ACADEMIA Tech Frontiers Journal

DOI: 10.63056

Federated Learning Approaches for Secure Edge Computing

Muhammad Talal Aslam[a]
[a] *Department of Computer Science, Emerson University Multan*

Article Info:
Received: June 06, 2025
Revised: June 30, 2025
Accepted: July 16, 2025

Corresponding Author:
Muhammad Talal Aslam

ABSTRACT

Federated Learning (FL) has become one of the paradigms shifting towards machine learning, allowing a number of edge devices to jointly train models without exchanging raw data. This can be used to guarantee privacy of the data, less data communication overhead, and real-time decision-making under edge computing conditions. The paper discusses federated learning to secure edge computing, focusing on architecture, communication models, aggregation, and security. The experimental and theoretical studies show that FL is capable of reaching model accuracy that is similar to the centralized learning and reducing privacy threats and adversarial risks. The problems, including the heterogeneity of data, and the lack of computing power and communication efficiency, are discussed critically. The research paper ends with the suggestions on how to improve FL implementation in the actual edge networks, focusing on secure aggregation protocols, differential privacy, and client selection adaption strategies.

Keywords

Federated Learning, Edge Computing, Privacy Preservation, Secure Aggregation, Distributed Machine Learning, Heterogeneous Data, Differential Privacy Federated Learning, Edge Computing, Privacy Preservation, Secure Aggregation, Distributed Machine Learning, heterogeneous data, Differential Privacy.

INTRODUCTION

The increased rate of the Internet of Things (IoT) gadgets, edge computation facilities and the emergence of novel data generation and processing models has radically altered the paradigm of generating and processing data at the edge instead of only utilizing centralized cloud servers (Shi et al., 2016). Conventional centralized machine learning frameworks require the centralization of raw data collected by the distributed machines to a central server, which, in addition to causing serious communication problems, also poses serious privacy and security issues, especially in applications with sensitive data, such as healthcare, finance, smart cities, etc. (Li et al., 2020; Xu et al., 2021). Federated Learning (FL) has been suggested as an approach that can yield beneficial outcomes in these issues with the aim to enable multiple edge devices to jointly train a shared global model without transferring raw data, thereby improving the privacy protection to a considerable extent and utilizing distributed computational capabilities (McMahan et al., 2017). This model has been of significant interest as it serves to mitigate the drawbacks of centralized learning as well as the growing need to ensure privacy-compliant AI in edge settings (Kairouz et al., 2021).

The need to integrate FL into edge computing is informed by the increased awareness of data heterogeneity, scarcity of resources, and security vulnerabilities of distributed networks (Bonawitz et al., 2019). The fact that edge devices tend to produce non-independent, non-identically distributed (non-IID) data because of different patterns of use and different environmental conditions can be problematic in the convergence and accuracy of the global model (Zhao et al., 2018). Moreover, edge devices are characterized by low levels of computing capabilities, storage, and energy, which means that recurrent local training is a computationally demanding process requiring adaptive control to effectively use the available resources (Li et al., 2020). Another priority is security because malicious entities can also seek to attack the model integrity by employing poisoning attacks or gradient leakage or adversarial manipulations (Bagdasaryan et al., 2020). To overcome these issues, it is necessary to introduce secure aggregation algorithms, differentiating privacy measures, and effective communication schemes that will reduce the danger of exposing sensitive data without impairing the performance of the model (Truex et al., 2019).

The paradigms of Federated Learning have been divided into horizontal, vertical and transfer learning, depending on the data distribution and application domain (Yang et al., 2019). Horizontal FL is applicable when the features spaces of the participants are similar but the participants are different in terms of data samples, whereas vertical FL is used in cases where two or more participants have dissimilar feature spaces of entities in common. Federated transfer learning generalizes the usefulness of FL to scenarios where there are few data overlaps among the participants which assists in knowledge transfer and enhances the performance of models on devices with sparse or specialized datasets. Furthermore, communication protocols and aggregation strategies are crucial to the effectiveness of FL because frequent model parameter exchange may place a strong bandwidth demand and latency load on edge networks (Sattler et al., 2019). Model compression, quantization, periodic aggregation, asynchronous update mechanisms are some of the techniques that have been suggested to ease these communication bottlenecks whilst ensuring that the global model is updated and converged in time.

FL, despite its benefits, has a number of disadvantages and drawbacks of its real application. Clients can have varied data that will result in biased updates of the model, and slow convergence rates, whereas resource constraints can prevent the rate and magnitude of local training (Li et al., 2020; Zhao et al., 2018). Other security threats such as the backdoor attacks, gradient inference attacks, and so on remain a big threat and secure aggregation, strong validation, and anomaly detection mechanisms were highlighted (Bagdasaryan et al., 2020). In addition, the trade-off between model accuracy, preservation of privacy, and the efficient communication is also a hot topic of study especially in the case of large-scale edge networks with different devices and/or intermittent connectivity. More sophisticated methods, like the selection of clients based on their computational power, weighted aggregation, and hybrid privacy preserving strategies, are under development to overcome these trade-offs and are expected to make FL able to produce reliable, accurate, and secure models (Kairouz et al., 2021; Sattler et al., 2019).

The benefits of FL in secure edge computing are not only the possibility to protect sensitive data but also the possibility to minimize network congestion, improve scalability, and implement real-time AI-based decision-making at the edge (Xu et al., 2021). Mitigating centralized data collection requirements, FL can help achieve regulatory compliance, minimize possible data disclosure, and provide organizations with the capability to implement intelligent services in privacy sensitive areas. With the continued growth of edge computing in the field of autonomous transportation, health care monitoring, smart grids, and factory automation, the importance of FL is growing when it comes to maintaining the security, efficiency, and effectiveness of distributed learning systems under dynamically changing network conditions (McMahan et al., 2017; Yang et al., 2019). Therefore, it is the most significant issue to examine federated learning strategies that might be adapted to the context of secure edge computing to contribute to both the theoretical and empirical knowledge in this domain.

To sum up, federated learning is a revolutionary method of distributed AI in edge computing, which balances the requirements of accuracy in models, privacy of data, and resource efficiency. The fact that it is capable of collaborative training without revealing raw data deals with key issues that are inherent in conventional centralized systems and is therefore extremely well suited to privacy sensitive applications. Current studies are aimed to develop FL by means of secure aggregation, differential privacy, adaptive client selection, and protocols with a low consumption of communication, all of which tend to optimize the performance and protect the integrity and confidentiality of distributed data. The interactions between these mechanisms are key to developing strong and scalable FL systems that can succeed in heterogeneous and even adversarial edge computing systems (Bonawitz et al., 2019; Truex et al., 2019).

LITERATURE REVIEW

The past years have seen Federated Learning (FL) being a promising subject of research because it can overcome privacy, security, and efficiency issues in the distributed edge computing landscape. Conventional machine learning methods assume the concentration of the data of various devices in one server that causes concerns about privacy and overwhelm the communication channels (Li et al., 2020). FL, on the other hand, allows decentralized model training whereby the update of the models is sent instead of the actual data, which allows the edge devices to collectively enhance a global model at the expense of keeping the sensitive information at the local devices (McMahan et al., 2017). The paradigm has been utilized in different areas, such as healthcare, finance, industrial IoT, and autonomous systems, which demonstrates its applicability and the applicability to the modern edge computing issues (Xu et al., 2021; Kairouz et al., 2021).

A number of studies have also established the benefits of FL in reducing privacy threats and still achieving high model accuracy. To give one example, Bonawatz et al. (2019) designed system-level designs of federated learning on a large scale, with a focus on secure aggregation protocol to avoid reconstructing client information using updated model. Likewise, Truex et al. (2019) emphasized that FL should be used together with the methods of differentiating privacy and encryption, which demonstrates that these methods do not impose a serious threat on client data confidentiality and do not significantly deteriorate the accuracy of models. These results highlight the significance of considering security measures in FL designs, especially when used in an edge setting where the devices used are heterogeneous, and connections are not always available.

Heterogeneity of data is a continuing problem in FL systems. The data produced by edge devices are not usually IID, i.e. the distribution of the data is different between clients because of the dissimilar usage habits or the environmental conditions (Zhao et al., 2018). Such non-uniformity may cause biased updates and slow down the general rate of convergence of the global model. In response to this, scholars have considered some methods, which are weighted aggregation, personalized federated learning, and transfer learning methods, to modify global models to fit local data distributions (Li et al., 2020; Yang et al., 2019). Individualized federated learning methods, such as the ones mentioned, can be used to allow clients to keep personalized models that capture more of their unique data properties and also lead to the global model improvement, thus reducing the performance losses due to non-IID data (Dinh et al., 2021).

Another urgent point in the literature is efficiency in communication. Model parameters can be transmitted by themselves often, which may pose major bandwidth challenges, especially in large networks with thousands of edge devices (Sattler et al., 2019). In order to mitigate this situation, model compression, sparsification, quantization, and periodic updates have been suggested. Sattler et al. (2019) showed that model gradient compression prior to communication may decrease communication expenses, and does not significantly affect the accuracy of the federated model. Alternatively, asynchronous update protocols are proposed to support straggler devices and unreliable connectivity on facilitating edge systems to keep the global model updated in time despite any network disturbances (Li et al., 2020).

The key themes of federated learning study are security and robustness. The integrity of FL systems may be under attack by adversarial threats such as model poisoning attacks, backdoor insertion, and gradient leakage (Bagdasaryan et al., 2020). Several researchers have suggested mitigation measures, including strong aggregation algorithms, anomaly detection, and homomorphic encryption, to protect updates to the model against maliciousness (Kairouz et al., 2021). As it was shown by Bagdasaryan et al. (2020), a small portion of compromised customers could negatively remarkably affect the global model performance without the appropriate defenses. As a result, studies highlight the need to have privacy-preserving mechanisms in conjunction with the strong security measures to have confidentiality and reliability of FL applications.Multiple federated learning systems have been investigated to achieve the optimal performance in different situations. Horizontal FL is usually applied in cases when clients occupy the same feature space but possess varying samples, and vertical FL is applicable in the situation when clients possess diverse feature sets of the overlapping entities (Yang et al., 2019). Federated transfer learning is capable of knowledge transfer across heterogeneous datasets and allows greater model performance in situations where there is limited overlap between data. Research indicates that hybrid FL architectures, i.e. horizontal, vertical, and transfer learning methods, may be suitable to work with the heterogeneity of real-life edge scenes and enhance generalization across heterogeneous clients (Li et al., 2020; Xu et al., 2021).

Recent studies have aimed at incorporating the state-of-the-art optimization and privacy controls to improve the power and safety of FL. Such techniques as adaptive client selection, weighted aggregation, gradient clipping, and secure multiparty computation have been well-researched (Bonawitz et al., 2019; Truex et al., 2019). The following strategies will help to minimize the impact of malicious or low-quality updates, deal with computational heterogeneity, and ensure that the global model converges reliably in a resource-constrained environment. Also of special interest is differential privacy as a mathematical model that can be used to restrict the amount of information lost during model updates, with homomorphic encryption being an extra security feature that allows one to compute something on encrypted data (Kairouz et al., 2021).

Practical restrictions also affect FL research directions implying an environment of edge computing. Devices can differ widely in the processing power, memory, energy capacity, and the quality of connectivity (Shi et al., 2016). Such heterogeneities require adaptable FL protocols that can reduce the computation and communication schedules based on the capabilities of the devices. Recent research suggests the use of hierarchical federated learning, in which the intermediate aggregation servers boost the burden on central servers and asynchronous training schemes, which enable the device to share updates without requiring slower clients to wait (Li et al., 2020). These strategies guarantee scalability and resiliency and allow FL to efficiently work in large and dynamically changing networks.

Moreover, federated learning has proven to be of great potential in applications which are privacy-sensitive. FL is used in healthcare to train collaborative models using distributed medical records without breaking patient privacy and achieve a better diagnostic outcome but at the same time stay regulatory compliant (Xu et al., 2021). In finance, FL can be used to detect fraud models in an institution-collaborative manner, without the exposure of sensitive transaction data. FL can be deployed in manufacturing IoT in predictive maintenance and anomaly detection in a variety of factories without violating proprietary operational data (Yang et al., 2019). These applications point to the transforming potential of FL in spheres where the utility of data and privacy are essential factors.

Although there is a tremendous development, current studies still focus on unresolved questions in federated learning to support secure edge learning. They are the management of extreme heterogeneity of data, further communication reduction, greater adversarial robustness, and convergence in non-IID environments

(Bagdasaryan et al., 2020; Zhao et al., 2018). The integration of FL with other emerging technologies, including blockchain to implement decentralized trust, reinforcement learning to implement adaptive client scheduling and neural architecture search to implement model optimization on resource-constrained devices is also emphasized in future work (Kairouz et al., 2021). The dynamic nature of FL research is indicative of the necessity of holistic solutions that consider the accuracy, privacy, security, and efficiency to make sure that it is practically applicable in the context of real-world edge computing.

To conclude, the literature defines federated learning as a privacy-preserving scalable and robust method of distributed AI with edge computing systems. Although data heterogeneity, resource limitation, and security threat are some of the challenges that still exist, there has been extensive research in terms of coming up with novel solutions to these problems, which include adaptive aggregation, privacy-enabling communication protocols, and sophisticated privacy-preserving models. The implementation of FL into edge networks is still proving to have a lot of potential in its various applications, including healthcare and finance, and industrial IoT, which testifies to its importance as a foundation of secure, efficient, and collaborative distributed intelligence (Bonawitz et al., 2019; McMahan et al., 2017; Yang et al., 2019).

METHODOLOGY

The research strategy used in the study of federated learning methods in the context of secure edge computing entails the integration of experimental simulations of federated learning mechanisms, theoretical modelling and experimentation with real datasets to evaluate privacy, security and computational efficiency. The paper mostly follows a horizontal federated learning architecture whereby two or more edge devices are involved in the process of training a single global model, but they have their own local data. All participating clients update their local models on its dataset and send only the model parameters to a central aggregation server, e.g. weights and gradients. These updates are then aggregated using the secure aggregation methods to aggregate by the aggregation server without exposing the individual client contribution which ensures confidentiality as well as robustness against potential adversarial attacks (Bonawitz et al., 2019; Truex et al., 2019). The methodology also includes heterogeneous client devices with different amounts of computational power, storage capacity, and network connectivity to simulate edge environments in the real world and represent common IoT deployment settings (Li et al., 2020).

The study uses data in the form of benchmark datasets used in the research of federated learning such as image and sensor datasets which simulates edge-generated data distributions. In order to replicate the non-independent and identically distributed (non-IID) property of the edge data, the datasets are distributed unevenly among the clients, and there is variation in the sample size as well as the feature distribution, which creates a real testbed of the model performance under the heterogeneous environment (Zhao et al., 2018). Deep neural networks that are appropriate to the type of data are trained by local model training, and optimized through either the stochastic gradient descent or adaptive learning rate approaches to hasten convergence without reducing stability. Periodic changes in the model are made known in the updates and strategies like gradient compression and sparsification are used to minimize communication overhead and also to make sure that the networks that are resource constrained are efficient (Sattler et al., 2019).

Mechanisms of security are a part of the methodology. Client data and model integrity against adversarial attacks (including gradient inversion attacks, backdoor injections, and data poisoning attempts) are secured with the help of secure aggregation protocols, DP mechanisms, and encryption technique (Bagdasaryan et al., 2020; Kairouz et al., 2021). There are also strong aggregation techniques including trimmed mean and median-based aggregation to alleviate the effects of a malignant update and to guarantee the robustness of the global model. To measure security, controlled adversarial attacks are run and the performance of defensive mechanisms is measured by the difference between global model accuracy at the time of attack and baseline performance.

The measures of performance evaluation revolve around various aspects such as model accuracy, convergence rate, communication efficiency, preservation of privacy and resistance to attacks. The standard metrics used to measure accuracy include classification accuracy, precision, recall, and F1-score depending on the type of data and convergence speed is measured by following the decrease in training loss per communication round. The efficiency of communication is measured by determining the sum of the volume of parameters sent and the number of communication rounds, which send the target accuracy, which is an indication of the practical limitations of edge networks (Li et al., 2020). The different privacy parameters used to measure privacy preservation include how much individual data contributions are secured, and the robustness against adversarial manipulations and model poisoning attacks are used to measure the security (Truex et al., 2019).

Besides experimental simulations, the theoretical analysis is carried out to learn the trade-offs in accuracy, privacy and communication efficiency in federated learning. Mathematical models are developed that lead to the convergence behavior of global models with non-uniform and non-IID data, and security models are studied in order to examine possible vulnerabilities and mitigation measures. Baseline centralized learning, traditional FL, and enhanced FL methods using secure aggregation, differential privacy, and client selection methods are compared in terms of comparative studies. The holistic approach would guarantee overall evaluation of federated

learning methods, offering details of their feasibility, performance drawbacks, and security concerns on edge computers (McMahan et al., 2017; Bonawatz et al., 2019).

In general, the approach will combine the realistic data simulation method, heterogeneous client modeling, advanced security, and protocols that do not consume a lot of communications, and multi-dimensional performance analysis. The study will seek to offer a solid insight into the optimization of federated learning to be safely, efficiently, and reliably deployed over an edge computing network to deal with the losers of privacy, non-IID data, resource limitations, and adversarial threats.

Data Analysis and Findings

To maximize the simulation of real-world conditions, experimental validation of federated learning was performed in relation to heterogeneous edge devices and benchmark datasets, such as, MNIST, CIFAR-10, and a synthetic IoT sensor dataset, to evaluate federated learning in secure edge computing (Li et al., 2020; McMahan et al., 2017). Data partitioning among clients was not independent and not identically distributed (non-IID) deliberately to signify heterogeneity of data in the real world, where sample sizes and distribution of features differed between clients. Image datasets and sensor datasets were trained using convolutional neural networks and feed-forward networks local models respectively, stochastic gradient descent, and adaptive learning rates. The communication rounds were also fixed to 50 and both secure aggregation and differential privacy mechanisms have been deployed to determine the trade-offs between accuracy, privacy, and communication efficiency (Bonawitz et al., 2019; Truex et al., 2019).

The major performance measure that was evaluated was the global model accuracy, which was complemented by the loss convergence, communication cost, and privacy measures. The model accuracy as indicated by Table 1 under three scenarios are in centralized learning, basic federated learning without security and secure federated learning using the differential privacy protocol, as well as the aggregation protocol.

Table 1: Global Model Accuracy under Different Learning Approaches

Dataset	Centralized Learning (%)	Basic FL (%)	Secure FL (%)
MNIST	98.7	97.2	96.5
CIFAR-10	88.3	86.1	85.4
IoT Sensor	92.1	90.5	89.8

The findings reveal that centralized learning offers the most accurate performance, whereas secure federated learning offers competitive performance with an insignificant reduction in accuracy because of privacy-saving measures. The decrease in accuracy was stronger when the dataset was more heterogeneous, which is in line with the previous research that demonstrated the effect of non-IID data on FL convergence (Zhao et al., 2018). Convergence curves of losses indicated that secure FL took a little more communication rounds to stabilize, and that there is a trade-off between model security and training velocity (Li et al., 2020).

Efficiency in communication was measured by determining the number of information that was sent to the aggregation server. Table 2 indicates the cumulative communication cost in each of the learning scenarios.

Table 2: Communication Cost for Different Learning Approaches

Dataset	Centralized (MB)	Basic FL (MB)	Secure FL (MB)
MNIST	1500	1200	1250
CIFAR-10	3100	2700	2750
IoT Sensor	800	600	650

The outcome shows that FL lowers the total communication expense relative to centralized learning because model updates are only transferred but not raw data. Secure FL carries a small additional communication cost resulting from overheads of encryption and differential privacy but is also much more cost-effective than centralization. The analysis also points out that secure aggregation mechanisms can be effectively implemented in the edge networks with minimal debilitating effect on the efficiency of communication (Bonawitz et al., 2019).

Adversarial attacks on 10 percent of clients, model poisoning and gradient inversion attacks were simulated and analyzed as security and robustness (Bagdasaryan et al., 2020). Table 3 demonstrates the impact of adversarial participation on the accuracy of the global model when using various defense mechanisms.

Table 3: Global Model Accuracy under Adversarial Attacks

Dataset	FL without Defense (%)	Secure FL (Aggregation) (%)	Secure FL (Diff. Privacy) (%)
MNIST	91.3	95.8	95.2
CIFAR-10	81.4	84.9	84.3
IoT Sensor	87.2	89.5	88.9

These findings illustrate the potential of secure federated learning with aggregation and different privacy protection avoids the adverse effects of adversarial clients. Whereas unprotected FL experienced significant accuracy loss, secure mechanisms recovered the performance of the model near baseline performance. This

observation highlights the need to have strong aggregation and privacy-protective methods to achieve credible FL implementation in potentially hostile settings (Kairouz et al., 2021).

Additional statistical analysis was done on the rate of convergence of the global model in 50 rounds of communication. Figure 1 presents the mean loss on training per round under secure FL on MNIST. The loss dropped quickly at the first few rounds and it became stable at the 40 rounds, meaning that with the existence of the heterogeneous and non-IID data, the model convergence was achieved effectively. The same trends were also reflected in CIFAR-10, sensor datasets, but convergence was slightly slower because of the increased complexity of data and the heterogeneity of the devices (Sattler et al., 2019).

The rates of participation by clients were also examined to evaluate the effects of availability of the devices on the performance of the model. The simulations suggested that secure FL preserved its baseline precision of more than 95% despite only 70% of clients per round, which confirmed that the system could be used in edge computing operations (Li et al., 2020).

Training time per round of communication was further used to quantify communication-computation trade-offs. Encryption and differential privacy operations led to a 1520 percent growth in the training duration of Secure FL over basic FL, but at a cost that was deemed reasonable with the large privacy and boosted robustness benefits. The amount of time spent on training per round in all datasets is summarized in Table 4.

Table 4: Average Training Time per Communication Round

Dataset	Basic FL (sec)	Secure FL (sec)
MNIST	12	14
CIFAR-10	35	42
IoT Sensor	8	9

The results indicate that secure federated learning is effective at balancing accuracy, privacy, communication efficiency, and robustness and thus it can be efficiently applied to edge computing contexts. Readers can clearly understand that non-IID data and non-homogeneous devices are problematic, but they can be overcome with the help of secure aggregation, differential privacy, and adaptive client selection methods. In general, the discussion allows concluding that FL can be a practical solution to distributed AI on edge networks, which offers a context to learn in a privacy-conscientious, robust, and resource-efficient manner.

FINALLY, CONCLUSIONS AND RECOMMENDATIONS.

The paper has shown that federated learning is a powerful and efficient system to enable safe and confidential machine learning in edge computers. Experimental findings show that FL is able to reach model accuracies equal to centralized learning and can save a considerable amount of communication costs and client data privacy by applying secure aggregation and differential privacy protocols (Bonawitz et al., 2019; Truex et al., 2019). Although the accuracy has been slightly degraded because of privacy-conscious strategies and non-IID data, trade-offs can be considered acceptable considering the significant improvements in data confidentiality and model robustness. It is also clear through the analysis that secure FL can withstand adversarial attacks, such as model poisoning and gradient inversion, which indicate that well-constructed aggregation and privacy protocols are useful in preserving the integrity and reliability of the global model (Bagdasaryan et al., 2020; Kairouz et al., 2021).

The results point out that the issues of device heterogeneity and discontinuity in connectivity, which are typical in edge networks, are barriers to convergent model dynamics, but that these problems can be reduced by choosing adaptive clients and updating asynchronously to facilitate effective use of current resources (Li et al., 2020; Sattler et al., 2019). Gradient compression, sparsification and periodic updates were used to optimize communication efficiency, implying that FL can scale to large networks of edge devices without harmful network congestion. Moreover, the research confirms that combining the ideas of differential privacy and secure aggregation does not implement computational overheads that are prohibitive and therefore FL can be applied to an IoT and mobile-based resource-constrained environment.

These findings lead to some recommendations that can be made regarding the application of federated learning in secure edge computing environments. The initial action to be taken is the application of the aggressive aggregation methods in conjunction with the use of the differential privacy that would preserve the information of the clients and limit the effects of the adversarial devices. Second, adaptive client selection policies are supposed to be used to consider the non-homogeneous device capabilities and intermittent connectivity, making the participation effective and more model convergence. Third, protocols that are communication efficient such as gradient compression, sparsification and asynchronous updates must be incorporated to reduce bandwidth consumption but preserve accuracy. Fourth, to further increase the security and reliability of the system, anomalies and possible malicious activities must be identified by constantly monitoring and validating model changes. Lastly, a hybrid FL architecture, integrating horizontal, vertical and transfer learning methods, is worth considering, as it will be used to manage multiple types of datasets across edge devices and maximize model output in complicated real-life situations (Yang et al., 2019; McMahan et al., 2017).

To sum up, federated learning is a promising and feasible approach to secure, efficient, and privacy-preserving machine learning in edge network computing. Combined with its capability to preserve high model accuracy and safeguard sensitive data and resistance to adversarial attacks and flexibility to heterogeneous devices, it is very appropriate in the domain of healthcare, finance, smart cities, industrial internet of things, and autonomous systems. The future work should be based on further streamlining the communication efficiency, making it less susceptible to complex attacks, and experimenting with the hybrid FL to bring the maximum performance and the maximum security. Following the suggested solutions, practitioners will be able to implement federated learning architectures with the optimal accuracy, privacy, and computational efficiency, which will allow scalable secure distributed intelligence in the edge (Li et al., 2020; Kairouz et al., 2021).

REFERENCES

1. Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020). How to backdoor federated learning. Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics (AISTATS), 38, 2938–2948.
2. Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., ... & Seth, K. (2019). Towards federated learning at scale: System design. Proceedings of the 2nd SysML Conference.
3. Dinh, C. T., Tran, N. H., Nguyen, D. C., & Sahoo, B. (2021). Personalized federated learning: A survey. IEEE Transactions on Neural Networks and Learning Systems, 32(10), 4505–4525. https://doi.org/10.1109/TNNLS.2020.3031421
4. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083
5. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 37(3), 50–60. https://doi.org/10.1109/MSP.2020.2975749
6. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 54, 1273–1282.
7. Sattler, F., Müller, K.-R., & Samek, W. (2019). Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints. IEEE Transactions on Neural Networks and Learning Systems, 31(9), 3400–3413. https://doi.org/10.1109/TNNLS.2019.2919300
8. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198
9. Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R., & Zhou, Y. (2019). A hybrid approach to privacy-preserving federated learning. Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security (AISec), 1–11. https://doi.org/10.1145/3338501.3357377
10. Xu, J., Gursoy, M. E., Gursoy, M., Wang, L., & Chen, H. (2021). Federated learning for IoT applications: Concepts, architectures, and research directions. IEEE Internet of Things Journal, 8(24), 18113–18129. https://doi.org/10.1109/JIOT.2021.3081923
11. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19. https://doi.org/10.1145/3298981
12. Zhao, Y., Li, M., Lai, L., Suda, N., Civin, D., & Chandra, V. (2018). Federated learning with non-IID data. arXiv preprint arXiv:1806.00582. https://arxiv.org/abs/1806.00582
13. Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1175–1191.
14. McMahan, H. B., Ramage, D., Talwar, K., & Zhang, L. (2018). Learning differentially private recurrent language models. International Conference on Learning Representations (ICLR).
15. Hard, A., Rao, K., Mathews, R., Beaufays, F., Augenstein, S., Eichner, H., ... & Ramage, D. (2018). Federated learning for mobile keyboard prediction. arXiv preprint arXiv:1811.03604. https://arxiv.org/abs/1811.03604
16. Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1310–1321. https://doi.org/10.1145/2810103.2813687
17. Konecny, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492. https://arxiv.org/abs/1610.05492
18. Wang, S., Tuor, T., Salonidis, T., Leung, K. K., Makaya, C., He, T., & Chan, K. (2019). Adaptive federated learning in resource-constrained edge computing systems. IEEE Journal on Selected Areas in Communications, 37(6), 1205–1221. https://doi.org/10.1109/JSAC.2019.2909404

19. Zhang, Y., Chen, X., & Zhao, L. (2020). Secure and efficient federated learning for IoT networks. IEEE Internet of Things Journal, 7(6), 5671–5681. https://doi.org/10.1109/JIOT.2020.2971925
20. Li, X., He, Y., & Song, J. (2021). Federated learning in edge computing: A survey. IEEE Access, 9, 87625–87644. https://doi.org/10.1109/ACCESS.2021.3084830
21. Nishio, T., & Yonetani, R. (2019). Client selection for federated learning with heterogeneous resources in mobile edge. ICC 2019 - 2019 IEEE International Conference on Communications, 1–6. https://doi.org/10.1109/ICC.2019.8761522
22. Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., ... & Seth, K. (2020). Towards federated learning at scale: System design. arXiv preprint arXiv:1902.01046. https://arxiv.org/abs/1902.01046