IJCR
International
Journal of
Convergent
Research

International Journal of Convergent Research

Journal homepage: International Journal of Convergent Research

Federated Learning: A Potentially Effective Method for Improving the Efficiency and Privacy of Machine Learning

Nishant Jakhar, Sajjan Singh *

Om Sterling Global University, Hisar, India

***Corresponding Author:** sajjansingh72277@gmail.com

Citation: Jakhar, N. & Singh, S. (2024). Federated Learning: A Potentially Effective Method for Improving the Efficiency and Privacy of Machine Learning. *International Journal of Convergent Research*, 1(1), 50-56.

ARTICLE INFO

Received: 27th August 2024
Accepted: 5th November 2024

ABSTRACT

A new AI paradigm called federated learning (FL) decentralizes data and enhances privacy by delivering education straight to the user's device. However, additional privacy concerns arose during the exchange and training of server and client parameters. Integrating FL privacy solutions at the edge level can result in higher computational and communication costs, which can compromise learning performance metrics and data value. To promote the best trade-offs among FL privateness and different performance-associated application needs, including precision, privation, convergency, value, computational protection and connection, this study offers a thorough research overview of key techniques and metrics. Reaching stability among privateness and different standards of factual-international Federated Learning utilization is the focus of this paper, which also explores quantitative methodologies for evaluating privacy in FL. To mitigate server-related risks, decentralized federated learning removes the server from the network and uses blockchain technology to compensate for its loss. However, this benefit comes at the expense of exposing the system to additional privacy risks. An extensive safety study is required in this new paradigm. This survey examines various security mechanisms and addresses potential adversaries and dangers in decentralized federated learning. The verifiability and trustworthiness of decentralized federated learning are also considered.

Keywords: Federated learning, privacy, security, blocking, adversarial attack, decentralized learning federation, approved federal training.

INTRODUCTION

Since personal data is used so widely, Data analysis and administration have improved thanks to centralized machine learning (ML) techniques across a range of sectors, but they have also raised privacy. The General Data Protection Regulation's (GDPR) objective is to provide individuals with greater control over their data and to safeguard their right to privacy. Federated Learning (FL) ensures privacy and security while offering GDPR-compliant solutions by using edge servers or user models for direct ML model training. Because FL enables healthcare organizations to train models with patient data while protecting sensitive information, it has attracted interest in the finance, healthcare, and Internet of Things (IoT) industries.

However, FL faces challenges in communicating model update parameters that can be accessed and analyzed by adversaries. This study reviews the most recent FL systems' privacy-preserving methods and examines how they affect associated operational needs. Existing research offers limited insight into the dimensions and methods of privacy assessment, creating a sizable void in the body of recent work. The study offers a thorough classification of the most modern privacy-preserving techniques in FL into four primary groups: hybrids, blocking, interference, and encryption. A detailed analysis of the body of current literature revealed that there are no generally accepted metrics or methods for evaluating privacy in FL. This work is the first thorough examination of the trade-off between privacy safeguards and operational concerns linked to performance in FL systems.

LITERATURE REVIEW

Joint learning, often known as federated learning (FL), is an algorithmic method that uses many separate, independent sessions, each with its database, to train an algorithm. FL takes care of standardized data sources, access rights, security, and privacy of data. Google first presented the local model update as a distributed learning model that was shared between mobile devices and a core server. It generates a general machine-learning version using the server by combining these local model changes. FL training involves three steps: broadcasting an initial global model, assigning it to selected participants, using local data to determine local model parameters from each participant and updating local parameters.

There are three types of data segmentation in machine learning (FL): vertical, horizontal, and FL. A unique FL configuration called horizontal FL is one where individuals working in a certain zone have varying illustrative data. A static FL database refers to a configuration that contains the same instances or users but has different characteristics. Instead of sharing data, federated transfer learning is utilized to address data gaps.

Numerous elements, including network connection and pricing status, influence customer decisions in Florida. However, this approach has its drawbacks, especially if the client's situation is different, which involves more training time. Numerous studies have put forth methods to address this problem, such as the launch of a recently developed Federated Learning procedure called FedCS. Improving the effectiveness of ML training, FedCS sets time constraints for users to access, sync, and improve Machine Learning versions.

The summarization algorithm is important in FL because it contributes to the global model's update. Building aggregation algorithms in the FL environment may be done in a variety of ways, based on the objectives, which could include protecting confidentiality, accelerating confluence, and reducing the risk caused by anomalous updates.

The FL approach has been popular for developing collaborative models that meet legal specifications regarding user privacy. Early scientists and inventors used FL in experimental and practical applications in medical systems, healthcare, and in the fight against infectious diseases such as COVID-19, managing Electronic Health Records (EHR), and developing the foundations of federated drug discovery.

METHODOLOGY

This paper examines strategies and standards that help achieve the best possible Federated Learning isolation and other operational production goals that should be balanced using the systematic literature review (SLR) method. The objective of this study is to highlight barriers, open questions, and future directions for FL privacy research.

The first stage of SLR is defining the research question and three primary RQs are addressed. ACM DL (Digital Library), Scopus and IEEE Xplorer were just some of the search engines and databases that were searched as part of the search strategy and procedure. Two search strings A and B are chosen to match the range of RQ.

The screening phase involves several steps, including removing many papers, reviewing abstracts, applying inclusion and exclusion criteria, and examining the remaining publications in their entirety to weed out those that don't relate to any of the research questions. Following the completion of the search, the chosen papers were assessed using a quality evaluation system. Among the requirements for admission are papers for peer-reviewed research that have been published in books, reviews, SLR papers, journals, and proceedings from respectable international conferences. Papers free of privacy mechanisms and ArXiv2 publications referenced by peer-reviewed articles published in primary sources are additional requirements under the FL framework that are not written in English and were one of the exclusion criteria or not available in the FL context, which did not address privacy mechanisms.

A quality assessment scheme is used to evaluate papers, scoring them based on three criteria: QC1(Citation rate): Data privacy protection is essential at FL. Techniques like secure multiparty computation and differential privacy were assessed.

QC2(Methodological contribution): FL requires regular connections between local devices and a central server. Reducing communication overhead is essential. Methods such as sparse updating and model compression have been investigated.

QC3: Providing a logical and comprehensible explanation of the results. Federated Averaging is one of the often-utilized techniques (FedAvg)

algorithm, which determines the weighted average of local model updates.

$$w_{t+1}=\sum_{K=1}^{K} \frac{nK}{n} w_t^{K}$$

where the entire number of samples from all clients is represented by the number of samples in the n, while the revised global model is denoted by w_{t+1} and the local model by w_t^K.

The overall quality score varies between 1.00 (lowest) and 5.00 (highest), giving equal weight to each criterion.

For each of the chosen publications, a data extraction page was made, containing details like the title, author, number of citations, year, location, source, and analysis of the work that addressed the study topic. All authors debate the study topic collectively, attempt to come to a consensus when there are unresolved conflicts, and record all data for analysis and synthesis in order in order to avoid bias when extracting data.

RESULTS & DISCUSSIONS

One system called Federated Learning (FL) tries to safeguard consumers' privacy by keeping private data on their gadgets. However, potential privacy concerns in FL require the development of privacy protections. This technique can be divided into four main categories: Federation Learning with encryption, perturbation-based, blocking, and hybrid privacy-preserves.

Encryption technologies like homomorphic encryption (HE) and secure multiparty computing (SMPC) are essential to maintain data privacy. However, they face challenges such as scalability and computational intensity. Alternative optimization methods include ElGamal encryption optional and distributed key generation, which can also be used in fault detection and prevention systems. Perturbation-based privacy-preserving techniques Differential Privacy (DP), for example, introduces regulated or randomized noise into the update pattern before aggregation, and protection of personal data during training.

Time-stamped, immutable blocks of data controlled by a distributed computer network are used in a blockchain-based privacy method to provide centralized control and transparency. Federated Learning and Blockchain Integration

represents a significant advance in distributed system security and privacy. In FL, a hybrid privacy protection mechanism combines multiple privacy protection mechanisms to provide a powerful privacy protection solution in various applications, especially healthcare.

Privacy assessments in FL are important because of the complexity and privacy concerns. It is imperative to have an all-encompassing assessment framework that extends beyond conventional technical standards. In mathematical privacy assessment, data privacy is evaluated and guaranteed throughout training through the application of formal measurements and mathematical frameworks. Scientists have investigated blockchain, encryption, and hybrid strategies to address these two problems.

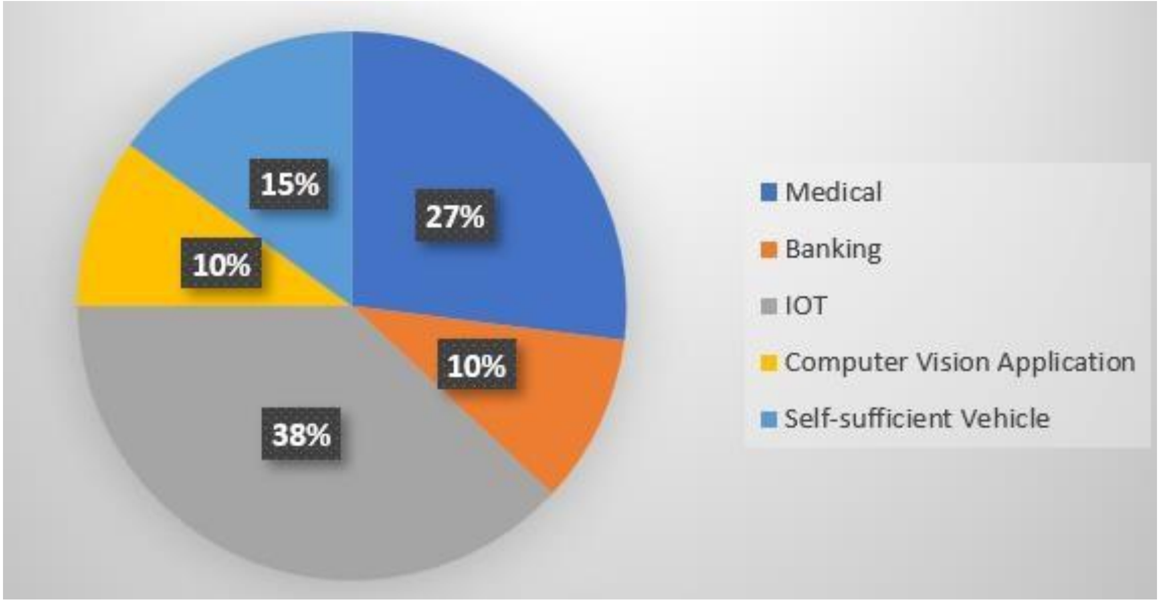
Discussion and future direction:

This study explores the application of financial liquidity (FL) encryption techniques for data security, particularly in industries such as healthcare and finance. However, this method suffers from problems such as computational complexity, latency, and increased communication. To solve this problem, the model can streamline communication compression and computing, while the encryption algorithm and parallel processing for edge devices will speed up the encryption process. Hybrid approaches that manage the computational burden, such as combining DP with encryption, increase privacy.

By introducing noise into the data or model parameters, perturbation-based privacy-preserving algorithms in FL provide a systematic increase in privacy without complex encryption. However, noise calibration is important, as too much noise will decrease the model's accuracy and jeopardize considerable privacy. Strategies include using GANs, optimizing noise scaling using stochastic gradient descent, and generating noise patterns that fit the data distribution.

In FL, block-based techniques enhance data traceability, transparency and integrity, but can be significantly problematic due to persistent ledger synchronization and scalability issues. To mitigate this weakness, lightweight protocols such as Blockchain technology and off-chain computing can be adopted. Layer 2 defences and solutions that increase operational ability and confidentiality are balanced by secure data obfuscation.

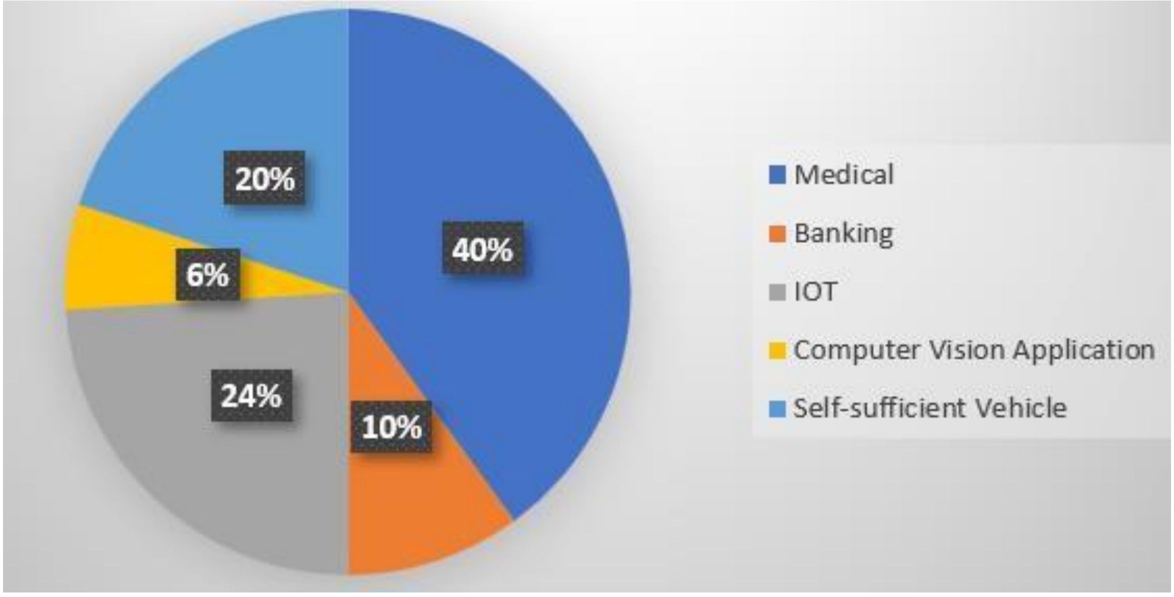
Figure 1: *Blockchain methods used in different sectors*



Source: Author's Compilation

Hybrid privacy solutions are increasingly popular because they balance privacy protection with operational performance needs. Reviewing the main methods as well as measures for evaluating Federated Learning's privacy reveals the necessity of thorough, context-sensitive metrics suitable for different application contexts and data sources. Subsequent research ought to provide coordinated and adaptive metrics, explore hybrid privacy techniques, and find metrics that accurately capture the compromises made in real-world FL implementations between performance, privacy, and usefulness.

Figure 2: *Hybrid Methods used in various sectors*



Source: Author's Compilation

Establishing a thorough research methodology was one of the accepted parameters for a systematic literature review (SLR) that this study adhered to. Validity assessment is important for empirical research, including SLRs. Threats to validity include those posed by concept, outcome, internal and external validity. External validity threats include the generalization of causal findings to the desired population and setting, and potential biases in study selection. To reduce this, synonyms or alternative keywords are added to the search string. Threats to internal validity include poor study design, study selection bias, and selected papers that do not meet our study quality standards. The threat of system reliability affects the ability to correctly infer treatment results. To mitigate this, two lines of research were created, one more general and the answer to the first RQ, and the other more focused. The relationship between the collected data and the conclusion of the analysis is affected by the reliability risk of the findings.

CONCLUSION

Decentralized machine learning (FL) protects sensitive data on end devices, reducing privacy risks. However, there are privacy concerns, especially when training models and exchanging parameters. This article explores recent approaches to privacy protection with a focus on balance. It emphasizes how crucial it is to strike the perfect harmony between privacy and performance and determines the criteria for assessing resilience against data leaks and potential attacks. For research, research and the industry community to address FL and implement measurable privacy protection mechanisms.

ETHICAL DECLARATION

Conflict of interest: The authors declare that there is no conflict of interest regarding the publication of this paper**.**
Financing: This research received no external funding.
Peer review: Double anonymous peer review.

REFERENCES

Abad, G., Picek, S., & Urbieta, A. (2021). SoK: On the security & privacy in federated learning. *arXiv preprint arXiv:2112.05423*.

Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 308–318).

AbdulRahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C., & Guizani, M. (2020). A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. *IEEE Internet of Things Journal*, *8*(7), 5476–5497.

Alzubi, J. A., Alzubi, O. A., Singh, A., & Ramachandran, M. (2022). Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. *IEEE Transactions on Industrial Informatics, 19*(1), 1080–1087.

Ampatzoglou, A., Bibi, S., Avgeriou, P., & Chatzigeorgiou, A. (2020). Guidelines for managing threats to validity of secondary studies in software engineering. In *Contemporary Empirical Methods in Software Engineering* (pp. 415–441). Springer.

Asad, M., Moustafa, A., & Aslam, M. (2021). CEEP-FL: A comprehensive approach for communication efficiency and enhanced privacy in federated learning. *Applied Soft Computing, 104*, 107235.

Baek, C., Kim, S., Nam, D., & Park, J. (2021). Enhancing differential privacy for federated learning at scale. *IEEE Access, 9*, 148090–148103.

Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020). How to backdoor federated learning. In *Proceedings of the International Conference on Artificial Intelligence and Statistics* (pp. 2938–2948). PMLR.

Bhagoji, A. N., Chakraborty, S., Mittal, P., & Calo, S. (2019). Analyzing federated learning through an adversarial lens. In *Proceedings of the International Conference on Machine Learning* (pp. 634–643). PMLR.

Bharati, S., Mondal, M., Podder, P., & Prasath, V. (2022). Federated learning: Applications, challenges, and future scopes. *International Journal of Hybrid Intelligent Systems.*

Blanco-Justicia, A., Domingo-Ferrer, J., Martínez, S., Sánchez, D., Flanagan, A., & Tan, K. E. (2021). Achieving security and privacy in federated learning systems: Survey, research challenges, and future directions. *Engineering Applications of Artificial Intelligence, 106*, 104468.

Boutet, A., Lebrun, T., Aalmoes, J., & Baud, A. (2021). Mixnn: Protection of federated learning against inference attacks by mixing neural network layers. *arXiv preprint arXiv:2109.12550*.

Chatterjee, P., Das, D., & Rawat, D. B. (2023). Next-generation financial services: Role of blockchain-enabled federated learning and metaverse. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 69–74). IEEE.

Jia, B., Zhang, X., Liu, J., Zhang, Y., Huang, K., & Liang, Y. (2021). Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. *IEEE Transactions on Industrial Informatics, 18*(6), 4049–4058.

Keele, S., et al. (2007). Guidelines for performing systematic literature reviews in software engineering (Version 2.3). *EBSE Technical Report, EBSE.*

Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., Alkhayyat, A., & Wang, W. (2022). Federated-learning-based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE Journal of Biomedical and Health Informatics, 27*(2), 664–672.

Lee, H., Kim, J., Hussain, R., Cho, S., & Son, J. (2021). On defensive neural networks against inference attack in federated learning. In *ICC 2021-IEEE International Conference on Communications* (pp. 1–6). IEEE.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide* (1st ed.). Springer International Publishing.

Wahab, O. A., Mourad, A., Otrok, H., & Taleb, T. (2021). Federated machine learning: Survey, multi-level classification, desirable criteria, and future directions in communication and networking systems. *IEEE Communications Surveys & Tutorials, 23*(2), 1342–1397.

Wainakh, A., Ventola, F., Müßig, T., Keim, J., Cordero, C. G., Zimmer, E., Grube, T., Kersting, K., & Mühlhäuser, M. (2021). User-level label leakage from gradients in federated learning. *arXiv preprint arXiv:2105.09369*.

Wang, C., Wu, X., Liu, G., Deng, T., Peng, K., & Wan, S. (2021). Safeguarding cross-silo federated learning with local differential privacy. *Digital Communications and Networks*.

Wang, F., Zhu, H., Lu, R., Zheng, Y., & Li, H. (2021). A privacy-preserving and non-interactive federated learning scheme for regression training with gradient descent. *Information Sciences, 552*, 183–200.

Wang, H., Yurochkin, M., Sun, Y., Papailiopoulos, D., & Khazaeni, Y. (2020). Federated learning with matched averaging. *arXiv preprint arXiv:2002.06440*.

Wang, N., Yang, W., Wang, X., Wu, L., Guan, Z., Du, X., & Guizani, M. (2022). A blockchain-based privacy-preserving federated learning scheme for Internet of Vehicles. *Digital Communications and Networks*.

Wang, Q., Liao, W., Guo, Y., McGuire, M., & Yu, W. (2023). Blockchain-empowered federated learning through model and feature calibration. *IEEE Internet of Things Journal*.

Wei, K., Li, J., Ding, M., Ma, C., Su, H., Zhang, B., & Poor, H. V. (2021). User-level privacy-preserving federated learning: Analysis and performance optimization. *IEEE Transactions on Mobile Computing*.

Wei, K., Li, J., Ding, M., Ma, C., Yang, H. H., Farokhi, F., Jin, S., Quek, T. Q., & Poor, H. V. (2020). Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Transactions on Information Forensics and Security, 15*, 3454–3469.

Wei, K., Li, J., Ma, C., Ding, M., Chen, C., Jin, S., Han, Z., & Poor, H. V. (2021). Low-latency federated learning over wireless channels with differential privacy. *IEEE Journal on Selected Areas in Communications, 40*(1), 290–307.

Zhang, M., Wei, E., & Berry, R. (2021). Faithful edge federated learning: Scalability and privacy. *IEEE Journal on Selected Areas in Communications, 39*(12), 3790–3804.

Zhao, B., Fan, K., Yang, K., Wang, Z., Li, H., & Yang, Y. (2021). Anonymous and privacy-preserving federated learning with industrial big data. *IEEE Transactions on Industrial Informatics, 17*(9), 6314–6323.

Zhou, C., Fu, A., Yu, S., Yang, W., Wang, H., & Zhang, Y. (2020). Privacy-preserving federated learning in fog computing. *IEEE Internet of Things Journal, 7*(11), 10782–10793.

Zhu, H., Wang, R., Jin, Y., Liang, K., & Ning, J. (2021). Distributed additive encryption and quantization for privacy-preserving federated deep learning. *Neurocomputing, 463*, 309–327.

Zhu, L., Liu, Z., & Han, S. (2019). Deep leakage from gradients. *Advances in Neural Information Processing Systems, 32*.

Zhu, S., & Han, M. (2023). Privacy-preserving federated learning and authentication for energy trading system in energy Internet of Things. *Future Generation Computer Systems, 135*, 339–353.