Exploring Federated Learning: The Framework, Applications, Security & Privacy

Ashim Saha, Lubaina Ali, Rudrita Rahman, Md Fahad Monir and Tarem Ahmed
Department of Computer Science and Engineering
Independent University, Bangladesh (IUB)
Dhaka, Bangladesh
Email:{2021278, 2021152, 2021059, fahad.monir, tarem}@iub.edu.bd

***Abstract*—The conventional approach to Machine Learning fails to provide comprehensive data security, leading to the emergence of Federated Learning (FL) as a promising alternative specially for the next generation wireless network. Future network frameworks like NextG or ORAN must facilitate federated learning because it enables collaborative learning without jeopardizing the privacy of sensitive data through centralization. This survey explores the existing literature on FL, with a focus on the core principles and classifications of FL, its potential applications and global model aggregation. Additionally, the paper examines the critical issue of security and privacy in FL and offers insights on future research directions. Through intensive analysis, the paper highlights the significance of FL as a privacy-preserving approach to Machine Learning and discusses its potential to shape the future of data-driven technologies.**

***Index Terms*—Federated Learning (FL), Open Radio Access Network (O-RAN), Fog and Edge Computing, Aggregating Algorithms, Security and Privacy**

I. Introduction

Recently, with the exponential growth of machine learning in various fields, such as security and privacy, Internet of Things (IoT), network optimization, 5G and beyond cellular networks etc., this subdomain of artificial intelligence (AI) is becoming increasingly prominent. Since, machine learning generally follows centralized models based on gathered datasets from participants for recognizing any pattern or intrinsic factors, therefore, centralized servers are less concerned with data privacy of participants. As a way of resolving privacy issues of client's shared datasets, researchers present Federated Learning (FL) with centralized and decentralized approaches along with the combination of data encryption mechanisms. Consequently, the significance of Federated Learning has increased significantly in preserving the security and privacy of local data of participants as compared to the conventional Machine Learning (ML) approaches.

Federated Learning is a category of Distributed Machine Learning that enables multiple devices and participants to share their data in local models rather than a central server, which can reduce communication costs and participant's privacy concerns. Currently, Federated Learning is an emerging sector due to its feasibility and scalability along with trustworthiness of participants or clients. FL can be extremely beneficial as it prevents crucial data from sharing with a centralized server, thus, creates high quality models and more accurate results.

FL is a decentralized technique to train models locally, where numerous devices, including smartphones and IoT devices, collaborate to construct a shared model without transmitting their sensitive data. The data remains decentralized, rather than being centralized on a single server, and only the model updates are aggregated and shared with the central server, guaranteeing data privacy and security. Federated Learning is becoming generally approved, ensuring the robustness and possible progression of several research sectors in the future.

This paper presents a thorough analysis on Federated Learning and how FL has been introduced in exchange of traditional machine learning to resolve data privacy along with core fundamentals of FL architecture. Also, this paper discusses Federated Learnings' most recent developments as a potentially revolutionary technology including Intelligent Transport Systems (ITS), IoT, Differential Privacy, Generative Adversarial Network (GAN), Open RAN (O-RAN) and other sectors. Then, it illustrates potential applications in security and privacy along with intrusion detection, network optimization, threat intelligence, firewall optimization, global model aggregation, Internet of Things (IoT) as well as edge and fog computing. In the following sections, this paper presents the applications and algorithms used in Global Model Aggregation for Federated Learning. Furthermore, an extensive survey on the security and privacy aspects of Federated Learning is provided. In addition to contributing a brief overview of existing research on Federated Learning, this paper identifies potential areas for future research directions, including the application of Federated Learning in fog and edge computing, NextG or 6G networks, and its role in resolving network congestion issues in Open Radio Access Networks (O-RAN) without using centralized data storage policies.

II. Background and Fundamentals of FL

In the current landscape, the significance of Machine Learning has become undeniable due to the progression in several sectors to train datasets without using any explicit program. Machine Learning (ML) is basically a sub classification of Artificial Intelligence (AI) that allows data analysts to train central models based on collected datasets for predicting human behaviors or extracting any sort of pattern. Several centralized approaches of ML like unsupervised learning, first collect data from various participants and then these datasets are being centrally aggregated by the central model using clustering techniques. Then, datasets are being trained with the help of AI for pattern recognition or finding intrinsic structures. As some participants are reluctant to share their sensitive data with a central server due to concerns about privacy where others such as hospitals, schools and supermarkets data are also preserved for finding behavioral patterns, for this reason, centralized ML approaches have security and privacy issues.

To generate models of high quality and integrate privacy preserving mechanisms in ML, researchers have introduced Federated Learning. Federated Learning is a subfield of Distributed Machine Learning which is more efficient than traditional centralized machine learning models since it performs local training on devices rather than a central server and FL can reduce communication costs and latency while ensuring trustworthiness of participants or clients. Overall, Federated Learning offers several advantages over traditional models concerning efficiency, scalability, and privacy. Since, Federated Learning is a sub field of Distributed Machine Learning, which is a branch of Artificial Intelligence (AI), therefore, the figure 1 represents the hierarchy of Artificial Intelligence, Distributed Machine Learning and Federated Learning.

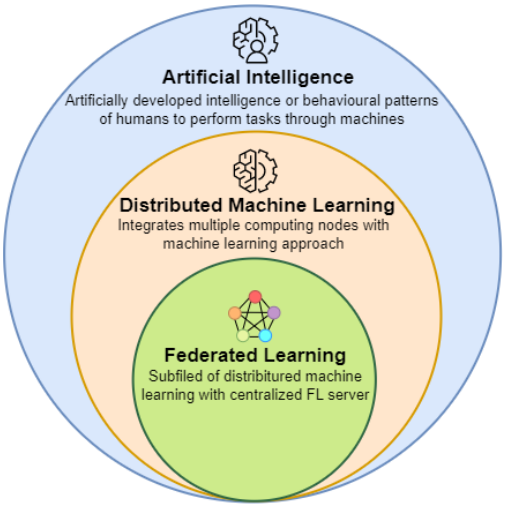

Fig. 1. Hierarchy of Artificial Intelligence, Distributed ML and FL

Federated Learning (FL) is established based on some core principles. These fundamentals are listed below:

1) Participants: Participants or clients are the users that provide data to the local models in Federated Learning infrastructure. These participants can be devices like smartphones, laptops, desktops, IoT based devices or people. In FL architecture, participants are extremely important because without clients, it is impossible to collect infos for training models.

2) Local Data: In FL, every participant has its own dataset and FL prevents crucial data for sharing with a centralized server for ensuring security and privacy. For instance, a hospital's info is never shared with other participants. Local data plays a major role for training models since more local data will be provided to local models, the machine performance will enhance more.

3) Local Models: Locals models are initialized by the central server and then distributed to each client to contribute their local data. In this segment, FL architecture basically collects local data from participants and then preserves data to train local models based on various machine learning algorithms, for instance, Stochastic Gradient Descent (SGD).

4) Global Model Aggregation: After termination of training local models, these model updates are sent to the global model or central server of FL. Then the central server aggregates local model updates from all participants using several global model aggregation algorithms like FedAvg, SecAgg etc and encryption policies are attached to secure data privacy. Then the aggregated model is sent back to each participant for checking all updates.

5) Recursive Approach: The entire process of local data collection, local models training and global model aggregation including updates are repeated multiple times until the shared datasets of participants reach a high level of performance.

III. Latest Research and Applications of FL

A. Related Works on Federated Learning

This section focuses on a review and analysis of the most recent research papers. The papers are examined, and their main points and areas of emphasis are summarized and presented.

The emergence of the Industrial Internet of Things (IIoT) collaborated with FL to present the FL transformed manufacturing paradigm including data partitioning, privacy preservation and local model transportation [1]. Another research paper includes the significance of FL in Vehicular IoT for enhancing the capabilities of autonomous driving cars with Intelligent Transport Systems (ITS) [2]. Conversely, integrating both IoT and FL in Information Centric Networking (ICN) enables us to enhance connection capabilities of 6G networks by 10-100 times over 5G networks [3]. Rahman et al. depicts the evolution of FL from centralized to distributed on-site learning, and its potential applications in edge computing and blockchain [4].

Another research paper represents multi-level classification, desirable criteria and future directions of FL in networking systems [5], [6]. Hua et al. proposed a protocol named as MUD-PQFed which can specifically detect malicious participants and imposes fair penalties for such action [7], [8]. Other researchers focus on the privacy and security of FL since participants in FL, upload data in the local models which is being aggregated by the central model. Hence, there remains a high chance of malicious data in local models resulting in breaking down of the central FL server [9], [10].

Liu et al. collaborated privacy-preserving aggregation techniques with FL, including secure multi-party computation, homomorphic encryption and their trade-offs in terms of accuracy and efficiency [11]. Zhang et al. surveyed Hybrid Federated Learning (HFL), on the contrary, Rahman et al. illustrated FL including privacy concerns, communication efficiency, and system architecture [12], [13]. Haftay et al. including other authors added the importance of FL in Edge Computing (EC) for mitigating the consumption of excessive bandwidth and launching an optimized model [14], [15]. Also Ramu et al. proposed an integration of FL with AI based Digital Twin (DT) in critical scenarios and smart governance based applications [16].

In addition, Patel et al. presented an overview of the adoption of Federated Learning for healthcare informatics, including its applications in clinical decision making, disease diagnosis, and patient monitoring [17]. Zhu et al. provided a detailed analysis on non independent and identically distributed (Non-IID) on horizontal and vertical Federated Learning and added the deviations of centralized and Non-IID based FL [18]. Thang et al. replaced classical ML with decentralized FL using blockchain to collect data sets of patients having adversaries with cerebellar ataxia dysfunction using kinematic sensors while ensuring security [19].

B. Exploring Real-World Applications of Federated Learning

Researchers have discovered the applications of Federated Learning (FL) across various domains where decentralized learning was a necessity. Below are some of the key applications of Federated Learning (FL):

1) In Networking Sectors such as Mobile Networks, 5G/6G Networks, Internet of Things (IoT), Edge Computing and Cybersecurity: Federated learning proves to provide a promising technique for inputting user data into machine learning models for networking. Network administrators can train models on user data without sending it to a centralized server by utilizing federated learning. By minimizing the quantity of data that must be transmitted over the network, this technique reduces latency and conserves bandwidth. Mobile devices may collaborate through federated learning to increase the precision of machine learning models while protecting user privacy.

2) In Security(e.g. Intrusion detection, Malware detection, Network optimization, Threat intelligence and Firewall Optimization): FL makes it possible to train models using data from various network nodes without sending the raw data, protecting the security and privacy of that data. By leveraging FL, multiple models can be trained on diverse data sources without requiring centralized data storage, minimizing the risk of data breaches and ensuring compliance with data privacy regulations. FL-based detection and optimization systems can improve the accuracy and effectiveness of network security while preserving data privacy. Consequently, FL is an attractive technique for enhancing network security in a privacy-preserving and distributed manner.

3) Beyond Network and Security: Harnessing the Power of Federated Learning in Healthcare, Finance, Transportation, and More:

a) Healthcare: In federated learning, the local model only needs to share the output of the locally trained data with the global model, rather than the actual data itself. By using Federated Learning in the healthcare Sector, researchers and doctors are training medical models on patient data without compromising patient information and security. This technique allows hospitals and healthcare researchers to work together to develop more accurate models to give patient-specific treatment effectively and efficiently.

b) Finance: It enables financial institutions to collaboratively train models to detect fraudulent activities such as credit card fraud or insider trading, while maintaining the privacy of sensitive customer data. Additionally, credit scoring models can be developed based on distributed customer data without sharing individual financial records. Federated Learning also allows for the collaborative assessment and prediction of risks in financial portfolios without exposing sensitive data.

c) Smart Cities and Transportation: It has revolutionized traffic management, public transportation, and urban planning by enabling privacy-preserving collaboration.

IV. Global Model Aggregation in FL

Global model aggregation is an essential step in Federated Learning that involves integrating locally trained model updates from various devices or clients into a single global model to enhance its performance. Typically, a central server or coordinating entity collects model updates from each device, appropriately weights them, and integrates them to create a new global model. A basic global model aggregation in Federated Learning is portrayed in Figure 2.

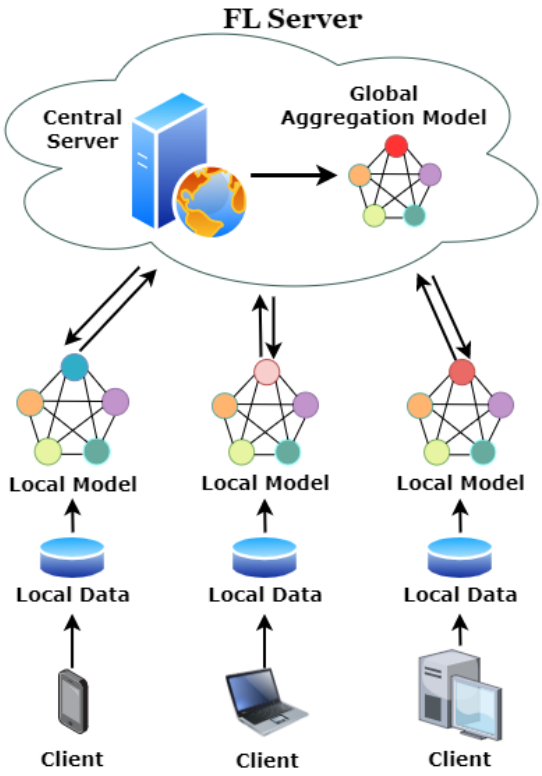

Fig. 2. Global Model Aggregation in FL

This work focuses on aggregation methods that enhance the system's overall performance. Our aim is to offer researchers a quick and detailed understanding of these methods in a single read. Several popular aggregation algorithms have been discussed in this regard. The suggested techniques, derived from current research findings, allow cooperative development of Machine Learning models without compromising data privacy and integrity, as the training data remains on each device and is never made publicly available to a central server. Additionally, it enables efficient use of computing resources, as model training is distributed among multiple devices rather than being centralized on a single server. In Table 1, the existing surveys on Global Model Aggregation algorithms are listed, and the objectives of each work are mentioned. Researchers could find this resource useful in getting a clear understanding of the most recent studies on global model aggregation.

Each device or client trains a local model with its own data, periodically sending updated model parameters to the central server. The central server combines the received models into a single model by weighting or averaging them, which is then provided to the devices or clients for further evaluation. This process is repeated until the model performs satisfactorily.

V. Security and Privacy in FL

The actual purpose of Federated Learning is to avoid direct access to participants' raw data in order to preserve its actual state; therefore, security is essential because sometimes low-quality models contain malicious programs that can easily receive contributions from high-quality global models.

Therefore, security becomes a great issue to preserve raw data from exploitation in Federated Learning. Here, we categorize our approaches into seven sections, and out of these

TABLE I
THE EXISTING SURVEYS ON AGGREGATION ALGORITHM

Aggregation Algorithm Name	***Reference***	***Objective***	***Outcome***
Federated Averaging (FedAvg)	[20]	It involves averaging the model parameters of clients after each round of training.	IID data shows comparison between FedAvg and centralized learning while non-IID data, the centralized method performs better than FedAvg.
Secure aggregation (SecAgg)	[21]	Safeguards client data confidentiality using encryption, allows central server to decrypt and aggregate models.	Significantly decreased communication cost under 1.2 bits/ parameter while preserving test-time performance..
Aggregated Momentum (AggMo)	[22]	Is a technique to accelerate the convergence of the gradient descent algorithm.	AggMo often delivers quicker convergence with little to no adjustment and is a good drop-in replacement for other momentum systems.
Median or Trimmed Mean	[23]	It uses the median or Trimmed mean of the models as the global model.	Deploys a Monte Carlo simulation experiment on a specific decision instance and finds that trimmed mean rank-order aggregation compares effectively with others.
Krum	[24]	It selects a subset of clients at random and computes the mean of the models on that subset.	The outcomes of the experiment support its efficacy. Table 2 reports the backdoor performance of four backdoor attacks using multiple aggregation techniques.
Federated Dropout (FedDrop)	[25]	Prevents over-fitting and improves the generalization of the model.	Reduction of both communication overhead and device computation loads in case of uniform dropout.
Federated BatchNorm (FedBN)	[26]	It uses the batch normalization technique to normalize the inputs of the models before aggregation.	On Office-Caltech10, FedBN significantly improves at least 6% on mean accuracy, FedBN outperforms SingleSet and Quickdraw over 10%.
Federated Distillation	[27]	Wireless implementations of FL, Federated Distillation, Hybrid Federated Distillation approach.	Over-the-air computing implementation of Hybrid Federated Distillation surpasses other techniques accurately.
	[28]	Minimizes communication payload size when compared to FL, especially for large models.	FD with FAug delivers 95-98% test accuracy with less communication overhead by approximately 26x.
Federated Adaptive Aggregation	[29]	For robust Federated Learning, an attack-adaptive aggregation technique is used to protect against different threats.	The method showed competitive performance in protecting against model poisoning and backdoor attacks in federated learning tasks on image and text datasets.
	[30]	This algorithm adapts the aggregation method depending on the characteristics of the data and models.	The Ray-based prototype expands to thousands of participants and achieves $> 90\%$ decrease in resource requirements with minimal effect on aggregation latency.

seven sections, the encryption segment is divided into three subsections: (1) Differential Privacy (DP); (2) Homomorphic Encryption; and (3) Secure Multi-party Computing. The entire Table 2 is classified into seven sections: Data Privacy, Intrusion Detection, Blockchain, IoT including encryption methods with some of the recent workings' objectives and what are the outcomes of conducting these researches.

a) Data Privacy: At present, unauthorized access into systems or firewalls is rapidly increasing at an alarming rate with a view to exploiting personalized data. Since, participants or clients in FL performs a significant role by sharing their data to local servers, hence, eliminating threats and data breaching activities is essential for decentralized Federated Learning. Nguyen et al. discussed methods for resolving data privacy and security by connecting FL with cloud edge intelligent collaborative computing including some challenges to integrate both systems all the while [19].

b) Intrusion Detection: An intrusion detection system basically finds anomalies to protect raw data from being exploited by intruders. Although Federated Learning follows a decentralized approach, at the time of aggregating local model updates to the central server, the central server contains a high possibility of getting attacked by malicious data. Therefore, an intrusion detection mechanism is integrated to FL for detecting anomalies without human intervention. In this sub field of security, combining FL with intrusion detection mechanisms can significantly reduce unauthorized access and data breaches since classical machine learning (ML) doesn't provide advanced security like FL [31].

c) Blockchain Under Decentralized Federated Learning: Blockchain technology follows decentralization and principles of cryptography across a distributed network, including participants. Thang et al. replaced classical ML with decentralized FL using blockchain to collect data sets of patients having adversaries with Cerebellar Ataxia Dysfunction using kinematic sensors while ensuring security [32]. Another related work proposed a security-enabled FL system, namely, Skunk, as well as supporting 5G/6G networks [33].

d) Internet of Thing (IoT): In today's world, IoT has become one of the most important terms integrated with embedded systems, such as motion sensors connected to our appliances or smartphones. Internet of Things and networking both terms are interrelated to identify, monitor and eliminate vulnerabilities from devices that contain high risk of getting exploited by attackers. Other research illustrates the cost and time efficiency of FL with wireless IoT and Stochastic Gradient Descent (SGD) [35], as well as the drawbacks of integrating Raspberry Pi into IoT devices [36].

e) Differential Privacy (DP): Differential Privacy is basically an encryption method that allows participants to

TABLE II
THE EXISTING SURVEYS ON SECURITY AND PRIVACY

Scenario	*Year*	*Reference*	*Objective*	*Outcome*
Data Privacy	2022	[19]	Cloud data privacy using FL	
Intrusion Detection	2021	[31]	Reducing anomaly detection rate	Surpasses FL over classical ML for recognizing intrusion
Blockchain	2022	[32]	Blockchained FL over classical ML with kinematic sensors of CA	Accuracy rate 89.3% with collected dataset of CA participants
	2022	[33]	Zero Trust Security enables FL (Skunk)	IoT based attack detection in 5G/6G sliced situation
	2022	[34]	Blockchain empowered Federated Learning	Better performance for flow detection, identification, attack source tracing
IoT	2020	[35]	FL integrated in wireless IoT and Stochastic Gradient Descent	Reduced energy consumption and finishing time
	2022	[36]	Integrating Raspberry PI Boards in IoT Devices	Could not outperform many traditional approaches
Differential Privacy (DP)	2019	[37]	Bayesian Differential Privacy to FL	Restricting privacy budget
	2020	[38]	Local Differential Privacy and Gaussian MAC	Wireless gradient aggregation scheme contrasting with orthogonal transmission
Homomorphic Encryption (HE)	2020	[39]	Cross-silo federated learning (FL)	BatchCrypt outperforms HE by encoding a batch of quantized gradients
	2021	[40]	Privacy preserving ML framework with partial HE and FL	Usage of Paillier algorithm can make computation faster by 25-28%
Secure Multi Party Computing (SMPC)	1996	[41]	Adaptivity in adverse channels for computing	New encryption protocol based on RSA (Rivest-Shamir-Adleman) assumption

gather data while preserving security and privacy by adding noise for encryption. Various types of noises are added by a synthesizer as an encryption policy. For instance, adding the Bayesian Differential Privacy in FL for minimizing cost in security sectors [37] and local differential privacy in FL using Gaussian multiple access channel (MAC) to create a wireless aggregation scheme [38].

f) Homomorphic Encryption(HE): Homomorphic Encryption works with ciphertext to secure participants' personal information. Homomorphic Encryption is integrated to Federated Learning at the time of aggregating local models and preserves the privacy of client's personal data. Zhang et al. presented a solution for Cross-silo Federated Learning, named BatchCrypt, and aggregating with a local gradient to prevent data loss while collecting data from clients [39]. Another related work is combining ML and FL with Homomorphic Encryption by sharing a new framework, named PFMLP (Paillier Federated Multi-layer Perceptron Algorithm), which is implemented with the Paillier algorithm to maximize speed up to 25–28% [40].

g) Secure Multi-Party Computing: Secure Multi-Party Computing (SMPC) is a potential option for protecting privacy and security in FL, especially when working with sensitive data. By allowing many parties to collaboratively compute a function without disclosing their inputs, SMPC enables secure cooperation between various businesses or people. In Secure Multi-Party Computing, Ran et al. proposed an encryption protocol for working with adverse environments using secure multi-party computing, and the new system is based on the Asymmetric Rivest-Shamir-Adleman (RSA) assumption [41].

VI. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This paper provide an extensive survey on some of the recent advancements of Federated Learning including how FL evolved from the Distributed Machine Learning approach. Then, the paper discusses the core principles of FL followed by local models being aggregated to the central server using various global model aggregation algorithms, for instance, FedAvg, SecAgg, Federated Dropout, Federated BatchNorm etc. Moreover, in this paper explain why data privacy is essential in FL infrastructure and the integration of several security sectors with FL for reducing vulnerabilities. Since unauthorized access and data breaches have frequently been addressed by clients, the optimization of Federated Learning performance and enhancement of data privacy have become concerns. Therefore, Federated Learning in fog and edge computing has its potential to resolve the issues of latency and scalability.

The O-RAN (Open Radio Access Network) is also working to develop a FL based open and intelligent RAN architecture that enables real-time network performance optimization. O-RAN is intended to accomplish network optimization while improving the user experience and 5G networks' effectiveness. Moreover, Network performance and user satisfaction are enhanced when network slicing and Federated Learning are implemented simultaneously because they facilitate the creation of individualized network slices that can be optimized in real-time based on user behavior and network conditions. Furthermore, the combination of Federated Learning and technologies has the potential to significantly operate NextG or 5G networks with more reliability and robustness. In addition, by identifying and fixing possible vulnerabilities in the firewall configuration, firewall optimization contributes to a greater level of network security. This will not only improve network efficiency but also decrease the possibility of cyberattacks, resulting in a more reliable and secure network infrastructure. However, further investigation has to be conducted to outperform shortcomings and challenges at the time of merging Federated Learning.

REFERENCES

[1] J. Zhou et al., "A Survey on Federated Learning and its Applications for Accelerating Industrial Internet of Things," arXiv:2104.10501 [cs], Apr. 2021. [Online]. Available: https://arxiv.org/abs/2104.10501

[2] Z. Du, C. Wu, T. Yoshinaga, K.-L. A. Yau, Y. Ji, and J. Li, "Federated Learning for Vehicular Internet of Things: Recent Advances and Open Issues," IEEE Open Journal of the Computer Society, vol. 1, pp. 45–61, 2020, doi: https://doi.org/10.1109/ojcs.2020.2992630

[3] A. Rahman et al., "On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives," Future Generation Computer Systems, vol. 138, pp. 61–88, Jan. 2023, doi: https://doi.org/10.1016/j.future.2022.08.004

[4] S. Abdulrahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, and M. Guizani, "A Survey on Federated Learning: The Journey From Centralized to Distributed On-Site Learning and Beyond," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5476–5497, Apr. 2021, doi: https://doi.org/10.1109/jiot.2020.3030072

[5] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb, "Federated Machine Learning: Survey, Multi-Level Classification, Desirable Criteria and Future Directions in Communication and Networking Systems," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1342–1397, 2021, doi: https://doi.org/10.1109/comst.2021.3058573

[6] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Access, vol. 8, pp. 140699–140725, 2020, doi: https://doi.org/10.1109/access.2020.3013541

[7] R. Gosselin, L. Vieu, F. Loukil, and A. Benoit, "Privacy and Security in Federated Learning: A Survey," Applied Sciences, vol. 12, no. 19, p. 9901, Oct. 2022, doi: https://doi.org/10.3390/app12199901

[8] H. Ma et al., "MUD-PQFed: Towards Malicious User Detection in Privacy-Preserving Quantized Federated Learning," arXiv:2207.09080 [cs], Jul. 2022. [Online]. Available: https://arxiv.org/abs/2207.09080

[9] K. Zhang, X. Song, C. Zhang, and S. Yu, "Challenges and future directions of secure federated learning: a survey," Frontiers of Computer Science, vol. 16, no. 5, Dec. 2021, doi: https://doi.org/10.1007/s11704-021-0598-z

[10] L. Lyu, H. Yu, and Q. Yang, "Threats to Federated Learning: A Survey," arXiv:2003.02133 [cs, stat], Mar. 2020, Available: https://arxiv.org/abs/2003.02133

[11] Z. Liu, J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, "Privacy-Preserving Aggregation in Federated Learning: A Survey," arXiv:2203.17005 [cs], Jul. 2022. [Online]. Available: https://arxiv.org/abs/2203.17005

[12] X. Zhang, W. Yin, M. Hong, and T. Chen, "Hybrid Federated Learning: Algorithms and Implementation," arXiv:2012.12420 [cs], Feb. 2021. [Online]. Available: https://arxiv.org/abs/2012.12420

[13] K. M. J. Rahman et al., "Challenges, Applications and Design Aspects of Federated Learning: A Survey," IEEE Access, vol. 9, pp. 124682–124700, 2021, doi: https://doi.org/10.1109/access.2021.3111118

[14] H. G. Abreha, M. Hayajneh, and M. A. Serhani, "Federated Learning in Edge Computing: A Systematic Survey," Sensors, vol. 22, no. 2, p. 450, Jan. 2022, doi: https://doi.org/10.3390/s22020450

[15] Y. Li, S. Yang, X. Ren, and C. Zhao, "Asynchronous Federated Learning with Differential Privacy for Edge Intelligence," arXiv:1912.07902 [cs, math, stat], Dec. 2019. [Online]. Available: https://arxiv.org/abs/1912.07902

[16] S. P. Ramu et al., "Federated Learning enabled Digital Twins for smart cities: Concepts, recent advances, and future directions," Sustainable Cities and Society, p. 103663, Jan. 2022, doi: https://doi.org/10.1016/j.scs.2021.103663

[17] V. A. Patel et al., "Adoption of Federated Learning for Healthcare Informatics: Emerging Applications and Future Directions," IEEE Access, vol. 10, pp. 90792–90826, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3201876

[18] H. Zhu, J. Xu, S. Liu, and Y. Jin, "Federated Learning on Non-IID Data: A Survey," arXiv:2106.06843 [cs], Jun. 2021. Available: https://arxiv.org/abs/2106.06843v1

[19] T. Ngo, D. C. Nguyen, P. N. Pathirana, L. A. Corben, M. Horne, and D. J. Szmulewicz, "Blockchained Federated Learning for Privacy and Security Preservation: Practical Example of Diagnosing Cerebellar Ataxia," IEEE Xplore, Jul. 01, 2022. https://ieeexplore.ieee.org/document/9871371

[20] A. Nilsson, S. Smith, G. Ulm, E. Gustavsson, and M. Jirstrand, "A Performance Evaluation of Federated Learning Algorithms," Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning, Dec. 2018, doi: https://doi.org/10.1145/3286490.3286559

[21] W.-N. Chen, C. A. Choquette-Choo, P. Kairouz, and A. T. Suresh, "The Fundamental Price of Secure Aggregation in Differentially Private Federated Learning," arXiv:2203.03761 [cs, stat], Mar. 2022. [Online]. Available: https://arxiv.org/abs/2203.03761

[22] J. Lucas, S. Sun, R. Zemel, and R. Grosse, "Aggregated Momentum: Stability Through Passive Damping," arXiv:1804.00325 [cs, math, stat], May 2019. [Online]. Available: https://arxiv.org/abs/1804.00325

[23] W. J. Hurley and D. U. Lior, "Combining expert judgment: On the performance of trimmed mean vote aggregation procedures in the presence of strategic voting," European Journal of Operational Research, vol. 140, no. 1, pp. 142–147, Jul. 2002, doi: https://doi.org/10.1016/s0377-2217(01)00226-0

[24] Z. Zhang, Q. Su, and X. Sun, "Dim-Krum: Backdoor-Resistant Federated Learning for NLP with Dimension-wise Krum-Based Aggregation," arXiv:2210.06894 [cs], Oct. 2022. [Online]. Available: https://arxiv.org/abs/2210.06894

[25] D. Wen, K.-J. Jeon, and K. Huang, "Federated Dropout—A Simple Approach for Enabling Federated Learning on Resource Constrained Devices," IEEE Wireless Communications Letters, vol. 11, no. 5, pp. 923–927, May 2022, doi: https://doi.org/10.1109/lwc.2022.3149783

[26] X. Li, M. Jiang, X. Zhang, M. Kamp, and Q. Dou, "FedBN: Federated Learning on Non-IID Features via Local Batch Normalization," arXiv:2102.07623 [cs], May 2021. [Online]. Available: https://arxiv.org/abs/2102.07623

[27] J.-H. Ahn, O. Simeone, and J. Kang, "Wireless Federated Distillation for Distributed Edge Learning with Heterogeneous Data," IEEE Xplore, Sep. 01, 2019. https://ieeexplore.ieee.org/abstract/document/8904164

[28] E. Jeong, S. Oh, H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Communication-Efficient On-Device Machine Learning: Federated Distillation and Augmentation under Non-IID Private Data," arXiv:1811.11479 [cs, stat], Nov. 2018. [Online]. Available: https://arxiv.org/abs/1811.11479

[29] C. P. Wan and Q. Chen, "Robust Federated Learning with Attack-Adaptive Aggregation," arXiv:2102.05257 [cs], Aug. 2021. [Online]. Available: https://arxiv.org/abs/2102.05257

[30] K. R. Jayaram, V. Muthusamy, G. Thomas, A. Verma, and M. Purcell, "Adaptive Aggregation For Federated Learning," arXiv:2203.12163 [cs], Nov. 2022. [Online]. Available: https://arxiv.org/abs/2203.12163

[31] G. Bao and P. Guo, "Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges," Journal of Cloud Computing, vol. 11, no. 1, Dec. 2022, doi: https://doi.org/10.1186/s13677-022-00377-4

[32] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated Learning-based Anomaly Detection for IoT Security Attacks," IEEE Internet of Things Journal, pp. 1–1, 2021, doi: https://doi.org/10.1109/jiot.2021.3077803

[33] E. Bandara, X. Liang, S. Shetty, R. Mukkamala, A. Rahman, and N. W. Keong, "Skunk — A Blockchain and Zero Trust Security Enabled Federated Learning Platform for 5G/6G Network Slicing," IEEE Xplore, Sep. 01, 2022. https://ieeexplore.ieee.org/document/9918536

[34] K. Li, H. Zhou, Z. Tu, F. Liu, and H. Zhang, "Blockchain Empowered Federated Learning for Distributed Network Security Behaviour Knowledge Base in 6G," Security and Communication Networks, vol. 2022, pp. 1–11, Apr. 2022, doi: https://doi.org/10.1155/2022/4233238

[35] V.-D. Nguyen, S. K. Sharma, T. X. Vu, S. Chatzinotas, and B. Ottersten, "Efficient Federated Learning Algorithm for Resource Allocation in Wireless IoT Networks," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3394–3409, Mar. 2021, doi: https://doi.org/10.1109/jiot.2020.3022534

[36] P. García Santaclara, A. Fernández Vilas, and R. P. Díaz Redondo, "Prototype of deployment of Federated Learning with IoT devices," Proceedings of the 19th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks on 19th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, Oct. 2022, doi: https://doi.org/10.1145/3551663.3558681

[37] A. Triastcyn and B. Faltings, "Federated Learning with Bayesian Differential Privacy," 2019 IEEE International Conference on Big Data (Big Data), pp. 2587–2596, Dec. 2019, doi: https://doi.org/10.1109/BigData47090.2019.9005465

[38] M. Seif, R. Tandon, and M. Li, "Wireless Federated Learning with Local Differential Privacy," arXiv:2002.05151 [cs, math], Feb. 2020. [Online]. Available: https://arxiv.org/abs/2002.05151

[39] C. Zhang et al., "BatchCrypt: Efficient Homomorphic Encryption for Cross-Silo Federated Learning BatchCrypt: Efficient Homomorphic Encryption for Cross-Silo Federated Learning," 2020. Available: https://www.usenix.org/system/files/atc20-zhang-chengliang.pdf

[40] H. Fang and Q. Qian, "Privacy Preserving Machine Learning with Homomorphic Encryption and Federated Learning," Future Internet, vol. 13, no. 4, p. 94, Apr. 2021, doi: https://doi.org/10.3390/fi13040094

[41] R. Canetti, U. Feige, O. Goldreich, and M. Naor, "Adaptively secure multi-party computation," Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96, 1996, doi: https://doi.org/10.1145/237814.238015