Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Survey of Federated Learning Privacy Preservation Techniques for Malicious Behavior Detection

Eman Shalabi[1], Walid Khedr[2], Ehab Rushdy[1], and Ahmad Salah[3]*
[1] *College of Computers and Informatics, Zagazig University, Zagazig, Egypt*
[2] *College of Computer Science and Engineering, Taibah University, Yanbu 966144, Saudi Arabia*
[3] *College of Computing and Information Sciences, University of Technology and Applied Sciences, Ibri, Oman*
* *Corresponding Author: ahmad.salah@utas.edu.om*

ARTICLE INFO

Received: 22 Dec 2024

Revised: 15 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Centralized machine learning requires the centralization of data in one server for model training, the data of individuals must be transmitted to the centralized server using its raw form which resulting in serious privacy and security concerns. Federated learning is a decentralization machine learning technique which improves the issues of security and privacy related to traditional machine learning by enabling local model training on devices without sharing raw data with the centralized server. Federated learning includes multiple clients and one central server. Clients perform training on its own data while the server coordinates the overall federated learning process. In federated learning, raw data never leaves its own place, ensuring data confidentiality. Only local model updates, form each client are transmitted to the central server that organizes the learning process. The server performs aggregation on received local model updates. Following the aggregation process, the global model is then updated by the server. The final global model is used then for evaluation. However federated learning improves privacy along with security of centralized machine learning, it is still targeted by attacks through model updates transmitted between clients and server. To improve privacy along with security related to federated learning, privacy preservation techniques are integrated with federated learning. We propose a survey of privacy preservation techniques combined with federated learning to improve privacy and security and achieve a good balance between utility and privacy. Private Aggregation of Teacher Ensembles, Homomorphic Encryption, as well as Secure Multi-Party Computation represent the most popular used privacy preservation techniques with federated learning for malicious behavior detection.

Keywords: Federated Learning, Privacy preservation, Secure Multi-Party Computation, Private Aggregation of Teacher Ensembles, Homomorphic Encryption.

1. INTRODUCTION

Massive volumes of data are essential to traditional machine learning (ML) models, but gathering and analyzing the enormous volumes of data generated from network-edge devices is expensive, ineffective, and presents significant privacy risks [1]. Because traditional ML relies on centralized server for performing training, there are serious privacy and security risks, including the possibility of data breaches and illegal access to private information [2]. Centralized ML is targeted by several attacks, inference and poisoning attacks. Inference Attacks compromise data confidentiality by allowing attackers to infer sensitive data via model outputs [3]. Data poisoning occurs when attackers alter training data, compromising the integrity of the model [4].

Federated learning (FL) addresses the centralized ML privacy along with security issues as it improves security and protects data privacy by allowing local ML model training using decentralized data [5]. **Figure 1** depicts the full diagram of FL. FL is a decentralized ML approach including a central server, multiple clients, global model, and local models. Firstly, the central FL server prepares a global ML model and transmits it to all clients participating in FL process. Clients then perform local model training on their private data and sending only local model updates to the central server for aggregation. After receiving the model updates via all FL participating clients, the server

Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

aggregates them and then updates global model. The updated FL global model is transmitted again to all clients for local training and the cycle continues for specific times. For evaluation process, the final global model is used.

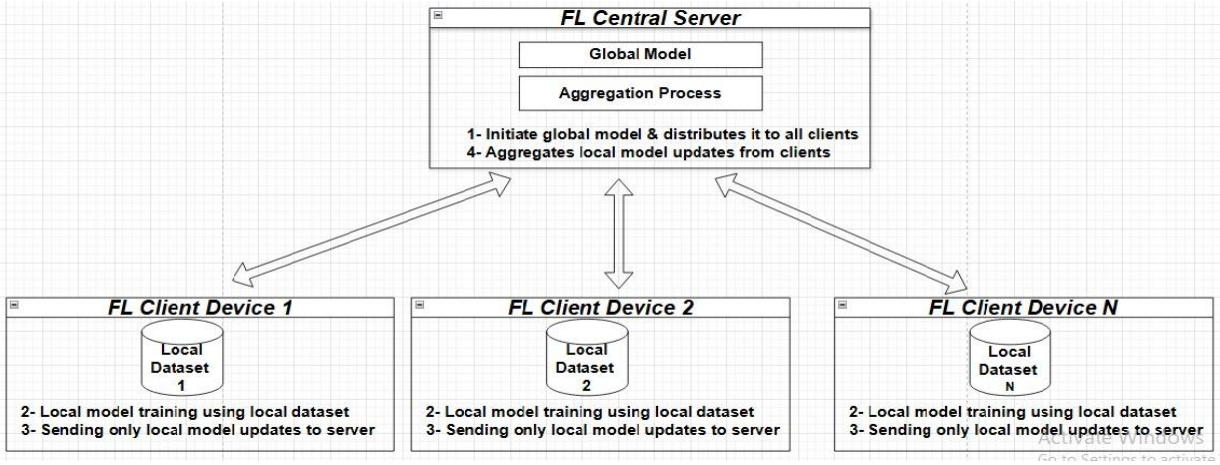

Figure 1. FL Diagram.

Numerous domains apply FL [6, 7] including malicious behavior detection, banking for the detection of fraud, healthcare for collaborative research, e-commerce for customized experiences, the Internet of Things (IoT) for intelligent networks, autonomous vehicles for updating models and interpreting data in real time, and telecommunications for customer support. **Table 1** shows various FL based studies for malicious behavior detection. The study [8] proposed a method for identifying Android malware that relies on FL, ML, and neural networks. The evaluation makes use of XGBoost, Random Forest, and a hybrid neural network model in which CNN as well as Long Short-Term Memory (LSTM) are combined. The study [7] proposed a FL based model for malware detection using ANN and Malware dataset.

Table 1. FL studies.

Paper	Year	ML Technique	Publisher
[9]	2022	Multi-layer perceptron, Autoencoder	Elsevier
[10]	2022	CNN, GNN	MDPI
[11]	2023	ResNet	IEEE
[8]	2024	XGBoost, Random Forest, LSTM, CNN	IEEE
[12]	2024	CNN	Elsevier
[7]	2025	ANN	MDPI

Although FL improves the privacy and security of traditional ML, it is also vulnerable to multiple attacks of model inversion, man in the middle (MITM), backdoor, and poisoning attacks [7]. To enhance the privacy and security of FL, privacy-preserving techniques are incorporated to FL including Private Aggregation of Teacher Ensembles (PATE) [13], Homomorphic Encryption (HE) [14] , and Secure Multi-Party Computation (SMPC) [15]. Through this study, we propose a survey of the techniques of privacy preservation in FL for malicious behavior detection. The remainder of the work is organized as follows: Section 2 addresses PATE, Section 3 addresses HE, Section 4 addresses SMPC, and Section 5 includes conclusion along with future work.

2. PRIVATE AGGREGATION OF TEACHER ENSEMBLES

PATE is a ML privacy preservation technique. It consists of multiple teacher models along with only one student model, allowing teacher models that have been trained on different sensitive data subsets to discreetly aggregate their predictions in order to label new training instances used for a student model [16]. PATE ensures privacy by

Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

preventing the predictions of the student model from disclosing private information regarding the data used for training [17]. The aggregated predictions are supplemented with noise in which a privacy budget is used to calibrate this noise, regulating the trade-off between utility and privacy as reduced privacy budget values increase noise, which could impair performance [18]. Gaussian and Laplace noise are used for noise addition [19]. **Table 2** shows various studies utilizing PATE for preserving privacy.

Table 2. Privacy-preserving studies using PATE.

Paper	Year	ML Technique	Privacy-preserving Technique	Publisher
[7]	2025	ANN	PATE	MDPI
[20]	2023	CNN	PATE	MDPI
[21]	2021	Knowledge Distillation	PATE	IEEE
[22]	2024	DNNs	PATE	IEEE
[13]	2023	SACN	PATE	IEEE

In [7], the authors proposed a FL based framework utilizing ANN and Malware Dataset for the task of malware detection. To enhance security and privacy, PATE was integrated with FL in FL_PATE model. PATE was implemented after FL process for protecting the final global model in FL from being attacked. The PATE procedure consisted of the training of ten teacher models along with a student model which learned from the trained teacher models and used for predictions. The student model was used as the final FL global model and utilized in the evaluation process. Adversarial attack robustness was also addressed in this paper. FL_PATE model which integrating FL with PATE, takes 186.43 s for training and achieved 85.30% accuracy, 85.73% precision, 85.30% recall, and 85.26% F1-Score. Several attacks including targeted and untargeted poisoning attacks, model inversion attacks, backdoor attacks, and man in the middle (MITM) attacks were evaluated. FL_PATE model outperformed FL base model for all evaluated attacks. FL_PATE achieved an attack success rate of 16.91 for model inversion attack, 0.24 for backdoor attack, 0.163 for untargeted poisoning attack, 0.144 for targeted poisoning attack, and an accuracy degradation of 34.73% for MITM attack.

In [20], the FL based framework called FREDY was proposed using Convolutional Neural Networks (CNN). PATE, and knowledge transfer was integrated with FL in FREDY to enhance privacy. In order to incorporate the PATE into FREDY, many teacher models were trained. On publically accessible unlabeled data, inference was conducted. By utilizing the noise of Laplace, the prediction aggregation was performed. On the produced labeled data, the training of the student model was performed. The evaluation was conducted on two datasets including MNIST dataset and CIFAR10 dataset. According to the study reported results, the test performance of the student model was generally enhanced by raising the total number of clients as well as the privacy measure (ε) for the two different datasets. CIFAR-10 models were outperformed by MNIST models. The 25-client model reached its highest accuracy of approximately 99% with ε=1 using MNIST and approximately 79% using CIFAR-10. With a 25% decrease in all measures, FREDY surpassed the baseline model with respect to the performance of attack of membership inference at ε=0.2. A single attack was used to measure the resistance of the proposed framework.

In [13], the authors proposed a FL based framework of FedMalDE for the purpose of detecting malware in IoT. The framework preserved the user privacy by combining PATE with FL. By investigating the underlying relationship among labeled along with unlabeled data, FedMalDE used the mechanism of knowledge transfer to infer labels for unlabeled data. To effectively capture a variety of harmful behaviors, a subgraph aggregated capsule network (SACN) that had been specially built is employed. FedMalDE ensured real-world experiments confirmed the system's effectiveness in detecting IoT malware without compromising user privacy or security. FedMalDE's efficacy in identifying IoT malware and its adequate privacy and security guarantees were demonstrated by the comprehensive experiments made on data from the real-world. Adversarial attack robustness is not addressed as

Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the resistance of FedMalDE against various attacks is not evaluated. The framework is not evaluated against any attack.

3. HOMOMORPHIC ENCRYPTION

HE is a privacy preservation technique used for privacy enhancement of FL [23]. Computations can be carried out directly using encrypted form of data with no need firstly for decryption thanks to this cryptographic technique [24]. After decryption, the outcome is identical to what would be the result achieved by applying the same procedures to the plain data [25]. HE is especially helpful in sensitive domains in which privacy and security concerns are crucial, including cloud services [26], financial transactions [27], and medical data interchange [28].

HE includes Fully Homomorphic Encryption (FHE) [29], Partially Homomorphic Encryption (PHE) [30], and Somewhat Homomorphic Encryption (SWHE) [31]. For PHE, an addition or multiplication operation is available, but not both, for certain operations, SWHE allowing both basic addition and multiplication, while FHE allows for any arbitrary operation using encrypted data with no need for decryption [7]. There are various HE schemas including CKKS, BFV, and TFHE [32]. Since BFV is designed for exact integer computations, it is perfect for applications that require precise results, like financial transactions, whereas CKKS is appropriate for applications that require approximate results, like machine learning and signal processing, because it enables operations on complex and real numbers.

HE is integrated to FL to enhance privacy and security by encrypting local model updates on client side prior transmission to the central FL server which performs the aggregation process on these encrypted local model updates from all participating clients without decrypting them. **Table 3** shows various studies integrate HE with FL for privacy preservation. In [33], the authors presented a FL based framework called RPFL using Multi-Layer Perceptron (MLP) and N-BaIoT dataset for the detection of IoT malware. HE, blockchain, along with Elliptic Curve Digital Signature Algorithm (ECDSA) was integrated with FL to preserve model utility and data privacy. Without compromising the detection accuracy, HE protected the confidentiality of transmitted local model updates, while ECDSA guaranteed reliable aggregation. When integrating HE, they discovered and talked about new difficulties, especially those involving the need for an outside aggregator. An incentive system and a mitigation plan to deal with possible aggregator failures were two smart contract-supported solutions they introduced to solve these issues. RPFL achieved an accuracy of 99.95%, a TPR of 99.98%, and a TNR of 99.63%. RPFL with HE had 18.66 min for total training time for 30 rounds and 37.32 s per round. The framework was not evaluated against attacks.

Table 3. HE based privacy-preserving studies.

Paper	Year	ML Technique	Privacy-preserving Technique	Publisher
[7]	2025	ANN	HE	MDPI
[33]	2025	MLP	HE	MDPI
[34]	2024	Ghost_BiNet	HE	IEEE
[35]	2024	DNN	HE	IEEE
[36]	2024	Logistic Regression, SecureBoost	HE	IEEE
[14]	2023	ResNet-50, BERT	HE	arXiv

In [7], the authors proposed a FL based framework utilizing ANN and Malware Dataset for the purpose of detecting malware. To enhance security as well as privacy, HE using CKKS schema was integrated with FL generating FL_CNN model. Coefficient modulus bit sizes, polynomial modulus degree, and global scale were the three parameters used in CKKS context. HE was implemented during FL process on clients and central server. The encryption was mainly conducted on client side. The FL server aggregated and processed the secured encrypted model updates via every party involved in FL process without requiring decryption, while clients encrypted their own model updates prior transmission to the server which performed the aggregation on these encrypted updates.

Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

FL_CKKS model which integrating FL with HE using CKKS schema, had 192.87 s for training and achieved 99.80% in accuracy, 99.80% in precision, 99.80% in recall, and 99.80% in F1-Score. FL_CKKS model enhanced privacy and security and also improved the performance of FL base model which achieved 99.30% for all metrics. Several attacks including untargeted and targeted poisoning attacks, model inversion attack, backdoor attack, and MITM attack were evaluated. FL_CKKS produced an attack success rate of 2.19 for model inversion attack, 0.50 for backdoor attack, 0.003 for untargeted poisoning attack, 0.002 for targeted poisoning attack, and an accuracy degradation of 16.95% for MITM attack.

In [34], the authors proposed a FL based approach using Enhanced Ghost_BiNet technique for intrusion detection to improve detection utility as well as information sharing security. Bidirectional Gated Recurrent Unit and GhostNet were combined in the hybrid technique of deep learning known as Enhanced Ghost_BiNet. The Chaotic Chebyshev Artificial Humming Bird method was used for the optimization of the model's performance. To improve data security and privacy, HE was used to encrypt the updates of FL local model. Communication overhead was reduced through the usage of HE and optimization. UNSW-NB15, KDD CUP 99, and CICIDS 2017 were the three utilized datasets. The highest performance of 99.24% accuracy, 97.30% precision, 99.56% recall, 98.42% F-Score, 0.01 MSE, and 1.13 FAR was achieved on the dataset of KDD CUP 99. For CICIDS 2017 dataset, an accuracy of 98.48%, a precision equal to 94.87%, a recall equal to 99.12%, F-Score equal to 96.95%, MSE equal to 0.02, and FAR equal to 1.15 were produced. Regarding UNSW-NB15, 98.10% accuracy, 93.075% precision, 98.90% recall, 96.26% F-Score, 0.02 MSE, and 1.15 FAR were produced. The study recognized possible constraints in terms of scalability and computational resources. No attack was evaluated in this this study.

4. SECURE MULTI-PARTY COMPUTATION

SMPC is also a cryptographic technique used for privacy preservation. It enables several parties to work together for the purpose of computing a function using their private data inputs while ensuring those inputs' privacy [37]. This approach allows for safe sharing of data along with analysis without sacrificing individual privacy, which is especially advantageous in areas involving sensitive data including healthcare [38], finance [39], and cloud [40]. SMPC is integrated with FL to enhance privacy along with security through permitting multiple clients to collaborate on training ML models without disclosing their private information. By using cryptographic mechanisms, SMPC ensures that model updates are kept secure from the centralized server and other participating clients inside FL process, in contrast to FL without SMPC, which shares model updates directly. **Table 4** shows several studies, integrating SMPC with FL for privacy preservation.

Table 4. Privacy-preserving studies using SMPC.

Paper	Year	ML Technique	Privacy-preserving Technique	Publisher
[7]	2025	ANN	SMPC	MDPI
[41]	2024	DNN, CNN, LSTM, hybrid model	SMPC	IEEE
[42]	2023	CNN	SMPC	IEEE
[43]	2022	ResNet	SMPC	IEEE
[15]	2024	Supervised ML, DL, GNN	SMPC	IEEE
[44]	2024	CNN	SMPC	ACM

In [7], the authors proposed a FL based framework utilizing ANN and Malware Dataset for detecting malware. For the purpose of enhancing privacy and security, SMPC was integrated with FL generating two combined models including FL_SMPC model as well as FL_SMPC_DP model. SMPC was implemented in FL through the ML library of PySyft which was used through their tensors for the management and transmission of model updates among the server and clients participating in FL. DP is implemented through Gaussian noise which incorporated to the average model updates resulting from the aggregation process on FL central server for the enhancement of privacy and security.

FL_SMPC model which integrating FL with SMPC, had a training time of 117.73 s and achieved 99.50% for all metrics. FL_SMPC model not only enhanced privacy and security but also enhanced the corresponding performance of the FL base model that achieved 99.30% for all metrics. FL_SMPC_DP model which integrating FL with SMPC and DP, consumed a training time of 128.54 s and produced 83.50% accuracy, 83.56% precision, 83.50% recall, and 83.49% F1-Score. FL_SMPC_DP model reduced the performance of the FL_SMPC model due to the used DP while enhancing privacy and security.

Several attacks including untargeted and targeted poisoning attacks, model inversion attack, backdoor attack as well as MITM attack were evaluated. FL_SMPC produced an attack success rate of 2.61 for model inversion attack, 0.466 for backdoor attack, 0.004 for untargeted poisoning attack, 0.04 for targeted poisoning attack, and an accuracy degradation of 48.51% for MITM attack. FL_SMPC_DP produced an attack success rate of 7.62 for model inversion attack, 0.132 for backdoor attack, 0.17 for untargeted poisoning attack, 0.01 for targeted poisoning attack, and an accuracy degradation of 24.92% for MITM attack.

In [41], the authors proposed a FL based FBMP-IDS framework for intrusion detection on 6G networks. SMPC and blockchain were integrated together with FL. SMPC preserved privacy by ensuring the adaptation in safe aggregation that optimizes computational complexity as well as communication overhead in real world, while enabling cooperative training of intrusion detection models and protecting data privacy. The FL process is distributed, transparent, and impenetrable thanks to blockchain.

They utilized a hybrid model architecture utilizing CNN along with Multi-head attention. CNN was utilized for the extraction of features. Multi-head attention is employed for improved contextual analysis to increase the rates of detection and lower false alarm rates. The evaluation was conducted using the dataset of CICIoT2023. With an average accuracy of 79.92%, a detection rate of 77.41% with a 2.55% low false alarm rate, the hybrid model was the most successful. Although the achieved 79.92% accuracy is good, there may still space for improvement. No attack simulation is conducted. Adversarial attacks testing is not addressed and evaluated.

In [15], the authors proposed a FL based framework for detecting Android malware using supervised ML combined with DL techniques. The dynamic feature extraction was introduced in this framework. For malware graphs, they suggested a graph-based on behavioral analysis that improvesd detection accuracy by capturing complex dependencies and relationships between system elements. In order to model malware into graph structures and detect intricate attack patterns, they incorporated graph-based analysis of behavior. Their framework outperformed current techniques in terms of performance metrics and classification accuracy on a variety of malware datasets. The simulation and evaluation of attacks are not addressed.

5. CONCLUSION

This study is mainly focus on FL. Through this work, we propose a survey of privacy preservation techniques in FL for malicious behavior detection. FL is a decentralized ML based approach. It overcomes the related risks of centralized ML by enabling collaborative training of ML model with no need for sharing raw data to a centralized server. In FL, the centralized server initiates a global model and then distributes it to all participating clients in the FL process. Each client performs local model training using its own private data. After training, clients transmit only model updates to FL central server. The server then aggregates local model updates from all client and updates FL global model. For evaluation process, the final global model is utilized. Although FL overcomes the challenges of traditional ML by improving privacy and security, it is exposed to attacks as model updates may leak information about training data. Privacy preservation techniques are combined with FL to enhance privacy and security of FL. PATE, HE, and SMPC are the most used privacy preservation techniques with FL. In order to provide more security and privacy, multiple privacy preservation techniques should be combined with FL. Integrating more privacy preservation techniques with FL enhances its security and privacy but will increase overhead of computational and communication and may also decrease performance. Future work includes the complete implementation of a FL based system with privacy-preserving techniques for malicious behavior detection, ensuring a balance between performance and privacy. The implemented framework will tested against several attacks using multiple datasets.

Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

REFRENCES

1. Ge, L., H. Li, X. Wang, and Z. Wang, *A review of secure federated learning: Privacy leakage threats, protection technologies, challenges and future directions*. Neurocomputing, 2023. **561**: p. 126897.
2. Maurya, J. and S. Prakash. *Privacy Preservation in Federated Learning: its Attacks and Defenses*. in *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)*. 2023.
3. Wang, H., Q. Wang, Y. Ding, S. Tang, and Y. Wang, *Privacy-preserving federated learning based on partial low-quality data*. Journal of Cloud Computing, 2024. **13**(1): p. 62.
4. Pathak, S. and D. Dasgupta. *Federated Learning with Authenticated Clients*. in *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. 2024.
5. Marfo, W., D.K. Tosh, and S.V. Moore, *Adaptive client selection in federated learning: A network anomaly detection use case*. arXiv preprint arXiv:2501.15038, 2025.
6. Annamalai, S., N. Sangeetha, M. Kumaresan, D. Tejavarma, G.H. Vardhan, and A.S. Kumar, *Application Domains of Federated Learning*. Model Optimization Methods for Efficient and Edge AI: Federated Learning Architectures, Frameworks and Applications, 2025: p. 127-144.
7. Shalabi, E., W. Khedr, E. Rushdy, and A. Salah *A Comparative Study of Privacy-Preserving Techniques in Federated Learning: A Performance and Security Analysis*. Information, 2025. **16**, DOI: 10.3390/info16030244.
8. Purkayastha, B.S., M.M. Rahman, and M. Shahpasand. *Android Malware Detection Using Machine Learning and Neural Network: A Hybrid Approach with Federated Learning*. in *2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet)*. 2024.
9. Rey, V., P.M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet, *Federated learning for malware detection in IoT devices*. Computer Networks, 2022. **204**: p. 108693.
10. Jiang, C., K. Yin, C. Xia, and W. Huang *FedHGCDroid: An Adaptive Multi-Dimensional Federated Learning for Privacy-Preserving Android Malware Classification*. Entropy, 2022. **24**, DOI: 10.3390/e24070919.
11. Fang, W., J. He, W. Li, X. Lan, Y. Chen, T. Li, J. Huang, and L. Zhang, *Comprehensive Android Malware Detection Based on Federated Learning Architecture*. IEEE Transactions on Information Forensics and Security, 2023. **18**: p. 3977-3990.
12. Nobakht, M., R. Javidan, and A. Pourebrahimi, *SIM-FED: Secure IoT malware detection model with federated learning*. Computers and Electrical Engineering, 2024. **116**: p. 109139.
13. Pei, X., X. Deng, S. Tian, L. Zhang, and K. Xue, *A Knowledge Transfer-Based Semi-Supervised Federated Learning for IoT Malware Detection*. IEEE Transactions on Dependable and Secure Computing, 2023. **20**(3): p. 2127-2143.
14. Jin, W., Y. Yao, S. Han, J. Gu, C. Joe-Wong, S. Ravi, S. Avestimehr, and C. He, *FedML-HE: An efficient homomorphic-encryption-based privacy-preserving federated learning system*. arXiv preprint arXiv:2303.10837, 2023.
15. Reddy, M.S., K. Chatterjee, M. Raju, S.S. Kumar, T.A.V. Reddy, and M.N. Thara. *Advancing Android Malware Detection: A Unified Framework with Dynamic Feature Extraction and Privacy-Preserving Collaboration*. in *2024 Asia Pacific Conference on Innovation in Technology (APCIT)*. 2024.
16. Cohen, E., B. Cohen-Wang, X. Lyu, J. Nelson, T. Sarlos, and U. Stemmer, *Hot pate: Private aggregation of distributions for diverse task*. arXiv preprint arXiv:2312.02132, 2023.
17. Tran, C. and F. Fioretto, *On the fairness impacts of private ensembles models*. arXiv preprint arXiv:2305.11807, 2023.
18. Yang, C.H.H., I.F. Chen, A. Stolcke, S.M. Siniscalchi, and C.H. Lee. *An Experimental Study on Private Aggregation of Teacher Ensemble Learning for End-to-End Speech Recognition*. in *2022 IEEE Spoken Language Technology Workshop (SLT)*. 2023.
19. Muthukrishnan, G. and S. Kalyani, *Grafting Laplace and Gaussian Distributions: A New Noise Mechanism for Differential Privacy*. IEEE Transactions on Information Forensics and Security, 2023. **18**: p. 5359-5374.

20. Anastasakis, Z., T.-H. Velivassaki, A. Voulkidis, S. Bourou, K. Psychogyios, D. Skias, and T. Zahariadis *FREDY: Federated Resilience Enhanced with Differential Privacy*. Future Internet, 2023. **15**, DOI: 10.3390/fi15090296.
21. Pan, Y., J. Ni, and Z. Su. *FL-PATE: Differentially Private Federated Learning with Knowledge Transfer*. in *2021 IEEE Global Communications Conference (GLOBECOM)*. 2021.
22. Watkins, W., H. Wang, S. Bae, H.H. Tseng, J. Cha, S.Y.C. Chen, and S. Yoo. *Quantum Privacy Aggregation of Teacher Ensembles (QPATE) for Privacy Preserving Quantum Machine Learning*. in *ICASSP 2024 - 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2024.
23. Choi, S., D. Patel, D. Zad Tootaghaj, L. Cao, F. Ahmed, and P. Sharma, *FedNIC: enhancing privacy-preserving federated learning via homomorphic encryption offload on SmartNIC.* Frontiers in Computer Science, 2024. **6**: p. 1465352.
24. Kabra, M., R. Nadig, H. Gupta, R. Bera, M. Frouzakis, V. Arulchelvan, Y. Liang, H. Mao, M. Sadrosadati, and O. Mutlu, *CIPHERMATCH: Accelerating Homomorphic Encryption-Based String Matching via Memory-Efficient Data Packing and In-Flash Processing*, in *Proceedings of the 30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2*. 2025, Association for Computing Machinery: Rotterdam, Netherlands. p. 111–130.
25. Ibrahim, M.A. and S.K. Hassan, *Power of Homomorphic Encryption in Secure Data Processing*. International Journal for Electronic Crime Investigation, 2024. **8**(3).
26. Fukuchi, Y., S. Hashimoto, K. Sakai, S. Fukumoto, M.T. Sun, and W.S. Ku, *Secure kNN For Distributed Cloud Environment Using Fully Homomorphic Encryption*. IEEE Transactions on Cloud Computing, 2025: p. 1-16.
27. Dakhare, B.S. and L.L. Ragha. *CKKS Homomorphic Encryption Scheme for Financial Dataset*. in *2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT)*. 2025.
28. Gandhi, B.M., S.B. Vaghadia, M. Kumhar, R. Gupta, N.K. Jadav, J. Bhatia, S. Tanwar, and A. Alabdulatif, *Homomorphic Encryption and Collaborative Machine Learning for Secure Healthcare Analytics.* Security and Privacy, 2025. **8**(1): p. e460.
29. Ali Zouaghi, Y., M. Mahamdioua, A. Lahoulou, and S. Chettibi, *Privacy preserving biometric authentication based on fully homomorphic encryption, blockchain, and IPFS data storage.* Multimedia Tools and Applications, 2025.
30. Ci, S., S. Hu, D. Guan, and Ç.K. Koç, *Privacy-preserving word vectors learning using partially homomorphic encryption*. Journal of Information Security and Applications, 2025. **89**: p. 103999.
31. Blevins, J. and J. Ueda, *Encrypted Model Reference Adaptive Control With False Data Injection Attack Resilience via Somewhat Homomorphic Encryption-Based Overflow Trap*. IEEE Transactions on Industrial Cyber-Physical Systems, 2025. **3**: p. 262-272.
32. Clet, P.-E., O. Stan, and M. Zuber. *BFV, CKKS, TFHE: Which One is the Best for a Secure Neural Network Evaluation in the Cloud?* in *Applied Cryptography and Network Security Workshops*. 2021. Cham: Springer International Publishing.
33. Asiri, M., M.A. Khemakhem, R.M. Alhebshi, B.S. Alsulami, and F.E. Eassa *RPFL: A Reliable and Privacy-Preserving Framework for Federated Learning-Based IoT Malware Detection*. Electronics, 2025. **14**, DOI: 10.3390/electronics14061089.
34. ChandraUmakantham, O.K., S. Gajendran, and S. Marappan, *Enhancing Intrusion Detection Through Federated Learning With Enhanced Ghost_BiNet and Homomorphic Encryption.* IEEE Access, 2024. **12**: p. 24879-24893.
35. Manh, B.D., C.H. Nguyen, D.T. Hoang, and D.N. Nguyen. *Homomorphic Encryption-Enabled Federated Learning for Privacy-Preserving Intrusion Detection in Resource-Constrained IoV Networks*. in *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*. 2024.
36. Guo, Y., L. Li, Z. Zheng, H. Yun, R. Zhang, X. Chang, and Z. Gao, *Efficient and Privacy-Preserving Federated Learning based on Full Homomorphic Encryption*. arXiv preprint arXiv:2403.11519, 2024.

Research Article

37. G. P, M.S., A. Mishra, A. Kaur, J.R. Sahoo, P. Aggarwal, and S. Mathur. *Secure Multi-party Computation for Privacy Preservation in Collaborative Networks*. in *2025 International Conference on Automation and Computation (AUTOCOM)*. 2025.
38. Daniel, J., *Secure Multi-Party Computation for Healthcare Big Data Queries*. 2025.
39. Salako, A.O., T.O. Adesokan-Imran, O.J. Tiwo, O.C. Metibemu, O.S. Onyenaucheya, and O.O. Olaniyi, *Securing Confidentiality in Distributed Ledger Systems with Secure Multi-party Computation for Financial Data Protection*. Journal of Engineering Research and Reports, 2025. **27**(3): p. 352-373.
40. Natarajan, D.R., S. Peddi, D.T. Valivarthi, S. Narla, S.S. Kethu, and G. Arulkumaran, *OPTIMIZED SECURE MULTI-PARTY COMPUTATION FOR CLOUD-BASED IOT DOCUMENT SHARING USING PRIVATE SET INTERSECTION*. 2025.
41. Sakraoui, S., A. Ahmim, M. Derdour, M. Ahmim, S. Namane, and I.B. Dhaou, *FBMP-IDS: FL-Based Blockchain-Powered Lightweight MPC-Secured IDS for 6G Networks*. IEEE Access, 2024. **12**: p. 105887-105905.
42. Kalapaaking, A.P., I. Khalil, and X. Yi, *Blockchain-Based Federated Learning With SMPC Model Verification Against Poisoning Attack for Healthcare Systems*. IEEE Transactions on Emerging Topics in Computing, 2024. **12**(1): p. 269-280.
43. Kalapaaking, A.P., V. Stephanie, I. Khalil, M. Atiquzzaman, X. Yi, and M. Almashor, *SMPC-Based Federated Learning for 6G-Enabled Internet of Medical Things*. IEEE Network, 2022. **36**(4): p. 182-189.
44. Elfares, M., P. Reisert, Z. Hu, W. Tang, R. Küsters, and A. Bulling, *PrivatEyes: appearance-based gaze estimation using federated secure multi-party computation*. Proceedings of the ACM on Human-Computer Interaction, 2024. **8**(ETRA): p. 1-23.