Dean&Francis

ISSN 2959-6157

Federated Learning Helps Improve IoT Privacy Security

Yiwei Jiang[1], Wenxuan Wang[2] and Chi Zhang[3,*]

[1]Waterford Institution, Nanjing University of Information Science and Technology, Nanjing, China
[2]Institute of Information Science and Technology, Henan University of Technology, Zhengzhou, China
[3]School of Computer Science, Beijing University of Technology, Beijing, China
*Corresponding author: 23070215@emails.bjut.edu.cn

Abstract:

With the rapid development of the Internet of Things (IoT), how to protect users' privacy security in the IoT environment has received extensive attention. Federated learning allows IoT devices to perform local training and only upload model parameters, avoiding the direct transmission of raw data, which provides a new solution for enhancing IoT privacy security. Many studies have tried to integrate federated learning with other technologies to further improve privacy protection. This paper summarizes various technologies used in recent studies to protect privacy security in different IoT scenarios with federated learning, including encryption techniques, secure model aggregation, and the integration of distributed trust mechanisms. In addition, this paper also introduces the applications of federated learning in various IoT scenarios, including industrial IoT, healthcare, and energy management fields. The paper also provides future prospects for research on using federated learning to protect privacy security in the IoT. Furthermore, it explores potential advancements in combining emerging technologies such as blockchain and differential privacy to achieve more efficient and secure privacy protection mechanisms in IoT environments.

Keywords: federated learning, internet-of-things, privacy

1. Introduction

The Internet of Things (IoT) refers to a network of interconnected devices that can exchange information with one another. Given that data is distributed across different devices, the secure and effective implementation of collaborative training empowered by artificial intelligence becomes particularly significant. Federated learning is a distributed machine learning framework that enables collaborative training without requiring the data from different devices to leave their local environments. This characteristic highlights the natural complementarity between the applications of federated learning and the needs of IoT.

Although federated learning provides a layer of privacy protection for the collaborative training of IoT devices, studies indicate that privacy and security risks still exist, such as gradient leakage attacks [1]. Research documented in reference [2] demonstrates that attackers can utilize Generative Adversarial Networks (GANs) to produce a data set similar to that of other participants, subsequently conducting covert data poisoning attacks.

In response, numerous studies have focused on enhancing the security of federated learning within IoT environments. In reference [3], the authors employ Trusted Execution Environments (TEEs) to safeguard sensitive model parameters from leakage. Reference [4] addresses the issue of Byzantine attacks occurring during the application of federated learning in Multi-Task Systems (MTS), proposing the DisBeZant algorithm, which establishes a reputation mechanism to identify Byzantine attackers based on federated learning.

This paper aims to summarize the latest innovative approaches utilizing federated learning to protect privacy and security in IoT environments, as well as their application domains, while also proposing future research directions. The second section primarily discusses the applications of federated learning in various fields of IoT for privacy protection. The third section summarizes the innovative algorithms employed by researchers to safeguard IoT privacy and security. The fourth section concludes the paper and outlines potential future research directions.

2. Overview of Relevant Technologies

2.1 Encryption Technology

Encryption technology ensures the security of data during transmission and storage by transforming it into a format that can only be interpreted by those possessing the key. Its application is particularly critical in the IoT environment, as it protects the data contained in RFID tags from unauthorized reading and modification, effectively preventing illegal access and tampering of data. The implementation of this technology not only enhances the privacy protection of IoT data but also provides a secure framework for data exchange in federated learning. Furthermore, the application of encryption technology involves strict management of access rights within RFID systems, ensuring that only authorized users can access system resources, thereby further safeguarding personal privacy. The role of encryption technology in protecting the privacy of federated learning within IoT environments cannot be overlooked. The most commonly used encryption techniques in IoT environments include transport encryption and homomorphic encryption.

2.1.1 Homomorphic Encryption

Homomorphic encryption is a specialized encryption scheme that allows computations to be performed on encrypted data without the need for decryption. This technology holds significant value in data privacy protection, particularly in the IoT environment, where data processing and privacy preservation are critical issues. With the development and application of IoT, the amount of confidential user information and private data, such as personal profiles and sensitive files, has been increasing. This information often needs to be encrypted before being stored on service providers' servers or processed by them before being returned to the user. Homomorphic encryption ensures that this confidential information remains unknown to others, including the service providers, while allowing for accurate and effective processing of encrypted data and extraction of valuable information, thereby addressing challenges that traditional encryption schemes struggle to overcome.

Although there are concerns regarding the transmission of sensitive data through insecure communication channels, these issues can be mitigated by employing fully homomorphic encryption (FHE). In this context, reference [5] proposes a secure FL method enabled in IoT smart cities, which combines FHE and FL to provide secure data while maintaining privacy in a distributed environment. This approach introduces four FHE methods based on different techniques: OUCM, OECM, MUCM, and MECM, wherein data is encrypted and transmitted over secure channels. In addition to providing robust privacy and security guarantees, this method achieves high accuracy, recall, precision, and F1 scores.

2.1.2 Transmission Encryption

Transport encryption provides additional security assurances for federated learning by ensuring the confidentiality of data during transmission. In the Internet of Things (IoT) environment, data frequently needs to be transmitted between multiple devices or servers, and transport encryption technology can prevent unauthorized third parties from intercepting and interpreting this data. By employing encryption techniques, sensitive information is transformed into a format that only the intended recipient can decrypt, thereby safeguarding the privacy and security of the data.

Trigger-Action Programming (TAP) is a classic user programming paradigm in IoT smart home platforms that allows users to create customized automation rules using remote sensing data to connect IoT devices and network services. To address threats to TAP rules, reference [6] proposes a novel federated learning framework called PFTAP, which introduces a hierarchical graph attention network composed of two modules: an intra-rule attention module and an inter-rule attention module. This framework is capable of learning comprehensive feature representations of triggers and actions. It also establishes a new model based on federated learning that integrates symmetric encryption (a form of transport encryption) and local differential privacy techniques, effectively protecting user privacy from unauthorized access or tampering.

The SecureBoost system, proposed in reference [7], represents an innovative framework in federated learning. In federated learning scenarios, data is typically distributed across multiple participants. To protect data privacy during the sample alignment (entity alignment) process, encryption techniques are employed. The privacy protection mechanism utilizes a secure intersection scheme similar to RSA (an asymmetric encryption algorithm) combined with a hashing mechanism, which can be regarded as a relevant application of asymmetric encryption technology. This scheme facilitates the identification and alignment of common user samples while safeguarding the data privacy of all participants, thus laying the groundwork for subsequent federated modeling.

2.2 Secure Aggregation of Model Parameters

2.2.1 Differential Privacy

Differential privacy is a mathematical framework designed to protect individual data privacy by adding random noise. The core idea is to introduce an appropriate amount of noise to the output results, such that the presence or absence of any single data record has a negligible impact on the final outcome. Specifically, differential privacy defines the concept of “neighboring” datasets, which are datasets that differ by only a single record. By adding random noise to the query results, it ensures that the differences between the outputs of neighboring datasets are controlled within a small range. This difference is typically measured by ε (epsilon), where a smaller ε indicates a higher level of privacy protection. Through differential privacy techniques, researchers or third parties can access processed datasets without exposing the original data, thereby facilitating broader data sharing and collaborative research. Furthermore, differential privacy can be applied in various scenarios such as recommendation systems and market research, ensuring user privacy while providing valuable information.

Decentralized energy management technologies based on communication channels are crucial for the economic operation of modern smart grids. However, the increased information exchange among participants raises the risk of privacy breaches, reduces optimization performance, and may lead to system failures. Reference [8] presents a novel optimized energy management strategy that combines an alternating direction method of multipliers based on decentralized consensus with differential privacy techniques. This strategy aims to address cooperative optimization challenges in microgrids, including conventional generators, energy storage systems, wind turbines, and transmission losses, while ensuring that the information of each participant remains protected from interception by neighboring nodes during the information exchange process. Simulations conducted on the modified IEEE 30-bus system and a simplified IEEE 118-bus system validate the effectiveness of this differential privacy approach in energy management strategies.

2.2.2 Secure Multi-Party Computation

Multi-Party Computation (MPC) is a cryptographic protocol that enables multiple participants to collaboratively execute computational tasks without revealing their individual inputs. The fundamental concept of MPC is to decompose a computational task into several subtasks, where each participant only performs a portion of the computation, ensuring that other participants cannot discern their input data through encryption techniques. Common implementation methods include secret sharing and homomorphic encryption. Secret sharing involves splitting a secret value into multiple shares, which can only reconstruct the original secret when enough shares are combined. Homomorphic encryption allows computations to be performed directly on ciphertexts, thereby preventing data leakage during the decryption process. By utilizing multi-party computation, different organizations can collaboratively train models or perform complex calculations without directly sharing sensitive data. This not only enhances data security but also provides new solutions for inter-organizational collaboration. Furthermore, MPC technology can be applied in various domains such as the Internet of Things and cloud computing, ensuring that data remains highly secure and private during transmission and processing.

References [9] presents a secure federated learning system that uses data fusion and multi-party computation with additive secret sharing to protect gradient parameters rather than actual data, aiming to balance prediction accuracy and data privacy. The model employs a convolutional neural network with an efficient weight-sharing mechanism, where model weights are encrypted. Extensive simulations confirm the model's effectiveness, and security analysis shows resilience against weighted majority voting attacks and other security threats.

2.3 Distributed Trust Mechanism

In the context of the Internet of Things (IoT), the number of intelligent terminals participating in federated learning is significantly large, which increases the likelihood of attacks from malicious participants during the model training process. Malicious participants may provide false model parameter updates, compromising the accuracy and integrity of the model. A distributed trust mechanism can enhance the model's security and reliability by monitoring participant behavior and verifying the authenticity of model parameters, thereby enabling the timely detection and exclusion of malicious participants. One of the most common approaches to integrate federated learning with distributed trust mechanisms in IoT environments is the introduction of blockchain technology and reputation assessment systems.

2.3.1 Blochchain

Federated learning faces significant challenges in ensuring privacy protection during large-scale collaborative training in the Internet of Things (IoT), such as ensuring the reliability of participants and preventing malicious tampering of model parameters. Blockchain technology, with its decentralized, immutable, and traceable characteristics, provides new approaches to address these issues. By combining blockchain with federated learning, a more secure and reliable privacy protection system for the internet can be established.

References [10] proposes a blockchain-based federated learning architecture that balances security and efficiency. This architecture addresses trust issues using the PoFW consensus algorithm and employs a reinforcement learning-based client selection strategy to optimize training efficiency.

References [11] presents an architecture based on federated learning, digital twins, and sharded blockchain. This architecture consists of three layers: the data layer, the blockchain layer, and the digital twin layer. The data layer is responsible for training the federated learning model, while the blockchain verifies updates to local and global models through a hierarchical consensus mechanism. The digital twin layer is used to build and maintain twin models. This architecture has been validated in multiple experiments.

References [12] introduces a blockchain-based federated learning architecture designed for intrusion detection in IoT networks. The architecture can be divided into three layers: the IoT layer, the intelligent aggregation layer, and the blockchain and distributed storage layer. This architecture has demonstrated excellent performance in various network attack detection experiments.

2.3.2 Reputation Assessment System

Establishing a reputation assessment system combined with federated learning in the Internet of Things (IoT) involves evaluating participants based on their historical data, including data quality, contribution level, and adherence to privacy protocols. Devices with higher reputations are assigned greater weights or more resource allocation, while devices with poor reputations may be restricted from participating in training. Many studies have employed reputation assessment systems to further enhance the security of federated learning in IoT environments.

Identifying reliable and trustworthy devices for training is crucial for safeguarding the security of federated learning. To better identify toxic devices, reference [13] measures the trustworthiness of each device using reputation and employs a reinforcement learning-based reputation mechanism to select reliable participants.

To enhance the security of hierarchical federated learning, reference [14] proposes the MADDPG algorithm, which aims to mitigate the negative impact of unreliable clients on the global model by optimizing client selection. Each federated learning terminal server is equipped with a reputation model based on deep reinforcement learning, which is used to select devices with higher trust levels within the cluster. Experimental results demonstrate that this approach improves both the accuracy and stability of hierarchical federated learning.

3. Application Field

3.1 Intelligent Industrial Internet of Things

The Industrial Internet of Things (IIoT) refers to the application of IoT technologies in the industrial sector, where the vast amounts of data generated by devices often contain sensitive information. Federated learning allows devices to perform model training locally, thereby protecting data privacy.

References [15] proposes a secure and efficient parameter aggregation technique that employs a lightweight smart contract consensus based on APOA. This study explores both public and private blockchain networks and utilizes Gaussian differential privacy to safeguard client privacy during the federated learning process.

References [16] introduces a federated learning-based privacy-preserving data aggregation scheme for IoT (FLP-DA). This approach protects the changes to individual user models during federated learning and employs the PBFT consensus algorithm to ensure it does not rely on any centralized entity. By combining a payment-based cryptographic system with secret sharing, it achieves secure data sharing, addresses the data island problem, and effectively protects data privacy against various attacks.

Traditional fault diagnosis methods in the IIoT face privacy risks due to cloud data uploads and struggle with the Non-IID problem in federated learning, which affects global model convergence. Additionally, without a detection mechanism for poisoning attacks from active nodes, incentive mechanisms are needed to encourage resource sharing. Reference [17] introduces a BCE-FL system to tackle these issues, featuring a contrastive loss function to address the Non-IID problem and a Byzantine-tolerant scoring mechanism for detection. An evaluation-based incentive algorithm is also included to promote cooperation among nodes. This approach enhances decentralization, tamper resistance, and auditability, improving the trustworthiness, security, and privacy of IIoT data.

3.2 Intelligent Healthcare

Healthcare is a field that contains a vast amount of sensitive personal information. To diagnose conditions or conduct real-time monitoring of patient data using machine learning, a substantial amount of data is required. The application of federated learning allows for precise lesion analysis while simultaneously protecting privacy.

Training deep networks for fundus screening recognition necessitates large datasets. To address the risk of data leakage during collaborative training across multiple sites, the method proposed in reference [18] incorporates a Gaussian randomization mechanism into federated learning and employs a two-step domain adaptation approach. Tests on multiple fundus screening datasets have validated the effectiveness of this framework.

To safeguard the privacy and security of mobile electronic health record systems, reference [19] presents a framework that combines federated learning with differential privacy and pseudonymization encryption techniques, further enhancing security.

When serverless computing is used to allocate resources to users, the system becomes vulnerable to privacy attacks. Reference [20] introduces the SPEI-FL architecture to address this issue. First, Gaussian noise is added before aggregation to mitigate adversarial attacks. Additionally, this architecture employs a cluster authentication method, requiring each new user to submit their geographic coordinates. Only when the ID value matches the dataset will the user be included; otherwise, they will be treated as an intruder. Testing results on the MNIST digit dataset, structured COVID-19 chest X-ray images, and the structured BoT-IoT dataset demonstrate that SPEI-FL can effectively protect sensitive patient data from disclosure in serverless computing environments.

References [21] proposes an architecture that integrates federated learning with edge analytics and blockchain technology, providing implementation methods and tools for this framework. The various components work in synergy, with the edge analytics component storing data on the blockchain, which offers enhanced security for data analysis in federated learning.

3.3 Intelligent Energy Management

Energy management is a critical issue that urgently needs to be addressed in the field of smart energy. The development of smart grid and IoT technologies has made the monitoring and management of energy systems more efficient and flexible, while also introducing challenges related to data privacy and security. By integrating and analyzing data from various sensors and devices, federated learning can enable more accurate energy demand forecasting, more efficient energy distribution, and more reliable fault detection. Federated learning achieves collaborative optimization of models while protecting data privacy, significantly reducing the risk of data leakage. Furthermore, federated learning can be combined with techniques such as secure multiparty computation and additive secret sharing to enhance system security.

References [22] introduces a blockchain-based authentication-protected data aggregation scheme aimed at balancing the security and computational costs of smart grids. By employing efficient cryptographic algorithms, this scheme seamlessly integrates blockchain technology into the smart grid, facilitating improved decentralization and avoiding the potential threats and high costs associated with centralized systems. The proposed solution demonstrates good scalability, capable of managing a large number of metering devices. Additionally, the introduction of one-time key pairs and signature mechanisms enhances the level of privacy protection in blockchain applications within the smart grid.

References [23] proposes a privacy-preserving data aggregation scheme for fog computing smart grids, aiming to achieve multi-dimensional and multi-subset data aggregation. This method effectively allocates privacy budgets by utilizing the parallel composability of differential privacy, thereby improving the data utility of multi-dimensional data aggregation. In addition, the user's multi-dimensional power consumption data is structured into composite data through the Chinese Remainder Theorem, further reducing computational overhead. Security analysis shows that this scheme can resist differential attacks, eavesdropping attacks, collusion attacks, and active attacks.

4. Conclusion

Due to the large-scale deployment of Internet of Things (IoT) devices, federated learning systems have become ubiquitous. This paper primarily discusses the applications of federated learning in the fields of industrial IoT, healthcare, and energy management, as well as related privacy protection technologies, including encryption techniques, secure model aggregation, and distributed trust mechanisms. While this paper focuses solely on the application of federated learning in IoT from the perspective of privacy security, it is important to note that most IoT devices are resource-constrained and operate under poor communication conditions, which hinders the large-scale deployment of federated learning. Therefore, in addition to further enhancing privacy security, improving the communication efficiency of federated learning training in IoT will be a key area of future research.

Authors Contribution
All the authors contributed equally and their names were listed in alphabetical order.

References

[1] Yang H, Ge M, Xue D, Xiang K, Li H, Lu R. Gradient Leakage Attacks in Federated Learning: Research Frontiers, Taxonomy, and Future Directions. IEEE Network, 2024, 38(2): 247-254.

[2] Hao R, Hussain R, Parra-Ullauri J M, Vasilakos X, Nejabati R, Simeonidou D. GAN-Based Privacy Abuse Attack on Federated Learning in IoT Networks. IEEE INFOCOM 2024 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2024.

[3] Cao Y, Zhang J, Zhao Y, Su P, Huang H. SRFL: A Secure & Robust Federated Learning framework for IoT with trusted execution environments. Expert Systems with Applications, 2024, 239.

[4] Ma X, Jiang Q, Shojafar M, Alazab M, Kumar S, Kumari S. DisBezant: Secure and Robust Federated Learning Against Byzantine Attack in IoT-Enabled MTS. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(2): 2492-2502.

[5] Hijazi N M, Aloqaily M, Guizani M, Ouni B, Karray F. Secure Federated Learning With Fully Homomorphic Encryption for IoT Communications. IEEE Internet of Things Journal, 2024, 11(3): 4289-4300.

[6] Xing Y, Hu L, Du X, Shen Z, Hu J, Wang F. A privacy-preserving federated graph learning framework for threat detection in IoT trigger-action programming. Expert Systems with Applications, 2024, 255, Part C.

[7] Cheng K, et al. SecureBoost: A Lossless Federated Learning Framework. IEEE Intelligent Systems, 2021, 36(6): 87-98.

[8] Zhao D, et al. Differential Privacy Energy Management for Islanded Microgrids With Distributed Consensus-Based ADMM Algorithm. IEEE Transactions on Control Systems Technology, 2023, 31(3): 1018-1031.

[9] Muazu T, Mao Y, Muhammad A U, Ibrahim M, Kumshe U M, Samuel O. A federated learning system with data fusion for healthcare using multi-party computation and additive secret sharing. Computer Communications, 2024, 216: 168-182.

[10] Fang F, et al. BCFL: A Trustworthy and Efficient Federated Learning Framework Based on Blockchain In IoT. 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2024.

[11] Jiang L, Liu Y, Tian H, Tang L, Xie S. Resource-Efficient Federated Learning and DAG Blockchain With Sharding in Digital-Twin-Driven Industrial IoT. IEEE Internet of Things Journal, 2024, 11(10): 17113-17127.

[12] Rashid M M, Choi P, Lee S H, Platos J, Huh Y and Kwon K R. Ensuring Privacy and Security of IoT Networks Utilizing Blockchain and Federated Learning, in 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud), Marrakesh, Morocco, 2023.

[13] Al-Maslamani N M, Ciftler B S, Abdallah M, Mahmoud M M E A. Toward Secure Federated Learning for IoT Using DRL-Enabled Reputation Mechanism. IEEE Internet of Things Journal, 2022, 9(21): 21971-21983.

[14] Al-Maslamani N M, Abdallah M, Ciftler B S. Reputation-Aware Multi-Agent DRL for Secure Hierarchical Federated Learning in IoT. IEEE Open Journal of the Communications Society, 2023, 4: 1274-1284.

[15] Putra M A P, Alief R N, Rachmawati S M, Sampedro G A, Kim D-S, Lee J-M. Proof-of-authority-based secure and efficient aggregation with differential privacy for federated learning in industrial IoT. Internet of Things, 2024, 25.

[16] Fan H, Huang C, Liu Y. Federated Learning-Based Privacy-Preserving Data Aggregation Scheme for IIoT. IEEE Access, 2023, 11: 6700-6707.

[17] Xiao Y, Shao H, Lin J, Huo Z, Liu B. BCE-FL: A Secure and Privacy-Preserving Federated Learning System for Device Fault Diagnosis Under Non-IID Condition in IIoT. IEEE Internet of Things Journal, 2024, 11(8): 14241-14252.

[18] Tang Z, Wong H-S, Yu Z. Privacy-Preserving Federated Learning With Domain Adaptation for Multi-Disease Ocular Disease Recognition. IEEE Journal of Biomedical and Health

Informatics, 2024, 28(6): 3219-3227.

[19] Ganadily N A, Xia H J. Privacy Preserving Machine Learning for Electronic Health Records using Federated Learning and Differential Privacy. ArXiv abs/2406.15962, 2024.

[20] Akter M, Moustafa N, Turnbull B. SPEI-FL: Serverless Privacy Edge Intelligence-Enabled Federated Learning in Smart Healthcare Systems. Cognitive Computing, 2024, 16: 2626-2641.

[21] Badidi E, Lamaazi H, Harrouss O E. Toward a Secure Healthcare Ecosystem: A Convergence of Edge Analytics, Blockchain, and Federated Learning. 2024 20th International Conference on the Design of Reliable Communication Networks (DRCN), 2024.

[22] Lee C-D, Li J-H, Chen T-H. A Blockchain-Enabled Authentication and Conserved Data Aggregation Scheme for Secure Smart Grids. IEEE Access, 2023, 11: 85202-85213.

[23] Zhao S, et al. PPMM-DA: Privacy-Preserving Multidimensional and Multisubset Data Aggregation With Differential Privacy for Fog-Based Smart Grids. IEEE Internet of Things Journal, 2024, 11(4): 6096-6110.