International Journal of Advanced Multidisciplinary Research and Innovation

E-ISSN: 3107-6157 editor@ijamri.com

Volume 1, Issue 1, March-April 2025

A Review of Federated Learning: Privacy-Preserving Techniques and Real-World Applications

Payal Joshi

Sankalchand Patel College of Engineering, Visnagar, Gujarat

Abstract

The process of Federated learning (FL) allows different devices to jointly create a model through collaboration without exchanging training information. FL protects diversified applications from sensitive data leakage through mechanics including differential privacy and homomorphic encryption and secure multi-party computation which meet privacy legislation. FL serves diverse healthcare and financial sectors as well as IoT operations alongside edge computing applications because it keeps sensitive information within individual devices. As much as FL provides benefits its implementation faces three main challenges related to communication overhead and non-IID data distributions together with security vulnerabilities.

Keywords: Federated Learning, Privacy-Preserving Machine Learning, Secure Multi-Party Computation, Differential Privacy, Decentralized AI

1. Introduction

Federated Learning serves as a distributed training method which enables numerous participants to build models in a collaborative fashion without disclosing their raw information data while achieving security and communication expense benefits. The techniques like differential privacy as well as secure multiparty computation combined with homomorphic encryption and trusted execution environment allow FL to minimize data breach risks and regulatory non-compliance. FL demonstrates practical usage in medical facilities, banking services and edge data processing applications since these domains require data storage at device source locations. FL enables hospitals to generate models together while keeping patient data private yet permits finance organizations to develop better fraud detection through secure institutional data sharing. FL operates in mobile applications to deliver personalized features through direct user data storage across the mobile devices [1]. Although federated learning holds great promise, several challenges still exist such as communication overhead, the relatively small number of devices globally, non-IID data distributions, and security vulnerabilities including the risk of poisoning in the network. Current research is still developing methods to improve privacy-preserving approaches as well as explore new approaches for scaling ML to heterogeneous networks in more practical settings.

2. Literature review

Federated learning (FL) is a novel AI training methodology that has prioritized privacy by performing collaborative training across devices (or organizations) in a manner where raw data never leaves the owner,

International Journal of Advanced Multidisciplinary Research and Innovation
E-ISSN: 3107-6157 editor@ijamri.com
Volume 1, Issue 1, March-April 2025

thus minimizing exposure of sensitive information. Some fields still have tight security controls around sensitive information such as healthcare and finance, and know well the importance of privacy-preserving techniques, so they have begun to put forward technical implementations of technologies such as differential privacy (DP), secure multi-party computation (SMPC), and homomorphic encryption [2]. DP performs randomization of the updates by adding noise to the model updates before sending it to the server so it is not even possible to distinguish an individual data point in the updates, SMPC comprises of both secret sharing and secure aggregation where the model update is stored in an encrypted manner using both secret sharing and secure aggregation techniques. Harden privacy in federated setting by allowing computation to be performed on encrypted data without decryption which is known as homomorphic encryption. The applications for FL are real, with FL for healthcare, enabling hospitals to collaboratively learn a diagnostic model to detect diseases, without the need for access to each other's patient records; FL for finance, allowing banks to jointly train a fraud detection model on their local transaction data, without the need to exchange that data; and FL for IoT/smart devices, such as Google Gboard, which learns to improve predictive text by learning directly on the device from its users, without having access to the users' typed data [3]. FL further enables autonomous driving by allowing cars to learn from distributed sensors while keeping driver data private. But they have problems, such as heterogeneous data, security threats including model poisoning, and communication overhead, which require advanced aggregation methods, Byzantine resistance algorithms, and efficient synchronization protocols. The research activities to improve FL scalability, to develop better trade-offs between privacy and utility, and to standardize FL frameworks for widespread adoption will continue in the future, with the evolution of adaptive DP and lightweight homomorphic encryption extending the scalability boundaries of FL to tackle new applications with more powerful computation and communication limitations. FL effectively balances the expanding potential of AI with the need for ethical and privacy respecting data use by decentralizing data processing and by layering privacy protective mechanisms on top of one another, opening the door to new collaborative AI ecosystems.

Research gaps in federated learning (FL) are significant challenges that need to be solved by researchers in these FL fields to advance the FL fields. A large gap appears in the area of combating data poisoning attacks since the current works in both detecting and prevention of adversarial threats in FL are very few, especially in the big data context. More importantly, there exists the high variability of data types from clients, resulting an inconsistency in model performances, but tailored aggregation for heterogeneous datasets is still not very well-investigated in the literature [4]. Apart from that, FL needs to rely on some of the least powerful devices (or worse, the least available) which requires more use of successfully optimized frameworks that can benefit from stronger efficiency but in an adaptive way, rather than forcing challenging, and often cumbersome, accuracy trade-offs. Though FL provides a level of privacy by default, current encryption and secure multi-party computation techniques are not capable of complete information leakage free learning. Furthermore, the model complexity of FL models and their suitability for different environments still need thorough exploration to enable smooth deployment, especially in resource-constrained environments. Although there are theoretical improvements in FL, its deployment is constrained for various reasons including limited collaboration from several parties (stakeholders) and investment on information technology (IT) infrastructure and records management particularly in domain such as healthcare [5]. By mitigating these research gaps, FL will emerge as secure, efficient, and pragmatic for a variety of industries, while preserving data privacy and integrity.

International Journal of Advanced Multidisciplinary Research and Innovation
E-ISSN: 3107-6157 editor@ijamri.com
Volume 1, Issue 1, March-April 2025

3. Method

This study employs a systematic approach to assess federated learning (FL) in terms of privacy-preserving methods and practical use cases. Using keywords such as "Federated Learning," "Privacy-Preserving Machine Learning," "Secure Multi-Party Computation," and "Differential Privacy in FL," relevant research papers, conference proceedings, and industry reports from IEEE Xplore, ACM Digital Library, Springer, and arXiv were reviewed. Over Articles published from 2019 to 2024 starting from the most recent paper were considered to vacant the gap because of new advances. Recent advances in centralized machine learning. We favoured papers reporting experimental evaluation, specifically case studies and comparative assessments of FL privacy mechanisms to enable us to carry out a comprehensive review of state-of-the-art FL privacy techniques and challenges.

4. Analysis and discussion

Federated learning (FL) is an emerging machine learning paradigm that allows devices to collaboratively train a model without requiring them to share their raw data, which preserves the privacy of their users and reduce resource consumption. The paper presents a detailed overview of the recent FL developments, approaches, applications, and challenges in different domains, and investigates the major challenges model heterogeneity, non-IIDness, communication, security, privacy, regulation, and fairness in more detail [6]. The expansion of Internet of Things (IoT)-connected devices has resulted in enormous quantities of edge data, wherein bandwidth constraints and privacy concerns make central processing infeasible, yet traditional cloud-centric paradigms cannot cope with the ensuing delay or privacy violations, nor provide scalability. FL eliminates those problems as it enables distributed learning without sharing the actual data, which makes it key for applications with restrictions on data sharing (privacy-sensitive use cases), low-bandwidth scenarios, and collaborative machine learning. However, FL has its own set of challenges such as privacy and security issue, extraordinarily need rigorous encryption and privacy-preserving techniques to prevent any unauthorized access or data breach, device heterogeneity that impact model accuracy, and also dealing with non-IID data, where having variations in distributions of data across clients poses a challenge in training a globally performant model. Second, the complexity of communication impedes the FL from being adopted, as network reliability, bandwidth, and communication inefficiencies lead to slower training and higher costs. FL has been successfully applied in diverse domains such as healthcare, where it allows joint model training on decentralized inputs while keeping patient data private for disease recognition and patient death prediction, agriculture, where it uses farm data and sensor data for precision agriculture and resource allotment, and education, where it applies student privacy preserving, personalized learning, resource distribution and teacher training practices [7]. In summary, FL is revolutionizing industries hindered by data privacy challenges by allowing secure sharing of data and accessing of models without exposing any sensitive information. This review describes the basic concepts, technology frameworks, state-of-the-art challenges, and applications of FL for key sectors including healthcare, agriculture, finance, and education, while identifying possible future directions by overviewing approaches to enhance FL methods, security and limitations to provide land maps for future advancements in FL and apposite fields.

5. Conclusion and recommendations

Federated learning (FL) is a novel paradigm for collaborative machine learning, allowing dynamic and secure distributed model training from data without the need to exchange raw data across data source.

While very powerful, FL still suffers from a few issues like privacy and security flaws, communication difficulties, differences in device types and how they work and other hard situations of non-IID data which degrade both the performance and scalability of models in FL. Solution of these challenges depends on strong encryption methods, high-performance model aggregation algorithms, and optimal communication methods to reduce computation cost with accuracy preservation. Moreover, future works should also attempt to design adaptive FL frameworks for different practical applications such as healthcare, finance, agriculture, and education keeping the heterogeneities of working conditions and resource limitations of the FL platforms in mind. Good work on improvement measures of security and especially efficiency of FL security and efficiency, could also explore advanced techniques — differential privacy, secure multi-party computation, and so on, or blockchain. However, that being said to translate theory into practice would require industry collaborations to build better regulations to guide deploying FL in a responsible and ethical manner. Overall, these challenges and more are being explored as FL can be better optimized for privacy, scalability, and efficiency to be a practical solution for a plethora of decentralized learning applications as we move forward in the near future with ethical and secure AI.

6. References

1. Chronis, C., Varlamis, I., Himeur, Y., Sayed, A.N., Al-Hasan, T.M., Nhlabatsi, A., Bensaali, F. and Dimitrakopoulos, G., 2024. A survey on the use of federated learning in privacy-preserving recommender systems. *IEEE Open Journal of the Computer Society*.
2. Aggarwal, M., Khullar, V. and Goyal, N., 2024. A comprehensive review of federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training. *Applied Data Science and Smart Systems*, pp.570-575.
3. Liu, Z., Guo, J., Yang, W., Fan, J., Lam, K.Y. and Zhao, J., 2022. Privacy-preserving aggregation in federated learning: A survey. *IEEE Transactions on Big Data*.
4. Hiwale, M., Walambe, R., Potdar, V. and Kotecha, K., 2023. A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. *Healthcare Analytics*, *3*, p.100192.
5. Koutsoubis, N., Waqas, A., Yilmaz, Y., Ramachandran, R.P., Schabath, M. and Rasool, G., 2024. Future-Proofing Medical Imaging with Privacy-Preserving Federated Learning and Uncertainty Quantification: A Review. *arXiv preprint arXiv:2409.16340*.
6. Jin, W., Yao, Y., Han, S., Gu, J., Joe-Wong, C., Ravi, S., Avestimehr, S. and He, C., 2023. FedML-HE: An efficient homomorphic-encryption-based privacy-preserving federated learning system. *arXiv preprint arXiv:2303.10837*.
7. Smahi, A., Li, H., Yang, Y., Yang, X., Lu, P., Zhong, Y. and Liu, C., 2023. BV-ICVs: A privacy-preserving and verifiable federated learning framework for V2X environments using blockchain and zkSNARKs. *Journal of King Saud University-Computer and Information Sciences*, *35*(6), p.101542.