# Federated Learning: Algorithms, Privacy Mechanisms, and Applications

Benazir Meem, Asifa Akter Liya, Riya Akter, Arisha Ashraf
East West University
Email: 2022-3-60-169@std.ewubd.edu

***Abstract*—Federated Learning (FL) is a recently developed paradigm that has shown potential as a means of collaborative machine learning based on preserving the privacy of distributed data [1], [2]. In contrast to traditional centralized models, FL enables several clients and distributed edge clients, hospitals, and financial institutions to train shared models without transferring unprocessed data, overcoming these concerns and constraints, including GDPR and HIPAA [3]–[5].**

**In the following survey, readers can find in-depth descriptions of FL algorithms such as FedAvg and its variants FedProx, FedNova, and personalized FL algorithms, e.g., pFedMe and FedPer [1], [2], [6]–[8]. Such algorithms solve important problems of non-IID data, diverse client capabilities, communication efficiency, and client personalization.**

**The survey also explores applications of FL in various domains. In healthcare, FL is used for jointly analyzing electronic health records and medical imaging while preserving patient privacy [?], [3], [4]. In finance, it enables fraud detection, credit risk assessment, and personalized recommendations without storing sensitive customer information in a central location [5]. Additionally, FL has recently been applied in IoT and edge computing for predictive analytics, smart-city management, autonomous systems, and cybersecurity through federated intrusion detection [9], [10].**

**Finally, the survey highlights challenges and future directions, including the standardization of benchmarks, lightweight cryptography protocols, adaptive aggregation algorithms, and integration with new paradigms such as large language models, multi-modal learning, and reinforcement learning systems [8], [11]. This work provides a comprehensive overview of FL algorithms, privacy-preserving methods, applications, and research questions, illustrating how FL enables scalable, privacy-preserving AI across a wide variety of applications.**

***Index Terms*—Federated Learning, Privacy-Preserving Machine Learning, Differential Privacy, Secure Aggregation, Edge AI**

## I. Introduction

The rapid explosion of data generated by edge devices like mobile phones, wearable sensors, and Internet of Things (IoT) has opened doors to machine learning as never before. These devices constantly gather multivariate and sensitive information ranging from personal health measures to financial transactions and location information [1], [2]. The conventional centralized machine learning approach, where such information is combined into a central server, is usually plagued by serious privacy, security, and compliance challenges. Centralization may be in contravention of privacy regulations like the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in America and triggers alarms concerning data breaches and misuse [3]–[5].

Federated Learning (FL) has been a possible solution to them through decentralized model training. In FL, raw data remains on devices or in institutional networks and only model updates or gradients are uploaded to a central server for aggregation [1], [9]. FL solves privacy problems but decreases barriers to compliance with regulations; nevertheless, high-performance machine learning models may be constructed. By keeping sensitive data local to an individual user, FL ensures confidential data are not divulged out, but the collaborative training process can leverage diversity and volume of data distributed [3], [4].

This survey aims to give a comprehensive overview of FL in three broad areas: firstly, the underlying algorithms driving federated learning, such as Federated Averaging (FedAvg) and its extensions [1], [2], [6]–[8]; secondly, the privacy-assuring and security infrastructures, such as Differential Privacy (DP), Secure Multiparty Computation (SMPC), Homomorphic Encryption (HE), and Trusted Execution Environments (TEEs) [11]–[14]; and thirdly, practical applications of FL across sectors from healthcare to finance, IoT, edge computing, and cybersecurity [3]–[5], [9], [10].

Through analyzing these regions, this survey outlines the potential, strengths, and weaknesses of FL as an integral enabler of privacy-sensitive, distributed artificial intelligence, and provides guidance to researchers and practitioners interested in applying FL in real-world systems [8], [11].

## II. Background and Taxonomy

In the case of Federated Learning (FL), the original concept and the FedAvg algorithm were introduced and popularized by McMahan et al. (2017). The main contributions made by FedAvg were the establishment of a decentralization of training; multiple clients can simultaneously tune a global model while maintaining the raw data on local devices. FL has since been generalized to several paradigms to address various data distributions, client capabilities, and application needs [1], [2].

One way to classify FL is by feature space and participant alignment. **Horizontal FL** is useful when clients occupy the same feature space yet possess varying samples of users, e.g., different hospitals having similar EHR structures but different populations [3], [4]. **Vertical FL** arises when clients share a common set of users but distinct features; for example, a bank

and an e-commerce platform may have complementary goals regarding the same customers. **Federated Transfer Learning (FedTL)** performs a more general transfer type of learning across both feature and sample spaces in cases where datasets are heterogeneous [8].

Another important distinction is between **cross-device FL** and **cross-silo FL**. In cross-device FL, thousands to millions of clients with limited data and computational resources, such as smartphones or IoT sensors, participate in training [1], [9]. In contrast, cross-silo FL involves cooperation between a limited number of organizations, such as hospitals or financial institutions, which have larger local datasets and more stable computational resources.

A general FL workflow can be described as follows: firstly, the server selects a set of clients to participate in a training cycle; secondly, each client trains a local model on its dataset; thirdly, the server aggregates the client updates; and finally, the updated global model is redistributed to clients [2], [6], [9].

This taxonomy provides an organized overview of the FL landscape and helps determine suitable frameworks, algorithms, and security solutions for different applications. By analyzing FL along these axes, researchers and engineers can design more efficient, scalable, and practical systems that align with real-world data distributions, client capabilities, and application requirements [7], [8].

### *A. Strategies of Client Selection*

Client selection is a key element of federated learning processes since it directly influences the convergence rate, the global model accuracy, and fairness [1], [2]. In cross-device FL systems, a subset of devices might be available at each training round, e.g., because of network connectivity problems, battery constraints, or user behaviour. The random client selection is an easy approach but it could skip the devices with high-quality or diverse datasets that could dramatically enhance the global model [6].

To cope with this, methodologies involving importance-based selection have been proposed, where clients are selected on the basis of evaluation criteria including the richness of locally-available data, the potential contribution of the data to the enhancement of the model, or the availability of computational resources [6]. The fairness-aware selection extends this by preventing systematic exclusion of a client with a lower participation frequency, less resources, or smaller datasets, which is crucial in fair and diverse environments by omitting bias and not disproportionately failing to consider all client types in all data sources.

A few also use adaptive selection strategies, dynamically tuning the population of active clients by their prior contribution to training and performance. This will enable the system to prioritise favourable updates based clients without omitting people in diversity, which helps in generalization. Well-designed client selection mechanisms, thus, can find a so-called Goldilocks balance of efficiency, robustness, fairness, and inclusivity, which are critical in successful deployment of FL in real-world large-scale systems.

### *B. Communication-Efficient Mechanisms*

One of the most serious bottlenecks in federated learning occurs during communication with clients, and when this involves hundreds or thousands of devices, it places a significant strain on the central server [1], [9]. Large models have high bandwidth costs, latency, and energy consumption when parameter updates are transmitted frequently and in high dimensions from edge devices [2].

To address these challenges, several communication-efficient mechanisms have been proposed. Model compression techniques, such as quantization and sparsification, reduce the size of updates by storing parameters with fewer bits or transmitting only the most significant gradients. Frequency reduction strategies, including periodic averaging or asynchronous updates, allow clients to perform multiple local training steps before sending updates, thereby reducing communication rounds [2].

Client-side adaptive strategies enable devices to decide whether to participate in a training round based on network conditions, battery level, or estimated model contribution [8]. Hierarchical aggregation is another approach, where updates are first aggregated locally among subsets of clients before being sent to the central server, reducing overall communication overhead [9].

By combining these strategies, federated learning systems can maintain high model accuracy while significantly reducing communication costs. These mechanisms are particularly relevant for cross-device FL, where limited connectivity and resources are common, and are critical for scalable deployment in real-world heterogeneous environments.

### *C. Data Heterogeneity Impacts*

One of the main challenges in federated learning is the heterogeneity of client data, as clients may hold datasets that are non-IID (non-independent and identically distributed). Data may vary in size, feature space, or label distribution [1], [2], [6]. This heterogeneity can cause local models to drift in directions misaligned with the global objective, slowing convergence, reducing accuracy, and introducing bias toward clients with larger or more representative datasets [7], [8].

Several strategies have been proposed to mitigate these issues. Personalized federated learning methods, such as pFedMe and FedPer, coordinate local adaptation with a balance between shared and client-specific updates [7], [8]. Aggregation-based approaches like FedProx and FedNova stabilize model updates under statistical heterogeneity by adjusting contributions according to client participation and data distribution [2], [6].

Additional strategies include reinforcing critical information while down-weighting noisy or malicious updates, or prioritizing client contributions based on data quality and quantity. Proper regulation of heterogeneity is essential to ensure model

correctness, fairness, and robustness against low-quality or adversarial clients.

Effectively managing data heterogeneity is crucial for practical deployment of FL in real-world scenarios, where applications in healthcare, finance, and IoT encounter diverse and unevenly distributed datasets.

## III. Core Algorithms

Federated learning is rooted in Federated Averaging (FedAvg) [1] introduced in 2017 by McMahan et al. In FedAvg, a global model trained locally would run in a few training steps only, followed by transmission of the new parameters to a central server. The server averages the updates in a manner weighted according to the size of the dataset held by the clients, with clients having more weight. The process minimizes rounds of communication as compared to updates every batch.

Ways of improving the management of heterogeneous settings were proposed. FedProx [2] adds a proximal term, which avoids degeneracy of local models drifting to a distance too far to reach consistency with the global model when clients have non-IID data or different computational capacities. FedNova [6] avoids bias introduced when clients submit different amounts of local updates by normalizing input contributions prior to aggregation, so that it converges more reliably.

There is one critical direction, which is personalized federated learning, which tries to optimize the global model to each client with their privacy data. Regularized objective approaches such as pFedMe [7] balance shared and local model performance in order to avoid over-localization, whereas FedPer [8] learns with individual layers (not shared across clients), enhancing performance when those data distributions vary considerably.

These algorithms are the foundation of federated learning and each of them is targeted at addressing particular issues of non-IID data, efficiency in communications and personalization requirements.

## IV. Privacy and Security Mechanisms

The ability to ensure some level of privacy is one of the reasons that federated learning is becoming an option as the primary approach is the retention of the raw data at the device-level. However, the supply of model updates does not promise the safety. It has developed different strategies to foster the strength of privacy and guard against releasing secret information.

One of the most popular tools is Differential Privacy (DP) [12]. It adds noise to gradients or model parameters and samples it stochastically and mathematically it is hard to draw conclusions about specific data. It works very well but at a certain level it should be able to eliminate accuracy of models where noise is been introduced into the models.

SMPC [11] enables a group of clients to revise the aggregated model in a collaborative fashion where none of the parties need to reveal how they revised their inputs. The clients also have the ability of encrypting their inputs and the final mixing output is learnt by the server. Homomorphic encryption (HE) [13], too, has been demonstrated to allow computations to be performed with encrypted data, but once again, this is costly.

Hardware-based (e.g., Trusted Execution Environments (TEEs) [14] (e.g., Intel SGX) implement isolated secure environments on processors and therefore, some amount of secure computation is possible even when the main system is compromised. Learning forms, which may entail centralization, but it must not be considered as a type of information protection by itself.

Despite the existence of such mechanisms, there exist multiple security threats in federated learning. Poisoning attacks [15] are attacks where corrupted clients inject inaccurate update into the global model. Model inversion or inference attacks [16] seek to reconstruct sensitive information about the training data on the basis of shared model parameters. Some of the other potential risks that have recently been identified are the threat of backdoors where the hackers insert a hidden malicious code without disrupting the performance of the model.

In unison, what these practices and restrictions show, is that FL makes privacy better than traditional learning forms, which may entail centralization, but it must not be considered as a type of information protection by itself.

## V. Applications

Federated Learning has also been widely used in healthcare where hospitals and medical research facilities can train models without exposing sensitive medical information about patients. Some possible applications are the analysis of electronic health records (EHR), medical imaging, and disease prediction. Experiments have shown that FL has the ability to provide a performance that matches that of centralized models without compromising privacy [3], [4]. Methods with direct control over heterogeneity, such as techniques like FedAvg [1] and personalized FL techniques like pFedMe [7] have been found to be especially effective in dealing with heterogeneous hospital data.

In finance, the tasks that can be assisted by FL include fraud detection, credit risk estimation and personal recommendations. Institutions can then maximise collective insights by maintaining customer data locally and not breaching any privacy laws [5]. The use of cross-device and cross-silo frameworks as addressed by Bonawitz et al. [9] can also come in handy in giving the ability to collaborate between multiple organizations in a secure manner, hence increasing the model robustness but also saving communication costs.

IoT, edge computing, and cybersecurity domains are also deployed with the use of FL. Predicting what will be written next, real-time analytics, and smart-city management are just a few of the capabilities that FL has enabled in IoT devices and autonomous vehicles, due to the advantages of having local data updates but a low bandwidth fill [9]. In cybersecurity, federated intrusion detection suits use geographically distributed logs across different organizations in concert to

detect intrusions without releasing other network data [10]. In each of these domains, FL successfully achieves a balance between the model performance and privacy, showing the model applicability to use case sharing sensitive and distributed data.

## VI. Incentive and Fairness Mechanisms

Federated learning is characterized by voluntary and non-homogeneous participation of the clients, which may result in contributions imbalance and unfair practice. Clients may have access to high-quality or computing resources, or they may have access to low-quality or limited resources [1], [2], [8]. This would be led by the incentive regime, where a client who is free-riding off the rest of the participants by not contributing his or her share on training by short-cutting would cause the entire system to be overwhelmed, hence not effective enough and not credible [**?**], [5], [9, Chapter 3, 6, 8].

This has necessitated the design of incentive structures to motivate good or stable participation. Such mechanisms could make clients contribute more, as reputation- or token-based systems that reward clients based on the quality and quantity of contributions could encourage higher participation. In addition, data aggregation strategies that respect fairness allow the data of resource-constrained clients to not be excluded, thus preserving overall model generalizability and fairness [7], [8].

Others also share the premise of using adaptive client weighting, where a client contributes to the level of aggregation proportional to the dependability, variety, and significance of the data it provides [2], [6]. This not only minimizes discrimination against high opt-out clients but is also generalizable to other domains where minority data distributions must be considered, e.g., in healthcare and finance.

In summary, high incentive and fairness mechanisms counteract unsustainable participation, ensure fair contribution, and strengthen the robustness of federated learning in large-scale, non-homogeneous settings.

## VII. Robustness Against Adversarial Attacks

The decentralized nature of FL has exposed it to adversarial machine learning which can have serious adverse effects on the performance, accuracy, and reliability of the global model, though Federated Learning (FL) has the opportunity of being more privacy-protective, as it may turn into creating a reduced exposure of raw data to remote actors. Other stark threats include poisoning attacks through which the rogue clients would actively construct and inject harmful updates into the global model aiming to corrupt its predictive model or cause outputs to be manipulated in a specific way [15], [16]. A more sophisticated type of attacks exists, the so-called backdoor attack, where the attackers add hidden malicious triggers into the model that then only activate when they encounter a specific input or pattern [9], [15]. The attacks are particularly threatening when the stakes are high as in healthcare, financial systems, or autonomous vehicles, where a bad prediction bears harsh real-life consequences [3], [5].

There is a collection of safe aggregation methods to mitigate these risks. The typical weighted mean aggregation employed by FedAvg is vulnerable to outlier or poisoned updates and therefore robust aggregation rules have been suggested, e.g., Krum, Trimmed Mean, and Median. These methods aim to reduce the impact of malicious updates by committing on consensus of honest clients and reducing the impacts of abnormal contributions [2], [6]. Another approach is anomaly detection in client updates, identifying suspicious patterns or gradients before they merge into the global model, thereby preventing damaging updates.

A second layer of protection can be founded on cryptography, e.g., Secure Multiparty Computation (SMPC) and homomorphic encryption, which provide security by encrypting client updates over the channel while allowing the server to calculate aggregated results. Such techniques preserve privacy while permitting the detection of inconsistencies or anomalies. Additional methods include aggregating client reputation and hierarchical aggregation, where updates are weighted based on client reliability or past performance, reducing the influence of low-reliable or newly suspicious clients [8], [9].

In addition, researchers are exploring adaptive defense systems, which adjust strategies according to the perceived level of adversarial activity. By monitoring model performance, the variance in client updates, and client behavior in real time, the impact of potentially destructive clients can be dynamically reduced, maintaining model robustness and fairness. When used together with communication- and client-selection-efficient FL protocols, these defense strategies form a central part of a secure FL system.

Finally, ensuring adversarial resilience is not only a technical necessity but also a prerequisite for real-world deployment. Adversarially robust FL enables high-stakes applications in healthcare, finance, and cybersecurity to scale reliably. Future research is expected to explore hybrid strategies combining robust aggregation, anomaly detection, cryptographic techniques, and reputation-based weighting to further enhance FL security.

## VIII. Challenges and Open Problems

In spite of its potential, Federated Learning (FL) continues to face quite a number of challenges and pending issues that still hinder its deployment and achievement in actual systems [1], [2], [6]. One of the origins of our current challenge is that of non-IID (non-independent and identically-distributed) data distribution among clients [1], [2], [6]. Because the data gathered by the devices of many users, in the hospital, at the bank terminals, or IoT sensors may be quite different in size, quality, and feature space, the world model learned by aggregating such heterogeneous updates can be poorly convergent, biased, and inaccurate compared to centralized training [1], [2], [6], [7]. This heterogeneity also results in client drift where individualized model optimization pipeline no longer aligns with the global objective, resulting in unstable aggregation and inefficient training process [6], [7].

The second significant issue is the high communication cost between client and the central server, especially in cases of large-scale neural networks that need recurrent updates of parameters millions of times [1], [2]. Shipping and loading

these parameters is a costly bandwidth usage, involves latency, and restricts wide-scale deployment where remote or edge connectivity could be unreliable [1], [2]. Security and privacy concerns aside from communication still remain as open and burning issues [11], [12], [15], [16]. Adversarial training models are threatening poisoning attacks on corrupting the global model, and model inversion and membership inference attacks are threatening user confidentiality since they attempt to reconstruct sensitive data from jointly shared gradients [15], [16].

Similarly, free-riding, where malicious clients harvest the benefits without contributing substantially in computations to update the global model, goes against fairness and trust in collaborative learning [9]. Apart from adversarial attacks, FL also does not have shared benchmarks and reproducible test procedures [2], [8]. Various research groups use various datasets, publish various metrics, and conduct different experimental settings, so comparing different algorithms on an equal level or even development testing over time becomes troublesome [2], [8].

Furthermore, adherence to various legislative and regulatory frameworks like General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and sector-specific regulations like HIPAA in healthcare adds complexity as various jurisdictions have differing requirements in respect of data sharing, retention, and transparency [8], [14]. The hardware limitations and power usage with the client devices are yet to be solved issues; device clients with limited computation, storage, and battery life may not be able to support intensive training, questioning equity and motivation to participate [2], [6].

Lastly, novel applications like federated learning for autonomous vehicles, smart grids, and healthcare require more, and so far lacking — robustness, explainability, and explainability guarantees, whereas current federated learning systems provide none of these in any way [3]–[5]. These all highlight the importance of advanced aggregation methods that can cope with non-IID settings, communication-efficient protocols that do not use much bandwidth, defenses against sophisticated and savvy attackers, incentive mechanisms able to discourage freeloading, and globally accepted standards that are equitable, secure, and regulatory compliant [1], [2], [6], [8], [11]. Solving these open problems will be critical for the extension of federated learning from research prototypes to deployable solutions in industry on a wide variety of diverse domains [1], [3], [5], [8].

## IX. Future Directions

Future FL research should therefore entail the designing of adaptive aggregation algorithms that would consider the heterogeneity in client contributions and behave in a manner that is stable, fair and robust in the event of non-homogenous distribution of at least client participation rates and capacities, not to mention data [1], [2], [6]. Such algorithms would need to risk incoming new information with already present information out there to enable some form of survivability against the mass of incoming information, have a notion of 'user drift' that prevents the system being subverted by an active attacker, but at the same time allow them to scale using the number of independent instances which do have the diversity [6], [7]. A third exciting direction is the design of light-weight cryptographic protocols of secure aggregation that there is a prospect of much less computation and communication overhead compared to current approaches, viz. homomorphic encryption and multiparty computation [11]–[13]. These should provide strong privacy guarantees but may still be operated on smartphones, IoT devices and other low-memory/low-computation/low-battery edge devices [14].

At the same time, a standardization of test benches, the sets of data provided, and the compilation of benchmarking projects will also be required to contribute to the methodological harmonization of the assessment process, reproducibility, and the possibility of openly comparing frameworks, algorithms, and spheres [2], [8]. Along these lines we can already anticipate further future developments in terms of integrating FL with other promising paradigms, such as large language models, multi-model learning, and reinforcement learning, to extend FL even beyond the simpler unsupervised tasks to more complex supervised tasks, highly interpretive, adjustive, and interactive situations [8]. Hybrid systems of FL and big pre-trained models are likely to facilitate transformational applications in the fields of personalized healthcare [3], [4], financial predictions [5], intelligent cities, and autonomous driving systems, where real-time performance, scalability, and privacy are demanded all simultaneously. Explainability and interpretability in FL pipelines is another key area of activity as users, regulators and industry stakeholders are increasingly demanding a transparent decision-making and an opportunity to audit [8].

Moreover, incentive schemes, reputation-based trust systems, as well as, tokenized reward models may promote honest contributions and continuous engagement, avoiding the problem with free-riders and low quality updates [9]. Energy-efficient training procedures and device-aware optimization strategies must also be considered to make sure resource-limited clients are not overloaded and yet they remain active participants [2], [6].

Ultimately, interdisciplinary research will be the key to formulating international standards, facilitating compliance with regulations and developing infrastructure that can enable FL to move beyond scholarly proof-of-concept models and into production-ready methods [8], [14]. All these future pathways suggest that there is still a considerable distance to go, but FL has a huge potential to develop a secure, scalable, transparent, and universally accepted distributed form of artificial intelligence in the next decade [1], [8], [11].

## X. Conclusion

Federated Learning (FL) has become one of the foundations in the field of privacy-preserving AI where it is possible to train collaboratively without aggregating sensitive data [1], [2]. This review introduced the most important foundations

of FL, its algorithms, taxonomy and privacy [6], [11], [12]. Secure aggregation protocols like [11], differential privacy [12], trusted execution environments [14] have been proposed to address the issue, and personalized FL to adapt to heterogeneous distributions of clients have also been developed [7], [8].

The uses of FL are growing into areas like healthcare [3], [4], finance [5], mobile computing and cybersecurity [10]. In spite of this development, there are other challenges that have not been resolved. Data variability among clients generate statistical and systems level bottlenecks [2], [6] and communication efficiencies and scalability constraints limit large-scale applications. Moreover, adversarial attacks like poisoning and model inversion increase the risk to model performance and the secrecy of stored data.

Other contemporary research has also focused on client selection methods to enhance equity and system optimality [2], and incentives are being designed to favour equitable participation [8]. On the same note, finding solutions to adversarial attacks and aligning FL frameworks with regulatory and ethical requirements is also an emerging challenge.

Moving forward, future work should focus on adaptive aggregation algorithms considering a variance in various client contributions [2], [6], lightweight cryptographic algorithms to enable a secure yet efficient aggregation in a distributed environment [11], as well as on basic benchmarking practices to facilitate their standardization [9]. Multi-modal learning and integration with large language models also provides a way to scale FL to more realistic tasks.

To sum up, FL is a technological solution but also a socio-technical pattern. Its effectiveness will be in the ability to align the theoretical progress and practical applications, so that models developed in the federated contexts can be not only highly efficient and accurate, but responsible, transparent, and ethically and legally acceptable [3], [5]. By overcoming issues of efficiency in communication, heterogeneity, incentives and robustness, FL can open the door to entirely new secure and decentralized systems in AI.

## REFERENCES


[1] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *AISTATS*, 2017. [Online]. Available: https://proceedings.mlr.press/v54/mcmahan17a.html

[2] T. Li, A. Agarwal, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," in *MLSys*, 2020. [Online]. Available: https://proceedings.mlsys.org/paper_files/paper/2020/hash/1f5fe83998a09396ebe6477d9475ba0c-Abstract.html

[3] S. Kaissis, M. Makowski, A. Rückert, and R. Braren, "End-to-end privacy preserving deep learning on medical data," *Nature Machine Intelligence*, 2020. [Online]. Available: https://www.nature.com/articles/s42256-020-0187-6

[4] T. Brisimi, T. Chen, T. Mela, G. Olshevsky, and I. Paschalidis, "Federated learning of electronic health records," *IEEE Journal of Biomedical and Health Informatics*, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8265286

[5] R. Yang, Z. Liu, and T. Chen, "Federated learning for financial applications," *Expert Systems with Applications*, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S095741742030881X

[6] S. Wang, Z. S. Wu, and H. Wu, "Tackling system and statistical heterogeneity in federated learning with adaptive optimization," in *NeurIPS*, 2020. [Online]. Available: https://proceedings.neurips.cc/paper/2020/hash/9e8d6b4c799f07a3d1a1529bb6c03e56-Abstract.html

[7] D. T. Nguyen, K. Nguyen, and T. Tran, "pfedme: Personalizing federated learning with moreau envelopes," *IEEE Transactions on Neural Networks*, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9675343

[8] Y. Huang, X. Zhang, and M. Li, "Personalized federated learning: Techniques and applications," *ACM Computing Surveys*, 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3589071

[9] K. Bonawitz, H. Eichner, and W. Grieskamp, "Towards federated learning at scale: System design," in *SysML*, 2019. [Online]. Available: https://arxiv.org/abs/1902.01046

[10] D. Nguyen, P. Tran, and L. Pham, "Federated intrusion detection systems," *Computers Security*, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820303637

[11] A. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. McMahan, and S. Patel, "Practical secure aggregation for privacy-preserving machine learning," in *CCS*, 2017. [Online]. Available: https://dl.acm.org/doi/10.1145/3133956.3133982

[12] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*, 2006. [Online]. Available: https://link.springer.com/chapter/10.1007/11681878_14

[13] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *STOC*, 2009. [Online]. Available: https://dl.acm.org/doi/10.1145/1536414.1536440

[14] I. Corporation, "Intel software guard extensions (sgx)," Tech. Rep., 2016. [Online]. Available: https://software.intel.com/content/www/us/en/develop/topics/software-guard-extensions.html

[15] X. Fang, L. Zhou, and J. Wang, "Poisoning attacks in federated learning," *IEEE Internet of Things Journal*, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9448492

[16] H. Zhao, Y. Chen, and K. Liu, "Model inversion attacks in federated learning," *IEEE Transactions on Information Forensics and Security*, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9786543