Privacy Protection in Mobile Edge Computing

Subjects: Computer Science, Artificial Intelligence

Contributor: Zhimo Cheng , Xinsheng Ji , Wei You , Yi Bai , Yunjie Chen , Xiaogang Qin

Data sharing and analyzing among different devices in mobile edge computing is valuable for social innovation and development. The limitation to the achievement of this goal is the data privacy risk. Therefore, existing studies mainly focus on enhancing the data privacy-protection capability. On the one hand, direct data leakage is avoided through federated learning by converting raw data into model parameters for transmission. On the other hand, the security of federated learning is further strengthened by privacy-protection techniques to defend against inference attack. However, privacy-protection techniques may reduce the training accuracy of the data while improving the security. Particularly, trading off data security and accuracy is a major challenge in dynamic mobile edge computing scenarios.

mobile edge computing | privacy protection | differential privacy

1. Introduction

With the rise of mobile edge computing (MEC), massive amounts of data are being generated by a wide variety of sensors, controllers and smart devices [1]. In the era of the Internet of Everything, data utilization is key to enabling innovation, driving growth and solving our major challenges [2]. By data mining, researchers can reveal the hidden patterns, trends and correlations. This information helps us make optimal decisions, for instance, the precise diagnosis and treatment of diseases in the medical field, or the optimization of traffic flow and resource allocation in urban planning. Evidently, the integrated utilization of data can bring great value and benefits [3].

However, it is often difficult to derive value from the data of a single user. More user data needs to be involved in the analysis and refinement to get comprehensive information [4]. In traditional centralized machine learning, data is often stored centrally in a centralized server. This leads to the isolated data island effect, i.e., data cannot be fully utilized and shared. Meanwhile, data privacy protection has become a key issue because of the centralization of users' sensitive personal data [5]. Data from mobile devices generally should not be shared with others in mobile edge computing scenarios. Therefore, breaking the isolated data island and ensuring data privacy is a current issue [6].

Federated learning (FL) [7], as a new technology paradigm based on cryptography and machine learning, can achieve information mining without local data. It can unite data distributed in different mobile devices and train them into a unified global model with more comprehensive information. Thus, it solves the problem of isolated data islands. The clients and server interact with data information through the model parameters without sharing the original data, improving their data privacy [8].

However, federated learning also leads to several security and privacy risks [9]. One of the main threats is model inference attack. Although communication is channeled through the model parameters, Zhu et al. [10] revealed that exchanged model parameters may also leak private information about the training data. They demonstrated that the original training data, including image and text data, can be inferred from the gradients. This poses a new challenge for data privacy-preserving techniques based on federated learning.

To address this issue, researchers propose a federated-learning-based privacy-protection scheme, FLPP. Then, researchers build a layered adaptive differential privacy model to dynamically adjust the privacy-protection level in different situations. Finally, researchers design a differential evolutionary algorithm to derive the most suitable privacy-protection policy for achieving the optimal overall performance. The simulation results show that FLPP has an advantage of 8%-34% in overall performance. This demonstrates that the scheme can enable data to be shared securely and accurately.

2. Privacy Protection in Mobile Edge Computing

Existing studies enhance the security of federated learning by combining with a variety of privacy-protection techniques, mainly including homomorphic encryption (HE), secure multi-party computation (SMPC) and differential privacy (DP) [11]. Extensive research demonstrates that the combination of federated learning with these privacy-protection techniques can provide sufficiently strong security.

Fang et al. [12] proposed a multi-party privacy-preserving machine learning framework, named PFMLP, based partially on HE and federated learning. Training accuracy is achieved while also improving the training efficiency. Xu et al. [13] proposed a privacy-protection scheme to apply HE in IoT-FL scenarios, which is highly adaptable with current IoT architectures. Zhang et al. [14] propose a privacy-enhanced federated-learning (PEFL) scheme to protect the gradients over an untrusted server. This is mainly enabled by encrypting participants' local gradients with a Paillier homomorphic cryptosystem. The HE approach can improve the security of federated learning, although it causes a large computation load. This poses a challenge to the limited computability of devices in mobile edge computing scenarios.

Kalapaaking et al. [15] proposed a federated-learning framework that combines SMPC-based aggregation and Encrypted Inference methods. This framework maintains data and model privacy. Houda et al. [16] presented a novel framework, called MiTFed, that allows multiple software defined network (SDN) domains to collaboratively build a global intrusion detection model without sharing their sensitive datasets. The scheme incorporates SMPC techniques to securely aggregate local model updates. Sotthiwat et al. [17] propose to encrypt a critical part of model parameters (gradients) to prevent deep leakage from gradient attacks. Fereidooni et al. [18] present SAFELearn, a generic design for efficient private FL systems that protects against inference attacks. In addition, recent studies [19][20][21] on secret sharing techniques as a kind of SMPC also hopefully enable federated learning and data sharing security. The above studies implement the secure construction of models but cannot afford the communication overhead of a large number of participants.

The differential privacy technique is a good way to avoid the computation load and communication overhead. Wang et al. [22] proposed a collaborative filtering algorithm recommendation system based on federated learning and end–edge–cloud computing. The exposure of private data was further prevented by adding Laplace noise to the training model through DP technology. Wei et al. [23] proposed a novel DP-based framework, NbAFL, in which artificial noise is added to parameters at the clients' side before aggregating. The strategy for achieving the optimal performance and privacy level is performed by selecting the number of clients participating in FL. Zhao et al. [24] propose an anonymous and privacy-preserving federated-learning scheme for the mining of industrial big data, which leverages differential privacy on shared parameters. They also test the effect of different privacy levels on accuracy. Adnan et al. [25] conduct a case study of applying a differentially private federated-learning framework for analysis of histopathology images, the largest and perhaps most complex medical images. Their work indicates that differentially private federated learning is a viable and reliable framework for the collaborative development of machine learning models in medical image analysis. However, the DP privacy level of these works is fixed so it cannot adapt to the dynamically changing sets of participating aggregation clients. In particular, non-IID data distribution with fixed privacy level may slow down the speed of FL model training to reach the anticipated accuracy.

In summary, the DP technique with adjustable privacy levels is clearly more suitable for privacy protection for federated learning in mobile edge computing. To this end, researchers propose FLPP, a privacy-protection scheme based on federated learning to adaptively determine a privacy level strategy, aiming to jointly optimize the accuracy and security of the training model.

References

1. Sun, X.; Ansari, N. EdgeIoT: Mobile Edge Computing for the Internet of Things. IEEE Commun. Mag. 2016, 54, 22–29.
2. Cao, K.; Liu, Y.; Meng, G.; Sun, Q. An Overview on Edge Computing Research. IEEE Access 2020, 8, 85714–85728.
3. Qiu, T.; Chi, J.; Zhou, X.; Ning, Z.; Atiquzzaman, M.; Wu, D.O. Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges. IEEE Commun. Surv. Tutor. 2020, 22, 2462–2488.
4. Leung, C.K.; Deng, D.; Hoi, C.S.H.; Lee, W. Constrained Big Data Mining in an Edge Computing Environment. In Proceedings of the Big Data Applications and Services 2017, Tashkent, Uzbekistan, 15–18 August 2017; Lee, W., Leung, C.K., Eds.; Springer: Singapore, 2019; pp. 61–68.
5. Du, M.; Wang, K.; Chen, Y.; Wang, X.; Sun, Y. Big Data Privacy Preserving in Multi-Access Edge Computing for Heterogeneous Internet of Things. IEEE Commun. Mag. 2018, 56, 62–67.

6. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated Machine Learning: Concept and Applications. ACM Trans. Intell. Syst. Technol. 2019, 10, 1–9.
7. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.Y. Communication-Efficient Learning of Deep Networks from Decentralized Data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, Fort Lauderdale, FL, USA, 20–22 April 2017; Singh, A., Zhu, J., Eds.; PMLR: London, UK, 2017; Volume 54, pp. 1273–1282.
8. Li, Z.; Sharma, V.; Mohanty, S.P. Preserving Data Privacy via Federated Learning: Challenges and Solutions. IEEE Consum. Electron. Mag. 2020, 9, 8–16.
9. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. Future Gener. Comput. Syst. 2021, 115, 619–640.
10. Zhu, L.; Liu, Z.; Han, S. Deep leakage from gradients. Adv. Neural Inf. Process. Syst. 2019, 32.
11. Li, T.; Sahu, A.K.; Talwalkar, A.; Smith, V. Federated Learning: Challenges, Methods, and Future Directions. IEEE Signal Process. Mag. 2020, 37, 50–60.
12. Fang, H.; Qian, Q. Privacy preserving machine learning with homomorphic encryption and federated learning. Future Internet 2021, 13, 94.
13. Xu, Y.; Mao, Y.; Li, S.; Li, J.; Chen, X. Privacy-Preserving Federal Learning Chain for Internet of Things. IEEE Internet Things J. 2023, 10, 18364–18374.
14. Zhang, J.; Chen, B.; Yu, S.; Deng, H. PEFL: A Privacy-Enhanced Federated Learning Scheme for Big Data Analytics. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
15. Kalapaaking, A.P.; Stephanie, V.; Khalil, I.; Atiquzzaman, M.; Yi, X.; Almashor, M. SMPC-Based Federated Learning for 6G-Enabled Internet of Medical Things. IEEE Netw. 2022, 36, 182–189.
16. Abou El Houda, Z.; Hafid, A.S.; Khoukhi, L. Mitfed: A privacy preserving collaborative network attack mitigation framework based on federated learning using sdn and blockchain. IEEE Trans. Netw. Sci. Eng. 2023, 10, 1985–2001.
17. Sotthiwat, E.; Zhen, L.; Li, Z.; Zhang, C. Partially Encrypted Multi-Party Computation for Federated Learning. In Proceedings of the 2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid), Melbourne, Australia, 10–13 May 2021; pp. 828–835.
18. Fereidooni, H.; Marchal, S.; Miettinen, M.; Mirhoseini, A.; Möllering, H.; Nguyen, T.D.; Rieger, P.; Sadeghi, A.R.; Schneider, T.; Yalame, H.; et al. SAFELearn: Secure Aggregation for private FEderated Learning. In Proceedings of the 2021 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 27 May 2021; pp. 56–62.

19. Galletta, A.; Taheri, J.; Celesti, A.; Fazio, M.; Villari, M. Investigating the Applicability of Nested Secret Share for Drone Fleet Photo Storage. IEEE Trans. Mob. Comput. 2023, 1–13.
20. Galletta, A.; Taheri, J.; Villari, M. On the Applicability of Secret Share Algorithms for Saving Data on IoT, Edge and Cloud Devices. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 14–21.
21. Galletta, A.; Taheri, J.; Fazio, M.; Celesti, A.; Villari, M. Overcoming security limitations of Secret Share techniques: The Nested Secret Share. In Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 20–22 October 2021; pp. 289–296.
22. Wang, Y.; Tian, Y.; Yin, X.; Hei, X. A trusted recommendation scheme for privacy protection based on federated learning. CCF Trans. Netw. 2020, 3, 218–228.
23. Wei, K.; Li, J.; Ding, M.; Ma, C.; Yang, H.H.; Farokhi, F.; Jin, S.; Quek, T.Q.S.; Vincent Poor, H. Federated Learning with Differential Privacy: Algorithms and Performance Analysis. IEEE Trans. Inf. Forensics Secur. 2020, 15, 3454–3469.
24. Zhao, B.; Fan, K.; Yang, K.; Wang, Z.; Li, H.; Yang, Y. Anonymous and Privacy-Preserving Federated Learning With Industrial Big Data. IEEE Trans. Ind. Inform. 2021, 17, 6314–6323.
25. Adnan, M.; Kalra, S.; Cresswell, J.C.; Taylor, G.W.; Tizhoosh, H.R. Federated learning and differential privacy for medical image analysis. Sci. Rep. 2022, 12, 1953.

Retrieved from https://encyclopedia.pub/entry/history/show/119807