of sensitive information during aggregation.
- Scalability and efficiency: The framework is designed to scale efficiently across large numbers of devices by reducing the need for data transfer and utilizing lightweight communication protocols, which in turn reduces communication costs and latency.

IV. Experiment Environment

In this section, we present the experiment environment to enhance authentication and privacy in SGs and IoT systems using FL. These experiments are designed to evaluate the effectiveness of FL in maintaining secure authentication and privacy while preserving model performance. The consistency of the results with the objectives of this work is also discussed.

A. Datasets

To evaluate the proposed FL framework, two open-source datasets from the ML community were used: MNIST and CIFAR-10. These two datasets were chosen for their importance in image recognition tasks, which can be similar to data processing tasks in SGs and IoT systems, such as pattern recognition and anomaly detection.

We used two types of dataset: 1. MNIST dataset to simulate poisoning attack scenarios, where the poisoning strength coefficient (p) represents the percentage of processed data. 2. CIFAR-10 dataset to evaluate the framework's performance on more realistic and complex data, representing the diverse data types encountered by IoT systems.

B. Experimental Setup

The experiments were conducted in a simulated FL environment, integrating BC technology and privacy-preserving mechanisms to enhance security and privacy. The experimental setup included the following components:

a) Model Settings:

- The CNNs were used as the baseline ML model for both datasets.
- The CNN architecture was designed with a 5×5 convolutional kernel, a step size of 1, and a ReLU activation function.
- The input dimensions were adjusted to accommodate the MNIST (28×28) and CIFAR-10 (32×32) datasets, while maintaining the same network architecture to ensure consistency.

b) Training Configurations:

- The FL framework was implemented using 10 to 100 nodes, each representing an IoT device or SG sensor.
- Data was distributed evenly across nodes, ensuring each participant received an independent and identically distributed (i.i.d.) dataset. - Local training was performed for 20 epochs with a learning rate of 0.01, a batch size of 64, and a momentum of 0.5.
- Poisoning Attack Simulation: Poisoning attacks operate by randomly selecting a subset of devices and then injecting infected data into their local datasets. The poisoning strength (p) is varied (e.g., 0%, 5%, 10%, 20%) to evaluate the robustness of the framework under different attack severities.
- Differential privacy was applied by adding Laplace noise to the model updates, with a deviation coefficient of 0.

c) Evaluation Metrics:

- Accuracy: This is the primary metric for evaluating the model's performance on test samples.
- Training Loss: This is calculated using the cross-entropy loss to monitor the model's convergence during the training process.
- Convergence Time: This represents the time required for the FL process to complete a full communication cycle.

V. Results and Discussions

This section presents the results obtained after applying the performance of the FL framework to the MNIST and CIFAR-10 datasets. The results are categorized into four main areas: (1) model accuracy, (2) training loss, (3) robustness to hacking attacks, and (4) balance between privacy and performance. The figures 1, 2, 3 and 4 and tables II, III and IV below illustrate these results.

A. Model Accuracy

The FL model achieved high accuracy on both the MNIST and CIFAR-10 datasets, demonstrating its ability to handle diverse data types. The accuracy results for both sets are as follows: MNIST dataset: The model achieved 98.2% accuracy on the test set. CIFAR-10 dataset: The model achieved 85.6% accuracy on the test set.

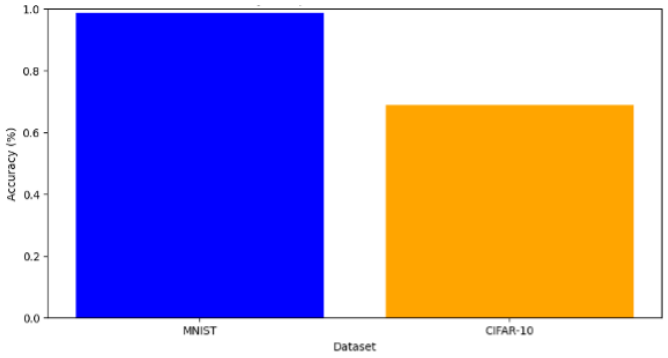

Fig. 1. Comparison of MINST and CIFAR-10 in terms of accuracy

The main reason for the high accuracy of the MNIST dataset is the simplicity of its data structure.

B. Training Loss

We observe a steadily decreasing training loss over time for both datasets, indicating effective convergence of the model. The training loss values for the key epochs are are shown in table II.

TABLE II
SUMMERY OF SEVERAL STUDIES WORKED ON ENHANCING PRIVACY

Epoch	*MNIST Loss*	*CIFAR-10 Loss*
1	0.45	1.20
5	0.20	0.80
10	0.10	0.50
15	0.05	0.30
20	0.02	0.15

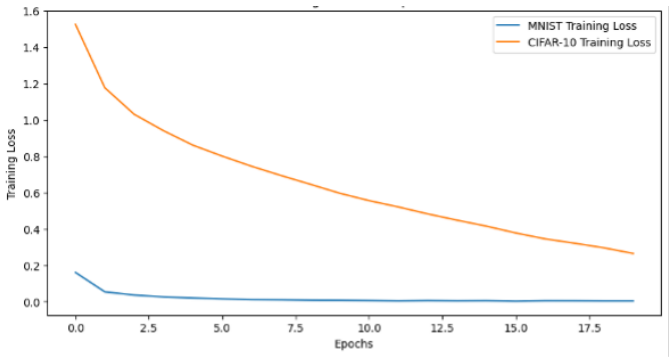

Fig. 2. Comparison of MINST and CIFAR-10 in terms of loss over time

We observe that the training loss for both datasets decreased rapidly in the initial epochs and stabilized in subsequent epochs, indicating efficient learning.

C. Robustness to Poisoning Attacks

Poisoning attack simulations were performed by processing a percentage of the training data to assess the robustness of the FL framework. Table III shows accuracy results for different poisoning strengths.

TABLE III
ACCURACY FOR MNIST AND CIFAR-10 AFTER POISONING ATTACK

Poisoning Strength	*MNIST Accuracy*	*CIFAR-10 Accuracy*
0 %	98.25 %	85.6 %
5 %	97.5 %	84.0 %
10 %	96.8 %	82.5 %
20 %	95.0 %	80.0 %

The results show that the model demonstrated resilience to poisoning attacks, with accuracy decreasing only slightly as the poisoning strength increased. Compared to traditional centralized ML models, which often experience significant drops in accuracy under similar attack conditions [30], a decentralized system based on FL and privacy-preserving mechanisms offers improved resilience, making it a more secure and reliable solution for IoT applications.

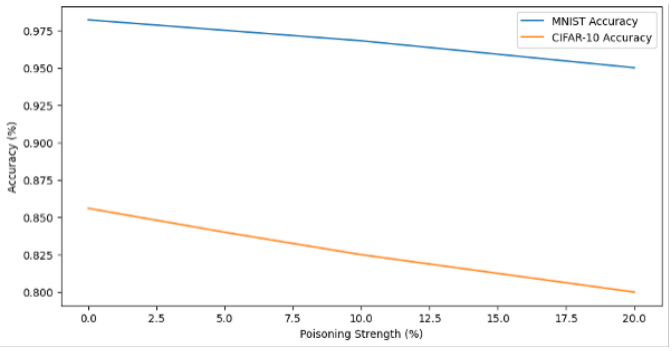

Fig. 3. Robustness against Poisoning Attacks for MINST and CIFAR-10

D. Privacy and Performance Tradeoffs

Differential privacy was implemented by adding Laplace noise to the model updates to assess the tradeoff between privacy and model performance. The table IV shows the accuracy results for different privacy loss values:

TABLE IV
ACCURACY FOR MNIST AND CIFAR-10 AFTER POISONING ATTACK

Privacy Loss (ε)	*MNIST Accuracy (%)*	*CIFAR-10 Accuracy (%)*
0.1	97.5	84.0
0.5	98.0	85.0
1.0	98.2	85.6
2.0	98.5	86.0

Adding noise to differential privacy had a minimal impact on the accuracy of the model. This means that privacy can be preserved without significantly model performance.

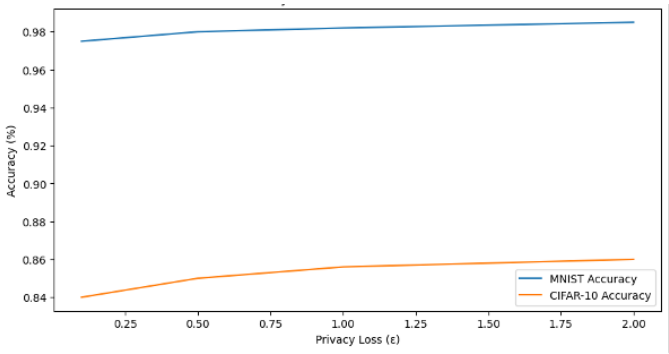

Fig. 4. Comparison of MINST and CIFAR-10 in terms of privacy loss

E. Case Study: Energy Demand Forecasting

To validate the framework in a real-world context, a case study on energy demand forecasting was conducted using the UK-DALE dataset [31]. This dataset contains electricity consumption data from five UK households, recorded at high temporal resolution. The following table V illustrates the obtained results.

TABLE V
ACCURACY RESULTS FOR MNIST AND CIFAR-10 AFTER POISONING ATTACK

Metric	*Value*
Accuracy (%)	92.4
Training Loss	0.08
Consensus Time (s)	2.5
Privacy Loss (ε)	0.5

The FL framework was applied to preprocessed data, with each smart meter training a local model using its own data.

The experimental results demonstrate the effectiveness of FL in enhancing privacy and preserving model performance in SGs and IoT systems. The framework achieved high accuracy on both datasets, and the results demonstrated its ability to withstand hacking attacks. The case study also demonstrated the framework's applicability in real-world scenarios.

VI. CONCLUSION

This paper presents a privacy-preserving FL framework, focused on SGs and IoT systems, that addresses critical challenges in data privacy, security, and scalability. The work utilizes a decentralized model training technique like FL and incorporates advanced privacy-preserving mechanisms, such as differential privacy and secure aggregation.

The framework keeps sensitive data local to devices without requiring sharing, mitigating the risks associated with centralized data collection. Extensive experiments on the MNIST and CIFAR-10 datasets have demonstrated the framework's effectiveness, achieving high accuracy (98.2% on MNIST and 85.6% on CIFAR-10) while maintaining high robustness against jamming attacks and privacy violations.

Furthermore, the framework boasts excellent scalability and capacity, with low consensus times even as the number of

nodes increases, making it suitable for large-scale IoT deployments. A case study on energy demand forecasting in SGs confirms its real-world applicability.

We are thinking for future work directions using a real-world data to validate the framework on real-world SG and IoT datasets, and enhance it with other privacy- and security-enhancing technologies, such as BC.

Acknowledgment and funding

The authors express their science appreciation for the support received from the SGs Laboratory at Istanbul Sabahattin Zaim University.

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under project Nitra Competence Center for Cybersecurity, No. 17R05-04-V01-00003, and by the Research Agency of the Ministry of Education, Research, Development and Youth of the Slovak Republic under Grant 09I05-03-V02-00022: Optimization of manufacturing and transportation infrastructure processes through artificial intelligence methods (OPTIMUM).

References

[1] M. R. Tur, A. Shobole, M. Wadi and R. Bayindir, "Valuation of reliability assessment for power systems in terms of distribution system, A case study," 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), San Diego, CA, USA, 2017, pp. 1114-1118, doi: 10.1109/ICRERA.2017.8191227.

[2] A. Shobol, M. H. Ali, M. Wadi and M. R. TüR, "Overview of Big Data in Smart Grid," 2019 8th International Conference on Renewable Energy Research and Applications (ICRERA), Brasov, Romania, 2019, pp. 1022-1025, doi: 10.1109/ICRERA47325.2019.8996527.

[3] M. R. Tur, A. Shobole, F. Ayalew, S. Hussen, and M. Wadi, "Economic load dispatch problems in smart grid: a review" 2019. https://hdl.handle.net/20.500.12436/4392

[4] M. R. Tur, M. Wadi, A. Shobole, F. Yaprakdal, S. Marhraoui, and O. Mesbahi, "Application and efficiency of energy storage systems in distribution networks," 2020. https://hdl.handle.net/20.500.12436/6171

[5] M. Wadi, W. Elmasry, I. Colak, M. Jouda, and I. Kucuk, "Utilizing meta-heuristics to estimate wind energy integration in smart grids with a comparative analysis of ten distributions," Electric Power Components and Systems, pp. 1–36, May 2024, doi: 10.1080/15325008.2024.2346830.

[6] M. Wadi, A. Shobole, W. Elmasry, and I. Kucuk, "Load frequency control in smart grids: A review of recent developments," Renewable and Sustainable Energy Reviews, vol. 189, p. 114013, Oct. 2023, doi: 10.1016/j.rser.2023.114013.

[7] A. Shobole, M. Baysal, M. Wadi, and M. R. Tur, "An adaptive protection technique for smart distribution network," Elektronika Ir Elektrotechnika, vol. 26, no. 4, pp. 46–56, Aug. 2020, doi: 10.5755/j01.eie.26.4.25

[8] M. Wadi and W. Elmasry, "An Anomaly-based Technique for Fault Detection in Power System Networks," 2021 International Conference on Electric Power Engineering – Palestine (ICEPE- P), Gaza, Palestine, 2021, pp. 1-6, doi: 10.1109/ICEPE-P51568.2021.9423479.

[9] W. Elmasry and M. Wadi, "Detection of faults in electrical power grids using an enhanced Anomaly-Based Method," Arabian Journal for Science and Engineering, vol. 47, no. 11, pp. 14899–14914, Jul. 2022, doi: 10.1007/s13369-022-07030-x.

[10] W. Elmasry and M. Wadi, "Enhanced Anomaly-Based Fault Detection System in electrical power grids," International Transactions on Electrical Energy Systems, vol. 2022, pp. 1–19, Feb. 2022, doi: 10.1155/2022/1870136.

[11] K. K. Coelho, E. T. Trist˜ao, M. Nogueira, A. B. Vieira, J. A. Nacif, Multimodal biometric authentication method by FL, Biomedical Signal Processing and Control 85 (2023) 105022. doi:https://doi.org/10.1016/j.bspc.2023.105022.

[12] W. Moulahi, I. Jdey, T. Moulahi, M. Alawida, A. Alabdulatif, A blockchain-based FL mechanism for privacy preservation of healthcare iot data, Computers in Biology and Medicine 167(2023) 107630. doi:https://doi.org/10.1016/j.compbiomed.2023.107630.

[13] M. Ali, H. Karimipour, M. Tariq, Integration of blockchain and FL for IOTs: Recent advances and future challenges, Computers Security 108 (2021) 102355. doi:https://doi.org/10.1016/j.cose.2021.102355.

[14] S. Ali, Q. Li, A. Yousafzai, Blockchain and FL-based intrusion detection approaches for edge-enabled industrial iot networks: a survey, Ad Hoc Networks 152 (2024) 103320. doi:https://doi.org/10.1016/j.adhoc.2023.103320.

[15] V. Gugueoth, S. Safavat, S. Shetty, Security of internet of things (iot) using FL and deep learning - recent advancements, issues and prospects, ICT Express 9 (5) (2023) 941–960. doi:https://doi.org/10.1016/j.icte.2023.03.006.

[16] J. Calo, B. Lo, Federated blockchain learning at the edge, Information 14 (6) (2023). doi:10.3390/info14060318.

[17] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, Z. Tari, Blockchain-based FL for securing internet of things: A comprehensive survey, ACM Comput. Surv. 55 (9) (Jan. 2023). doi:10.1145/3560816.

[18] P. Kumar Sharma, P. Gope, D. Puthal, Blockchain and FL-enabled distributed secure and privacy-preserving computing architecture for iot network, in: 2022 IEEE European Symposium on Security and Privacy Workshops (EuroSPW), 2022, pp. 1–9. doi: 10.1109/EuroSPW55150.2022.00008.

[19] M. Fan, Z. Zhang, Z. Li, G. Sun, H. Yu, M. Guizani, Blockchain-based decentralized and lightweight anonymous authentication for FL, IEEE Transactions on Vehicular Technology 72 (9) (2023) 12075–12086. doi:10.1109/TVT.2023.3265366.

[20] S. Arumugam, S. K. Shandilya, N. Bacanin, FL-based privacy preservation with blockchain assistance in iot 5g heterogeneous networks, Journal of Web Engineering 21 (4) (2022) 1323–1346. doi:10.13052/jwe1540-9589.21414.

[21] M. Guduri, C. Chakraborty, U. V, M. Margala, Blockchain-based FL technique for privacy preservation and security of smart electronic health records, IEEE Transactions on Consumer Electronics PP (2023) 1–1. doi:10.1109/TCE.2023.3315415.

[22] A. P. Kalapaaking, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi, M. Almashor, Blockchain-based FL with secure aggregation in trusted execution environment for internet-of-things, IEEE Transactions on Industrial Informatics 19 (2) (2023) 1703–1714. doi: 10.1109/tii.2022.3170348.

[23] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat, W. Wang, Federated-learning based privacy preservation and fraud-enabled blockchain iomt system for healthcare,6 IEEE Journal of Biomedical and Health Informatics 27 (2) (2023) 664–672. doi:10.1109/JBHI.2022.3165945.

[24] M. Al Asqah, T. Moulahi, FL and blockchain integration for privacy protection in the internet of things: Challenges and solutions, Future Internet 15 (6) (2023).

[25] Z. Qin, J. Ye, J. Meng, B. Lu, L. Wang, Privacy-preserving blockchain-based FL for marine internet of things, IEEE Transactions on Computational Social Systems 9 (1) (2022) 159–173. doi:10.1109/TCSS.2021.3100258.

[26] J. Xu, J. Lin, W. Liang, K.-C. Li, Privacy preserving personalized blockchain reliability prediction via FL in IoT environments, Cluster Comput. 25 (4) (2022) 2515–2526.

[27] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, G. Muhammad, Secure and provenance enhanced internet of health things framework: A blockchain managed FL approach, IEEE Access 8 (2020) 205071–205087. doi:10.1109/ACCESS.2020.3037474.

[28] S. Ji, J. Zhang, Y. Zhang, Z. Han, C. Ma, Lafed: A lightweight authentication mechanism for blockchain-enabled FL system, Future Generation Computer Systems 145 (2023) 56–67. doi:https://doi.org/10.1016/j.future.2023.03.014.

[29] A. Alghamdi, J. Zhu, G. Yin, M. Shorfuzzaman, N. Alsufyani, S. Alyami, S. Biswas, Blockchain empowered FL ecosystem for securing consumer iot features analysis, Sensors 22 (18) (2022). doi:10.3390/s22186786.

[30] B. Biggio et al., "Evasion Attacks against Machine Learning at Test Time," in Lecture notes in computer science, 2013, pp. 387–402. doi: 10.1007/978-3-642-40994-3 25.

[31] J. Kelly and W. Knottenbelt, "The UK-DALE dataset, domestic appliance-level electricity demand and whole-house demand from five UK homes," Scientific Data, vol. 2, no. 1, Mar. 2015, doi: 10.1038/sdata.2015.7.