Federated Learning for Privacy-Preserving Severity Classification in Healthcare: A Secure Edge-Aggregated Approach

- **Author:** Maurya, Ankita ; Haripriya, Rahul ; Pandey, Manish ; Choudhary, Jaytrilok ; Pratap Singh, Dhirendra ; Solanki, Surendra ; Sharma, Duansh
- **Subject:** Cryptography ; Data privacy ; Edge computing ; Medical care ; Training
- **Is Part Of:** IEEE access, 2025, Vol.13, p.102339-102358
- **Description:** Federated learning (FL) has emerged as a promising paradigm for privacy-preserving machine learning across decentralized healthcare systems. This study proposes a secure and adaptive FL framework tailored for multi-institutional healthcare environments, combining structured electronic health records (EHR) and real-world ICU datasets (MIMIC-III) to predict patient severity levels. The framework incorporates secure multiparty computation (SMPC) with Shamir's Secret Sharing to ensure encrypted communication between clients and edge aggregators, preserving data confidentiality throughout the training process. A key enhancement in this work is the integration of a dynamic edge thresholding mechanism that filters client updates based on round-wise gradient variance. Unlike static thresholds, this adaptive strategy enables real-time decision-making to accept or reject updates, improving robustness against noisy or unstable contributions and simulating real-world client dropout. The system was evaluated on both synthetic and MIMIC-III datasets using CatBoost, XGBoost, and TabNet across multiple threshold configurations and client setups. Performance metrics were reported with statistical confidence, standard deviation and 95% confidence intervals across five independent runs per model. The proposed framework demonstrates high classification accuracy, scalability across clients, and improved resilience to data heterogeneity and communication noise. It further incorporates deployment-aware considerations such as latency, update frequency, and dropout tolerance, making it suitable for integration in production healthcare networks. Experimental results highlight that dynamic thresholding not only improves model convergence but also contributes to reliable, fault-tolerant learning under practical constraints.
- **Publisher:** IEEE
- **Language:** English
- **Identifier:** EISSN: 2169-3536; DOI: 10.1109/ACCESS.2025.3576135; CODEN: IAECCG

Advancing Disability Healthcare Solutions Through Privacy-Preserving Federated Learning With Theme Framework

- **Author:** Alruwaili, Madallah ; Siddiqi, Muhammad Hameed ; Idris, Muhammad ; Alruwaili, Salman ; Alanazi, Abdullah Saleh ; Khan, Faheem
- **Subject:** Liability (Law) ; Machine learning ; Medical care ; Privacy ; Reliability ; Robust control ; Trust
- **Is Part Of:** Expert systems, 2025-01, Vol.42 (1), p.n/a
- **Description:** ABSTRACT The application of machine learning, particularly federated learning, in collaborative model training, has demonstrated significant potential for enhancing diversity and efficiency in outcomes. In the healthcare domain, particularly healthcare with disabilities, the sensitive nature of data presents a significant challenge as sharing even the computation on these data can risk exposing personal health information. This research addresses the problem of enabling shared model training for healthcare data—particularly with disabilities decreasing the risk of leaking or compromising sensitive information. Technologies such as federated learning provide

solution for decentralised model training but fall short in addressing concerns related to trust building, accountability and control over participation and data. We propose a framework that integrates federated learning with advanced identity management as well as privacy and trust management technologies. Our framework called Theme (Trusted Healthcare Machine Learning Environment) leverages digital identities (e.g., W3C decentralised identifiers and verified credentials) and policy enforcements to regulate participation. This is to ensure that only authorised and trusted entities can contribute to the model training. Additionally, we introduce the mechanisms to track contributions per participant and offer the flexibility for participants to opt out of model training at any point. Participants can choose to be either contributors (providers) or consumers (model users) or both, and they can also choose to participate in subset of activities. This is particularly important in healthcare settings, where individuals and healthcare institutions have the flexibility to control how their data are used without compromising the benefits. In summary, this research work contributes to privacy preserving shared model training leveraging federated learning without exposing sensitive data; trust and accountability mechanisms; contribution tracking per participant for accountability and back-tracking; and fine-grained control and autonomy per participant. By addressing the specific needs of healthcare data for people with disabilities or such institutions, the Theme framework offers a robust solution to balance the benefits of shared machine learning with critical need to protecting sensitive data.

- **Publisher:** Oxford: Blackwell Publishing Ltd
- **Language:** English
- **Identifier:** ISSN: 0266-4720; EISSN: 1468-0394; DOI: 10.1111/exsy.13807

Enhancing Efficiency in Privacy-preserving Federated Learning for Healthcare : Adaptive Gaussian Clipping with DFT Aggregator

- **Author:** Hidayat, Muhammad Ayat ; Nakamura, Yugo ; Arakawa, Yutaka
- **Subject:** Costs ; Medical care ; Noise ; Training
- **Is Part Of:** IEEE access, 2024-01, p.1-1
- **Description:** Machine learning's exponential growth has transformed healthcare, with Federated Learning (FL) playing a pivotal role. Despite its significance, FL is vulnerable to privacy attacks. In response, researchers have integrated differential privacy (DP) into FL. Nevertheless, incorporating DP introduces challenges such as increased total communication costs and computational overheads due to the introduction of noise. This drawback renders FL with DP less viable for healthcare systems, characterized by numerous low-resource devices and network bandwidth constraints. To overcome this limitation, we propose integrating a Discrete Fourier Transform (DFT) aggregator post-noise addition to transform the gradient generated by local training before sending it to the central server. This process reduces the gradient size and provides rudimentary encryption. The evaluation results reveal the superior performance of our proposed method, demonstrating an enhanced accuracy ranging from 0.2% to 2% compared to existing differential privacy techniques, including RDP, DP-SGD, ZcDP, LDP-Fed, and DP-AdapClip. Our approach substantially reduces the total communication costs (ranging from 6% to 43% across different privacy budgets) with faster training times in healthcare datasets such as the PIMA Indian database and Breast Cancer Histopathology Images.
- **Publisher:** IEEE
- **Language:** English
- **Identifier:** EISSN: 2169-3536; DOI: 10.1109/ACCESS.2024.3418016; CODEN: IAECCG

A privacy preserving framework for federated learning in smart healthcare systems

- **Author:** Wang, Wenshuo ; Li, Xu ; Qiu, Xiuqin ; Zhang, Xiang ; Brusic, Vladimir ; Zhao, Jindong
- **Is Part Of:** Information processing & management, 2023-01, Vol.60 (1), p.103167, Article 103167
- **Description:** Federated Learning (FL) is a platform for smart healthcare systems that use wearables and other Internet of Things enabled devices. However, source inference attacks (SIAs) can infer the connection between physiological data in training datasets with FL clients and reveal the identities of participants to the attackers. We propose a comprehensive smart healthcare framework for sharing physiological data, named FRESH, that is based on FL and ring signature defense from the attacks. In FRESH, physiological data are collected from individuals by wearable devices. These data are processed by edge computing devices (e.g., mobile phones, tablet PCs) that train ML models using local data. The model parameters are uploaded by edge computing devices to the central server for joint training of FL models of disease prediction. In this procedure, certificateless ring signature is used to hide the source of parameter updates during joint training for FL to effectively resist SIAs. In the proposed ring signature schema, an improved batch verification algorithm is designed to leverage additivity of linear operations on elliptic curves and to help reduce the computing workload of the server. Experimental results demonstrate that FRESH effectively reduces the success rate of SIAs and the batch verification method significantly improves the efficiency of signature verification. FRESH can be applied to large scale smart healthcare systems with FL involving large numbers of users.
- **Publisher:** Elsevier Ltd
- **Language:** English
- **Identifier:** ISSN: 0306-4573; EISSN: 1873-5371; DOI: 10.1016/j.ipm.2022.103167

Privacy-Preserving Hybrid Federated Learning Framework for Mental Healthcare Applications: Clustered and Quantum Approaches

- **Author:** Gupta, Arti ; Kumar Maurya, Manish ; Dhere, Khyati ; Kumar Chaurasiya, Vijay
- **Subject:** Data privacy ; Medical care ; Mental health ; Quantum computing ; Training
- **Is Part Of:** IEEE access, 2024, Vol.12, p.145054-145068
- **Description:** Privacy-preserving approaches are essential in health- care applications where sensitive data is involved. Federated learning (FL) has emerged as a widely adopted approach for collaboratively training decentralized models without sharing individual health records. However, ensuring privacy in health- care data, both during training and when clients exchange their models with a central server, remains a challenge. Bias, fairness, clients heterogeneity, and constrained computation are also challenging factors. To address this challenge, in this paper, a communication-efficient and privacy-preserving hybrid Federated learning (HFL) framework is specifically designed for mental healthcare applications. Two HFL approaches, namely Clustered Federated Learning (CFL) and Quantum Federated Learning (QFL), have been proposed. CFL focuses on leveraging the learning behaviour of clients and Conversely, QFL introduces a new phase to FL by incorporating a variational quantum classifier (VQC) for classification tasks. Angle encoding is used for a quantum state preparation to enhance data encoding and learning the quantum model. Experiments were conducted on independent and identically distributed (iid) and non-independent and identically distributed (non-iid) data to evaluate the performance of the proposed methods with state-of-the-art results available in the literature. The results demonstrate exceptional performance in the case of QFL, achieving an accuracy of 84.00%. CFL also exhibits promising results with an accuracy of 78.396%. Additionally, QFL achieves 18.75% better recall and CFL has 6.24% better precision than traditional FL. Nevertheless, it's crucial to remember that every model has advantages and disadvantages of its own.

- **Publisher:** IEEE
- **Language:** English
- **Identifier:** EISSN: 2169-3536; DOI: 10.1109/ACCESS.2024.3464240; CODEN: IAECCG

Federated learning for preserving data privacy in collaborative healthcare research

- **Author:** Loftus, Tyler J ; Ruppert, Matthew M ; Shickel, Benjamin ; Ozrazgat-Baslanti, Tezcan ; Balch, Jeremy A ; Efron, Philip A ; Upchurch, Gilbert R ; Rashidi, Parisa ; Tignanelli, Christopher ; Bian, Jiang ; Bihorac, Azra
- **Subject:** Artificial intelligence ; Data integrity ; Practice Guidelines as Topic ; Privacy
- **Is Part Of:** Digital health, 2022, Vol.8, p.205520762211344-20552076221134455
- **Description:** Generalizability, external validity, and reproducibility are high priorities for artificial intelligence applications in healthcare. Traditional approaches to addressing these elements involve sharing patient data between institutions or practice settings, which can compromise data privacy (individuals' right to prevent the sharing and disclosure of information about themselves) and data security (simultaneously preserving confidentiality, accuracy, fidelity, and availability of data). This article describes insights from real-world implementation of federated learning techniques that offer opportunities to maintain both data privacy and availability via collaborative machine learning that shares knowledge, not data. Local models are trained separately on local data. As they train, they send local model updates (e.g. coefficients or gradients) for consolidation into a global model. In some use cases, global models outperform local models on new, previously unseen local datasets, suggesting that collaborative learning from a greater number of examples, including a greater number of rare cases, may improve predictive performance. Even when sharing model updates rather than data, privacy leakage can occur when adversaries perform property or membership inference attacks which can be used to ascertain information about the training set. Emerging techniques mitigate risk from adversarial attacks, allowing investigators to maintain both data privacy and availability in collaborative healthcare research. When data heterogeneity between participating centers is high, personalized algorithms may offer greater generalizability by improving performance on data from centers with proportionately smaller training sample sizes. Properly applied, federated learning has the potential to optimize the reproducibility and performance of collaborative learning while preserving data security and privacy.
- **Publisher:** London, England: SAGE Publications
- **Language:** English
- **Identifier:** ISSN: 2055-2076; EISSN: 2055-2076; DOI: 10.1177/20552076221134455; PMID: 36325438

Energy-Efficient and Privacy-Preserving Blockchain Based Federated Learning for Smart Healthcare System

- **Author:** Singh, Moirangthem Biken ; Singh, Himanshu ; Pratap, Ajay
- **Subject:** Training
- **Is Part Of:** IEEE transactions on services computing, 2024-09, Vol.17 (5), p.2392-2403
- **Description:** The privacy-focused concept of Federated Learning (FL) allows local data processing without disclosing patients' health details to a central server. However, its vulnerability to privacy breaches through shared model weights and susceptibility to a single point of failure remain concerns. Energy constraints of Wireless Body Area Networks (WBANs) necessitate considering computation and transmission energy in the FL process. Thus, this article introduces a smart

healthcare system prioritizing energy efficiency and privacy through a blockchain-backed FL model. Yet, WBAN users might be unwilling to share data without adequate incentives, and miners might hesitate due to the high energy usage associated with maintaining the blockchain. Therefore, an optimization problem is formulated to maximize system utility while considering energy, WBAN incentives, miner revenue, and FL loss. A computationally efficient stable matching-based algorithm is proposed for optimizing utility via associating WBANs and miners. Associated WBANs use Quantized Neural Networks (QNNs) to minimize computation energy. Moreover, this work integrates Differential Privacy (DP) and Homomorphic Encryption (HE) mechanisms to prevent information leakage by adding noise to gradients before updating model weights and encrypting consequences before transmitting them to miners. Real-world experiments validate the framework, yielding an average of 15.1%, 9.03%, and 15.35% improvements over existing methods.

- **Publisher:** IEEE
- **Language:** English
- **Identifier:** ISSN: 1939-1374; EISSN: 2372-0204; DOI: 10.1109/TSC.2023.3332955; CODEN: ITSCAD

Robust and Privacy-Preserving Decentralized Deep Federated Learning Training: Focusing on Digital Healthcare Applications

- **Author:** Tian, Youliang ; Wang, Shuai ; Xiong, Jinbo ; Bi, Renwan ; Zhou, Zhou ; Bhuiyan, Md Zakirul Alam
- **Subject:** Training
- **Is Part Of:** IEEE/ACM transactions on computational biology and bioinformatics, 2024-07, Vol.21 (4), p.890-901
- **Description:** Federated learning of deep neural networks has emerged as an evolving paradigm for distributed machine learning, gaining widespread attention due to its ability to update parameters without collecting raw data from users, especially in digital healthcare applications. However, the traditional centralized architecture of federated learning suffers from several problems (e.g., single point of failure, communication bottlenecks, etc.), especially malicious servers inferring gradients and causing gradient leakage. To tackle the above issues, we propose a robust and privacy-preserving decentralized deep federated learning (RPDFL) training scheme. Specifically, we design a novel ring FL structure and a Ring-Allreduce-based data sharing scheme to improve the communication efficiency in RPDFL training. Furthermore, we improve the process of distributing parameters of the Chinese residual theorem to update the execution process of the threshold secret sharing, supporting healthcare edge to drop out during the training process without causing data leakage, and ensuring the robustness of the RPDFL training under the Ring-Allreduce-based data sharing scheme. Security analysis indicates that RPDFL is provable secure. Experiment results show that RPDFL is significantly superior to standard FL methods in terms of model accuracy and convergence, and is suitable for digital healthcare applications.
- **Publisher:** United States: IEEE
- **Language:** English
- **Identifier:** ISSN: 1545-5963; ISSN: 1557-9964; EISSN: 1557-9964; DOI: 10.1109/TCBB.2023.3243932; PMID: 37028039; CODEN: ITCBCY

LEAF: A Federated Learning-Aware Privacy-Preserving Framework for Healthcare Ecosystem

- **Author:** Patel, Nisarg P. ; Parekh, Raj ; Amin, Saad Ali ; Gupta, Rajesh ; Tanwar, Sudeep ; Kumar, Neeraj ; Iqbal, Rahat ; Sharma, Ravi
- **Subject:** Algorithms ; Artificial intelligence ; Cryptography ; Machine learning ; Privacy ; Training ; Tumors
- **Is Part Of:** IEEE eTransactions on network and service management, 2024-02, Vol.21 (1), p.1129-1141
- **Description:** Over the last decades, the healthcare industry has been revolutionized heavily, especially after the Covid-19 surge. Various artificial intelligence (AI) approaches have also been explored during this era for their applicability in healthcare. However, traditional AI techniques and algorithms are prone to overfitting with minimal robustness to unseen or untrained data. So, there is a need for new techniques which can overcome the issues mentioned earlier. Federated learning (FL) can help design specific AI services for the network of hospitals with less overfitting and more robust modules. However, with the inclusion of FL, the problem related to user privacy is the biggest challenge, making the use of FL in the real world a grand challenge. Most solutions presented in the literature used blockchain technology to mitigate the issues mentioned earlier. However, it prevents third-party systems from penetrating the decision process, but the network devices can access shared data. Moreover, blockchain implementation requires new paradigms and infrastructure with an additional overhead cost. Motivated by these facts, the paper presents a limited access encryption algorithm incorporating FL (LEAF) framework, i.e., an encryption technique that solves privacy issues with the help of edge-enabled AI models. The proposed LEAF framework preserves user privacy and minimizes overhead costs. The authors have evaluated the performance of the LEAF framework using extensive simulations and achieved superior results. The achieved accuracy of the proposed LEAF framework is 3% higher than that of the traditional centralized and FL-based systems without compromising user privacy. In the best scenario, the proposed framework's encryption process also compresses the data size by 4-5 times.
- **Publisher:** New York: IEEE
- **Language:** English
- **Identifier:** ISSN: 1932-4537; EISSN: 1932-4537; DOI: 10.1109/TNSM.2023.3287393; CODEN: ITNSC4

A Fog-Based Privacy-Preserving Federated Learning System for Smart Healthcare Applications

- **Author:** Butt, Maryum ; Tariq, Noshina ; Ashraf, Muhammad ; Alsagri, Hatoon S. ; Moqurrab, Syed Atif ; Alhakbani, Haya Abdullah A. ; Alduraywish, Yousef A.
- **Subject:** Artificial intelligence ; Classification ; Computer architecture ; Coronaviruses ; COVID-19 Pandemic, 2020- ; Diagnostic imaging ; Edge computing ; Health Care Sector ; Health facilities ; Machine learning ; Medical electronics ; Neural networks (Computer science) ; Privacy ; X-rays
- **Is Part Of:** Electronics (Basel), 2023-10, Vol.12 (19), p.4074
- **Description:** During the COVID-19 pandemic, the urgency of effective testing strategies had never been more apparent. The fusion of Artificial Intelligence (AI) and Machine Learning (ML) models, particularly within medical imaging (e.g., chest X-rays), holds promise in smart healthcare systems. Deep Learning (DL), a subset of AI, has exhibited prowess in enhancing classification accuracy, a crucial aspect in expediting COVID-19 diagnosis. However, the journey to harness DL's potential is rife with challenges: notably, the intricate landscape of medical data privacy. Striking a balance between utilizing patient data for insights while upholding privacy is formidable. Federated Learning (FL) emerges as a solution by enabling collaborative model training across decentralized data sources, thus bypassing data centralization and preserving data privacy. This study presents a tailored, collaborative FL architecture for COVID-19 screening via chest X-ray images. Designed to facilitate cooperation among medical institutions, the framework ensures patient data remain

localized, eliminating the need for direct data sharing. Addressing imbalanced and non-identically distributed data, the architecture is a robust solution. Implementation entails localized and fog-computing-based FL models. Localized models utilize Convolutional Neural Networks (CNNs) on institution-specific datasets, while the FL model, refined iteratively, takes precedence in the final classification. Intriguingly, the global FL model, fortified by fog computing, emerges as the frontrunner in classification after weight refinement, surpassing local models. Validation within the COLAB platform gauges the model's performance through metrics such as accuracy, precision, recall, and F1-score. Remarkably, the proposed model excels across these metrics, solidifying its efficacy. This research navigates the confluence of AI, FL, and medical imaging, unveiling insights that could reshape healthcare delivery. The study enriches scientific discourse by addressing data privacy in collaborative learning and carries potential implications for enhanced patient care.
- **Publisher:** Basel: MDPI AG
- **Language:** English
- **Identifier:** ISSN: 2079-9292; EISSN: 2079-9292; DOI: 10.3390/electronics12194074

AP2FL: Auditable Privacy-Preserving Federated Learning Framework for Electronics in Healthcare

- **Author:** Yazdinejad, Abbas ; Dehghantanha, Ali ; Srivastava, Gautam
- **Subject:** Auditing ; Data privacy ; Electronics ; Machine learning ; Medical care ; Privacy ; Training
- **Is Part Of:** IEEE transactions on consumer electronics, 2024-02, Vol.70 (1), p.2527-2535
- **Description:** The growing application of machine learning (ML) techniques in healthcare has led to increased interest in federated learning (FL), which enables the secure and private training of robust ML models. However, conventional FL methods often fall short of providing adequate privacy protection and face challenges in handling non-independent and identically distributed (Non-IID) training data. These shortcomings are of significant concern when employing FL in electronic devices in healthcare. To address these issues, we propose an Auditable Privacy-Preserving Federated Learning (AP2FL) model tailored for electronics in healthcare settings. By leveraging Trusted Execution Environments (TEE), AP2FL ensures secure training and aggregation processes on both client and server sides, effectively mitigating data leakage risks. To manage Non-IID data within the proposed framework, we incorporate the Active Personalized Federated Learning (ActPerFL) model and Batch Normalization (BN) techniques to consolidate user updates and identify data similarities. Additionally, we introduce an auditing mechanism in AP2FL that reveals the contribution of each client to the FL process, facilitating the updating of the global model following diverse data types and distributions. In other words, it ensures the FL process's integrity, transparency, fairness, and robustness. Our results demonstrate that the proposed AP2FL model outperforms existing methods in accuracy and effectively eliminates privacy leakage.
- **Publisher:** New York: IEEE
- **Language:** English
- **Identifier:** ISSN: 0098-3063; EISSN: 1558-4127; DOI: 10.1109/TCE.2023.3318509; CODEN: ITCEDA

Homomorphic Encryption-Based Privacy-Preserving Federated Learning in IoT-Enabled Healthcare System

- **Author:** Zhang, Li ; Xu, Jianbo ; Vijayakumar, Pandi ; Sharma, Pradip Kumar ; Ghosh, Uttam
- **Subject:** Cryptography ; Internet of things ; Medical care ; Privacy

- **Is Part Of:** IEEE transactions on network science and engineering, 2023-09, Vol.10 (5), p.2864-2880
- **Description:** In this work, the federated learning mechanism is introduced into the deep learning of medical models in Internet of Things (IoT)-based healthcare system. Cryptographic primitives, including masks and homomorphic encryption, are applied for further protecting local models, so as to prevent the adversary from inferring private medical data by various attacks such as model reconstruction attack or model inversion attack, etc. The qualities of the datasets owned by different participants are considered as the main factor for measuring the contribution rate of the local model to the global model in each training epoch, instead of the size of datasets commonly used in deep learning. A dropout-tolerable scheme is proposed in which the process of federated learning would not be terminated if the number of online clients is not less than a preset threshold. Through the analysis of the security, it shows that the proposed scheme satisfies data privacy. Computation cost and communication cost are also analyzed theoretically. Finally, skin lesion classification using training images provided by the HAM10000 medical dataset is set as an example of healthcare applications. Experimental results show that compared with existing schemes, the proposed scheme obtained promising results while ensuring privacy preserving.
- **Publisher:** Piscataway: IEEE
- **Language:** English
- **Identifier:** ISSN: 2327-4697; EISSN: 2334-329X; DOI: 10.1109/TNSE.2022.3185327; CODEN: ITNSD5

Privacy-Preserving Federated Learning in Healthcare, E-Commerce, and Finance: A Taxonomy of Security Threats and Mitigation Strategies

- **Author:** Kumar Rahul ; Shieh Chin-Shiuh ; Chakrabarti Prasun ; Kumar Ashok ; Moolchandani Jhankar ; Sinha Raj
- **Is Part Of:** EPJ Web of conferences, 2025-01, Vol.328, p.01066
- **Description:** Federated Learning (FL) transformed decentralized machine learning by allowing joint model training without mutually sharing raw data, hence being especially useful in privacy-sensitive applications like healthcare, e-commerce, and finance. Even with its privacy-focused architecture, FL is vulnerable to a range of security attacks such as data poisoning, model inversion, membership inference attacks, and communication interception. These attacks compromise the confidentiality of patients in healthcare, consumer data privacy in e-commerce, and financial safety in banking, thus necessitating effective privacy-preserving mechanisms. This survey presents a classification of security threats in FL, grouping them by their source, effect, and attack mode. We review state-of-the-art countermeasures, such as differential privacy, secure multi-party computation, homomorphic encryption, and resilient aggregation methods, their effectiveness, trade-offs, and real-world applicability to FL. In medicine, FL enables joint disease diagnosis without compromising patient confidentiality; in online shopping, it provides personalized suggestions without revealing customer tastes; and in banking, it improves fraud detection without violating regulatory requirements. In addition, we discuss future horizons in privacy-preserving FL, including adversarial robustness, blockchain-protected models, and tailored FL architectures, improving security and resiliency in these domains. We also discuss the balancing problems between security, accuracy, and computational efficiency with possible trade-offs in scaling privacy-preserving FL By analyzing threats and mitigation strategies systematically, this paper will provide direction to future research on designing secure, scalable, and privacy-preserving FL frameworks for the changing healthcare, e-commerce, and finance needs.
- **Publisher:** EDP Sciences
- **Language:** English

- **Identifier:** EISSN: 2100-014X; DOI: 10.1051/epjconf/202532801066

Advancing Privacy-Preserving Health Care Analytics and Implementation of the Personal Health Train: Federated Deep Learning Study

- **Author:** Choudhury, Ananya ; Volmer, Leroy ; Martin, Frank ; Fijten, Rianne ; Wee, Leonard ; Dekker, Andre ; Soest, Johan van
- **Is Part Of:** JMIR AI, 2025-02, Vol.4, p.e60847
- **Description:** The rapid advancement of deep learning in health care presents significant opportunities for automating complex medical tasks and improving clinical workflows. However, widespread adoption is impeded by data privacy concerns and the necessity for large, diverse datasets across multiple institutions. Federated learning (FL) has emerged as a viable solution, enabling collaborative artificial intelligence model development without sharing individual patient data. To effectively implement FL in health care, robust and secure infrastructures are essential. Developing such federated deep learning frameworks is crucial to harnessing the full potential of artificial intelligence while ensuring patient data privacy and regulatory compliance. The objective is to introduce an innovative FL infrastructure called the Personal Health Train (PHT) that includes the procedural, technical, and governance components needed to implement FL on real-world health care data, including training deep learning neural networks. The study aims to apply this federated deep learning infrastructure to the use case of gross tumor volume segmentation on chest computed tomography images of patients with lung cancer and present the results from a proof-of-concept experiment. The PHT framework addresses the challenges of data privacy when sharing data, by keeping data close to the source and instead bringing the analysis to the data. Technologically, PHT requires 3 interdependent components: "tracks" (protected communication channels), "trains" (containerized software apps), and "stations" (institutional data repositories), which are supported by the open source "Vantage6" software. The study applies this federated deep learning infrastructure to the use case of gross tumor volume segmentation on chest computed tomography images of patients with lung cancer, with the introduction of an additional component called the secure aggregation server, where the model averaging is done in a trusted and inaccessible environment. We demonstrated the feasibility of executing deep learning algorithms in a federated manner using PHT and presented the results from a proof-of-concept study. The infrastructure linked 12 hospitals across 8 nations, covering 4 continents, demonstrating the scalability and global reach of the proposed approach. During the execution and training of the deep learning algorithm, no data were shared outside the hospital. The findings of the proof-of-concept study, as well as the implications and limitations of the infrastructure and the results, are discussed. The application of federated deep learning to unstructured medical imaging data, facilitated by the PHT framework and Vantage6 platform, represents a significant advancement in the field. The proposed infrastructure addresses the challenges of data privacy and enables collaborative model development, paving the way for the widespread adoption of deep learning-based tools in the medical domain and beyond. The introduction of the secure aggregation server implied that data leakage problems in FL can be prevented by careful design decisions of the infrastructure. ClinicalTrials.gov NCT05775068; https://clinicaltrials.gov/study/NCT05775068.
- **Publisher:** Canada
- **Language:** English
- **Identifier:** ISSN: 2817-1705; EISSN: 2817-1705; DOI: 10.2196/60847; PMID: 39912580

Generative Federated Learning with Small and Large Models In Consumer Electronics for Privacy preserving Data Fusion in Healthcare Internet of Things

- **Author:** Ghazal, Taher M. ; Islam, Shayla ; Hasan, Mohammad Kamrul ; Abu-Shareha, Ahmad A. ; Mokhtar, Umi A. ; Khan, M. Attique ; Baili, Jamel ; Saeed, Ali Q ; Bhattt, Mohammed Wasim ; Ahmad, Munir
- **Subject:** Data privacy ; Internet of things ; Medical care
- **Is Part Of:** IEEE transactions on consumer electronics, 2025, p.1-1
- **Description:** Healthcare Internet of Things (HIoT) requires large-scale privacy features to ensure maximum security in sharing sensitive physiological data in consumer electronics. Recent approaches utilize the fusion concept to provide maximum privacy in health data sharing. Embedded signing data fusion with the health observed data ensures privacy preserved sharing across heterogeneous medical consumer devices for diagnosis. This article proposes a Dependency-correlated Data Fusion Scheme (DcDFS) to maximize the privacy of the health data-sharing process. The proposed scheme prepares separate key signing procedures using triple-DES (data encryption standard) to embed with the accumulated health data. The fusion process is carried out by defining key headers and integrity footers for authentication and verification. Therefore, the fusion generates a combined sequence of linear authentication and validation procedures enclosing the health data. In this scheme, the role of federated learning is to prevent permuted sequences for the same health data. This research integrates Small Language Model (SLM) and Large Language Model (LLM) into the federated learning module to support secure, scalable, and intelligent healthcare data sharing. Their collaboration enhances context-aware training while preserving privacy across decentralized, encrypted environments. A similar sequence mapped between the header and footer is responsible for discarding unauthorized data handling. The learning process verifies the permutation for many-to-one header to footer and vice versa. Therefore, the proposed fusion scheme generates a linear dependency between the actual and security-related data for maximum privacy. The proposed scheme achieves the following: the computation time is confined by 12.424%, the privacy leakage by 12.923%, and the computation efficiency is improved by 11.46%, as observed under the maximum sequences.
- **Publisher:** IEEE
- **Language:** English
- **Identifier:** ISSN: 0098-3063; EISSN: 1558-4127; DOI: 10.1109/TCE.2025.3572629; CODEN: ITCEDA

Studying the association of diabetes and healthcare cost on distributed data from the Maastricht Study and Statistics Netherlands using a privacy-preserving federated learning infrastructure

- **Author:** Sun, Chang ; van Soest, Johan ; Koster, Annemarie ; Eussen, Simone J.P.M. ; Schram, Miranda T. ; Stehouwer, Coen D.A. ; Dagnelie, Pieter C. ; Dumontier, Michel
- **Subject:** Type 2 diabetes
- **Is Part Of:** Journal of biomedical informatics, 2022-10, Vol.134, p.104194-104194, Article 104194
- **Description:** The mining of personal data collected by multiple organizations remains challenging in the presence of technical barriers, privacy concerns, and legal and/or organizational restrictions. While a number of privacy-preserving and data mining frameworks have recently emerged, much remains to show their practical utility. In this study, we implement and utilize a secure infrastructure using data from Statistics Netherlands and the Maastricht Study to learn the association between Type 2 Diabetes Mellitus (T2DM) and healthcare expenses considering the impact of lifestyle, physical activities, and complications of T2DM. Through experiments using real-world distributed personal data, we present the feasibility and effectiveness of the secure infrastructure for practical use cases of linking and analyzing vertically partitioned data across multiple organizations. We

discovered that individuals diagnosed with T2DM had significantly higher expenses than those with prediabetes, while participants with prediabetes spent more than those without T2DM in all the included healthcare categories to different degrees. We further discuss a joint effort from technical, ethical–legal, and domain-specific experts that is highly valued for applying such a secure infrastructure to real-life use cases to protect data privacy. [Display omitted]

- **Publisher:** Elsevier Inc
- **Language:** English
- **Identifier:** ISSN: 1532-0464; EISSN: 1532-0480; DOI: 10.1016/j.jbi.2022.104194

Secure, privacy-preserving and federated machine learning in medical imaging

- **Author:** Kaissis, Georgios A. ; Makowski, Marcus R. ; Rückert, Daniel ; Braren, Rickmer F.
- **Subject:** Algorithms ; Artificial intelligence ; Computer peripherals ; Diagnostic imaging ; Digital images ; Digitization ; Electronic Health Records ; Engineering ; Hospitals ; Implements ; Information retrieval ; Liability (Law) ; Machine learning ; Medicine ; Perspective ; Privacy ; Transparency
- **Is Part Of:** Nature machine intelligence, 2020-06, Vol.2 (6), p.305-311
- **Description:** The broad application of artificial intelligence techniques in medicine is currently hindered by limited dataset availability for algorithm training and validation, due to the absence of standardized electronic medical records, and strict legal and ethical requirements to protect patient privacy. In medical imaging, harmonized data exchange formats such as Digital Imaging and Communication in Medicine and electronic data storage are the standard, partially addressing the first issue, but the requirements for privacy preservation are equally strict. To prevent patient privacy compromise while promoting scientific research on large datasets that aims to improve patient care, the implementation of technical solutions to simultaneously address the demands for data protection and utilization is mandatory. Here we present an overview of current and next-generation methods for federated, secure and privacy-preserving artificial intelligence with a focus on medical imaging applications, alongside potential attack vectors and future prospects in medical imaging and beyond. Medical imaging data is often subject to privacy and intellectual property restrictions. AI techniques can help out by offering tools like federated learning to bridge the gap between personal data protection and data utilisation for research and clinical routine, but these tools need to be secure.
- **Publisher:** London: Nature Publishing Group UK
- **Language:** English
- **Identifier:** ISSN: 2522-5839; EISSN: 2522-5839; DOI: 10.1038/s42256-020-0186-1

Toward Secure Weighted Aggregation for Privacy-Preserving Federated Learning

- **Author:** He, Yunlong ; Yu, Jia
- **Subject:** Cryptography ; Data privacy ; Interpolation ; Polynomials ; Privacy ; Training
- **Is Part Of:** IEEE transactions on information forensics and security, 2025, Vol.20, p.3475-3488
- **Description:** Privacy-preserving federated learning can protect the privacy of model gradients/parameters in the model aggregation phase. Most existing schemes only consider the scenario where user models have the same weight in model aggregation. However, users often hold different numbers of training samples in practice. This makes the model convergence speed of existing schemes very slow. To solve this problem, we propose a privacy-preserving federated learning scheme with secure weighted aggregation. It is able to allocate appropriate user weights

based on the user's local data size with privacy protection. In addition, it is impossible for the cloud server to obtain the user's original model parameters and local data size in the proposed scheme. Specifically, we use Lagrange interpolation to combine the model parameters and local data size into a set of ciphertexts. The cloud server can smoothly perform weighted aggregation based on these ciphertexts. Leveraging the Chinese Remainder Theorem, we convert the local data size into a series of verification values. This enables the user to verify the correctness of results returned from the server. We provide a theoretical analysis for the proposed scheme, demonstrating its effectiveness, privacy, and verifiability. We perform extensive experiments on the MNIST dataset. Experimental results demonstrate its model performance, computation overhead, and communication overhead.
- **Publisher:** IEEE
- **Language:** English
- **Identifier:** ISSN: 1556-6013; EISSN: 1556-6021; DOI: 10.1109/TIFS.2025.3550787; CODEN: ITIFA6

BPS-FL: Blockchain-Based Privacy-Preserving and Secure Federated Learning

- **Author:** Yu, Jianping ; Yao, Hang ; Ouyang, Kai ; Cao, Xiaojun ; Zhang, Lianming
- **Subject:** Privacy
- **Is Part Of:** Big Data Mining and Analytics, 2025-02, Vol.8 (1), p.189-213
- **Description:** Federated Learning (FL) enables clients to securely share gradients computed on their local data with the server, thereby eliminating the necessity to directly expose their sensitive local datasets. In traditional FL, the server might take advantage of its dominant position during the model aggregation process to infer sensitive information from the shared gradients of the clients. At the same time, malicious clients may submit forged and malicious gradients during model training. Such behavior not only compromises the integrity of the global model, but also diminishes the usability and reliability of trained models. To effectively address such privacy and security attack issues, this work proposes a Blockchain-based Privacy-preserving and Secure Federated Learning (BPS-FL) scheme, which employs the threshold homomorphic encryption to protect the local gradients of clients. To resist malicious gradient attacks, we design a Byzantine-robust aggregation protocol for BPS-FL to realize the cipher-text level secure model aggregation. Moreover, we use a blockchain as the underlying distributed architecture to record all learning processes, which ensures the immutability and traceability of the data. Our extensive security analysis and numerical evaluation demonstrate that BPS-FL satisfies the privacy requirements and can effectively defend against poisoning attacks.
- **Publisher:** Beijing: Tsinghua University Press
- **Language:** English
- **Identifier:** ISSN: 2096-0654; EISSN: 2097-406X; DOI: 10.26599/BDMA.2024.9020053

PQSF: post-quantum secure privacy-preserving federated learning

- **Author:** Zhang, Xia ; Deng, Haitao ; Wu, Rui ; Ren, Jingjing ; Ren, Yongjun
- **Subject:** Computers ; Learning ; Privacy ; Science
- **Is Part Of:** Scientific reports, 2024-10, Vol.14 (1), p.23553-16, Article 23553
- **Description:** In federated learning, secret sharing is a key technology to maintain the privacy of participants' local models. Moreover, with the rapid development of quantum computers, existing federated learning privacy protection schemes based on secret sharing will no longer be able to

guarantee the data security of participants in the post-quantum era. In addition, existing privacy protection methods have the problem of high communication and computational overhead. Although the multi-stage secret sharing scheme proposed by Pilaram et al. is one of the effective solutions to the above problems, existing studies have proven the privacy leakage risk of this scheme. This paper firstly designs a new lattice-based multi-stage secret sharing scheme Improved-Pilaram to solve the security problem, which allows participants to use public vectors to reconstruct different secret values without changing the secret sharing. Based on Improved-Pilaram , this article proposes a post-quantum secure federated learning scheme PQSF . PQSF uses double masking technology to encrypt model parameters and achieves mask reconstruction through secret sharing. Since Improved-Pilaram is multi-stage, participants do not need to update their local secret shares frequently during training. Analysis and experimental results show that the PQSF proposed in this paper reduces the communication complexity between participants and reduces the computational overhead by about 20% compared with existing solutions.

- **Publisher:** London: Nature Publishing Group UK
- **Language:** English
- **Identifier:** ISSN: 2045-2322; EISSN: 2045-2322; DOI: 10.1038/s41598-024-74377-6; PMID: 39384909

Privacy preserving and secure robust federated learning: A survey

- **Author:** Han, Qingdi ; Lu, Siqi ; Wang, Wenhao ; Qu, Haipeng ; Li, Jingsheng ; Gao, Yang
- **Subject:** Cluster analysis ; Cryptography ; Machine learning ; Privacy
- **Is Part Of:** Concurrency and computation, 2024-06, Vol.36 (13), p.n/a
- **Description:** Summary Federated learning (FL) has emerged as a promising solution to address the challenges posed by data silos and the need for global data fusion. It offers a distributed machine learning framework with privacy-preserving features, allowing model training without the need to collect user data. However, FL also presents significant security and privacy threats that hinder its widespread adoption. The requirements of privacy and security in FL are inherently conflicting. Privacy necessitates the concealment of individual client updates, while security requires the disclosure of client updates to detect anomalies. While most existing research focused on the privacy and security aspects of FL, very few studies have addressed the compatibility of these two demands. In this work, we aim to bridge this gap by proposing a comprehensive defense scheme that ensures privacy, security, and compatibility in FL. We categorize the existing literature into two key directions: privacy defense and security defense. Privacy defense includes methods based on additive masks, differential privacy, homomorphic encryption, and trusted execution environment, whereas security defense encompasses distance-, performance-, clustering-, and similarity-based anomaly detection techniques and statistical information-based anomaly update bypassing techniques when the server is trusted and privacy-compatible anomaly update detection techniques when the server is not trusted. In addition, this article presents decentralized FL solutions based on blockchain. For each direction, we discuss specific technical solutions, their advantages, and disadvantages. By evaluating various defense methods, we identify the most suitable approach to address the primary challenge of “achieving a secure and robust FL system against malicious adversaries while protecting users' privacy.” We then propose a theoretical reference framework for end-to-end protection of privacy and security in FL for the key problem, which summarizes the attack surface of FL systems from the client to the server under the security model where the client and server are malicious. Leveraging the strengths and characteristics of existing schemes, our proposed framework integrates multiple techniques to strike a balance between privacy, usability, and efficiency. This framework serves as a valuable reference and provides insights for future work in the field. Finally, we also provide recommendations for future research directions in this field.

- **Publisher:** Hoboken: Wiley Subscription Services, Inc
- **Language:** English
- **Identifier:** ISSN: 1532-0626; EISSN: 1532-0634; DOI: 10.1002/cpe.8084

An Innovative Secure and Privacy-Preserving Federated Learning-Based Hybrid Deep Learning Model for Intrusion Detection in Internet-Enabled Wireless Sensor Networks

- **Author:** Jeyakumar, Soumya Ranjan ; Rahman, Mohammad Zia Ur ; Sinha, Deepak K. ; Kumar, P. Rajendra ; Vimal, Vrince ; Singh, Kamred Udham ; Syamsundararao, Thalakola ; Kumar, J. N. V. R. Swarup ; Balajee, J.
- **Subject:** Computer architecture ; Decision making ; Internet of things ; Microcomputers ; Microprocessors ; Wireless sensor networks
- **Is Part Of:** IEEE transactions on consumer electronics, 2024, Vol.71 (1), p.273-280
- **Description:** Cyberspace faces numerous security challenges, necessitating advanced research in intrusion detection systems (IDS) to mitigate vulnerabilities. Wireless Sensor Networks (WSNs) connected to the Internet are particularly vulnerable, requiring robust protection mechanisms. Traditional IDS struggle with identifying unknown attacks and maintaining data privacy, especially in WSNs. This study proposes a novel approach integrating Stacked Convolutional Neural Networks (SCNN), Bidirectional Long Short Term Memory (Bi-LSTM), and the African Vulture Optimization Algorithm (AVOA) within a framework of Federated Learning (FL). The integrated model, SCNN-Bi-LSTM-AVOA-FL, aims to enhance intrusion detection efficacy while preserving data privacy. A tailored AVOA optimization method fine-tunes SCNN-Bi-LSTM hyperparameters, leveraging specialized datasets (WSN-DS, CIC-IDS-2017, and WSN-BFSF) for attack detection and categorization. Evaluations compare variants with and without FL techniques (proposed-1 and proposed-2) across metrics such as accuracy, precision, recall, and F1-Score. Results demonstrate significant improvements in prediction performance, validating the efficacy of the proposed approach in enhancing IDS capabilities for WSNs. This research contributes a comprehensive framework for addressing security challenges in WSNs through advanced machine learning and optimization techniques.
- **Publisher:** IEEE
- **Language:** English
- **Identifier:** ISSN: 0098-3063; EISSN: 1558-4127; DOI: 10.1109/TCE.2024.3442015; CODEN: ITCEDA

Masking and Homomorphic Encryption-Combined Secure Aggregation for Privacy-Preserving Federated Learning

- **Author:** Park, Soyoung ; Lee, Junyoung ; Harada, Kaho ; Chi, Jeonghee
- **Subject:** Communication ; Learning ; Methodology ; Methods ; Privacy
- **Is Part Of:** Electronics (Basel), 2025-01, Vol.14 (1), p.177
- **Description:** Secure aggregation of local learning model parameters is crucial for achieving privacy-preserving federated learning. This paper presents a novel and practical aggregation method that effectively combines the advantages of masking-based aggregation with those of homomorphic encryption-based techniques. Each node conceals its local parameters using a randomly selected mask, independently chosen, thereby eliminating the need for additional computations to generate or exchange mask values with other nodes. Instead, each node homomorphically encrypts its random mask using its own encryption key. During each federated learning round, nodes send their

masked parameters and the homomorphically encrypted mask to the federated learning server. The server then aggregates these updates in an encrypted state, directly calculating the average of actual local parameters across all nodes without the necessity to decrypt the aggregated result separately. To facilitate this, we introduce a new multi-key homomorphic encryption technique tailored for secure aggregation in federated learning environments. Each node uses a different encryption key to encrypt its mask value. Importantly, the ciphertext of each mask includes a partial decryption component from the node, allowing the collective sum of encrypted masks to be automatically decrypted once all are aggregated. Consequently, the server computes the average of the actual local parameters by simply subtracting the decrypted total sum of mask values from the cumulative sum of the masked local parameters. Our approach effectively eliminates the need for interactions between nodes and the server for mask generation and sharing, while addressing the limitation of a single key homomorphic encryption. Moreover, the proposed aggregation process completes the global model update in just two interactions (in the absence of dropouts), significantly simplifying the aggregation procedure. Utilizing the CKKS (Cheon-Kim-Kim-Song) homomorphic encryption scheme, our method ensures efficient aggregation without compromising security or accuracy. We demonstrate the accuracy and efficiency of the proposed method through varied experiments on MNIST data.
- **Publisher:** Basel: MDPI AG
- **Language:** English
- **Identifier:** ISSN: 2079-9292; EISSN: 2079-9292; DOI: 10.3390/electronics14010177

VANTAGE6: an open source priVAcy preserviNg federaTed leArninG infrastructurE for Secure Insight eXchange

- **Author:** Moncada-Torres, Arturo ; Martin, Frank ; Sieswerda, Melle ; Van Soest, Johan ; Geleijnse, Gijs
- **Subject:** Confidential communications ; Human beings ; Learning ; Machine learning ; Privacy
- **Is Part Of:** AMIA ... Annual Symposium proceedings, 2020, Vol.2020, p.870-877
- **Description:** Answering many of the research questions in the field of cancer informatics requires incorporating and centralizing data that are hosted by different parties. Federated Learning (FL) has emerged as a new approach in which a global model can be generated without disclosing private patient data by keeping them at their original location. Flexible, user-friendly, and robust infrastructures are crucial for bringing FL solutions to the day-to-day work of the cancer epidemiologist. In this paper, we present an open source priVAcy preserviNg federaTed leArninG infrastructurE for Secure Insight eXchange, VANTAGE6. We provide a detailed description of its conceptual design, modular architecture, and components. We also show a few examples where VANTAGE6 has been successfully used in research on observational cancer data. Developing and deploying technology to support federated analyses - such as VANTAGE6 - will pave the way for the adoption and mainstream practice of this new approach for analyzing decentralized data.
- **Publisher:** United States: American Medical Informatics Association
- **Language:** English
- **Identifier:** EISSN: 1559-4076; PMID: 33936462

Secure and Flexible Privacy-Preserving Federated Learning Based on Multi-Key Fully Homomorphic Encryption

- **Author:** Shen, Jiachen ; Zhao, Yekang ; Huang, Shitao ; Ren, Yongjun

- **Subject:** Algorithms ; Communication ; Confidential communications ; Cryptography ; Efficiency ; Investment analysis ; Machine learning ; Multiplication ; Privacy ; Privacy, Right of
- **Is Part Of:** Electronics (Basel), 2024-11, Vol.13 (22), p.4478
- **Description:** Federated learning avoids centralizing data in a central server by distributing the model training process across devices, thus protecting privacy to some extent. However, existing research shows that model updates (e.g., gradients or weights) exchanged during federated learning may still indirectly leak sensitive information about the original data. Currently, single-key homomorphic encryption methods applied in federated learning cannot solve the problem of privacy leakage that may be caused by the collusion between the participant and the federated learning server, whereas existing privacy-preserving federated learning schemes based on multi-key homomorphic encryption in semi-honest environments have deficiencies and limitations in terms of security and application conditions. To this end, this paper proposes a privacy-preserving federated learning scheme based on multi-key fully homomorphic encryption to cope with the potential risk of privacy leakage in traditional federated learning. We designed a multi-key fully homomorphic encryption scheme, mMFHE, that encrypts by aggregating public keys and requires all participants to jointly participate in decryption sharing, thus ensuring data security and privacy. The proposed privacy-preserving federated learning scheme encrypts the model updates through multi-key fully homomorphic encryption, ensuring confidentiality under the CRS model and in a semi-honest environment. As a fully homomorphic encryption scheme, mMFHE supports homomorphic addition and homomorphic multiplication for more flexible applications. Our security analysis proves that the scheme can withstand collusive attacks by up to N−1 users and servers, where N is the total number of users. Performance analysis and experimental results show that our scheme reduces the complexity of the NAND gate, which reduces the computational load and improves the efficiency while ensuring the accuracy of the model.
- **Publisher:** Basel: MDPI AG
- **Language:** English
- **Identifier:** ISSN: 2079-9292; EISSN: 2079-9292; DOI: 10.3390/electronics13224478

[PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for Industrial IoTs]

- **Author:** Hamouda, Djallel ; Ferrag, Mohamed Amine ; Benhamida, Nadjette ; Seridi, Hamid
- **Is Part Of:** Pervasive and mobile computing, 2023-01, Vol.88, p.101738, Article 101738
- **Description:** The growing reliance of industry 4.0/5.0 on emergent technologies has dramatically increased the scope of cyber threats and data privacy issues. Recently, federated learning (FL) based intrusion detection systems (IDS) promote the detection of large-scale cyber-attacks in resource-constrained and heterogeneous industrial systems without exposing data to privacy issues. However, the inherent characteristics of the latter have led to problems such as a trusted validation and consensus of the federation, unreliability, and privacy protection of model upload. To address these challenges, this paper proposes a novel privacy-preserving secure framework, named PPSS, based on the use of blockchain-enabled FL with improved privacy, verifiability, and transparency. The PPSS framework adopts the permissioned-blockchain system to secure multi-party computation as well as to incentivize cross-silo FL based on a lightweight and energy-efficient consensus protocol named Proof-of-Federated Deep-Learning (PoFDL). Specifically, we design two federated stages for global model aggregation. The first stage uses differentially private training of Stochastic Gradient Descent (DP-SGD) to enforce privacy protection of client updates, while the second stage uses PoFDL protocol to prove and add new model-containing blocks to the blockchain. We study the performance of the proposed PPSS framework using a new cyber security dataset (Edge-IIoT dataset) in terms of detection rate, precision, accuracy, computation, and energy

cost. The results demonstrate that the PPSS framework system can detect industrial IIoT attacks with high classification performance under two distribution modes, namely, non-independent and identically distributed (Non-IID) and independent and identically distributed (IID).
- **Publisher:** Elsevier B.V
- **Language:** English
- **Identifier:** ISSN: 1574-1192; EISSN: 1873-1589; DOI: 10.1016/j.pmcj.2022.101738

NSPFL: A Novel Secure and Privacy-Preserving Federated Learning With Data Integrity Auditing

- **Author:** Zhang, Zehu ; Li, Yanping
- **Subject:** Data integrity ; Data privacy ; Integrity ; Machine learning ; Privacy ; Training
- **Is Part Of:** IEEE transactions on information forensics and security, 2024, Vol.19, p.4494-4506
- **Description:** Federated learning (FL) is a new distributed machine learning framework that emerged in recent years, which can protect the participants' data privacy to a certain extent without exchanging the participants' original data. Unfortunately, it can still be vulnerable to privacy attacks (e.g. membership inference attacks) or security attacks (e.g. model poisoning attacks), which can compromise participants' data or corrupt the trained model. Inspired by the existing works, we propose a novel federated learning framework with data integrity auditing called NSPFL. First, NSPFL protects against privacy attacks by using a single mask to hide the participants' original data. Second, NSPFL constructs a novel reputation evaluation method to resist security attacks by measuring the distance between the previous and current aggregated gradients. Third, NSPFL utilizes the data stored on the cloud to prevent malicious Byzantine participants from denying behaviors. Finally, sufficient theoretical analysis proves the reliability of the scheme, and a large number of experiments demonstrate the effectiveness of the NSPFL.
- **Publisher:** New York: IEEE
- **Language:** English
- **Identifier:** ISSN: 1556-6013; EISSN: 1556-6021; DOI: 10.1109/TIFS.2024.3379852; CODEN: ITIFA6

Advancements in Privacy-Preserving Techniques for Federated Learning: A Machine Learning Perspective

- **Author:** Rokade, Monika Dhananjay ; Deshmukh, Suruchi ; Gumaste, Smita ; Shelake, Rekha Maruti ; Inamdar, Saba Afreen Ghayasuddin ; Chandre, Pankaj
- **Subject:** Algorithms ; Big data ; Communication ; Confidential communications ; Data integrity ; Ethics ; Machine learning ; Privacy
- **Is Part Of:** Journal of Electrical Systems, 2024-03, Vol.20 (2s), p.1075-1088
- **Description:** Federated learning has emerged as a promising paradigm for collaborative machine learning while preserving data privacy. However, concerns about data privacy remain significant, particularly in scenarios where sensitive information is involved. This paper reviews recent advancements in privacy-preserving techniques for federated learning from a machine learning perspective. It categorizes and analyses state-of-the-art approaches within a unified framework, highlighting their strengths, limitations, and potential applications. By providing insights into the landscape of privacy-preserving federated learning, this review aims to guide researchers and practitioners in developing robust and privacy-conscious machine learning solutions for collaborative environments. The paper concludes with future research directions to address ongoing challenges and further enhance the effectiveness and scalability of privacy-preserving federated

learning.
- **Publisher:** Paris: Engineering and Scientific Research Groups
- **Language:** English
- **Identifier:** EISSN: 1112-5209; DOI: 10.52783/jes.1754

Secure and Privacy-Preserving Decentralized Federated Learning for Personalized Recommendations in Consumer Electronics Using Blockchain and Homomorphic Encryption

- **Author:** Gupta, Brij B. ; Gaurav, Akshat ; Arya, Varsha
- **Subject:** Cryptography ; Data privacy ; Electronic industries ; Electronics ; Household electronics ; Information Dissemination ; Learning ; Privacy
- **Is Part Of:** IEEE transactions on consumer electronics, 2024-02, Vol.70 (1), p.2546-2556
- **Description:** Over the past few years, personalized recommendations have emerged as a fundamental component of the consumer electronics sector. The rise of decentralized federated learning has expanded the horizons of personalized recommendations, offering significant potential. Nonetheless, the utilization of confidential data from diverse clients raises legitimate concerns regarding privacy and security. In response to these challenges, we present an innovative framework for secure and privacy-preserving decentralized federated learning, tailored to personalized recommendations within the consumer electronics sector. Our approach strives to facilitate the collective contribution of data from multiple clients to the learning process while safeguarding their privacy. To accomplish this, we harness the power of homomorphic encryption, ensuring that clients' data remains encrypted and impervious to prying eyes. Additionally, we leverage blockchain technology to establish a secure, decentralized foundation for data exchange and management. Through the utilization of blockchain, we empower clients to validate the integrity of the learning process, guarantee system transparency, and thwart any malicious attempts at result manipulation. Our framework is rigorously assessed using real-world consumer electronics data, highlighting its capacity to provide a secure, decentralized, and privacy-centric solution for personalized recommendations. This approach not only enriches the user experience but also offers robust safeguards for sensitive data.
- **Publisher:** New York: IEEE
- **Language:** English
- **Identifier:** ISSN: 0098-3063; EISSN: 1558-4127; DOI: 10.1109/TCE.2023.3329480; CODEN: ITCEDA

A Comprehensive Privacy-Preserving Federated Learning Scheme With Secure Authentication and Aggregation for Internet of Medical Things

- **Author:** Liu, Jingwei ; Zhang, Jin ; Jan, Mian Ahmad ; Sun, Rong ; Liu, Lei ; Verma, Sahil ; Chatterjee, Pushpita
- **Subject:** Algorithms ; Authentication ; Big data ; Computer security ; Confidential communications ; Data mining ; Human beings ; Internet of things ; Learning ; Machine learning ; Privacy ; Training
- **Is Part Of:** IEEE journal of biomedical and health informatics, 2024-06, Vol.28 (6), p.3282-3292
- **Description:** Data mining, integration, and utilization are the inevitable trend of the Internet of Medical Things (IoMT) in the context of Big Data. With the increasing demand for data privacy, federated learning has emerged as a new paradigm, which enables distributed joint training of medical data sources without leaving the private domain. However, federated learning is suffering from security threats as the shared local model will reveal original datasets. Privacy leakage is even

more fatal in healthcare because medical data contains critically sensitive information. In addition, open wireless channels are susceptible to malicious attacks. To further safeguard the privacy of IoMT, we propose a comprehensive privacy-preserving federated learning scheme with a tactful dropout handling mechanism. The proposed scheme leverages blind masking and certificateless proxy re-encryption (CL-PRE) for secure aggregation, ensuring the confidentiality of the local model and rendering the global model invisible to any parties other than clients. It also provides authentication of uploaded models while protecting identity privacy. Compared with other relevant schemes, our solution has better performance on functional features and efficiency, and is more applicable to IoMT systems with many devices.

- **Publisher:** United States: IEEE
- **Language:** English
- **Identifier:** ISSN: 2168-2194; ISSN: 2168-2208; EISSN: 2168-2208; DOI: 10.1109/JBHI.2023.3304361; PMID: 37610908; CODEN: IJBHA9

A Comparative Study of Privacy-Preserving Techniques in Federated Learning: A Performance and Security Analysis

- **Author:** Shalabi, Eman ; Khedr, Walid ; Rushdy, Ehab ; Salah, Ahmad
- **Subject:** Communication ; Comparative studies ; Computational linguistics ; Cryptography ; Investment analysis ; Learning ; Machine learning ; Methodology ; Methods ; Neural networks (Computer science) ; Poisoning ; Poisons ; Privacy ; Teachers ; Training
- **Is Part Of:** Information (Basel), 2025-03, Vol.16 (3), p.244
- **Description:** Federated learning (FL) is a machine learning technique where clients exchange only local model updates with a central server that combines them to create a global model after local training. While FL offers privacy benefits through local training, privacy-preserving strategies are needed since model updates can leak training data information due to various attacks. To enhance privacy and attack robustness, techniques like homomorphic encryption (HE), Secure Multi-Party Computation (SMPC), and the Private Aggregation of Teacher Ensembles (PATE) can be combined with FL. Currently, no study has combined more than two privacy-preserving techniques with FL or comparatively analyzed their combinations. We conducted a comparative study of privacy-preserving techniques in FL, analyzing performance and security. We implemented FL using an artificial neural network (ANN) with a Malware Dataset from Kaggle for malware detection. To enhance privacy, we proposed models combining FL with the PATE, SMPC, and HE. All models were evaluated against poisoning attacks (targeted and untargeted), a backdoor attack, a model inversion attack, and a man in the middle attack. The combined models maintained performance while improving attack robustness. FL_SMPC, FL_CKKS, and FL_CKKS_SMPC improved both their performance and attack resistance. All the combined models outperformed the base FL model against the evaluated attacks. FL_PATE_CKKS_SMPC achieved the lowest backdoor attack success rate (0.0920). FL_CKKS_SMPC best resisted untargeted poisoning attacks (0.0010 success rate). FL_CKKS and FL_CKKS_SMPC best defended against targeted poisoning attacks (0.0020 success rate). FL_PATE_SMPC best resisted model inversion attacks (19.267 MSE). FL_PATE_CKKS_SMPC best defended against man in the middle attacks with the lowest degradation in accuracy (1.68%), precision (1.94%), recall (1.68%), and the F1-score (1.64%).
- **Publisher:** Basel: MDPI AG
- **Language:** English
- **Identifier:** ISSN: 2078-2489; EISSN: 2078-2489; DOI: 10.3390/info16030244

Privacy-Preserving Federated Learning-Based Intrusion Detection Technique for Cyber-Physical Systems

- **Author:** Mahmud, Syeda Aunanya ; Islam, Nazmul ; Islam, Zahidul ; Rahman, Ziaur ; Mehedi, Sk. Tanzir
- **Subject:** Algorithms ; Computer security ; Denial of service attacks ; Efficiency ; Energy consumption ; Internet of things ; Machine learning ; Methodology ; Methods ; Privacy
- **Is Part Of:** Mathematics (Basel), 2024-10, Vol.12 (20), p.3194
- **Description:** The Internet of Things (IoT) has revolutionized various industries, but the increased dependence on all kinds of IoT devices and the sensitive nature of the data accumulated by them pose a formidable threat to privacy and security. While traditional IDSs have been effective in securing critical infrastructures, the centralized nature of these systems raises serious data privacy concerns as sensitive information is sent to a central server for analysis. This research paper introduces a Federated Learning (FL) approach designed for detecting intrusions in diverse IoT networks to address the issue of data privacy by ensuring that sensitive information is kept in the individual IoT devices during model training. Our framework utilizes the Federated Averaging (FedAvg) algorithm, which aggregates model weights from distributed devices to refine the global model iteratively. The proposed model manages to achieve above 90% accuracies across various metrics, including precision, recall, and F1 score, while maintaining low computational demands. The results show that the proposed system successfully identifies various types of cyberattacks, including Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), data injection, ransomware, and several others, showcasing its robustness. This research makes a great advancement to the IDSs by providing an efficient and reliable solution that is more scalable and privacy friendly than any of the existing models.
- **Publisher:** Basel: MDPI AG
- **Language:** English
- **Identifier:** ISSN: 2227-7390; EISSN: 2227-7390; DOI: 10.3390/math12203194

Exploring Threats, Defenses, and Privacy-Preserving Techniques in Federated Learning: A Survey

- **Author:** Huang, Ren-Yi ; Samaraweera, Dumindu ; Chang, J. Morris
- **Subject:** Surveys
- **Is Part Of:** Computer (Long Beach, Calif.), 2024-04, Vol.57 (4), p.46-56
- **Description:** This article presents a comprehensive survey of both attack and defense mechanisms within the federated learning (FL) landscape. Furthermore, it explores the challenges involved and outlines future directions for the development of a robust and efficient FL solution.
- **Publisher:** New York: IEEE
- **Language:** English
- **Identifier:** ISSN: 0018-9162; EISSN: 1558-0814; DOI: 10.1109/MC.2023.3324975; CODEN: CPTRB4

Advancing Power System Services With Privacy-Preserving Federated Learning Techniques: A Review

- **Author:** Zheng, Ran ; Sumper, Andreas ; Aragues-Penalba, Monica ; Galceran-Arellano, Samuel
- **Subject:** Artificial intelligence ; Data privacy ; Training
- **Is Part Of:** IEEE access, 2024, Vol.12, p.76753-76780
- **Description:** Digitalization has enabled the potential for artificial intelligence techniques to lead the power system to a sustainable transition by extracting the data generated by widely deployed edge

devices, including advanced sensing and metering. Due to the increasing concerns about data privacy, federated learning has attracted much attention and is emerging as an innovative application for machine learning solutions in the power and energy sector. This paper presents a holistic analysis of federated learning applications in the energy sector, ranging from applications in generation, microgrids, and distribution systems to the energy market and cyber security. The following federated learning-based services for energy sectors are analyzed: non-intrusive load monitoring, fault detection, energy theft detection, demand forecasting, generation forecasting, energy management systems, voltage control, anomaly detection, and energy trading. The identification and classification of the data-driven methods are conducted in collaboration with federated learning implemented in these services. Furthermore, the interrelation is mapped between the categories of machine learning, data-driven techniques, the application domain, and application services. Finally, the future opportunities and challenges of applying federated learning in the energy sector will be discussed.
- **Publisher:** IEEE
- **Language:** English
- **Identifier:** EISSN: 2169-3536; DOI: 10.1109/ACCESS.2024.3407121; CODEN: IAECCG

A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique

- **Author:** Rehman, Abdur ; Abbas, Sagheer ; Khan, M.A ; Ghazal, Taher M ; Adnan, Khan Muhammad ; Mosavi, Amir
- **Subject:** Algorithms ; Artificial intelligence ; Cryptography ; Health Care Sector ; Health facilities ; Human beings ; Internal medicine ; Internet of things ; Machine learning ; Medical care ; Medical electronics ; Medical instruments and apparatus ; Medical records ; Patients ; Privacy ; Quality of life ; Spawning ; Technology ; Telecommunication in medicine
- **Is Part Of:** Computers in biology and medicine, 2022-11, Vol.150, p.106019-106019, Article 106019
- **Description:** AbstractIn recent years, the global Internet of Medical Things (IoMT) industry has evolved at a tremendous speed. Security and privacy are key concerns on the IoMT, owing to the huge scale and deployment of IoMT networks. Machine learning (ML) and blockchain (BC) technologies have significantly enhanced the capabilities and facilities of healthcare 5.0, spawning a new area known as “Smart Healthcare.” By identifying concerns early, a smart healthcare system can help avoid long-term damage. This will enhance the quality of life for patients while reducing their stress and healthcare costs. The IoMT enables a range of functionalities in the field of information technology, one of which is smart and interactive health care. However, combining medical data into a single storage location to train a powerful machine learning model raises concerns about privacy, ownership, and compliance with greater concentration. Federated learning (FL) overcomes the preceding difficulties by utilizing a centralized aggregate server to disseminate a global learning model. Simultaneously, the local participant keeps control of patient information, assuring data confidentiality and security. This article conducts a comprehensive analysis of the findings on blockchain technology entangled with federated learning in healthcare. 5.0. The purpose of this study is to construct a secure health monitoring system in healthcare 5.0 by utilizing a blockchain technology and Intrusion Detection System (IDS) to detect any malicious activity in a healthcare network and enables physicians to monitor patients through medical sensors and take necessary measures periodically by predicting diseases. The proposed system demonstrates that the approach is optimized effectively for healthcare monitoring. In contrast, the proposed healthcare 5.0 system entangled with FL Approach achieves 93.22% accuracy for disease prediction, and the proposed RTS-DELM-based secure healthcare 5.0 system achieves 96.18% accuracy for the

estimation of intrusion detection.
- **Publisher:** United States: Elsevier Ltd
- **Language:** English
- **Identifier:** ISSN: 0010-4825; ISSN: 1879-0534; EISSN: 1879-0534; DOI: 10.1016/j.compbiomed.2022.106019; PMID: 36162198

Exploring Homomorphic Encryption and Differential Privacy Techniques towards Secure Federated Learning Paradigm

- **Author:** Aziz, Rezak ; Banerjee, Soumya ; Bouzefrane, Samia ; Le Vinh, Thinh
- **Subject:** Algorithms ; Artificial intelligence ; Computer science ; Internet ; Internet of things ; Machine learning ; Methodology ; Methods ; Privacy
- **Is Part Of:** Future internet, 2023-09, Vol.15 (9), p.310
- **Description:** The trend of the next generation of the internet has already been scrutinized by top analytics enterprises. According to Gartner investigations, it is predicted that, by 2024, 75% of the global population will have their personal data covered under privacy regulations. This alarming statistic necessitates the orchestration of several security components to address the enormous challenges posed by federated and distributed learning environments. Federated learning (FL) is a promising technique that allows multiple parties to collaboratively train a model without sharing their data. However, even though FL is seen as a privacy-preserving distributed machine learning method, recent works have demonstrated that FL is vulnerable to some privacy attacks. Homomorphic encryption (HE) and differential privacy (DP) are two promising techniques that can be used to address these privacy concerns. HE allows secure computations on encrypted data, while DP provides strong privacy guarantees by adding noise to the data. This paper first presents consistent attacks on privacy in federated learning and then provides an overview of HE and DP techniques for secure federated learning in next-generation internet applications. It discusses the strengths and weaknesses of these techniques in different settings as described in the literature, with a particular focus on the trade-off between privacy and convergence, as well as the computation overheads involved. The objective of this paper is to analyze the challenges associated with each technique and identify potential opportunities and solutions for designing a more robust, privacy-preserving federated learning framework.
- **Publisher:** Basel: MDPI AG
- **Language:** English
- **Identifier:** ISSN: 1999-5903; EISSN: 1999-5903; DOI: 10.3390/fi15090310

Privacy-preserving techniques for decentralized and secure machine learning in drug discovery

- **Author:** Smajić, Aljoša ; Grandits, Melanie ; Ecker, Gerhard F.
- **Subject:** Drug Discovery ; Machine learning ; Privacy
- **Is Part Of:** Drug discovery today, 2023-12, Vol.28 (12), p.103820-103820, Article 103820
- **Description:** Data availability, data security, and privacy concerns often hamper optimal performance efficiency of machine learning (ML) techniques. Therefore, novel techniques for the utilization of private/sensitive data in the field of drug discovery have been proposed for ML model-building tasks. Some examples of the different techniques are secure multiparty computation, distributed deep learning, homomorphic encryption, blockchain-based peer-to-peer networking, differential privacy, and federated learning, as well as combinations of such techniques. In this paper, we present an overview of these techniques for decentralized ML to illustrate its benefits and

drawbacks in the field of drug discovery.
- **Publisher:** England
- **Language:** English
- **Identifier:** ISSN: 1359-6446; EISSN: 1878-5832; DOI: 10.1016/j.drudis.2023.103820; PMID: 37935330

Privacy-preserving edge federated learning for intelligent mobile-health systems

- **Author:** Aminifar, Amin ; Shokri, Matin ; Aminifar, Amir
- **Subject:** Communication systems ; Telecommunication systems
- **Is Part Of:** Future generation computer systems, 2024-12, Vol.161, p.625
- **Description:** Machine Learning (ML) algorithms are generally designed for scenarios in which all data is stored in one data center, where the training is performed. However, in many applications, e.g., in the healthcare domain, the training data is distributed among several entities, e.g., different hospitals or patients' mobile devices/sensors. At the same time, transferring the data to a central location for learning is certainly not an option, due to privacy concerns and legal issues, and in certain cases, because of the communication and computation overheads. Federated Learning (FL) is the state-of-the-art collaborative ML approach for training an ML model across multiple parties holding local data samples, without sharing them. However, enabling learning from distributed data over such edge Internet of Things (IoT) systems (e.g., mobile-health and wearable technologies, involving sensitive personal/medical data) in a privacy-preserving fashion presents a major challenge mainly due to their stringent resource constraints, i.e., limited computing capacity, communication bandwidth, memory storage, and battery lifetime. In this paper, we propose a privacy-preserving edge FL framework for resource-constrained mobile-health and wearable technologies over the IoT infrastructure. We evaluate our proposed framework extensively and provide the implementation of our technique on Amazon's AWS cloud platform based on the seizure detection application in epilepsy monitoring using wearable technologies.
- **Language:** English
- **Identifier:** ISSN: 0167-739X; DOI: 10.1016/j.future.2024.07.035

Enhanced Consumer Healthcare Data Protection Through AI-Driven TinyML and Privacy-Preserving Techniques

- **Author:** Aanjankumar, S. ; Muchahari, Monoj Kumar ; Urooj, Shabana ; Kaur, Ishmeet ; Dhanaraj, Rajesh Kumar ; Mengash, Hanan Abdullah ; Poonkuntran, S. ; Kaveri, Parag Ravikant
- **Subject:** Data privacy ; Electrocardiography ; Medical care ; Privacy ; Training
- **Is Part Of:** IEEE access, 2025, Vol.13, p.97428-97440
- **Description:** In the recent digital landscape, securing healthcare data stored on personal devices has become imperative due to increasing cyberattacks. Healthcare data inside an organization is often vulnerable to security breaches and requires privacy-preserving mechanisms to ensure secure storage and sharing across various platforms. This research proposes a novel method by integrating TinyML (machine learning) with federated learning (FL) and differential privacy (DP) to ensure the security and privacy of health-related data on resource-constrained edge devices. The proposed method with TinyML looks at patient data, like ECG readings and reports of unusual heartbeats, right on local edge devices that have limited resources, enabled immediate privacy checks while using minimal computing power. Federated learning trains the model on local edge devices by ensuring sensitive data remains on user devices, which are accessed centrally. Finally, differential

privacy techniques strengthen security by additionally adding noise to data for safeguarding against malicious attacks without compromising the data's accessibility. The proposed model achieves a high accuracy of 99%, significantly outperforming the traditional models, like decision trees at 76%, random forests at 98.1%, and federated learning with deep Q at 95%. The proposed methodology provides a scalable and efficient solution for real-time healthcare data sharing by ensuring data privacy and security across healthcare data source environments. The analysis of experimental results validates the model's efficiency in securing healthcare data, with implications for broader applications in secure, privacy-preserving medical data security analysis.
- **Publisher:** IEEE
- **Language:** English
- **Identifier:** EISSN: 2169-3536; DOI: 10.1109/ACCESS.2025.3573076; CODEN: IAECCG

Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images

- **Author:** Kumar, Rajesh ; Kumar, Jay ; Khan, Abdullah Aman ; Zakria ; Ali, Hub ; Bernard, Cobbinah M ; Khan, Riaz Ullah ; Zeng, Shaoning
- **Subject:** Algorithms ; Artificial intelligence ; COVID-19 Pandemic, 2020- ; Human beings ; Internal medicine ; Privacy
- **Is Part Of:** Computerized medical imaging and graphics, 2022-12, Vol.102, p.102139-102139, Article 102139
- **Description:** AbstractMedical healthcare centers are envisioned as a promising paradigm to handle the massive volume of data for COVID-19 patients using artificial intelligence (AI). Traditionally, AI techniques require centralized data collection and training models within a single organization. This practice can be considered a weakness as it leads to several privacy and security concerns related to raw data communication. To overcome this weakness and secure raw data communication, we propose a blockchain-based federated learning framework that provides a solution for collaborative data training. The proposed framework enables the coordination of multiple hospitals to train and share encrypted federated models while preserving data privacy. Blockchain ledger technology provides decentralization of federated learning models without relying on a central server. Moreover, the proposed homomorphic encryption scheme encrypts and decrypts the gradients of the model to preserve privacy. More precisely, the proposed framework: (i) train the local model by a novel capsule network for segmentation and classification of COVID-19 images, (ii) furthermore, we use the homomorphic encryption scheme to secure the local model that encrypts and decrypts the gradients, (iii) finally, the model is shared over a decentralized platform through the proposed blockchain-based federated learning algorithm. The integration of blockchain and federated learning leads to a new paradigm for medical image data sharing over the decentralized network. To validate our proposed model, we conducted comprehensive experiments and the results demonstrate the superior performance of the proposed scheme.
- **Publisher:** United States: Elsevier Ltd
- **Language:** English
- **Identifier:** ISSN: 0895-6111; EISSN: 1879-0771; DOI: 10.1016/j.compmedimag.2022.102139; PMID: 36395604

PriMed: Private federated training and encrypted inference on medical images in healthcare

- **Author:** Gopalakrishnan, Aparna ; Kulkarni, Narayan P. ; Raghavendra, Chethan B. ; Manjappa, Raghavendra ; Honnavalli, Prasad ; Eswaran, Sivaraman

- **Subject:** Algorithms ; Artificial intelligence ; Diagnostic imaging ; Inference ; Machine learning ; Neural networks (Computer science) ; Privacy
- **Is Part Of:** Expert systems, 2025-01, Vol.42 (1), p.n/a
- **Description:** In healthcare, patient information is a sparse critical asset considered as private data and is often protected by law. It is also the domain which is least explored in the field of Machine Learning. The main reason for this is to build efficient artificial intelligence (AI) based models for preliminary diagnosis of various diseases, it would require a large corpus of data which can be obtained by pooling in patient information from multiple sources. However, for these sources to agree to sharing their data across distributed systems for training algorithms and models, there has to be an assurance that there will be no disclosure of the personally identifiable information (PII) of the respective Data Owners. This paper proposes PriMed, an approach to build robust privacy preserving additions to convolutional neural networks (CNN) for training and performing inference on medical images without compromising privacy. Since privacy of the data is preserved, large amounts of data can be effectively accumulated to increase the accuracy and efficiency of AI models in the field of healthcare. This involves implementing a hybrid of privacy-enhancing techniques like Federated Learning, Differential Privacy, and Homomorphic Encryption to provide a private and secure environment for learning through data.
- **Publisher:** Oxford: Blackwell Publishing Ltd
- **Language:** English
- **Identifier:** ISSN: 0266-4720; EISSN: 1468-0394; DOI: 10.1111/exsy.13283

Data Obfuscation Through Latent Space Projection for Privacy-Preserving AI Governance: Case Studies in Medical Diagnosis and Finance Fraud Detection

- **Author:** Vaijainthymala Krishnamoorthy, Mahesh
- **Subject:** Machine learning
- **Is Part Of:** JMIRx med, 2025-03, Vol.6, p.e70100-e70100
- **Description:** The increasing integration of artificial intelligence (AI) systems into critical societal sectors has created an urgent demand for robust privacy-preserving methods. Traditional approaches such as differential privacy and homomorphic encryption often struggle to maintain an effective balance between protecting sensitive information and preserving data utility for AI applications. This challenge has become particularly acute as organizations must comply with evolving AI governance frameworks while maintaining the effectiveness of their AI systems. This paper aims to introduce and validate data obfuscation through latent space projection (LSP), a novel privacy-preserving technique designed to enhance AI governance and ensure responsible AI compliance. The primary goal is to develop a method that can effectively protect sensitive data while maintaining essential features necessary for AI model training and inference, thereby addressing the limitations of existing privacy-preserving approaches. We developed LSP using a combination of advanced machine learning techniques, specifically leveraging autoencoder architectures and adversarial training. The method projects sensitive data into a lower-dimensional latent space, where it separates sensitive from nonsensitive information. This separation enables precise control over privacy-utility trade-offs. We validated LSP through comprehensive experiments on benchmark datasets and implemented 2 real-world case studies: a health care application focusing on cancer diagnosis and a financial services application analyzing fraud detection. LSP demonstrated superior performance across multiple evaluation metrics. In image classification tasks, the method achieved 98.7% accuracy while maintaining strong privacy protection, providing 97.3% effectiveness against sensitive attribute inference attacks. This performance significantly exceeded that of traditional anonymization and privacy-preserving methods. The real-world case studies further validated LSP's effectiveness, showing robust

performance in both health care and financial applications. Additionally, LSP demonstrated strong alignment with global AI governance frameworks, including the General Data Protection Regulation, the California Consumer Privacy Act, and the Health Insurance Portability and Accountability Act. LSP represents a significant advancement in privacy-preserving AI, offering a promising approach to developing AI systems that respect individual privacy while delivering valuable insights. By embedding privacy protection directly within the machine learning pipeline, LSP contributes to key principles of fairness, transparency, and accountability. Future research directions include developing theoretical privacy guarantees, exploring integration with federated learning systems, and enhancing latent space interpretability. These developments position LSP as a crucial tool for advancing ethical AI practices and ensuring responsible technology deployment in privacy-sensitive domains.
- **Publisher:** Canada: JMIR Publications
- **Language:** English
- **Identifier:** ISSN: 2563-6316; EISSN: 2563-6316; DOI: 10.2196/70100; PMID: 40072927

FAItH: Federated Analytics and Integrated Differential Privacy with Clustering for Healthcare Monitoring

- **Author:** Alsenani, Yousef
- **Subject:** Algorithms ; Chronic diseases ; Cluster analysis ; Computer security ; Confidential communications ; Exercise ; Human beings ; Machine learning ; Medical informatics ; Privacy ; Science ; Wearable technology
- **Is Part Of:** Scientific reports, 2025-03, Vol.15 (1), p.10155-17, Article 10155
- **Description:** Monitoring physical activity is crucial for assessing patient health, particularly in managing chronic diseases and rehabilitation. Wearable devices tracking physical movement play a key role in monitoring elderly individuals or patients with chronic diseases. However, sharing of this data is often restricted by privacy regulations such as GDPR, as well as data ownership and security concerns, limiting its use in collaborative healthcare analysis. Federated analytics (FA) offers a promising solution that enables multiple parties to gain insights without sharing data, but current research focuses more on data protection than actionable insights. Limited exploration exists on analyzing privacy-preserved, aggregated data to uncover patterns for patient monitoring and healthcare interventions. This paper addresses this gap by proposing FAItH, a dual-stage solution that integrates privacy-preserving techniques - Laplace, Gaussian, Exponential and Locally Differentially Private (LDP) noise - on statistical functions (mean, variance, quantile) within a federated analytics environment. The solution employs feature-specific scaling to fine-tune the privacy-utility trade-off, ensuring sensitive features are protected while retaining utility for less sensitive ones. After applying federated analytics (FA) with differential privacy (DP) to generate insights, we introduce clustering to identify patterns in patient activity relevant to healthcare. Using the Human Activity Recognition (HAR) dataset, FAItH shows that privacy-preserving configurations achieve clustering utility nearly equal to non-DP setups, outperforming privacy-preserving clustering algorithms. This balances privacy with effective insights. These results validate FA with DP as a viable solution for secure collaborative analysis in healthcare, enabling meaningful insights without compromising patient privacy.
- **Publisher:** London: Nature Publishing Group UK
- **Language:** English
- **Identifier:** ISSN: 2045-2322; EISSN: 2045-2322; DOI: 10.1038/s41598-025-94501-4; PMID: 40128311

Privacy preservation for federated learning in health care

- **Author:** Pati, Sarthak ; Kumar, Sourav ; Varma, Amokh ; Edwards, Brandon ; Lu, Charles ; Qu, Liangqiong ; Wang, Justin J. ; Lakshminarayanan, Anantharaman ; Wang, Shih-han ; Sheller, Micah J. ; Chang, Ken ; Singh, Praveer ; Rubin, Daniel L. ; Kalpathy-Cramer, Jayashree ; Bakas, Spyridon
- **Subject:** Privacy ; Review
- **Is Part Of:** Patterns (New York, N.Y.), 2024-07, Vol.5 (7), p.100974, Article 100974
- **Description:** Artificial intelligence (AI) shows potential to improve health care by leveraging data to build models that can inform clinical workflows. However, access to large quantities of diverse data is needed to develop robust generalizable models. Data sharing across institutions is not always feasible due to legal, security, and privacy concerns. Federated learning (FL) allows for multi-institutional training of AI models, obviating data sharing, albeit with different security and privacy concerns. Specifically, insights exchanged during FL can leak information about institutional data. In addition, FL can introduce issues when there is limited trust among the entities performing the compute. With the growing adoption of FL in health care, it is imperative to elucidate the potential risks. We thus summarize privacy-preserving FL literature in this work with special regard to health care. We draw attention to threats and review mitigation approaches. We anticipate this review to become a health-care researcher's guide to security and privacy in FL. [Display omitted] Significant improvements can be made to clinical AI applications when multiple health-care institutions collaborate to build models that leverage large and diverse datasets. Federated learning (FL) provides a method for such AI model training, where each institution shares only model updates derived from their private training data, rather than the explicit patient data. This has been demonstrated to advance the state of the art for many clinical AI applications. However, open and persistent federations bring up the question of trust, and model updates have raised considerations of possible information leakage. Prior work has gone into understanding the inherent privacy risks and into developing mitigation techniques. Focusing on FL in health care, we review the privacy risks and the costs and limitations associated with state-of-the-art mitigations. We hope to provide a guide to health-care researchers seeking to engage in FL as a new paradigm of secure and private collaborative AI. AI can enhance health care by using data to create useful models. However, sharing data between institutions is challenging due to legal and privacy issues. Federated learning (FL) allows institutions to train AI models without sharing data, but it also has its own security concerns. As FL becomes more commonplace in health care, it is crucial to understand its risks. This work reviews the literature on privacy-preserving FL, highlighting threats and solutions, aiming to guide health-care researchers on FL's security and privacy aspects.
- **Publisher:** United States: Elsevier Inc
- **Language:** English
- **Identifier:** ISSN: 2666-3899; EISSN: 2666-3899; DOI: 10.1016/j.patter.2024.100974; PMID: 39081567

ESB-FL: Efficient and Secure Blockchain-Based Federated Learning With Fair Payment

- **Author:** Chen, Biwen ; Zeng, Honghong ; Xiang, Tao ; Guo, Shangwei ; Zhang, Tianwei ; Liu, Yang
- **Subject:** Cryptography ; Data privacy ; Diagnostic imaging ; Image processing ; Privacy ; Task analysis ; Training
- **Is Part Of:** IEEE transactions on big data, 2024-12, Vol.10 (6), p.761-774
- **Description:** Federated learning (FL) is a technique that enables multiple parties to collaboratively train a model without sharing raw private data, and it is ideal for smart healthcare. However, it raises new privacy concerns due to the risk of privacy-sensitive medical data leakage. It is not until

recently that the privacy-preserving FL (PPFL) has been introduced as a solution to ensure the privacy of training processes. Unfortunately, most existing PPFL schemes are highly dependent on complex cryptographic mechanisms or fail to guarantee the accuracy of training models. Besides, there has been little research on the fairness of the payment procedure in the PPFL with incentive mechanisms. To address the above concerns, we first construct an efficient non-interactive designated decryptor function encryption (NDD-FE) scheme to protect the privacy of training data while maintaining high communication performance. We then propose a blockchain-based PPFL framework with fair payment for medical image detection, namely ESB-FL, by combining the NDD-FE and an elaborately designed blockchain. ESB-FL not only inherits the characteristics of the NDD-FE scheme, but it also ensures the interests of each participant. We finally conduct extensive security analysis and experiments to show that our new framework has enhanced security, good accuracy, and high efficiency.

- **Publisher:** Piscataway: IEEE
- **Language:** English
- **Identifier:** ISSN: 2332-7790; EISSN: 2372-2096; DOI: 10.1109/TBDATA.2022.3177170; CODEN: ITBDAX

Enhancing Intrusion Detection Through Federated Learning With Enhanced GhostBiNet and Homomorphic Encryption

- **Author:** ChandraUmakantham, Om Kumar ; Gajendran, Sudhakaran ; Marappan, Suguna
- **Subject:** Data privacy ; Machine learning ; Privacy ; Training
- **Is Part Of:** IEEE access, 2024, Vol.12, p.24879-24893
- **Description:** Intrusion detection is essential for safeguarding computer systems and networks against unauthorized access, malicious activities, and security breaches. Its application domains include network security, information security, and cybersecurity across various sectors such as finance, healthcare, government, and industry. Federated learning-based intrusion detection offers improved performance compared to conventional mechanisms by leveraging decentralized data sources, preserving data privacy, and enhancing model generalization through collaboration among multiple organizations. However, challenges faced by existing federated learning-based intrusion detection mechanisms include ensuring data privacy and security, mitigating communication overhead, and enhancing detection accuracy. In order to overcome these issues, this research article proposes a federated learning-based intrusion detection methodology that leverages Enhanced Ghost_BiNet, a novel deep learning model, to enhance the security of information sharing and detection accuracy. Federated learning, a privacy-preserving machine learning technique, is utilized to enable multiple entities to collaboratively train a global intrusion detection model without sharing sensitive data. The proposed system first trains local models using Enhanced Ghost_BiNet, which integrates GhostNet and Bidirectional Gated Recurrent Unit (BiGRU). To optimize the model's performance, the Chaotic Chebyshev Artificial Humming Bird (CAh) algorithm is employed. Homomorphic encryption is applied to encrypt the local model updates, enhancing data privacy and security. Server-side aggregation of updates and collaborative optimization are introduced to minimize communication rounds during data aggregation. The results demonstrate that the Enhanced Ghost_BiNet outperforms traditional models like GhostNet, BiGRU, RNN, Auto Encoder, and CNN in terms of accuracy, precision, recall, F-Score, and mean square error (MSE). For instance, the Enhanced Ghost_BiNet achieves an accuracy of 99.24% on the KDD CUP 99 dataset, surpassing the other models by a significant margin. The proposed methodology provides a robust and secure approach to intrusion detection, ensuring the confidentiality of sensitive data while improving detection accuracy.
- **Publisher:** IEEE

- **Language:** English
- **Identifier:** EISSN: 2169-3536; DOI: 10.1109/ACCESS.2024.3362347; CODEN: IAECCG

Securing the Internet of Health Things: Embedded Federated Learning-Driven Long Short-Term Memory for Cyberattack Detection

- **Author:** Kumar, Manish ; Kim, Sunggon
- **Subject:** Computer security ; Confidential communications ; Ferroelectric storage cells ; Hospitals ; Internet ; Medical instruments and apparatus ; Patients ; Privacy
- **Is Part Of:** Electronics (Basel), 2024-09, Vol.13 (17), p.3461
- **Description:** The proliferation of the Internet of Health Things (IoHT) introduces significant benefits for healthcare through enhanced connectivity and data-driven insights, but it also presents substantial cybersecurity challenges. Protecting sensitive health data from cyberattacks is critical. This paper proposes a novel approach for detecting cyberattacks in IoHT environments using a Federated Learning (FL) framework integrated with Long Short-Term Memory (LSTM) networks. The FL paradigm ensures data privacy by allowing individual IoHT devices to collaboratively train a global model without sharing local data, thereby maintaining patient confidentiality. LSTM networks, known for their effectiveness in handling time-series data, are employed to capture and analyze temporal patterns indicative of cyberthreats. Our proposed system uses an embedded feature selection technique that minimizes the computational complexity of the cyberattack detection model and leverages the decentralized nature of FL to create a robust and scalable cyberattack detection mechanism. We refer to the proposed approach as Embedded Federated Learning-Driven Long Short-Term Memory (EFL-LSTM). Extensive experiments using real-world ECU-IoHT data demonstrate that our proposed model outperforms traditional models regarding accuracy (97.16%) and data privacy. The outcomes highlight the feasibility and advantages of integrating Federated Learning with LSTM networks to enhance the cybersecurity posture of IoHT infrastructures. This research paves the way for future developments in secure and privacy-preserving IoHT systems, ensuring reliable protection against evolving cyberthreats.
- **Publisher:** Basel: MDPI AG
- **Language:** English
- **Identifier:** ISSN: 2079-9292; EISSN: 2079-9292; DOI: 10.3390/electronics13173461

Neural gradient boosting in federated learning for hemodynamic instability prediction: towards a distributed and scalable deep learning-based solution

- **Author:** Manni, Francesca ; Bukharev, Aleksandr ; Jain, Anshul ; Moorthy, Shiva ; Rahman, Asif ; Bucur, Anca
- **Subject:** Databases, Factual ; Hemodynamics ; Hospitals ; Human beings ; Machine learning ; Privacy
- **Is Part Of:** AMIA ... Annual Symposium proceedings, 2022, Vol.2022, p.729-738
- **Description:** Federated learning (FL) is a privacy preserving approach to learning that overcome issues related to data access, privacy, and security, which represent key challenges in the healthcare sector. FL enables hospitals to collaboratively learn a shared prediction model without moving the data outside their secure infrastructure. To do so, after having sent model updates to a central server, an update aggregation is performed, and the model is sent back to the sites for further training. Although widely applied on neural networks, the deployment of FL architectures is lacking scalability and support for machine learning techniques such as decision tree-based models. The

latter, when embedded in FL, suffer from costly encryption techniques applied for sharing sensitive information such as the splitting decisions within the trees. In this work, we focus on predicting hemodynamic instability on ICU patients by enabling distributed gradient boosting in FL. We employ a clinical dataset from 25 hospitals generated based on the Philips eICU database and we design a FL pipeline that supports neural-based boosting models as well as conventional neural networks. This enhancement enables decision tree models in FL, which represent the state-of-the-art approach for classification tasks involving tabular clinical data. Comparable performances in terms of accuracy, precision, recall and F1 score have been reached when detecting hemodynamic instability in FL, and in a centralized setup. In summary, we demonstrate the feasibility of a scalable FL for detecting hemodynamic instability in ICU data, which preserves privacy and holds the deployment benefits of a neural-based architecture.
- **Publisher:** United States
- **Language:** English
- **Identifier:** EISSN: 1559-4076; PMID: 37128389

Neural gradient boosting in federated learning for hemodynamic instability prediction: towards a distributed and scalable deep learning-based solution

- **Author:** Manni, Francesca ; Bukharev, Aleksandr ; Jain, Anshul ; Moorthy, Shiva ; Rahman, Asif ; Bucur, Anca
- **Is Part Of:** AMIA ... Annual Symposium proceedings, 2023-04, Vol.2022, p.729-738
- **Description:** Federated learning (FL) is a privacy preserving approach to learning that overcome issues related to data access, privacy, and security, which represent key challenges in the healthcare sector. FL enables hospitals to collaboratively learn a shared prediction model without moving the data outside their secure infrastructure. To do so, after having sent model updates to a central server, an update aggregation is performed, and the model is sent back to the sites for further training. Although widely applied on neural networks, the deployment of FL architectures is lacking scalability and support for machine learning techniques such as decision tree-based models. The latter, when embedded in FL, suffer from costly encryption techniques applied for sharing sensitive information such as the splitting decisions within the trees. In this work, we focus on predicting hemodynamic instability on ICU patients by enabling distributed gradient boosting in FL. We employ a clinical dataset from 25 hospitals generated based on the Philips eICU database and we design a FL pipeline that supports neural-based boosting models as well as conventional neural networks. This enhancement enables decision tree models in FL, which represent the state-of-the-art approach for classification tasks involving tabular clinical data. Comparable performances in terms of accuracy, precision, recall and F1 score have been reached when detecting hemodynamic instability in FL, and in a centralized setup. In summary, we demonstrate the feasibility of a scalable FL for detecting hemodynamic instability in ICU data, which preserves privacy and holds the deployment benefits of a neural-based architecture.
- **Publisher:** American Medical Informatics Association
- **Language:** English
- **Identifier:** EISSN: 1559-4076

A Randomized Response Framework to Achieve Differential Privacy in Medical Data

- **Author:** Ioannidis, Andreas ; Litke, Antonios ; Papadakis, Nikolaos K.
- **Subject:** Algorithms ; Computer security ; Data integrity ; Health Care Sector ; Machine learning ;

Medical electronics ; Medical instruments and apparatus ; Physiological apparatus ; Privacy ; Random variables ; Statistics

- **Is Part Of:** Electronics (Basel), 2025-01, Vol.14 (2), p.326
- **Description:** In recent years, differential privacy has gained substantial traction in the medical domain, where the need to balance privacy preservation with data utility is paramount. As medical data increasingly relies on cloud platforms and distributed sharing among multiple stakeholders, such as healthcare providers, researchers, and policymakers, the importance of privacy-preserving techniques has become more pronounced. Trends in the field focus on designing efficient algorithms tailored to high-dimensional medical datasets, incorporating privacy guarantees into federated learning for distributed medical devices, and addressing challenges posed by adversarial attacks. Our work lays a foundation for these emerging applications by emphasizing the role of randomized response within the broader differential privacy framework, paving the way for advancements in secure medical data sharing and analysis. In this paper, we analyze the classical concept of a randomized response and investigate how it relates to the fundamental concept of differential privacy. Our approach is both mathematical and algorithmic in nature, and our purpose is twofold. On the one hand, we provide a formal and precise definition of differential privacy within a natural and convenient probabilistic—statistical framework. On the other hand, we position a randomized response as a special yet significant instance of differential privacy, demonstrating its utility in preserving individual privacy in sensitive data scenarios. To substantiate our findings, we include key theoretical proofs and provide indicative simulations, accompanied by open-access code to facilitate reproducibility and further exploration.
- **Publisher:** Basel: MDPI AG
- **Language:** English
- **Identifier:** ISSN: 2079-9292; EISSN: 2079-9292; DOI: 10.3390/electronics14020326