An Enhanced Survey on Privacy Preservation Strategies in Federated Learning: Techniques, Challenges, and Future Directions

Raushan Kumar
MTech Scholar, CSE Department NRI Bhopal
rsinha203200@gmail.com

Prof. Anurag Shrivastava
Asso. Professor, CSE Department NRI Bhopal
anurag.shri08@gmail.com

Abstract: Federated Learning (FL) has emerged as a powerful approach that enables collaborative model training across decentralized devices while preserving data privacy. However, despite its advantages, FL remains vulnerable to privacy breaches, model inversion attacks, and communication inefficiencies. This study presents an enhanced survey on privacy preservation strategies in federated learning, exploring state-of-the-art techniques such as differential privacy, homomorphic encryption, secure multi-party computation, and blockchain integration. The paper systematically examines their effectiveness, trade-offs, and applicability in various domains. Additionally, it highlights key challenges, including scalability, computation overhead, and trust management among clients. Finally, future research directions are discussed to strengthen the privacy and efficiency of federated learning systems, contributing to the development of secure and trustworthy artificial intelligence.

Keywords— ***Federated Learning, Privacy Preservation, Differential Privacy, Secure Multiparty Computation, Homomorphic Encryption***

I. INTRODUCTION

Federated Learning (FL) has rapidly gained attention as an innovative approach to training machine learning models across decentralized data sources. Unlike traditional centralized training methods, federated learning enables multiple clients, such as mobile devices or organizations, to collaboratively learn a shared model while keeping their data locally stored. This decentralized nature inherently addresses some privacy concerns by preventing the need to transfer raw data to a central server [1]. However, federated learning is not immune to privacy threats. The exchange of model updates during the training process can still leak sensitive information, necessitating robust privacy preservation strategies [2]. This paper aims to survey the current techniques and trends in privacy preservation within federated learning. We delve into various strategies that have been developed to enhance privacy in FL, including differential privacy, which introduces noise to model updates to obscure individual data contributions, and secure multiparty computation, which enables collaborative computation without revealing individual inputs. Homomorphic encryption, another powerful tool, allows computations on encrypted data, thus ensuring data privacy even during the processing stages [3].

Despite these advancements, the implementation of privacy-preserving techniques in federated learning poses several challenges. Scalability, communication overhead, and the delicate balance between privacy and model accuracy are critical issues that need to be addressed to make these methods viable for real-world applications [4]. Moreover, as the deployment of FL expands across diverse domains such as healthcare, finance, and the Internet of Things (IoT), the demand for robust and efficient privacy solutions intensifies. This survey provides a comprehensive overview of the state-of-the-art privacy preservation techniques in federated learning, categorizing and analyzing the strengths and limitations of each approach. By identifying the current trends and pinpointing areas for future research, this paper aims to guide researchers and practitioners in developing more secure and effective federated learning systems [5].

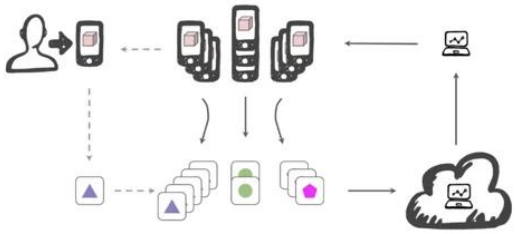

Figure 1. Federated Learning & Privacy Preserving

The paper also explores emerging trends such as hybrid approaches that combine multiple privacy-preserving techniques to leverage their respective strengths. Additionally, it discusses the application-specific challenges and solutions, highlighting case studies from various industries to illustrate practical implementations [5]. By providing a thorough examination of these strategies and their implications, this survey aims to bridge the gap between theoretical research and practical deployment, ensuring that federated learning can be safely and effectively used in privacy-sensitive environments. Ultimately, this survey serves as a valuable resource for advancing the field of privacy-preserving federated learning [6].

II. LITRETURE REVIEW

The literature survey provides an extensive review of existing research on privacy preservation in federated learning, examining a range of techniques such as differential privacy, secure multiparty computation, and homomorphic encryption. It highlights the strengths and limitations of these methods, offering insights into their practical applicability and performance. Additionally, the survey identifies emerging trends and key challenges, setting the stage for future advancements in the field.

This paper [1] presents a privacy-preserving federated learning framework specifically designed for resource-constrained mobile health and wearable IoT devices. The proposed framework effectively addresses key challenges such as limited computation power, communication bandwidth, and energy efficiency in edge environments. Furthermore, the study implements and evaluates the framework on Amazon AWS cloud infrastructure, using a seizure detection application for epilepsy monitoring as a case study.

Author [2] proposed a framework function with arbitrary types of input features that emphasize its usability with natural language data. The text input on the client-side is encoded using a rolling hash-based representation, which provides a combined solution for the high resource demands of embedding algorithms and the privacy concerns of sharing sensitive data. Authors evaluate method in a sentiment analysis task using the IMDB Movie Reviews dataset as well as a rating prediction task with the Movie Lens dataset augmented with additional movie keywords.

In this work [3] is dedicated to surveying state-of-the-art privacy-preservation techniques in FL in relations with GDPR requirements. Furthermore, insights into the existing challenges are examined along with the prospective approaches following the GDPR regulatory guidelines that FL-based systems shall implement to fully comply with the GDPR.

In [4] results suggest that proposed algorithms are an effective method of implementing differential privacy with federated learning, and clinical data scientists can use our general framework to produce differentially private models on federated datasets.

In [5] conduct a detailed study on FL, the categorization of FL, the challenges of FL, and various attacks that can be executed to disclose the users' sensitive data used during learning. In this survey, authors review and compare different privacy solutions for FL to prevent data leakage and discuss secret sharing (SS)-based security solutions for FL proposed by various researchers in concise form. Authors also briefly discuss quantum federated learning (QFL) and privacy-preservation techniques in QFL.

In this [6] paper, we reiterate the concept of federated learning and propose secure federated learning (SFL), where the goal is to build trustworthy and safe AI with strong privacy-preserving and IP-right-preserving. We provide a prehensive overview of existing works, including threats, attacks, and defenses in each phase of SFL from the lifecycle perspective.

The paper [7] presents a novel privacy-preserving federated learning solution, PPFL-LQDP that addresses the issue of excessive participation of low-quality data in Federated training. By constructing a composite evaluation value for the data, the negative impact of low-quality data on Federated training is reduced, while ensuring privacy and security of participant data through a secure framework.

Author's [8] prevent patient privacy compromise while promoting scientific research on large datasets that aims to improve patient care, the implementation of technical solutions to simultaneously address the demands for data protection and utilization is mandatory. Here we present an overview of current and next-generation methods for federated, secure and privacy-preserving artificial intelligence with a focus on medical imaging applications, alongside potential attack vectors and future prospects in medical imaging and beyond.

III. FINDINGS OF THE SURVEY

The comprehensive survey of privacy preservation strategies in federated learning reveals several key findings:

Effectiveness of Differential Privacy (DP): Differential privacy is widely adopted due to its strong theoretical guarantees of privacy. The addition of noise to model updates effectively obscures individual data contributions. However, a trade-off exists between privacy and model accuracy, with higher levels of noise potentially degrading performance.

Utility of Secure Multiparty Computation (SMC): Secure multiparty computation has proven effective for secure aggregation in federated learning. SMC enables multiple parties to collaboratively compute model updates without revealing individual data points. While SMC provides robust privacy guarantees, its computational complexity and overhead communication can be significant, posing challenges for large-scale implementations.

Advancements in Homomorphic Encryption (HE): Homomorphic encryption allows computations on encrypted data, ensuring data privacy throughout the training process. While HE offers strong privacy protection, it is computationally intensive and can introduce significant latency. Recent advancements have focused on optimizing HE for practical use in federated learning, though scalability remains an issue.

Emergence of Hybrid Approaches: Combining multiple privacy-preserving techniques, such as differential privacy and secure multiparty computation, has shown promise in enhancing privacy without severely impacting model performance. Hybrid approaches leverage the strengths of individual methods to achieve a better balance between privacy, efficiency, and accuracy.

Scalability and Communication Overhead: A recurring challenge across all privacy-preserving techniques is scalability. Federated learning systems need to efficiently handle large numbers of participants and substantial communication overhead. Optimizing communication protocols and reducing the computational burden of privacy-preserving methods are critical areas for future research.

Domain-Specific Challenges: The application of federated learning in various domains, such as healthcare, finance, and IoT, presents unique challenges. Privacy-preserving techniques must be tailored to address the specific requirements and constraints of each domain. For instance, healthcare applications demand stringent privacy guarantees due to the sensitivity of medical data, while IoT applications require efficient solutions that can operate on resource-constrained devices.

The survey identifies several key areas for future research, including the development of more efficient and scalable privacy-preserving techniques, the exploration of novel hybrid approaches, and the adaptation of existing methods to domain-specific challenges. Additionally, there is a need for standardized benchmarks and datasets to evaluate performance, and privacy guarantees different approaches in federated learning.

Overall, the survey highlights significant progress in privacy preservation for federated learning, while also emphasizing the need for continued research to address the remaining challenges and enhance the applicability of federated learning in privacy-sensitive environments.

CONCLUSION

This survey provides a comprehensive overview of current privacy preservation strategies in federated learning, highlighting the significant advancements and ongoing challenges in the field. Differential privacy, secure multiparty computation, and homomorphic encryption emerge as key techniques, each offering unique strengths and facing specific limitations. The adoption of hybrid approaches demonstrates promising results in balancing privacy and model performance, yet scalability and communication overhead remain critical hurdles. Additionally, domain-specific challenges necessitate tailored solutions to meet the unique privacy requirements of various applications, such as healthcare and IoT. Despite substantial progress, the field requires further research to develop more efficient, scalable, and practical privacy-preserving techniques. The future of federated learning depends on overcoming these obstacles to ensure robust privacy protection while maintaining high model accuracy and operational efficiency. Standardized benchmarks and datasets are essential for evaluating and comparing different methods, guiding the development of advanced solutions. This survey serves as a valuable resource for researchers and practitioners, offering insights and direction for future advancements in privacy-preserving federated learning.

REFERENCES

[1] Amin Aminifar et. Al. “Privacy-preserving edge federated learning for intelligent mobile-health systems” https://doi.org/10.1016/j.future.2024.07.035 , Elsevier 2024

[1] Balázs Nagy et al.” Privacy-preserving Federated Learning and its application to natural language processing” https://doi.org/10.1016/j.knosys.2023.110475 Published by Elsevier 2023

[2] Nguyen Truong et. al. “Privacy preservation in federated learning: An insightful survey from the GDPR perspective” https:// doi.org/10.1016/j.cose.2021.102402 Elsevier Ltd 2021

[3] Amol Khanna et al “Privacy-preserving Model Training for Disease Prediction Using Federated Learning with Differential Privacy” 2022 44th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC) Scottish Event Campus, Glasgow, UK, July 11-15, 2022

[4] Sanchita Saha1, “A multifaceted survey on privacy preservation of federated learning: progress, challenges, and opportunities” Artificial Intelligence Review (2024) 57:184 https://doi.org/10.1007/s10462-024-10766-7, 2024

[5] Qiang Yang et al “Federated Learning with Privacy-preserving and Model IP-right-protection” 20(1), February 2023, 19-37 DOI: 10.1007/s11633-022-1343-2 www.mi-research.net

[6] Huiyong Wang1, et. al. “Privacy‑preserving federated learning based on partial low‑quality data” Wang et al. Journal of Cloud Computing (2024) 13:62 https://doi.org/10.1186/s13677-024-00618-8

[7] Georgios A. Kaissis et. al. “Secure, privacy-preserving and federated machine learning in medical imaging” Nature Machine Intelligence | VOL 2 | June 2020 | 305–311 | www.nature.com/natmachintell

[8] Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: Concept and applications, ACM Trans. Intell. Syst. Technol. 10 (2) (2019) 1–19, http://dx.doi.org/10.1145/3298981.

[9] Q. Xia, W. Ye, Z. Tao, J. Wu, Q. Li, A survey of federated learning for edge computing: Research problems and solutions, High-Confi. Comput. (2021) 100008, http://dx.doi.org/10.1016/j.hcc.2021.100008.

[10] M. Aledhari, R. Razzak, R.M. Parizi, F. Saeed, Federated learning: A survey on enabling technologies, protocols, and applications, IEEE Access 8 (2020) 140699–140725, http://dx.doi.org/10.1109/ACCESS.2020.3013541.

[11] Z. Li, Z. Huang, C. Chen, C. Hong, Quantification of the leakage in federated learning, 2020, arXiv:1910.05467.

[12] A. Wainakh, F. Ventola, T.M. ig, J. Keim, C.G. Cordero, E. Zimmer, T. Grube, K. Kersting, M. Mühlhäuser, User label leakage from gradients in federated learning, 2021, arXiv:2105.09369.

[13] S.P. Kasiviswanathan, H.K. Lee, K. Nissim, S. Raskhodnikova, A. Smith, What can we learn privately? SIAM J. Comput. 40 (3) (2011) 793–826, http://dx.doi.org/10.1137/090756090.

[14] X. Xiong, S. Liu, D. Li, Z. Cai, X. Niu, A comprehensive survey on local differential privacy, in: A.M. Del Rey (Ed.), Secur. Commun. Netw. 2020 1–29, http://dx.doi.org/10.1155/2020/8829523.

[15] L. Sun, J. Qian, X. Chen, P.S. Yu, LDP-FL: Practical private aggregation in federated learning with local differential privacy, 2020, arXiv: 2007 15789.