Advanced Privacy-Preserving Mechanisms in Federated Learning: A Comprehensive Literature Review, Methodological Analysis, and Future Directions

Mohammad F. Alkhaldi [1], Firas M. Alkhaldi [2]*
[1,] STS, Amman, Jordan; [2] College of Business, Al Zaytoonah University of Jordan, Amman, Jordan
Email: [1] Mohammad.alkhaldi@zaintec.com; f.alkhaldi@zuj.edu.jo
*Corresponding Author

***Abstract*— Federated Learning (FL) represents a groundbreaking approach to distributed machine learning which allows model training across various decentralized datasets while keeping data storage confined to local location points. The privacy benefits of FL work against diverse attacks such as model inversion attacks and both membership inference attacks and participant collusion threats. This research examines all key privacy-preserving methods which developed for FL including Differential Privacy (DP), Homomorphic Encryption (HE), Knowledge Distillation (KD), Dataset Distillation (DD), and Blockchain Integration. Our study employs methodological comparison to analyze these privacy techniques and their FL workflow integration as well as their privacy-scale-efficiency trade-offs. The combination of DP with HE methods together with integrating KD with dataset distillation denotes strong potential in enhancing security features of federated learning systems.**

Keywords— Privacy-Preserving Federated Learning, Homomorphic Encryption Optimization, Dynamic Noise Management, Blockchain for FL, Explainable Privacy Mechanisms

1. INTRODUCTION

Adaptive learning methods have been shown to enhance workflow efficiency in distributed environment in the context of the modern-day research [1]. As a result, the insights encourage the adoption of methods of learning-based optimization in the framework of privacy-protected federated learning (PPFL). It has become a paradigm shift in the field of collaborative model training in the era of intelligence based on data [2], [3], [4]. Traditional machine-learning processes require centralization of the data aggregation, which often provokes justified objections on the subject of confidentiality, regulatory and user trust. PPFL is a good way of addressing these problems because it enables a cohort of distributed clients to share fully train a common model without providing their raw data [5], [6]. Rather, model parameters or model updates are only shared, and advanced privacy-related tools, including secure multi-party computation, differential privacy, and homomorphic encryption, are implemented to provide an additional layer of protection to sensitive data. This method is becoming more and more relevant in such fields as healthcare, finances, and the Internet of Things where the privacy of the data is the key factor. Therefore, PPFL is considered as a prospective remedy that would balance innovation and ethical, legal, and safe data practices thus paving the way to scalable, privacy-conscious artificial intelligence.

The distributed model training approach of Federated Learning conserves user data privacy through data decentralization and reduces the expenses of sending information between participating parties. The present advantages of FL are threatened by multiple privacy weaknesses which incorporate inference attacks together with data leakage compromises as well as collusion threats. The protection of FL systems from these vulnerabilities gets attention through the introduction of privacy-preservation techniques that include Differential Privacy (DP), Homomorphic Encryption (HE), and Dataset Distillation (DD). Various privacy mechanisms in FL produce performance trade-offs that affect both privacy protection capabilities and model operational efficiency and accuracy. The research reviews modern privacy-preservation techniques used in FL by examining their core methods along with their main achievements and technical boundaries. Three main contributions of this review include: (1) it summarises and compares the fundamental privacy-preserving approaches relevant to federated learning, i.e. DP, HE, KD, DD and Blockchain integration (BI), within a unified methodological framework in elucidating the points of convergence and the intrinsic trade-offs; (2) it hypothesises a new taxonomy of hybrid integration patterns, i.e. encryption-first, noise-first, distillation-first Such additions seek to make the current review stand out among the surveys that are extant by providing prescriptive decision support and not a simple descriptive catalogue.

2. LITRETURE REVIEW

2.1 Differential Privacy (DP) in Federated Learning

Received: 5-10-2025
Revised: 24-10-2025
Published: 31-12-2025

Differ DP proves to be the base technique for protecting privacy in FL by adding statistical noise to model update transmissions before server sharing. Jalil Piran et al. [7] developed FedHDPrivacy which adjusts noise levels across successive training rounds to stop accumulating noise from damaging model performance. The deployment of DP successfully addresses membership inference attacks but this protection comes with accuracy limitations that affect model accuracy versus privacy levels. Inside their FLiP model Xu et al. [8] integrated DP to utilize dataset distillation techniques which both preserve privacy and restrict knowledge distribution [9]. The implementation of DP faces two major obstacles which include expensive calculations and the difficult task of determining optimal noise-to-utility ratios.

2.2 Homomorphic Encryption (HE) in Federated Learning

The computing framework of HE operates on encrypted data in order to safeguard privacy throughout aggregation duties while concealing all intermediate outcome data. The researchers at Shen et al. [10] created mMFHE as a multi-key fully homomorphic encryption system focused on protecting model updates against collusion attacks. The Double Verifiable Privacy-Preserving FL framework by Wang et al. merges HE with verifiable secret sharing and linear homomorphic hashing functions to create improved data privacy protection [11]. HE-based security methods deliver durable protection but tend to create major processing delays combined with increased communication traffic making their deployment difficult throughout different scales of operation [12].

2.3 Knowledge Distillation (KD) for Privacy Preservation

FL developers have integrated KD into their framework to provide privacy protection in addition to managing client data heterogeneity. FedMD-CG represents a framework developed by Luo et al. [13] that uses conditional generators with knowledge distillation to create independent feature extractors from classifiers for maintaining model alignment between local and global components. KD enables consistent model behavior across distributed nodes because it limits the requirement to access raw data [14]. The KD method requires considerable computational power because it needs training extensions and demands generator models leading to resource constraints in certain deployment situations [15].

2.4 Dataset Distillation (DD) in Federated Learning

The privacy-preserving approach known as DD functions as an essential technique in FL by extracting crucial task-related information from datasets for minimal information exchange. Xu et al. [8] defined FLiP as a method which compresses dataset contents to minimize privacy risks during operations. Drawing from DD enables success in distributed environments where clients possess non-independent and indistinguishable distributed (non-IID) data. The generation of distilled datasets for dd involves substantial computational expenses which create difficulties mainly when operating in diverse data environments.

2.5 Blockchain Integration for Federated Learning

The adoption of blockchain solutions within FL continues to grow for the purpose of establishing complete transparency while adding system audit functions and protecting against unauthorized interference [16]. The research team of Biswas et al. developed BPFL which uses blockchain technology to create an FL platform with optimized scalability and decreased transaction management requirements [17]. While Cai, et. al., [18] proposed the Decentralized Federated Learning (BC -DFL) system based on the Blockchain enables the implementation of transparent audit controls and incentive contracts to control trust and protect data integrity. These clauses ensure fair compensations on benign nodes and at the same time penalize ill motives by a stringent mutual assessment system. Although blockchain integration boosts FL security as well as trust levels it potentially slows down systems and increases energy consumption thus posing problems for resource-limited environments.

Table 1, which is a brief comparative summary of the five major methods used in Federated Learning Differentiated DP, HE, KD, DD and BI, serves as a continuation of the above review on privacy-preserving techniques. The table identifies the basic mechanisms, key benefits and key constraints of each methodology besides highlighting the deployment contexts where each methodology can best be utilized. By doing this, the summary would be useful in bridging the conceptual overlay to the in-depth methodological analysis that comes in sequence.

Table 1 — Summary of Privacy-Preserving Methods in Federated Learning

Method	Core Concept	Key Advantage	Main Limitation	Best Use Case
DP	Adds random noise to updates.	Strong privacy with simple integration.	May reduce accuracy.	Cross-silo and healthcare FL.
HE	Aggregates encrypted gradients.	Ensures full confidentiality.	High computational cost.	Finance and medical data.
KD	Shares distilled model outputs.	Reduces communication and data sharing.	Needs auxiliary data.	Edge/IoT learning.
DD	Uses small synthetic datasets.	Minimizes transfer and storage.	High preprocessing cost.	Fast retraining , meta-learning.
BI	Records updates on a ledger.	Traceable and tamper-resistant.	Latency and energy overhead.	Multi-party or regulated FL.

3. METHODOLOGY

This work analyzes five principal privacy-preserving approaches applied in Federated Learning. For each technique we summarize the core mechanism, typical deployment patterns in FL, computational and communication overhead, and resilience to common attacks (membership inference, model inversion, and collusion). The detailed algorithmic descriptions are presented in the

Methodology section to avoid redundancy with the Literature Review.

3.1 Hybrid Integration Patterns Taxonomy.

This paper describes four hybrid patterns of integration that have been proposed in the scholarly literature as well as through practical implementations: (1) Encryption-first: every client executes an encrypt-then-aggregate protocol, and (2) Noise-first: DP noise is applied at the client update step, and (3) Distillation-first: clients either train or distil local networks and send distilled knowledge-or-synthetic data to the aggregation server, which then uses it to perform aggregation under encryption; (4) Consensus-first: a blockchain or consensus Table1 specifies the operational implications of each pattern.

3.2 Hybrid Mechanisms for Secure and Transparent Federated Learning

FedMD-CG integrates KD for privacy enhancement by using conditional generators to realize secure model training and inference procedures. Through this method FL participants switch distilled knowledge instead of raw data thus minimizing privacy risks without affecting performance levels [19]. FLiP introduces Dataset Distillation (DD) in addition to strengthen privacy through the framework which performs optimized data information refinement and data compression. As a technique this approach shares a limited amount of data with essential job-related knowledge which maintains both data security and job performance precision [20]. The figure below represents a schematic flowchart visually representing how these methods integrate in a federated learning pipeline. Blockchain Integration is achieved through BPFL which provides a blockchain-based federated learning platform that enhances trust transparency and scalability throughout the system. The decentralized ledger technology deployed by BPFL supports secure and auditable model update processes as well as transaction integrity [21].

These multiple approaches function together as a comprehensive system for privacy protection in FL which guarantees both data safety and retention of model integrity while adhering to strict privacy law requirements. These techniques create integrated solutions which both protect current system weaknesses and improve the balance between data privacy and operational speed and computing resources usage.

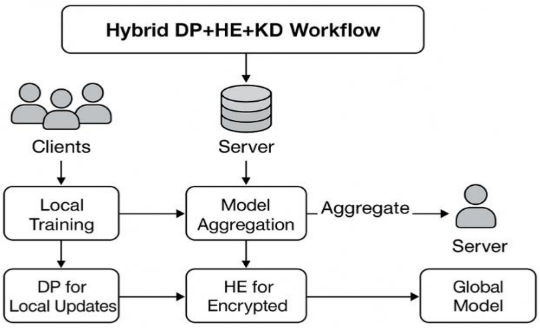

Figure 1. Hybrid DP+HE+KD Workflow Diagram

4. DISCUSSION

4.1 Trade-Offs Between Privacy and Performance

To facilitate understanding of the techniques discussed, Table 2 summarizes a brief privacy-performance trade-off matrix that is used to describe the way both techniques balance the aspects of confidentiality, model accuracy, computational efficiency, and scalability. This matrix summarises the comparison insights described above and forms the foundation of the further discussion of the practical implications and choice of privacy-saving mechanisms in a range of Federated Learning settings**.**

Table 2: Privacy–Performance Trade-offs

Method	P	A	E	S	Best Fit
DP	H	MO	H	EX	Large networks
HE	VH	H	L	M	Sensitive data
KD	MD	H	H	Ex	Edge clients
DD	MD	MO	MO	G	Small datasets
Blockchain	VH	MO	L	LM	Auditable systems

P: Privacy, A: Accuracy, S: Scalability, E: Efficiency. H: high, L: Low, MD: Medium, MO: Moderate, Ex: excellent, G: Good, LM: Limited

Privacy-preserving methods in Federated Learning systems need to make decisions about how much data protection will affect model performance standards. FL techniques need careful optimization to find proper balances between privacy requirements and efficiency goals because each technique has distinctive advantages and difficulties to handle. The privacy protection mechanism based on Differential Privacy (DP) implements statistical noise in model update data to prevent attackers from accessing sensitive data points. The process of adding too much noise during calibration will decrease model accuracy levels substantially. A recent survey on privacy-friendly FL showed that the application of DP successfully blocks attacks on membership but poorly controlled noise results in major model performance decline [22]. Homomorphic Encryption (HE) provides a strong privacy solution by allowing confidential computations on encrypted data from start to finish in the FL process. Higher resource utilization together with longer processing periods are typical outcomes of HE security measures although it provides strong protection. Informative investigations into privacy-preserving FL show that HE encryption causes such significant computational burdens that large-scale FL implementations become impractical [23], [24]. DD serves as a substitute which turns large datasets into smaller informative subsets thus decreasing training data transfers. The data leakage risk restriction achieved by this approach becomes less effective because heterogeneous FL environments usually incorporate non-IID data distribution patterns. The generalization abilities of DD remain inadequate when processing various client datasets because of its restricted effectiveness in environments with diverse data distributions [25]. By using KD the method helps preserve privacy because it performs knowledge transfer between large and small models reducing the necessity of sharing original data. The implementation of KD enables privacy protection together with model performance but needs additional computational resources stemming from its requirement for auxiliary models and additional training procedures. A deep study of privacy-protecting FL techniques indicates that KD improves model precision together with reduced dependency on individual data elements but the increased computational needs need optimized execution to prevent excess resource utilization. Each privacy-preserving method used in FL systems brings unique difficulties alongside their strong capabilities to shield sensitive data. The research field continues to face challenges in finding the best balance between data protection and system performance and computational speed because adaptive privacy methods and optimization methods need constant development.

4.2 Scalability and Efficiency Challenges

FL scalability proves limited when implementing privacy-preserving mechanisms with HE and blockchain-based approaches. The powerful security provided by these methods makes deployment difficult due to high computational and communication requirements which needs future optimization.

HE provides strong data confidentiality through operations which happen directly on encrypted information so aggregation lacks decryption requirements yet its security benefit leads to higher computational burden and resource intake. The restrictions on running massive scale FL implementations derive from these particular factors. According to Gentry the seminal FHE work exhibits major computational challenges that make practical large-scale federated system adoption of HE difficult [26]. The integration of blockchain solution in FL achieves better security alongside decentralization along with improved trust management but creates new issues with latency levels and energy usage. The scalable BPFL solution was created to address scalability issues while the expense linked to blockchain consensus mechanisms restricts its deployment in limited resource environments. FL Coin presents a blockchain-enabled FL architecture which implements a consensus method through committees to enhance efficiency along with scalability. The method provides effective communication overhead reduction yet suffers from significant consensus latency problems that become more pronounced with enlarging network sizes [16]. New studies concentrate on optimization methods which seek to boost efficiency together with scalability. Some scalable blockchain-enabled FL systems adopt adaptive consensus protocols which maintain secure performance along with performance stability throughout network growth. Research has attained fewer communication costs with a simultaneous preservation of system integrity and trustworthiness through blockchain protocol optimization efforts employing committee-based consensus models. The research community faces ongoing difficulties in achieving an ideal balance between FL system scalability efficiency and privacy. For the advancement of blockchain research scientists should focus on creating novel lightweight cryptographic solutions alongside optimized HE protocols and low-latency cryptographic frameworks. The future integration of these improvements will lower computational along with energy requirements so that privacy-preserving FL can function effectively in real-world conditions with restricted resources.

4.3 Hybrid Mechanisms and Integration

The goal of FL hybrid approaches is to strengthen privacy and performance by using multiple privacy-preserving techniques which complement each other. The joint application of Homomorphic Encryption and Differential Privacy forms a dual security system that relies on statistical noise protection from DP and prevents unencrypted computations through HE. Through combined usage these methods become stronger than they are on their own which enables better elimination of privacy threats. Making use of these combination solutions presents complex management requirements because their execution needs efficient infrastructure development to manage system complexities and associated costs. The paper by Grivet Sébert et al. studies how DP and HE systems operate together in FL while maintaining awareness of their performance boundaries regarding privacy level vs processing efficiency [27]. A hybrid method which connects KD features with Dataset DD offers a solution to handle diverse data while minimizing FL transmission requirements. KD allows the transmission of model understanding from bigger complex frameworks to simpler calculative efficient frameworks to perform better training activities in restricted resource environments. The DD process develops abbreviated dataset summaries to cut down the training data exchange between participants. These two techniques unite to provide enhanced protection of privacy as well as generalized model performance in FL systems where data distributions diverge from IID patterns. When these integration methods merge processing systems they create challenges because they need advanced computing frameworks that maintain optimal operational efficiency. Zhang et al. present research in [28] which uses Generative Adversarial Networks (GANs) for a federated data-free knowledge distillation approach to demonstrate both strengths and weaknesses of such combined methods. The implementation of hybrid privacy-preserving mechanisms in FL leads to better security and performance although these advantages create additional program complexity and computational requirements. The successful deployment needs optimized implementation strategies which combine benefits alongside management of the limitations between integrated procedures. Future investigations should concentrate on creating dynamic flexible hybrid FL frameworks which make runtime adjustments to strike equilibrium between system privacy metrics and operational efficiency and network scalability while supporting the execution of upcoming FL systems.

4.4 Real-World Applications and Adoption

Physical applications adopt Federated Learning (FL) solutions to advance in deployment areas that require extensive data security and efficient network connectivity. FL finds its implementation in two main areas which include vehicular networks and smart home ecosystems because it enables collaborative training of machine learning models between devices without sharing data directly. Vehicular Networks In vehicular networks, FL facilitates the collaborative training of models for applications such as traffic prediction, autonomous driving, and intelligent transportation systems. FL provides vehicles with the ability to learn distributed data patterns without exposing locally kept sensitive information thereby maintaining privacy and reducing data transmission costs. FL technology provides numerous benefits but network congestion together with security issues have become major deployment barriers for large-scale vehicular FL applications. Researchers address security and trust issues in FL by proposing to connect blockchain technology with participating vehicles [29]. The integrity and transparencies and tamper-proof features of blockchain prove valuable for decentralized vehicular networks which require these properties.

The authors of [30] presented a hybrid FL-blockchain framework to boost privacy security and protect network integrity in vehicular environments for decentralized model training along with attack vulnerability reduction. These technologies jointly enable vehicles to participate in training models in an environment without trust requirements thereby minimizing security threats from breaches or poisoning attacks. Smart Home Environments FL enables smart home systems to build individualized models directly on each device maintaining user privacy protection and boosting device performance. FL helps smart homes produce individualized automation services which include predictive maintenance for appliances and energy-saving features and voice command recognition through its localized training approach while maintaining privacy.

The proposed implementation of blockchain technology works to enhance security levels together with trust maintenance and data integrity between networked smart devices. A BPFL architecture using blockchain technology offers smart homes a combined system which protects privacy and scales efficiently. The deployment of blockchain technologies for smart home environments encounters essential obstacles throughout widespread adoption due to resource limitations and computational cost and energy efficiency requirements. Blockchains enabling FL solutions must achieve optimization for limited smart devices since these systems typically possess constrained processing power together with restricted battery life.

The combined use of blockchain with FL brings better security and privacy and trust but generates scalability and efficiency issues. The implementation of blockchain-based solutions in vehicular networks and smart homes requires addressing problems relating to latency and energy inefficiency and high computational demands to obtain mass acceptance. Scientists currently develop three key blockchain protocols and adaptive FL algorithms and energy-efficient consensus mechanisms to overcome these limitations. Research endeavors to boost the operational feasibility of privacy-protecting FL applications through cryptographic improvements together with communication overhead reduction for resource-limited environments. These technological advancements will drive the dissemination of FL into decentralized real-world programs while maintaining digital security throughout the new technological era.

5. FUTURE RESEARCH DIRECTIONS

The development of privacy-preserving federated learning needs research to focus on specific critical aspects. The future of privacy-preserving FL research should focus on two streams: resolving remaining challenges and creating new balanced solutions that protect privacy and enhance operation speed and scale width. Researchers propose using adaptive noise systems for real-time privacy adjustments in federated learning processes [31]. During training FL systems equipped with this method would preserve both model accuracy and privacy boundaries while preventing degrading performance results. The main shortcoming in homomorphic encryption exists in its ability to scale effectively. The computational demands of HE coupled with its long communication times limit its practical use for running large-scale FL deployments because of the strong data confidentiality it provides. Future investigations should develop HE algorithms for better efficiency with reduced latency while requiring fewer resources so they can be applied to operational applications. Research should examine how various privacy-preserving schemes integrate as a single solution for enhanced data protection efforts. The integration of DP with HE and KD under an aggregated framework enables researchers to secure patient data while maintaining decent model performance. The integration between these techniques remains complex because optimization work is needed to balance performance and scalability as well as complexity. Blockchain optimization stands as an essential area because scientists need to develop minimal protocols for blockchain systems operating with limited resources.

The future advancement of blockchain integration with FL demands improvements in time-consuming consensus procedures and transaction handling methods along with architecture scalability solutions. Better system design will produce a secure decentralized learning capability that does not strain system resources. The exploration of two additional fields emerges as crucial for additional research work: FL Systems under Real-Time Conditions must optimize their functionality for latency-responsive applications because autonomous vehicles along with smart cities and IoT networks need timely processing. The creation of privacy-preserving algorithms should focus on developing mechanisms which boost transparency alongside interpretability and trust in entertainment and medical services along with financial institutions.

Research targeting these privacy challenges and application opportunities will significantly enhance privacy-protected federated learning methods which will become suitable for various real-world implementations. Upcoming innovations for federated learning systems will determine their next-generation form by uniting privacy concerns with performance capabilities to enable extensive adoption.

6. CONCLUSION

A comprehensive overview of privacy protecting FL methods appears alongside an examination of their unique advantages and technical limitations in this document. Differential Privacy, Homomorphic Encryption, Knowledge Distillation and Dataset Distillation together with Blockchain Integration are techniques which offer specific benefits to protect sensitive data in FL systems. Each privacy technique creates computational, scaling and performance challenges that require proper management. The study demonstrates that combining multiple privacy techniques in FL produces a promising approach to preserve user privacy. FL systems augment their security profile by using synergy between different privacy methods to overcome weaknesses that individual approaches have difficulty handling. An illustration is the combination of DP and HE or KD and DD. Careful optimization of these techniques in privacy and computation as well as model accuracy makes the hybrid scheme perform better. Upcoming scholarly investigations should aim their research at dominant regions including: The challenge remains to discover effective ways for making FL frameworks capable of handling extensive deployment scale together with privacy features and efficiency requirements. Dynamic noise control methods for DP need improvement to automatically measure and optimize noise levels without hurting accuracy. The design of energy-efficient blockchain protocols which operate on FL needs to focus on reducing blockchain transactions along with latency and performance overhead. The progress made in these research areas will establish a future FL system generation that can be deployed effectively in medical systems and financial applications and autonomous devices and Internet of Things networks. Ongoing developments in privacy-preserving FL systems will establish secure yet reliable and scalable machine learning solutions that address the escalating needs for confidential data and enable significant data owners to collaborate on joint model training without losing data confidentiality.

References

[1] F. M. Alkhaldi and A. M. Ishtaiwi, "Business Workflow Optimization Using Reinforcement Learning: A Q-Learning Approach," in Conference on Sustainability and Cutting-Edge Business Technologies, Cham: Springer Nature Switzerland, 2025.

[2] A. El Ouadrhiri, P. H. Phung, N. Nasser, B. Boudine, and A. Abdelhadi, “Privacy-Preserving Federated Learning Approach Based on Hensel’s Compression and Differential Privacy,” Aug. 2025, doi: 10.21203/rs.3.rs-7255758/v1.

[3] Y. Yao and N. Yu, “Efficient secure aggregation for privacy-preserving federated learning based on secret sharing,” Journal of University of Science and Technology of China, vol. 53, no. 4, p. 1, Jan. 2023, doi: 10.52396/justc-2022-0116.

[4] K. Bhosale, M. Waghmare, Ms. K. Kamble, and S. Chouhan, “Privacy-Preserving Federated Learning: A Comparative Study of Techniques and their Practical Implementations,” International Journal For Science Technology And Engineering, vol. 13, no. 4, pp. 4028–4030, Apr. 2025, doi: 10.22214/ijraset.2025.69141.

[5] M. Hasan, “Federated learning models for privacy-preserving ai in enterprise decision systems,” vol. 05, no. 03, pp. 238–269, Sep. 2025, doi: 10.63125/ry033286.

[6] L. T. Phong, T. T. Phuong, L. Wang, and S. Ozawa, “Frameworks for Privacy-Preserving Federated Learning,” Jan. 2024, doi: 10.1587/transinf.2023mui0001.

[7] F. J. Piran, Z. Chen, M. Imani, and F. Imani, “Privacy-Preserving Federated Learning with Differentially Private Hyperdimensional Computing,” *arXiv preprint*, arXiv:2411.01140, Nov. 2024. [Online]. Available: https://arxiv.org/abs/2411.01140

[8] Y. Xu, J. Wang, and H. Li, “FLiP: A Federated Learning Framework with Dataset Distillation,” *arXiv preprint*, arXiv:2410.19548, Oct. 2024. [Online]. Available: https://arxiv.org/abs/2410.19548

[9] X. Ren, S. Yang, C. Zhao, J. A. McCann, and Z. Xu, “Belt and Braces: When Federated Learning Meets Differential Privacy,” Communications of The ACM, Nov. 2024, doi: 10.1145/3650028.

[10] J. Shen, Y. Zhao, S. Huang, and Y. Ren, “Secure and Flexible Privacy-Preserving Federated Learning Based on Multi-Key Fully Homomorphic Encryption,” *Electronics*, vol. 13, no. 22, p. 4478, Nov. 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/22/4478

[11] C. Wang, Z. Sun, and J. Lu, “A Secure and Efficient Federated Learning Scheme Based on Homomorphic Encryption and Secret Sharing,” pp. 1170–1175, Jul. 2024, doi: 10.1109/cisat62382.2024.10695339.

[12] R.-Y. Huang, G. D. Samaraweera, and J. M. Chang, “Toward Efficient Homomorphic Encryption-Based Federated Learning: A Magnitude-Sensitivity Approach,” pp. 7810–7821, Dec. 2024, doi: 10.1109/bigdata62323.2024.10825533.

[13] X. Luo, Y. Huang, and L. Chen, “FedMD-CG: Federated Learning via Model Distillation and Conditional Generators,” *arXiv preprint*, arXiv:2409.06955, Sep. 2024. [Online]. Available: https://arxiv.org/abs/2409.06955

[14] A. Mora, I. Tenison, P. Bellavista, and I. Rish, “Knowledge Distillation in Federated Learning: A Practical Guide,” Aug. 2024, doi: 10.24963/ijcai.2024/905.

[15] A. Kulkarni, N. Panchi, and S. S. Chiddarwar, “Stagewise Knowledge Distillation,” Nov. 2019, [Online]. Available: https://dblp.uni-trier.de/db/journals/corr/corr1911.html#abs-1911-06786

[16] J. Tang, “Federated Dynamic Client Selection Based on Comprehensive Performance Evaluation,” pp. 314–318, Oct. 2024, doi: 10.1109/cbase64041.2024.10824396.

[17] S. Biswas, A. Gupta, and N. Kumar, “Blockchain Controlled Trustworthy Federated Learning Platform for Smart Healthcare,” *IET Communications*, vol. 18, no. 2, pp. 128–137, Feb. 2024. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/cmu2.12870

[18] Z. Cai, J. Chen, Z. Diao, and H. Xiang, "A Blockchain-Enabled Decentralized Federated Learning System with Transparent and Open Incentive and Audit Contracts," Springer Science+Business Media, 2023, pp. 259–269. doi: 10.1007/978-981-99-8101-4_18

[19] S. A. Wadho, A. F. Meghji, A. Yichiet, R. Kumar, and F. B. Shaikh, "Encryption Techniques and Algorithms to Combat Cybersecurity Attacks: A Review," *VAWKUM Transactions on Computer Sciences*, vol. 11, no. 1, pp. 295–305, June 2023. [Online]. Available: https://vfast.org/journals/index.php/VTCS/article/view/1521

[20] C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014. [Online]. Available: https://dl.acm.org/doi/10.1561/0400000042

[21] B. Han, Z. Liang, M. Qin, R. Jiang, and W. Dai, "Research on Blockchain-based Decentralized Federated Learning," pp. 23–29, Sep. 2023, doi: 10.1109/ccat59108.2023.00012.Available: https://dl.acm.org/doi/10.1145/1536414.1536440

[22] R. Song, X. Liu, J. Zhang, and M. J. Reed, "Federated Learning via Decentralized Dataset Distillation in Resource-Constrained Edge Environments," *arXiv preprint*, arXiv:2208.11311, Aug. 2022. [Online]. Available: https://arxiv.org/abs/2208.11311

[23] R.-Y. Huang, G. D. Samaraweera, and J. M. Chang, "Toward Efficient Homomorphic Encryption-Based Federated Learning: A Magnitude-Sensitivity Approach," pp. 7810–7821, Dec. 2024, doi: 10.1109/bigdata62323.2024.10825533.

[24] H. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, "Privacy-Preserving Deep Learning via Additively Homomorphic Encryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 5, pp. 1333–1345, May 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8241854

[25] Z. Wu, Z. Xu, D. Zeng, and Q. Wang, "Federated Generalization via Information-Theoretic Distribution Diversification," *arXiv.org*, vol. abs/2310.07171, Oct. 2023, doi: 10.48550/arxiv.2310.07171.

[26] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, Bethesda, MD, USA, 2009, pp. 169–178. [Online].

[27] A. Grivet Sébert, R. Sirdey, O. Stan, and C. Gouy-Pailler, "Protecting Data from all Parties: Combining FHE and DP in Federated Learning," *arXiv preprint*, arXiv:2205.04330, 2022. [Online]. Available: https://arxiv.org/abs/2205.04330

[28] Z. Zhang, T. Shen, J. Zhang, and C. Wu, "FedDTG: Federated Data-Free Knowledge Distillation via Three-Player Generative Adversarial Networks," *arXiv preprint*, arXiv:2201.03169, 2022. [Online]. Available: https://arxiv.org/abs/2201.03169

[29] "Fairness, integrity, and privacy in a scalable blockchain-based federated learning system," *Computer networks*, vol. 202, p. 108621, Jan. 2022, doi: 10.1016/j.comnet.2021.108621.

[30] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," *arXiv preprint*, arXiv:1608.05187, 2016. [Online]. Available: https://arxiv.org/abs/1608.05187

[31] W. Zheng, Q. Zhao, and H. Xie, "Research on Adaptive Noise Mechanism for Differential Privacy Optimization in Federated Learning," *Journal of knowledge learning and science technology*, vol. 3, no. 4, pp. 383–392, Dec. 2024, doi: 10.60087/jklst.v3.n4.p383.