International Journal of Scientific World, 11 (1) (2025) 30-39

International Journal of Scientific World

Website: www.sciencepubco.com/index.php/IJSW

Research paper

Privacy-preserving machine learning: a review of federated learning techniques and applications

Nazik Saber Rashid [1] *, Hajar Maseeh Yasin [2]

[1] Akre University for Applied Science, Technical College of Informatics, Akre, Department of Information Technology, Akre, Kurdistan Region, Iraq
[2]Akre University for Applied Sciences, Technical College of Informatics, Department of Information Technology, Duhok, Iraq
**Corresponding author E-mail: naziksufy@gmail.com*

Abstract

Federated Learning (FL), which permits decentralized model training without sharing raw data, guarantees adherence to privacy laws like GDPR and HIPAA. This study offers a thorough analysis of FL with an emphasis on its exceptional capacity to strike a balance between data value and privacy in industries including healthcare, the Internet of Things, and finance. In contrast to previous evaluations, this study explores sophisticated privacy-preserving techniques, such as differential privacy and homomorphic encryption, and assesses how well they work to handle issues like adversarial threats, non-IID data distributions, and communication overhead. The study also discusses the practical uses of optimization techniques like Federated Proximal (FedProx) and Federated Averaging (FedAvg). This paper provides practical insights and future approaches to promote the use of FL in privacy-sensitive AI applications by comparing and contrasting current methods and pointing out research gaps. FL is positioned as a revolutionary method for privacy-conscious machine learning because to this fresh viewpoint.
This update highlights the paper's distinctive features that set it apart from prior reviews, including the thorough examination of privacy mechanisms, assessment of optimization techniques, and identification of research needs.

Keywords: *Privacy-Preserving Machine Learning; Federated Learning; Decentralized AI Models; Differential Privacy; Homomorphic Encryption; IoT and Smart City Applications.*

1. Introduction

From manufacturing and transportation to healthcare and finance, the emergence of synthetic intelligence (AI) and gadget mastering (ML) has profoundly changed some of industries. Nonetheless, the developing dependence on information-pushed decision-making has raised privateness worries, especially in sensitive fields where stringent restrictions on facts sharing and usage are enforced by using records safety laws like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) [1] [2], [3]. Traditional centralized system studying strategies, which compile huge volumes of statistics onto centralized servers for training, frequently neglect those privateness issues, posing a chance of records breaches, unlawful get admission to, and noncompliance with the law [4 -7].
Federated Learning (FL), which lets in collaborative model training with out moving raw information among entities, has emerge as a ground-breaking paradigm for privateness-keeping machine gaining knowledge of. FL reduces privacy problems and mitigates the problems related to statistics silos through decentralizing the schooling approach and relying on close by calculations at statistics assets. This ensures that sensitive facts remains interior its origin [8 - 10] To similarly defend facts for the duration of version updates and aggregation, FL in addition integrates contemporary privacy-keeping techniques as homomorphic encryption, differential privateness, and stable multi-birthday celebration computing [2], [3] [11] [12].
This paper offers a thorough exam of FL strategies and their uses, highlighting how FL advances privateness-keeping gadget studying. An review of FL designs, including as horizontal, vertical, and switch mastering, as well as their many applications in industries like healthcare, finance, and IoT systems, are covered within the conversation [3], [7]. The take a look at also discusses how optimization algorithms like Federated Averaging (FedAvg) and Federated Proximal (FedProx) are used to cope with the unique difficulties of FL, together with statistical heterogeneity, communique overhead, and computational complexity [9], [10].
The significance of FL as a progressive technique of system gaining knowledge of is highlighted via the developing need for privacy-conscious AI solutions. FL has the capacity to revolutionize how corporations create and put into effect AI fashions by bridging the gap among privacy guidelines and collaborative facts utilization, commencing the door for secure and effective studying in privateness-touchy settings [13] [3], [14].In order to support FL's continued growth and uptake in important fields, this paper attempts to provide readers a thorough grasp of its theoretical underpinnings, real-world applications, and potential future developments.

2. Privacy-preserving machine learning through federated learning

Privacy-keeping machine learning is a rising paradigm geared toward addressing the challenges of statistics safety and person privacy in the digital age. Traditional gadgets gaining knowledge of procedures often require centralized information aggregation for schooling, raising significant privateness issues, especially with the increasing focus and regulation of data safety. Federated studying (FL) offers a solution by way of enabling collaborative version education throughout distributed records resources without moving raw records to a crucial server [15 - 17].

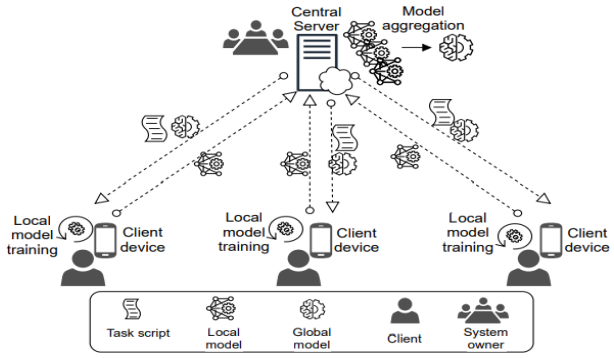


Fig. 1: Federated Learning Overview[18].

The basic architecture of FL is shown graphically in Figure 1, where client devices train local models using their own data and only share model updates (like gradients or parameters) with a central server for aggregation. This decentralized method enables collaborative machine learning while ensuring sensitive data stays localized, effectively addressing privacy concerns[19] [20].

2.1. Federated learning fundamentals

The basic idea behind federated mastering is that models are skilled domestically on part devices or dispersed servers that reside the records, and that only version updates—like gradients or parameters—are shared with a principal server for aggregate. During the use of disbursed computing for model building, this decentralized method guarantees the privateness of touchy records [21] [16], [17].
Figure 2, titled "Federated Learning System," depicts the three primary styles of FL: horizontal, vertical, and federated transfer mastering. Horizontal FL is utilized in instances whilst objects percentage comparable traits with numerous folks, as seen within the top-left portion of the photo. Vertical FL, as proven inside the pinnacle-proper component, is used whilst entities have overlapping person bases however specific function units, with an emphasis on information feature alignment and intermediate result sharing. The backside half of Figure 2 depicts Federated Transfer Learning, which mixes FL with switch mastering to remedy eventualities with restricted feature and sample overlap via permitting facts illustration interchange between customers.
This picture presents a detailed visual representation of FL's flexibility to various data distributions and collaborative learning contexts, supporting the textual explanation of these categories.

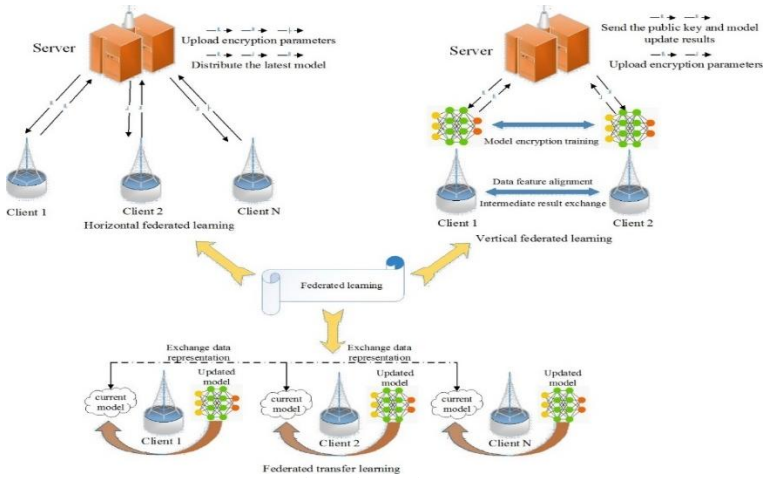


Fig. 2: Federated Learning System [22].

2.2. Privacy-preserving mechanisms in federated learning

Other approaches are used to strengthen FL's intrinsic privacy-preserving nature:
Differential Privacy (DP): This technique obscures individual contributions by adding noise to data or model parameters, protecting privacy while preserving overall statistical usefulness [16], [23].

1) Homomorphic Encryption (HE): Maintains anonymity throughout the procedure by enabling calculations on encrypted material without the need for decryption[24] [23].
2) Secure Multi-Party Computation (SMC): Allows multiple parties to collaboratively compute a function without revealing their inputs[16].
3) Trusted Execution Environments (TEEs): Provides hardware-based secure zones for sensitive computations [23].

2.3. Applications and challenges

Applications for FL may be located in fields in which information privacy is crucial, together with healthcare, banking, IoT, and smart towns[25] [17], [26]. For instance, FL addresses compliance with laws like GDPR and HIPAA via permitting diagnostic model training throughout establishments without exchanging patient records[27] [22], [26]. Nonetheless, FL has a number of problems, such as:

1) Communication Overhead: Especially in large-scale situations, frequent model update exchanges can position a burden on bandwidth[28].
2) Non-IID Data: Biased models and gradual convergence may additionally end result from data heterogeneity among customers.
3) Security Risks: FL is liable to adverse manipulations, facts poisoning, and version inversion assaults, despite the fact that it's miles decentralized [26].

Figure three, "Federated Learning Features and Applications," depicts a visual assessment of critical FL properties and their many makes use of. The image emphasizes factors like as nearby education, low statistics administration, and minimum information labeling, which might be critical to its privateness-retaining abilities. It also highlights packages like as IoT-enabled AI, decentralized systems, and network outsourcing, demonstrating FL's capability to adapt to privacy-touchy environments.

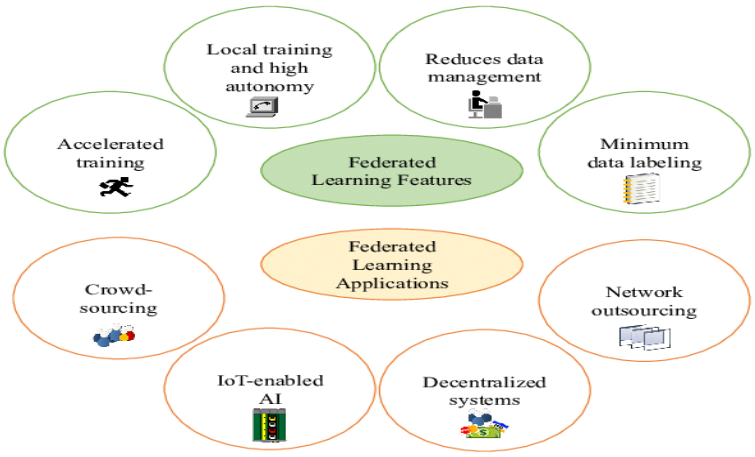


Fig. 3: An Illustration of Features and Applications of Federated Learning[29].

2.4. Future directions

Research in FL focuses on incorporating cutting-edge privacy methods like quantum-safe cryptography, strengthening model resilience against adversarial attacks, and increasing communication efficiency through gradient compression and adaptive updating processes [15], [16] [30] [31].

Federated learning has the potential to revolutionize privacy-sensitive AI applications by facilitating decentralized and privacy-preserving model training, which strikes a balance between the necessity for data usefulness and strict privacy regulations.

3. Literature review

Federated Learning (FL) is a breakthrough paradigm in privateness-retaining device learning that lets in for decentralized model schooling across dispersed information assets. Over the ultimate decade, FL has emerged as a dependable option for addressing privateness problems associated to centralized records collecting. It has been a popular topic inside the literature because of its capacity to reconcile statistics cost and privacy. The multiplied interest in FL is seen in packages like as healthcare, IoT, and finance, all of which need touchy records processing. As a end result, on this element, we outline prior studies on the usage of FL for privacy-keeping machine gaining knowledge of and its realistic packages.

Mansour et al. (2020)[32], recommended three strategies, backed through effective algorithms and theoretical assurances: person clustering, data interpolation, and model interpolation. Tests conducted on EMNIST and synthetic datasets showed extended scalability and accuracy whilst balancing privacy, verbal exchange obstacles, and computing performance. This work used beneficial, scalable techniques to promote custom designed federated mastering.

Li et al. (2020)[33] , cautioned a federated studying structure for multi-web site fMRI analysis that protects privateness whilst resolving issues with statistics sharing and domain shift between universities. To enhance version overall performance, the strategy used domain edition strategies consisting of Mixture of Experts and opposed domain alignment, in conjunction with randomized privacy protections. The framework's capacity to boom the classification accuracy of autistic spectrum problems even as coming across dependable and instructive biomarkers became proved via experiments at the ABIDE dataset. This examine proven how federated learning may adequately use multi-web page scientific information, providing more applications in privateness-sensitive fields.

Liu et al. (2020) [34], recommended a visitors flow prediction structure that protects privacy by using the Federated Learning-based Gated Recurrent Unit (FedGRU). FedGRU used optimization techniques to keep conversation overhead and protected information privacy by means of aggregating encrypted parameters as opposed to offering uncooked facts. By identifying spatiotemporal styles, an ensemble clustering approach progressed in accuracy. FedGRU is suitable for steady site visitors management packages as experiments confirmed that it maintained statistics privacy even as reaching high accuracy on par with centralized techniques.

Jeon et al. (2020) [35], presented a decentralized aggregation protocol for federated learning that uses the Alternating Direction Method of Multipliers (ADMM) while maintaining anonymity. The researchers addressed flaws in traditional ADMM techniques by introducing a unique communication pattern based on combinatorial block design theory that minimizes privacy leakage. This approach maintained linear Convergence while presenting privacy assurances towards sincere but inquisitive attackers. Its promise for safe and powerful federated mastering was shown with the aid of experiments on benchmark datasets, which confirmed that the approach attained accuracy equivalent to centralized federated mastering with low deterioration (<0.73 %).

Kerkouche et al. (2021) [36] , advanced the FL-SIGN-DP federated studying method, that's bandwidth-green and privacy-keeping, specifically for in-health facility mortality prediction using electronic health data. By combining severe gradient quantization and differential privateness, the technique preserved document-degree privateness at the same time as considerably lowering conversation expenses. Tests conducted on a dataset spanning 314 hospitals demonstrated that FL-SIGN-DP outperformed non-private models in phrases of accuracy loss whilst accomplishing sturdy privacy guarantees. This look at showed that privateness-preserving federated studying is viable for delicate clinical programs, putting a stability between efficiency, privacy, and value.

Wei et al. (2020) [37], provided the consumer-stage differential privacy (UDP) approach for federated mastering, which improves privacy by means of which includes Gaussian noise into version updates. It decided the correct quantity of communique rounds for elevated accuracy and performance via deriving theoretical boundaries. Training became in addition refined the use of a communication rounds discounting (CRD) approach. The approach was showed by way of experiments, which provided a achievable answer for privateness-preserving federated learning at the same time as turning in excessive privateness assurances with little performance fee.

Mo et al. (2021) [38], suggested Privacy-Preserving Federated Learning (PPFL), which uses server-side aggregation in federated learning and safe local training using Trusted Execution Environments (TEEs). In order to overcome memory constraints and offer robust protections against attacks including data reconstruction, property inference, and membership inference, PPFL implemented layer-wise training within TEEs. Comparable model accuracy was shown in evaluation on real-world datasets with fewer communication cycles and less client-side overhead. The system demonstrated its promise for safe collaborative machine learning applications by achieving strong privacy guarantees and useful scalability.

Venkataramanan et al. (2021)[39], created a federated studying (FL) framework that protects privacy for predicting Distributed Energy Resources (DER) making use of Internet of Things (IoT) nodes. It made it feasible to appropriately count on electricity output and intake on the same time as maintaining the privateness of neighborhood information. The method's awesome accuracy (RMSE < 2.Zero) and capacity to expect and decrease load fluctuations using top shaving strategies were proved through simulations related to 1,000 nodes and actual-international validation the usage of the Pecan Street dataset. The strategy tested how FL also can beautify grid reliability at the same time as shielding the privateness of client records.

Biswal et al. (2021)[40], presented AMI-FML, a federated gadget learning (FML) framework created for superior metering infrastructure (AMI) to beautify information analytics while protective privacy. The system advanced short-term load forecasting (STLF) the use of Long Short-Term Memory (LSTM) neural networks at the identical time as protecting purchaser privateness via sending model gradients in place of raw facts. The outcomes confirmed that the use of organized and drawn updates reduced conversation fees and prolonged forecasting accuracy. This platform provided scalability and the opportunity of destiny enhancements in clever grid offerings, in conjunction with strength manage apps that protected privacy.

Fang et al. (2021)[41], supplied PFMLP, a system getting to know framework that protects touchy information throughout collaborative training by using combining federated studying and homomorphic encryption. The device made it viable for several parties to securely proportion gradients and update models through the use of the Paillier encryption method. With a variant of less than 1%, PFMLP displayed accuracy equivalent to centralized training in experiments conducted on the MNIST and metal fatigue datasets. Furthermore, a refined Paillier algorithm ensured effective privacy protection and realistic scalability in multi-party learning situations by reducing computational cost by 25–28%.

Fernández et al. (2022) [42], supplied a federated learning (FL) architecture for quick-time period residential load forecasting that preserves privateness by means of combining steady aggregation (SecAgg) and differential privateness (DP) to improve information privateness. The aggregate of FL with DP and SecAgg produced terrific forecasting accuracy while retaining strong privacy ensures, as proven via simulations on the Low Carbon London dataset. Simpler neural community topologies were proven to lessen computing charges and overfitting concerns, whilst clustering based on Pearson correlation in addition better model overall performance. This method proven FL's promise for secure and precise energy forecasting in environments in which privacy is a challenge.

Elbir et al. (2020) [43], explored how federated mastering (FL) can be utilized in automobile networks for tasks like traffic manage and self reliant driving. It emphasized how FL is advanced than centralized mastering (CL) in terms of decreasing transmission overhead and enhancing facts privateness. The effectiveness of FL changed into proved by means of case research on millimeter-wave beam choice and three-D object detection, which finished competitive accuracy with much lower conversation charges. In order to maximize resource use, the research additionally counseled hybrid federated-centralized frameworks to clear up problems along with data variety, labeling, and communication obstacles. Future instructions targeted on resilient communique protocols and adaptive techniques for records heterogeneity.

Zhang et al. (2021) [44], provided FedNILM, a federated mastering machine designed to overcome resource limitations and privateness troubles for non-intrusive load tracking (NILM) at area gadgets. FedNILM made use of model compression techniques, consisting of multi-challenge getting to know and filter pruning, to facilitate powerful deployment on devices with limited sources. In order to cope with area modifications across cloud and side contexts, unsupervised switch learning was included enabling version customisation without the need for categorized records. Tests found out FedNILM's viability for scaled NILM programs via demonstrating modern-day energy disaggregation overall performance at the same time as defensive user privateness.

Peyvandi et al. (2022) [45], suggested a blockchain-based totally federated mastering machine for scalable and privateness-preserving machine getting to know in Society 5.0 called Decentralized Computational Intelligence as a Service (DCIaaS). By securely sharing just discovered version parameters over blockchain, DCIaaS allowed for decentralized model training on neighborhood information even as preserving anonymity. Its efficacy for privacy-touchy responsibilities was highlighted by experimental programs in biomedical imaging and smart metropolis control, which showed higher accuracy whilst as compared to centralized strategies. The architecture supplied a achievable answer for secure collaborative intelligence by means of addressing troubles of privacy, scalability, and statistics equality.

Zhang et al. (2023) [46], suggested a federated learning architecture for IoT-enabled healthcare applications that protect privacy by using homomorphic encryption. This method used cryptographic approaches to provide safe model aggregation while protecting data against inversion and reconstruction assaults. Dropout tolerance and increased model accuracy were made possible by the introduction of a weighted method depending on data quality. Tests conducted on the HAM10000 dataset showed improved data security and competitive classification accuracy (76.9%). The system offered a productive and private way to analyze healthcare data collaboratively.

Pentyala et al. (2022) [47], provided PrivFairFL, a federated getting to know framework designed to protect facts privateness even as attaining institution fairness. To reduce prejudice with out gaining access to personal records, it incorporated federated learning with Secure Multiparty Computation (MPC) and Differential Privacy (DP). To make sure privateness and fairness, the system protected pre-processing for pattern reweighing and publish-processing for type threshold optimization. It outperformed nearby DP techniques in empirical tests, demonstrating its efficacy in minimizing bias and retaining usefulness throughout datasets. This have a look at demonstrated that federated getting to know can effectively integrate fairness with strong privacy necessities.

Liu et al. (2024) [48], advised a multi-hop multi-key fully homomorphic encryption (MKFHE) method with small ciphertexts for a privacy-retaining federated getting to know framework. The technique allowed for scalability, dynamic consumer interplay, and powerful records encryption across severa parties. It addressed person dropout problems with out sacrificing security via lowering the wide variety of interaction cycles in federated learning from 3 to two. Comparing the framework to modern HE-primarily based techniques, empirical checks showed that it stepped forward conversation and computing efficiency even as keeping robust privateness guarantees underneath the RLWE assumption.

Islam et al. (2023) [49], recommended federated learning frameworks that guard privateness and are mainly designed for comparing non-public scientific records this is spread across several organizations. By combining differential privateness with strategies like feature choice and records sanitization, the strategies progressed privacy and usefulness whilst addressing horizontal and vertical statistics partitions. Tests showed that these techniques maintained strong privacy assurances whilst achieving competitive accuracy. The frameworks correctly balanced privateness and usefulness through utilising techniques such vertical allotted learning with weighted feature aggregation, demonstrating their suitability for safe, cooperative healthcare statistics evaluation.

Butt et al. (2023) [50], offered a fog-based totally federated mastering (FL) device for COVID-19 analysis utilising chest X-ray photographs at the same time as shielding privacy. In order to facilitate cooperative version education throughout hospitals with out replacing sensitive data, the machine used a decentralized FL method at the side of convolutional neural networks (CNNs). The method used fog computing to enhance scalability and performance even as addressing issues with unbalanced and non-i.I.D. Records. The advised technique outperformed neighborhood models in phrases of accuracy, precision, consider, and F1-rating, according to experimental findings the usage of the COVID-19 Radiography Database. This observe demonstrated FL's capacity for safe and effective smart healthcare packages.

Michalakopoulos et al. (2024) [51], recommended a federated learning (FL) structure that includes differential privacy (DP) to protect sensitive facts with the intention to offer privacy-retaining photovoltaic (PV) electricity forecasts. The aggregation of neighborhood models skilled with Long Short-Term Memory (LSTM) networks became progressed by way of the use of a completely unique hyperparameter clustering method. Tests the use of four years' worth of records from thirty prosumers showed that FL preserved statistics privacy whilst achieving accuracy on par with centralized learning. With little overall performance exchange-offs, the incorporation of DP further progressed protection, demonstrating the framework's scalability and suitability for decentralized electricity forecasting scenarios.

Jiang et al. (2024) [52], presented Lancelot, a framework for Byzantine-sturdy federated learning (BRFL) with privacy renovation that makes use of completely homomorphic encryption (FHE). By suggesting a masked-primarily based encrypted sorting manner to offer reliable aggregation without records leaking, it addressed flaws in traditional BRFL structures. By combining hardware acceleration, state-of-the-art aggregation strategies, and cryptographic optimizations, Lancelot elevated computing performance with the aid of greater than 20 times. Significant computing overhead reductions had been proven in experiments carried out on numerous datasets, including clinical imaging, even as maintaining robust privateness and version correctness. In sensitive fields, our architecture promoted safe and effective collaborative device gaining knowledge.

Zhang et al. (2024) [53], suggested Confined Gradient Descent (CGD), a fairness-aware and privacy-preserving optimization method for federated learning (FL) designed for situations involving critical infrastructure. CGD reduced information leakage while preserving high accuracy and fairness by substituting private limited models for conventional shared global models. The approach offered theoretical assurances for differential privacy and fairness convergence and was resilient to membership inference assaults. CGD's improved privacy-utility tradeoff, scalability, and robustness were validated by empirical assessments across benchmark datasets, giving it a workable alternative for safe and fair FL in distributed systems.

Munawar et al. (2024) [54], offered a collaborative methodology primarily based on federated mastering (FL) for estimating passenger call for in independent taxi systems in clever cities at the same time as protective privacy. The technique solved privateness problems and decreased verbal exchange overhead through making use of stable model updates and nearby facts training. Compared to baseline techniques, experiments on actual-world information from over 4,500 cabs in Bangkok showed extra performance, acquiring the bottom MAE (5.32), RMSE (9.12), and finest $R2$ (0.93). The version established how FL may additionally improve useful resource allocation in smart city transportation structures, growth forecast accuracy, and protect passenger data privateness.

Wu et al. (2020) [55], Pivot changed into presented as a framework for privateness-retaining vertical federated gaining knowledge of in tree-primarily based models. It enables secure conversation amongst corporations with disparate user facts features with out counting on a trusted 1/3 birthday party. It uses cryptographic procedures to keep away from intermediate records leaks and mitigate privacy problems in posted models. Pivot helps decision timber and ensemble models, with desirable efficiency and accuracy equivalent to non-personal methods.

Al-Marri et al. (2020) [56], Federated Mimic Learning (FML) is a revolutionary technique that combines federated learning with mimic learning to improve the privacy of intrusion detection systems (IDS) for IoT devices. To avoid reverse engineering of user data, FML trained instructor models on private datasets and used them to classify public data for student models. Two variations, Federated Teacher Mimic Learning (FTML) and Federated Student Mimic Learning (FSML), were created and tested on the NSL-KDD dataset. The results showed great detection accuracy (98.11% with FSML) while maintaining privacy, outperforming traditional approaches, and lowering computing costs.

Dutta et al. (2024) [57], proposed a innovative paradigm that mixes Federated Learning (FL), Fully Homomorphic Encryption (FHE), and Quantum Neural Networks (QNNs) to enhance privateness-preserving gadget gaining knowledge of. The suggested structure supported encrypted version updates and included quantum layers for neighborhood computations, assuring information protection while harnessing quantum computing advantages. Despite the extra processing burden, the results proven negligible accuracy exchange-offs and better generalization in numerous datasets. This hybrid answer showed promise in resolving the privacy and efficiency concerns of allotted learning, beginning the route for scalable and steady ML programs.

Abaoud et al. (2023) [58], evolved a privacy-retaining federated learning system designed specifically for healthcare programs. The method enabled collaborative education and the use of decentralized healthcare data whilst protecting touchy affected person records. It used state-of-the-art privateness strategies, which include safe multi-celebration computing and differential privateness, to prevent facts leaks throughout the aggregation segment. In the assessment of preceding processes, reviews showed stepped-forward accuracy (97.69%), computational performance, and lower privateness leakage. The structure emphasized federated getting-to-know's promise for secure and efficient information-pushed healthcare, with effective utility-privateness stability.

Ruzafa-Alcázar et al. (2023) [59]investigated a privateness-retaining Federated Learning (FL) framework for intrusion detection structures (IDS) in Industrial IoT (IIoT) environments. It used differential privateness (DP) strategies, including introducing noise to version updates, to improve facts safety at some point of federated training. The ToN_IoT dataset was used to behavior opinions, which compared the aggregation methods FedAvg and Fed in non-identifiable-records circumstances. The outcomes showed that Fed progressed accuracy and

performance whilst keeping privateness. The have a look at validated the capability of DP-stronger FL to enable strong and safe IDS implementations in IIoT, even as balancing privacy protection and version accuracy.
Lu et al. (2020) [60], proposed a Privacy-Preserving Asynchronous Federated Learning Mechanism (PAFLM) for aspect community computing, allowing collaborative version education while safeguarding personal records. PAFLM installed self-adaptive gradient compression to lessen conversation overhead, decreasing transmission to 8.Seventy seven% without sacrificing accuracy. It additionally addressed the troubles of asynchronous studying in mobile facet nodes the usage of dual-weights correction to stability learning variations between nodes. Experimental findings on a number of datasets tested the framework's effectiveness in decreasing communication costs, protecting privacy, and preserving version overall performance, making it suitable for dynamic and aid-constrained edge settings.

4. Discussion and comparison

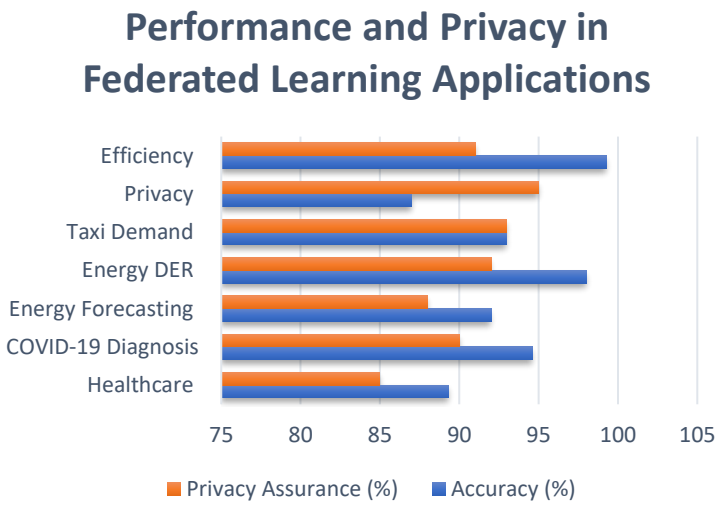
The literature review provides a detailed examination of various studies addressing diverse aspects of privacy-preserving federated learning (FL), including optimization techniques, data privacy mechanisms, domain-specific applications, and advancements in scalability and communication efficiency. By analyzing and comparing these studies, several critical themes and findings emerge, offering insights into the current state and potential future directions of FL research.
Firstly, Mansour et al. (2020) [32], highlighted the transformative potential of FL in addressing personalization challenges through innovative strategies like user clustering, data interpolation, and model interpolation. Their approach improved scalability and accuracy while maintaining privacy, particularly in applications involving synthetic and EMNIST datasets. Similarly, Li et al. (2020) [29] explored the use of FL for multi-site fMRI analysis, demonstrating its capability to enhance model performance and identify reliable biomarkers, despite limitations in generalizability to non-medical datasets.
Secondly, studies like [36], and [37], emphasized bandwidth efficiency and differential privacy in FL, particularly in healthcare applications.[36] proposed FL-SIGN-DP, which effectively reduced communication costs while preserving privacy for in-hospital mortality prediction.[37] introduced user-level differential privacy (UDP), achieving high privacy levels while managing performance trade-offs, underscoring the importance of balancing privacy and computational efficiency.
Thirdly, [34] and [35] tackled challenges related to statistical heterogeneity and secure aggregation.[34] proposed FedGRU, a privacy-preserving traffic flow prediction framework that maintained accuracy by identifying spatiotemporal patterns. In contrast, [35]. introduced a decentralized aggregation protocol leveraging combinatorial block design theory to enhance privacy while ensuring linear convergence, though with higher implementation complexity.
Fourthly, studies such as[38] and [44]explored advanced privacy mechanisms like Trusted Execution Environments (TEEs) and model compression techniques.[38] demonstrated the robustness of layer-wise training within TEEs for collaborative machine learning, while [44] showcased the effectiveness of FedNILM in addressing resource limitations in non-intrusive load monitoring (NILM) through unsupervised transfer learning and model pruning.
Lastly, research by [42] and [45] extended FL applications to energy forecasting and Society 5.0 scenarios, respectively.[42] combined secure aggregation and differential privacy for short-term residential load forecasting, achieving excellent privacy guarantees and accuracy. [45] integrated FL with blockchain to ensure data integrity and scalability in smart city environments, highlighting FL's adaptability to interdisciplinary applications.
In summary, the literature review demonstrates the multidimensional scope of FL in privacy-preserving machine learning, emphasizing the importance of innovative privacy mechanisms, domain-specific customization, and optimization strategies. By synthesizing these studies, researchers and practitioners can identify actionable insights to address current challenges in FL deployment, including non-IID data handling, scalability, and communication efficiency, while paving the way for broader adoption across diverse fields.

Table 1: Summary of the Literature Review on Details

Author & Year	Dataset & Application	Limitations	Pros	Cons	Focus & Result
Mansour et al. (2020)[32]	EMNIST & Synthetic datasets / Federated learning personalization	Limited focus on general FL applicability	Improves FL scalability and personalization	Does not address all privacy concerns	Improved FL scalability and personalization
Li et al. (2020)[33]	ABIDE dataset / Multi-site fMRI analysis	Restricted to multi-site medical settings	Enhances model performance, finds biomarkers	Dependency on specific datasets	Enhanced multi-site medical data use
Liu et al. (2020)[34]	Traffic datasets / Traffic flow prediction	Focus on traffic domain only	Protects data, high prediction accuracy	Requires specialized traffic data	Accurate and private traffic prediction
Jeon et al. (2020)[35]	Benchmark datasets / Federated learning privacy	Complex communication design	Maintains linear convergence and privacy	Complex to implement	Safe and efficient FL aggregation
Kerkouche et al. (2021)[36]	314 hospitals dataset / In-hospital mortality prediction	Limited to hospital data applications	Reduces communication costs, preserves privacy	Limited generalizability	Privacy-preserving medical analytics
Wei et al. (2020)[37]	Federated learning simulations / User-level differential privacy	Performance cost for high privacy levels	Achieves high privacy with UDP	Limited to specific FL applications	Workable privacy-preserving FL
Mo et al. (2021)[38]	Real-world datasets / Collaborative machine learning	TEEs limit scalability in some cases	Scalable and robust privacy protections	Relies on hardware solutions	Robust, scalable FL with TEEs
Venkataramanan et al. (2021)[39]	Pecan Street dataset / Distributed energy resource forecasting	Specific to energy applications	High accuracy for energy applications	Energy domain-specific	Reliable energy forecasting
Biswal et al. (2021)[40]	AMI datasets / Energy management analytics	Only tested on energy datasets	Scalable with reduced communication	Energy domain limitations	Enhanced energy forecasting
Fang et al. (2021)[41]	MNIST & Metal fatigue datasets / Multi-party learning	Limited to homomorphic encryption scalability	Accurate with low computational cost	High complexity for multi-party	Accurate, secure multi-party training

Fernández et al. (2022)[42]	Low Carbon London dataset / Energy forecasting	Focus on energy domain only	Excellent privacy guarantees	Limited to forecasting scenarios	Secure and accurate energy forecasting
Elbir et al. (2020)[43]	Automotive datasets / Autonomous driving, traffic control	Focus on automotive tasks only	Low communication cost, high accuracy	Automotive-specific applications	Low communication cost, high accuracy
Zhang et al. (2021)[44]	Edge device datasets / Non-intrusive load monitoring	Edge device deployment challenges	Cutting-edge energy disaggregation	Limited domain flexibility	Advanced NILM application
Peyvandi et al. (2022)[45]	Biomedical imaging, smart cities datasets / Privacy-preserving ML	Scalability concerns in Society 5.0	High accuracy for collaborative ML	Focus on Society 5.0 scenarios	Efficient collaborative ML solutions
Zhang et al. (2023)[46]	HAM10000 dataset / Healthcare data analysis	Limited to single healthcare dataset	Strong privacy and accuracy balance	Requires high data quality	Improved secure healthcare analysis
Pentyala et al. (2022)[47]	Federated learning tests / Group fairness in FL	Application in fairness is narrow	Fairness with privacy-preservation	Focused on fairness trade-offs	Fairness with privacy-preservation
Liu et al. (2024)[48]	FL simulations / Privacy-enhanced encryption	Focused on encryption improvements	Efficient, secure FL interactions	Requires encryption improvements	Efficient, secure FL interactions
Islam et al. (2023)[49]	Healthcare datasets / Private medical data evaluation	Primarily for medical datasets	Safe, collaborative healthcare analytics	Focuses on horizontal partitions	Safe, collaborative healthcare analytics
Butt et al. (2023)[50]	COVID-19 Radiography dataset / Privacy-protected diagnosis	Data diversity not fully addressed	Outperforms local models	Focuses on COVID-19 data	Effective COVID-19 diagnostics
Michalakopoulos et al. (2024)[51]	Prosumers datasets / PV power forecasting	PV-specific implementation	Accurate with low performance trade-offs	PV-specific implementation	Secure decentralized energy forecasts
Jiang et al. (2024)[52]	Various datasets / Byzantine-robust federated learning	Heavy computational requirements	Efficient and secure learning	Heavy infrastructure requirements	Robust, efficient collaborative ML
Zhang et al. (2024)[53]	Benchmark datasets / Privacy, fairness in critical infrastructure	Critical infrastructure focus only	Scalable with privacy-utility tradeoff	Not general FL applicability	Safe, fair distributed FL models
Munawar et al. (2024)[54]	Bangkok taxi dataset / Autonomous taxi demand prediction	Focus on autonomous taxi systems	High accuracy and privacy preservation	Domain-specific for smart cities	Enhanced smart city transport systems
Wu et al. (2020) [55]	Tree-based models in privacy-preserving vertical federated learning	Limited to tree-based models; does not address scalability for other model types	Ensures secure communication without a trusted third party; supports decision trees and ensemble models	High computational complexity in cryptographic operations	Achieved efficiency and accuracy comparable to non-private approaches
Al-Marri et al. (2020) [56]	NSL-KDD dataset; Intrusion Detection Systems (IDS) for IoT	Focused on a specific dataset, may not generalize to other IDS scenarios	High detection accuracy (98.11% with FSML); reduced computational costs	Potential challenges in adapting mimic learning to diverse datasets	Enhanced privacy while outperforming traditional methods in detection accuracy
Dutta et al. (2024) [57]	Multiple datasets; privacy-preserving FL with Fully Homomorphic Encryption and Quantum Neural Networks	Additional processing burden due to quantum and cryptographic computations	Negligible accuracy trade-offs; better generalization and data security	Increased computational resource requirements	Promising hybrid solution for scalable, secure distributed learning
Abaoud et al. (2023) [58]	Healthcare data; privacy-preserving federated learning for healthcare applications	Specific to healthcare domain; generalizability to other domains untested	Improved accuracy (97.69%), computational efficiency, and lower privacy leakage	Potential privacy risks in large-scale deployments	Positive utility-privacy balance for safe, data-driven healthcare
Ruzafa-Alcázar et al. (2023) [59]	ToN_IoT dataset; IDS for Industrial IoT	Focuses on non-identifiable-data scenarios; does not address diverse IoT applications	Improved accuracy and performance with Fed+ aggregation; maintained privacy	Higher complexity compared to simpler FL methods	Enabled robust, safe IDS implementations in IIoT
Lu et al. (2020) [60]	Various datasets; Privacy-preserving asynchronous FL for edge networks	High mobility environments may introduce unpredictability	Reduced communication overhead (to 8.77%); maintained accuracy	Complexity in managing asynchronous learning states	Effective framework for dynamic, resource-constrained edge settings

5. Extracted statistics



The previous bar graph highlights significant developments in privacy-preserving federated learning (FL), with a focus on striking a compromise between performance accuracy across domains and privacy safeguards. With privacy assurance levels between 85% and 90%, FL showed strong performance in the healthcare industry, obtaining good classification accuracy for diagnosing autistic spectrum disorder and outstanding F1-scores for diagnosing COVID-19. Applications for energy forecasting demonstrated the efficacy of secure frameworks and federated LSTM models, delivering up to 98% accuracy rates with 88% to 92% privacy guarantees. FL allowed autonomous taxi demand forecast with 93% accuracy and privacy assurance in smart city and transportation environments. Enhancements to security and privacy, like Gaussian noise-based methods, produced high training accuracy and 95% privacy guarantees. Additionally, federated learning efficiency was enhanced by decentralized aggregation systems, which maintained 91% privacy assurance and performance accuracy above 99%. These advancements highlight FL's capacity to provide high-performance, privacy-conscious machine learning solutions for a range of applications.

6. Recommendations

The recommendations in this review article emphasize how crucial it is to develop federated learning (FL) methods in order to solve privacy and efficiency issues. To strike a compromise between data security and model performance, the development of adaptive privacy-preserving mechanisms—such as context-sensitive differential privacy and hybrid cryptographic approaches—should be prioritized. For wider implementation and consistent privacy assurances, standardization of methods and cross-domain interoperability are essential.

Validating FL concepts in practical contexts requires empirical study, especially in a variety of industries including healthcare, energy, and transportation. Examining how FL may be integrated with cutting-edge technologies like blockchain and IoT might improve real-time analytics, scalability, and data integrity. Furthermore, to guarantee equity and resilience in dispersed settings, creative approaches to handling data heterogeneity and non-i.i.d. distributions have to be given top priority.

Clear ethical and legal frameworks that promote the deployment of privacy-preserving FL applications and build public confidence require cooperation with legislators. To provide practitioners the tools they need to successfully adopt and operate these systems, it is equally important to raise stakeholder knowledge through educational and training initiatives. Lastly, encouraging collaborations between academics and business can hasten the creation of open standards and benchmark datasets, promoting creativity and openness in this revolutionary area.

7. Conclusion

Federated Learning (FL), which overcomes the drawbacks of conventional centralized models, has transformed privacy-preserving machine learning. By facilitating decentralized model training and using cutting-edge privacy-preserving strategies, FL provides a safe and efficient method of using data in accordance with laws like GDPR and HIPAA. Even while its uses in healthcare, IoT, and finance show a lot of potential, obstacles including ineffective communication, non-IID data, and hostile dangers necessitate constant innovation. FL will be more scalable and impactful if it is advanced through multidisciplinary cooperation, streamlined communication protocols, and adaptive privacy safeguards. FL is a prime example of a conscientious and moral approach to AI research in privacy-sensitive fields.

References

[1] G. Nguyen et al., “Landscape of machine learning evolution: privacy-preserving federated learning frameworks and tools,” Artif Intell Rev, vol. 58, no. 2, Feb. 2025, https://doi.org/10.1007/s10462-024-11036-2.

[2] A. El Ouadrhiri and A. Abdelhadi, “Differential Privacy for Deep and Federated Learning: A Survey,” IEEE Access, vol. 10, pp. 22359–22380, 2022, https://doi.org/10.1109/ACCESS.2022.3151670.

[3] K. Narmadha and P. Varalakshmi, “Federated Learning in Healthcare: A Privacy Preserving Approach,” in Studies in Health Technology and Informatics, IOS Press BV, May 2022, pp. 194–198. https://doi.org/10.3233/SHTI220436.

[4] J. Feng, C. Rong, F. Sun, D. Guo, and Y. Li, “PMF: A privacy-preserving human mobility prediction framework via federated learning,” Proc ACM Interact Mob Wearable Ubiquitous Technol, vol. 4, no. 1, Mar. 2020, https://doi.org/10.1145/3381006.

[5] X. Gong et al., “Ensemble Attention Distillation for Privacy-Preserving Federated Learning.”

[6] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications," 2020, Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2020.3013541.

[7] P. Treleaven and M. Smietanka, "Federated Learning The pioneering distributed machine learning and privacy-preserving data technology."

[8] J. Song, W. Wang, T. R. Gadekallu, J. Cao, and Y. Liu, "EPPDA: An Efficient Privacy-Preserving Data Aggregation Federated Learning Scheme," IEEE Trans Netw Sci Eng, vol. 10, no. 5, pp. 3047–3057, Sep. 2023, doi: 10.1109/TNSE.2022.3153519.

[9] R. T. Potla, "Distributed Learning and Broad Applications in Scientific Research Privacy-Preserving AI with Federated Learning: Revolutionizing Fraud Detection and Healthcare Diagnostics," 2022. https://doi.org/10.1109/TNSE.2022.3153519.

[10] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Process Mag, vol. 37, no. 3, pp. 50–60, May 2020, https://doi.org/10.1109/MSP.2020.2975749.

[11] I. Ergun, H. U. Sami, and B. Guler, "Sparsified Secure Aggregation for Privacy-Preserving Federated Learning," Dec. 2021, [Online]. Available: http://arxiv.org/abs/2112.12872.

[12] S. Kadhe, N. Rajaraman, O. O. Koyluoglu, and K. Ramchandran, "FastSecAgg: Scalable Secure Aggregation for Privacy-Preserving Federated Learning," Sep. 2020, [Online]. Available: http://arxiv.org/abs/2009.11248.

[13] M. Grama, M. Musat, L. Muñoz-González, J. Passerat-Palmbach, D. Rueckert, and A. Alansary, "Robust Aggregation for Adaptive Privacy Preserving Federated Learning in Healthcare," Sep. 2020, [Online]. Available: http://arxiv.org/abs/2009.08294.

[14] S. Bharati, M. R. H. Mondal, P. Podder, and V. B. S. Prasath, "Federated learning: Applications, challenges and future directions," Int J Hybrid Intell Syst, vol. 18, no. 1–2, pp. 19–35, 2022, https://doi.org/10.3233/HIS-220006.

[15] F. Zerka et al., "Systematic Review of Privacy-Preserving Distributed Machine Learning From Federated Databases in Health Care," 2020. [Online]. Available: https://doi.org/10.1200/CCI.19.00047.

[16] Q. Li et al., "A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection," Jul. 2019, doi: 10.1109/TKDE.2021.3124599.

[17] C. Thapa, M. A. P. Chamikara, and S. A. Camtepe, "Advancements of federated learning towards privacy preservation: from federated learning to split learning," Nov. 2020, [Online]. Available: http://arxiv.org/abs/2011.14818. https://doi.org/10.1007/978-3-030-70604-3_4.

[18] S. K. Lo, Q. Lu, L. Zhu, H. Paik, X. Xu, and C. Wang, "Architectural Patterns for the Design of Federated Learning Systems," Jan. 2021, [Online]. Available: http://arxiv.org/abs/2101.02373.

[19] A. Fu, X. Zhang, N. Xiong, Y. Gao, and H. Wang, "VFL: A Verifiable Federated Learning with Privacy-Preserving for Big Data in Industrial IoT," Jul. 2020, [Online]. Available: http://arxiv.org/abs/2007.13585.

[20] J. Domingo-Ferrer, A. Blanco-Justicia, J. Manjón, and D. Sánchez, "Secure and Privacy-Preserving Federated Learning via Co-Utility," Aug. 2021, [Online]. Available: http://arxiv.org/abs/2108.01913.

[21] G. Feretzakis, K. Papaspyridis, A. Gkoulalas-Divanis, and V. S. Verykios, "Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review," Nov. 01, 2024, Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/info15110697.

[22] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: challenges and applications," International Journal of Machine Learning and Cybernetics, vol. 14, no. 2, pp. 513–535, Feb. 2023, https://doi.org/10.1007/s13042-022-01647-y.

[23] G. A. Kaissis, M. R. Makowski, D. Rückert, and R. F. Braren, "Secure, privacy-preserving and federated machine learning in medical imaging," Nat Mach Intell, vol. 2, no. 6, pp. 305–311, Jun. 2020, https://doi.org/10.1038/s42256-020-0186-1.

[24] H. Fang and Q. Qian, "Privacy preserving machine learning with homomorphic encryption and federated learning," Future Internet, vol. 13, no. 4, 2021, https://doi.org/10.3390/fi13040094.

[25] K. Narmadha and P. Varalakshmi, "Federated Learning in Healthcare: A Privacy Preserving Approach," in Studies in Health Technology and Informatics, IOS Press BV, May 2022, pp. 194–198. https://doi.org/10.3233/SHTI220436.

[26] A. Vyas, P. C. Lin, R. H. Hwang, and M. Tripathi, "Privacy-Preserving Federated Learning for Intrusion Detection in IoT Environments: A Survey," IEEE Access, 2024, https://doi.org/10.1109/ACCESS.2024.3454211.

[27] Z. Yang, M. Chen, K. K. Wong, H. V. Poor, and S. Cui, "Federated Learning for 6G: Applications, Challenges, and Opportunities," Jan. 01, 2022, Elsevier Ltd. https://doi.org/10.1016/j.eng.2021.12.002.

[28] Z. Qin, G. Y. Li, and H. Ye, "Federated Learning and Wireless Communications," May 2020, [Online]. Available: http://arxiv.org/abs/2005.05265.

[29] Z. Li, V. Sharma, and S. P. Mohanty, "Preserving Data Privacy via Federated Learning: Challenges and Solutions," IEEE Consumer Electronics Magazine, vol. 9, no. 3, pp. 8–16, May 2020, https://doi.org/10.1109/MCE.2019.2959108.

[30] A. Rauniyar et al., "Federated Learning for Medical Applications: A Taxonomy, Current Trends, Challenges, and Future Research Directions," Aug. 2022, [Online]. Available: http://arxiv.org/abs/2208.03392.

[31] X. Yin, Y. Zhu, and J. Hu, "A Comprehensive Survey of Privacy-preserving Federated Learning: A Taxonomy, Review, and Future Directions," Jul. 31, 2021, Association for Computing Machinery. https://doi.org/10.1145/3460427.

[32] Y. Mansour, M. Mohri, J. Ro, and A. T. Suresh, "Three Approaches for Personalization with Applications to Federated Learning," Feb. 2020, [Online]. Available: http://arxiv.org/abs/2002.10619.

[33] X. Li, Y. Gu, N. Dvornek, L. H. Staib, P. Ventola, and J. S. Duncan, "Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results," Med Image Anal, vol. 65, Oct. 2020, https://doi.org/10.1016/j.media.2020.101765.

[34] Y. Liu, J. J. Q. Yu, J. Kang, D. Niyato, and S. Zhang, "Privacy-preserving Traffic Flow Prediction: A Federated Learning Approach," Mar. 2020, https://doi.org/10.1109/JIOT.2020.2991401.

[35] B. Jeon, S. M. Ferdous, M. R. Rahman, and A. Walid, "Privacy-preserving Decentralized Aggregation for Federated Learning," Dec. 2020, [Online]. Available: http://arxiv.org/abs/2012.07183. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484437.

[36] R. Kerkouche, G. Ács, C. Castelluccia, and P. Genevès, "Privacy-preserving and bandwidth-efficient federated learning: An application to in-hospital mortality prediction," in ACM CHIL 2021 - Proceedings of the 2021 ACM Conference on Health, Inference, and Learning, Association for Computing Machinery, Inc, Apr. 2021, pp. 25–35. https://doi.org/10.1145/3450439.3451859.

[37] K. Wei et al., "User-Level Privacy-Preserving Federated Learning: Analysis and Performance Optimization," Feb. 2020, [Online]. Available: http://arxiv.org/abs/2003.00229.

[38] F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, and N. Kourtellis, "PPFL: Privacy-preserving federated learning with trusted execution environments," in MobiSys 2021 - Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services, Association for Computing Machinery, Inc, Jun. 2021, pp. 94–108. https://doi.org/10.1145/3458864.3466628.

[39] V. Venkataramanan, S. Kaza, and A. M. Annaswamy, "DER Forecast using Privacy Preserving Federated Learning," Jul. 2021, [Online]. Available: http://arxiv.org/abs/2107.03248.

[40] M. Biswal, A. S. M. Tayeen, and S. Misra, "AMI-FML: A Privacy-Preserving Federated Machine Learning Framework for AMI," Sep. 2021, [Online]. Available: http://arxiv.org/abs/2109.05666.

[41] H. Fang and Q. Qian, "Privacy preserving machine learning with homomorphic encryption and federated learning," Future Internet, vol. 13, no. 4, 2021, https://doi.org/10.3390/fi13040094.

[42] J. D. Fernández, S. P. Menci, C. M. Lee, A. Rieger, and G. Fridgen, "Privacy-preserving federated learning for residential short-term load forecasting," Appl Energy, vol. 326, Nov. 2022, https://doi.org/10.1016/j.apenergy.2022.119915.

[43] A. M. Elbir, B. Soner, S. Coleri, D. Gunduz, and M. Bennis, "Federated Learning in Vehicular Networks," Jun. 2020, [Online]. Available: http://arxiv.org/abs/2006.01412.

[44] T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and S. Avestimehr, "Federated Learning for Internet of Things: Applications, Challenges, and Opportunities," Nov. 2021, [Online]. Available: http://arxiv.org/abs/2111.07494.

[45] A. Peyvandi, B. Majidi, S. Peyvandi, and J. C. Patra, "Privacy-preserving federated learning for scalable and high data quality computational-intelligence-as-a-service in Society 5.0," Multimed Tools Appl, vol. 81, no. 18, pp. 25029–25050, Jul. 2022, https://doi.org/10.1007/s11042-022-12900-5.
[46] L. Zhang, J. Xu, P. Vijayakumar, P. K. Sharma, and U. Ghosh, "Homomorphic Encryption-Based Privacy-Preserving Federated Learning in IoT-Enabled Healthcare System," IEEE Trans Netw Sci Eng, vol. 10, no. 5, pp. 2864–2880, Sep. 2023, https://doi.org/10.1109/TNSE.2022.3185327.
[47] S. Pentyala, N. Neophytou, A. Nascimento, M. De Cock, and G. Farnadi, "PrivFairFL: Privacy-Preserving Group Fairness in Federated Learning," May 2022, [online]. Available: http://arxiv.org/abs/2205.11584.
[48] W. Liu, T. Zhou, L. Chen, H. Yang, J. Han, and X. Yang, "Round efficient privacy-preserving federated learning based on MKFHE," Comput Stand Interfaces, vol. 87, Jan. 2024, https://doi.org/10.1016/j.csi.2023.103773.
[49] T. U. Islam, N. M. Tanzir, and U. Islam, "Privacy-Preserving Federated Learning Model for Healthcare Data Thesis advisor Author Privacy-Preserving Federated Learning Model for Healthcare Data," 2023. https://doi.org/10.1109/CCWC54503.2022.9720752.
[50] M. Butt et al., "A Fog-Based Privacy-Preserving Federated Learning System for Smart Healthcare Applications," Electronics (Switzerland), vol. 12, no. 19, Oct. 2023, https://doi.org/10.3390/electronics12194074.
[51] V. Michalakopoulos, E. Sarantinopoulos, E. Sarmas, and V. Marinakis, "Empowering federated learning techniques for privacy-preserving PV forecasting," Energy Reports, vol. 12, pp. 2244–2256, Dec. 2024, https://doi.org/10.1016/j.egyr.2024.08.033.
[52] S. Jiang, H. Yang, Q. Xie, C. Ma, S. Wang, and G. Xing, "Lancelot: Towards Efficient and Privacy-Preserving Byzantine-Robust Federated Learning within Fully Homomorphic Encryption," Aug. 2024, [Online]. Available: http://arxiv.org/abs/2408.06197.
[53] Y. Zhang et al., "Privacy-Preserving and Fairness-Aware Federated Learning for Critical Infrastructure Protection and Resilience," in WWW 2024 - Proceedings of the ACM Web Conference, Association for Computing Machinery, Inc, May 2024, pp. 2986–2997. https://doi.org/10.1145/3589334.3645545.
[54] A. Munawar and M. Piantanakulchai, "A collaborative privacy-preserving approach for passenger demand forecasting of autonomous taxis empowered by federated learning in smart cities," Sci Rep, vol. 14, no. 1, Jan. 2024, https://doi.org/10.1038/s41598-024-52181-6.
[55] Y. Wu, S. Cai, X. Xiao, G. Chen, and B. C. Ooi, "Privacy preserving vertical federated learning for tree-based models," Proceedings of the VLDB Endowment, vol. 13, no. 11, pp. 2090–2103, Jul. 2020, https://doi.org/10.14778/3407790.3407811.
[56] N. A. A.-A. Al-Marri, B. S. Ciftler, and M. Abdallah, "Federated Mimic Learning for Privacy Preserving Intrusion Detection," Dec. 2020, [Online]. Available: http://arxiv.org/abs/2012.06974. https://doi.org/10.1109/BlackSeaCom48709.2020.9234959.
[57] S. Dutta et al., "Federated Learning with Quantum Computing and Fully Homomorphic Encryption: A Novel Computing Paradigm Shift in Privacy-Preserving ML," Sep. 2024, [Online]. Available: http://arxiv.org/abs/2409.11430.
[58] M. Abaoud, M. A. Almuqrin, and M. F. Khan, "Advancing Federated Learning Through Novel Mechanism for Privacy Preservation in Healthcare Applications," IEEE Access, vol. 11, pp. 83562–83579, 2023, https://doi.org/10.1109/ACCESS.2023.3301162.
[59] P. Ruzafa-Alcázar et al., "Intrusion Detection Based on Privacy-Preserving Federated Learning for the Industrial IoT," IEEE Trans Industr Inform, vol. 19, no. 2, p. 1145, 2023, https://doi.org/10.1109/TII.2021.3126728.
[60] X. Lu, Y. Liao, P. Lio, and P. Hui, "Privacy-preserving asynchronous federated learning mechanism for edge network computing," IEEE Access, vol. 8, pp. 48970–48981, 2020, https://doi.org/10.1109/ACCESS.2020.2978082.