Peertechz

ENGINEERING GROUP

TRENDS IN Computer Science and Information Technology
OPEN ACCESS JOURNAL

ISSN: 2641-3086 DOI: https://dx.doi.org/10.17352/tcsit

Literature Review

Security and privacy in federated learning: A survey

Dasaradharami Reddy Kandati[1]* and S Anusha[2]

[1]School of Computer Science Engineering & Information Systems , Vellore Institute of Technology, India

[2]Department of Computer Science & Engineering, NBKRIST, Vidyanagar, A.P, India

Received: 28 February, 2023
Accepted: 14 August, 2023
Published: 16 August, 2023

***Corresponding author**: Dasaradharami Reddy Kandati, School of Computer Science Engineering & Information Systems , Vellore Institute of Technology, India, Tel: +91- 8328471226;
E-mail: dasaradharami.k@vit.ac.in

Keywords: Federated learning; Healthcare; Privacy; Security

https://www.peertechzpublications.org

Check for updates

Abstract

Federated Learning (FL) allows multiple nodes without actually sharing data with other confidential nodes to retrain a common model. This is particularly relevant in healthcare applications, where data such as medical records are private and confidential. Although federated learning avoids the exchange of actual data, it still remains possible to fight protection on parameter values revealed in the training process or on a generated Machine Learning (ML) model. This study examines FL's privacy and security concerns and deals with several issues related to privacy protection and safety when developing FL systems. In addition, we have detailed simulation results to illustrate the problems under discussion and potential solutions.

Introduction

Recent technological developments are currently changing the way data is produced and analyzed. During the last few years, the quantity of intelligent devices in the world has increased exponentially with the advent of Internet-of-Things (IoT). Many of these devices are integrated with multiple sensors and increasingly powerful hardware that enable them not only to collect but more importantly, to process data on an enormous scale. In the fields of computational vision, language processing, speech recognition, etc. [1] at the same time, technology has revolutionized how revolutionary data access is obtained. There is also a high demand for the use of wealthy data that is generated by distributed devices to develop ML models.

At the same time, the protection of data has become a growing issue for clients. In particular, the development of centralized publicly accessible data repositories has made leakage of private information, e.g. health conditions, travel, and financial information, an urgent social problem [2]. In addition, the diverse collection of open data applications, such as survey data distribution and social networks focus heavily on privacy issues. Access to real-life datasets can lead to leakage of information even in pure research activities. Privacy has since become a critical issue. In order to implement further models of ML with multiple privacy-preserving methods, it is important to construct frameworks and infrastructural facilities to facilitate the development of different unified learning algorithms [3].

Many ML algorithms are hungry for data, and data is actually spread through various entities in the context of privacy constraints. As a result, FL [4] has become a hot research area in machine learning. Due to strict data security regulations, it is often deemed impractical to store and share consumer data in a single place. This also contradicts standard ML algorithms because they involve a broad variety of data training examples to be understood [5]. The clarification of why traditional ML algorithms have these limitations is the manner in which their models are trained [6,7]. Unified Learning has specific business scenarios, with a number of studies related to FL implementations, for example in the healthcare field [8].

Citation: Kandati DR, Anusha S (2023) Security and privacy in federated learning: A survey. Trends Comput Sci Inf Technol 8(2): 029-037.
DOI: https://dx.doi.org/10.17352/tcsit.000066

Figure 1 depicts an example process in which someone who sees the outcome of privacy-preserving analysis will draw relatively similar assumptions.

However, public healthcare records are typically scattered and confidential, making it impossible to produce reliable outcomes around communities. For example, different clinics have Electronic Health Records (EHRs) with various patient demographics, which are complicated to exchange among hospitals due to their delicate existence [9]. It presents a huge obstacle to successful growth analytical methods that are broadly applicable and include a wide variety of "predictive analytics." Institutions such as clinics can also be considered as remote 'devices' providing a variety of health information for personalized healthcare coverage. Clinics, moreover, work under stringent privacy standards and can face regulatory, logistical, or ethical restrictions requiring data to stay local. FL is a potential tool for such implementations since it can lighten the stress on a system and allow personal communication among different technologies/institutions [10].

Figure 2 depicts an example application in which a model is learned from distributed electronic health data. FL will be implemented in practice by large organizations and plays an important role in promoting privacy-sensitive technologies whose training samples are disseminated at the corner. As per MIT health science associate professor Ramesh Raskar, the contradiction between the privacy of the data and the advantages of using the records in the modern world is inaccurate. A rationale is that we should attain functionality and protection, so privacy and security can be significantly reduced. A hierarchical ML approach for prediction in this environment will allow each independent system to add data to the composite design by exchanging any original data. Such a framework will obtain optimal precision using this considerably reduced computational resources and throughput connectivity just like conventional numerical methods.

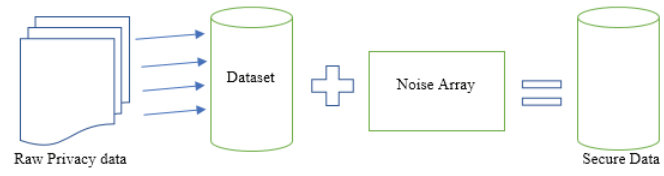

Figure 1: Differential privacy process (google courtesy).

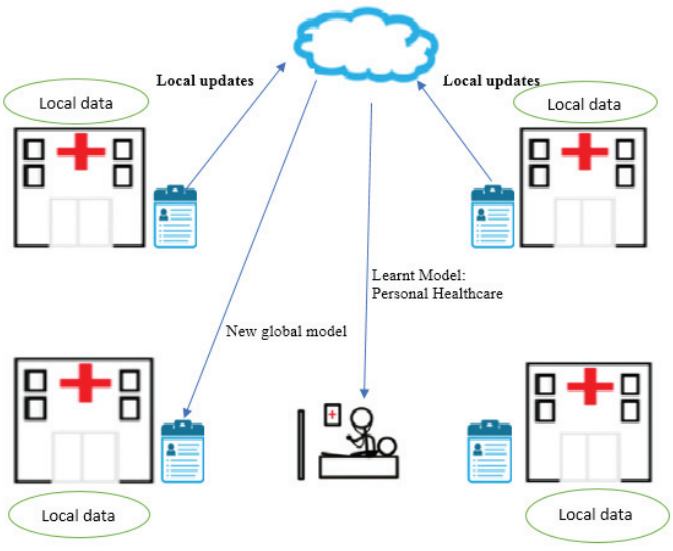

Figure 2: Application of federated learning for personal healthcare (google courtesy).

Collaborative learning would be a new framework for artificial processes that enables several network operators to create a model together without sharing their confidential data with each other. The principle of FL is expanded to include possibilities and creates a comprehensive, protected federated learning method, such as Horizontal Federated Learning (HFL), Vertical Federated Learning (VFL), and Federated Transfer Learning (FTL) [11]. Vertical learning also referred to as property-based learning, can be used in situations when data sets access certain objects and Data fields at which asset properties are distinct. For this learning model, the principles are merged to build a better field for ML. Data encryption is often used to guarantee the protection of records.

Confidentiality has become one of the main features of FL. It often requires authentication methods and assessments that provide worthwhile guarantees of privacy. Throughout this section, they thoroughly analyze and evaluate various privacy strategies for FL and describe methods and possible obstacles to the prevention of apparent exposure. This is hard to build an authentication protocol for Stable Multi-Party Computation under a medium security constraint in return for performance. Authors [12] also implemented a differential approach to privacy in FL in order to maintain the security of client-side data by covering the client's inputs during preparation. In this case, the trustworthy manager consolidates variables configured by several clients in a secured environment. The results obtained were further later spread to all customers and eventually converges to a standard implementation scheme through specifically sharing the details.

Homomorphic Encryption is often used to secure the privacy of customer data by sharing parameters under the encryption technique throughout ML. Usually; a VFL process thinks of genuine-but curious participants, please. In the case of two parties, for example, the two parties are non-compliant, and at best, the competitor is harmed. The security concept is that the opponent could only learn data from the user that is compromised but not data from some other client except what is exposed by input and output.

At the conclusion of the learning process, each party retains only the parameters of the model associated with its own characteristics, and thus, at the time of inference, the two parties still need to work together to produce output. In our understanding, there are only a few solutions to secure the privacy of VFL. But these solutions are not sufficient in terms of either performance or data protection.

Literature review

Wang X, et al. (2019) Authors suggest the integration of Deep Reinforcement Learning techniques and the FL Platform

Citation: Kandati DR, Anusha S (2023) Security and privacy in federated learning: A survey. Trends Comput Sci Inf Technol 8(2): 029-037.
DOI: https://dx.doi.org/10.17352/tcsit.000066

with mobile edge systems to improve mobile edge computing, caching, and communication [1]. Finally, experiments have been conducted to investigate the scenarios of edge caching and computation unloading in a mobile edge device, and the "In-Edge AI" is tested and has been shown to be capable of achieving near-optimal efficiency.

Liu B, et al. (2019) In this paper, authors introduced a mechanism to protect the privacy of images against deep learning tools, along with two new steps to measure the privacy of images. In addition, they suggest two separate schemes for the protection of privacy based on two metrics, using the adversarial example idea [2]. The output of our solution is validated by simulation on two separate datasets. Our analysis demonstrates that we can protect the privacy of the image by adding a small amount of noise that has a humanly unmeasurable effect on the quality of the image, particularly for images of complex structures and textures.

Li Q, et al.(2019) Authors focus on providing complexity reduction against FLSs on six different aspects, including the distribution of data, the machine learning model, the privacy mechanism, the communication architecture, the size of the federation, and the motivation of the federation, which may be common building blocks and system abstractions of FLSs [3]. Current traditional and state-of-the-art experiments are summarized by their contexts, which is useful for users and professionals to refer to. They describe the design considerations for the effective FLS and evaluate the solutions for each case in a detailed manner. The authors suggest fascinating research avenues and opportunities for future iterations of FLS.

Shi E, et al. (2017) Authors first demonstrate a lower bound, that is, under information-theoretical differential privacy; any multi-party protocol with a minimal number of messages must have a significant additive error. Developers then show that by adopting a definition of computational differential privacy, this lower bound can be manipulated and functional protocols designed for the periodic distributed summation problem [4]. One's designs guarantee the privacy of honest individuals, even if a portion of the stakeholders may be compromised and cooperated. In addition, designers suggest a new distributed noise addition mechanism to ensure a minimal total error.

Larson DB, et al. (2020) suggest an ethical policy for the use and exchange of medical information for the development of artificial intelligence (AI) applications [5]. The authors expand this concept to issues related to the indirect use of medical evidence for AI applications. Specifically, they recommend that almost all people and institutions with access to medical records become privacy stewardesses, with trustee obligation on the part of patients to protect patient confidentiality and on the part of the public to ensure that data are made publicly accessible for the advancement of information and resources to support prospective patients. The authors further recommend that patient permission is not needed until records are used for private purposes where securing such permission is extremely expensive or cumbersome, as far as procedures are in effect to guarantee quality commitment to safety principles.

Konečný J, et al. (2016) concluded that implementing an expanding and relatively important environment for distributed optimization in ML, for which data-determining computation is widely spread across an incredibly large number of nodes. The aim is to train a unified, high-quality model [6]. This setting is referred to as Federated Optimization. Communication performance must be of vital importance throughout this environment and reducing the amount of interaction sessions is the key priority. In federated optimization, computers are used as simulated nodes for computing their specific information to modify the linear model. We assume that we do have an incredibly large number of computers on the network as well. Even have a number of subscribers of a given program, each of whom has just a small percentage of data available. In fact, we expect the amount of data points found currently to be far lower than the number of devices available.

Ilias C, et al. (2019) found that ML and, in particular, deep learning are suitable for the solution of various problems in diverse domains. Learning such models, however, requires considerable computing power and visualization of data. FL is a concept that literally addresses these issues since different users make up a global architecture and each of them exercises a model globally with their results [7]. Customers should provide or engage in the data or storage capacity needed solely for the purpose of training their models. Public key cryptographic techniques are used to allow the training process on encrypted data. Cryptographic algorithms are used as payment systems to manage workflows and agreements made by all involved parties while, at the same time, token transfers by nodes offer the requisite benefits for participants to engage in the system and to behave reasonably.

Xu J, et al. (2019) In this paper, they examine the recent success of FL, including even if not limited to the world of healthcare [8]. Users are summarizing the general solutions to the various problems in federated learning and aim to get a more valuable platform for investigators to identify. Consequently, healthcare records are typically scattered and confidential, making it impossible to produce robust outcomes across communities. For example, different clinics have electronic health records (EHRs) with various patient groups but these records are complicated to exchange across health clinics to their fragile existence. This poses a significant obstacle to designing successful methodological methods that are generalizable and include a wide variety of "big data."

Yang Q, et al. (2019) studied the basic definition, design, and procedures of FL and addresses its usefulness in different applications. It is anticipated that, within the immediate future, FL will remove barriers among organizations and create a network where data and information might be exchanged with protection, but the benefits might be equally spread as per the participation of each individual [11]. It will create a cohesive paradigm for various organizations while preserving local data, such that companies should succeed together instead of accepting security and privacy as an assumption.

Geyer RC, et al. (2017) concluded that they have been able to demonstrate through initial empiric experiments that distinct

Citation: Kandati DR, Anusha S (2023) Security and privacy in federated learning: A survey. Trends Comput Sci Inf Technol 8(2): 029-037.
DOI: https://dx.doi.org/10.17352/tcsit.000066

privacy at the patient level is achievable and that strong model precision can be accomplished when a large number of clients are active [12]. In addition, we have shown that thorough current assessment and dissemination changes will lead to optimized budgeting for confidentiality. The goal is to mask the achievements of the clients during preparation, matching the exchange-off between loss of security and model results. Academic research shows that, with a sufficiently large number of active clients, the proposed protocol will preserve client differential privacy at only a small loss in model efficiency. Table 1 summarizes the key findings from recent works relating to Federated Learning.

Here, this research review reveals all the existing security and privacy approaches done through federated learning, whereas the current work focuses on healthcare-related security and privacy issues.

Background

The key component of federated learning is that it allows data scientists to train distributed statistical models based on decentralized devices or servers with a local data set [13]. This means that data scientists use the same model to learn, and no need to upload private data to the cloud or to share data with other data scientists or research teams. Compared to conventional centralized machine learning approaches requiring data sets to reside on a single server, federated learning eliminates data protection and privacy issues by utilizing existing data stores [14].

FL has gained a great deal of interest in the way that technology addresses the problem of securing user privacy by separating data from end-user equipment and machine learning model aggregation, such as deep learning network parameters on a centralized server. FL's particular aim is to work together to learn a global model without explicitly compromising data privacy [15-17]. In particular, FL has significant privacy advantages over data center training in data collection. Also keeping an "anonymized" data set on a server may still put client privacy at risk by connecting it to other data sets. In comparison, the information transmitted to FL consists of limited changes to enhance the accuracy of a specific machine-learning model. Updates themselves can be transient and may never contain more details than raw training data.

Recent rapid growth in medical digitization and subsequent advances in clinical science electronic data processing generate vast volumes of health data. The proper use of these big data is closely related to the performance of the entire health system,

Table 1: A summary of recent works relating to Federated Learning.

Ref. No	Technologies Used	Key Contributions	Limitations
1	We plan to use AI techniques (especially DRLs) as an artificial intelligence method for building an Android-based edge computing, caching, and communication framework.	We conduct experiments to investigate the scenarios of edge caching and computation unloading in the mobile edge device, and the In-Edge AI" is evaluated and demonstrated to have the capability to achieve near-optimal efficiency.	Analyze some of the most promising research directions of In-Edge AI and address a range of outstanding issues from the perspective of improving and extending the use of AI and Edge Computing.
2	Specially introduced deep learning techniques would have a significant and long-lasting effect on privacy issues.	Two privacy metrics are proposed: Image classification probability metric and Image classification entropy metric to assess the privacy of the image.	Deep learning performs better than conventional methods, especially in the areas of computing vision and big data mining, making it a very difficult challenge to maintain privacy.
3	PyTorch and TensorFlow stimulate the development of deep learning, federated learning systems.	Seen that heterogeneity and autonomy are two essential considerations in the creation of functional federated learning systems.	Effectiveness, efficiency, and privacy.
4	Distributed noise addition process that ensures a minimal overall error.	Privacy to truthful parties, even when a minority of the members may be corrupted and colluded.	User's privacy, distributed summation problem.
5	Artificial Intelligence algorithms	Instead of assuming that non-profit organizations could not be trusted, their strategy applies the position of trustee, with its associated obligations, to all those who use clinical evidence to create information and build resources for the good of customers, as well as for-profit organizations.	Safeguard the privacy of patients and the public and ensure the data are made publicly accessible for the advancement of information and resources to support prospective patients.
6	Baseline algorithms, A Novel Breed of Randomized algorithms.	It is possible to develop algorithms that function remarkably effectively in the difficult environment of federated optimization, making vision conceptually feasible.	In general, they contend that the massively distributed, non-IID, imbalanced, and sparse features of federated optimization issues have to be discussed by the optimization community.
7	Blockchain technology, Homomorphic encryption algorithms	Federated learning is a valuable method for implementing machine learning through distributed networks.	Privacy and integrity
8	Modern data mining and Machine Learning (ML) technologies are used.	The naive approach to solving the problem of federated learning is by a Federated Averaging (FedAvg) algorithm.	Statistical challenges, system challenges, and privacy issues in federated learning.
11	A comprehensive secure federated learning framework, which includes horizontal federated learning, vertical federated learning, and federated transfer learning.	Building data networks between entities focused on federated mechanisms is an efficient solution for sharing information without violating user privacy.	Isolation of data, Data Privacy and Security.
12	A differential Privacy-preserving randomized mechanism (e.g. the Gaussian mechanism).	Customer-level differential anonymity is possible and high model precision can be accomplished where a large number of parties are involved.	The difficulty of federated optimization is to develop a model with reduced overhead knowledge between the clients and the curator.

Citation: Kandati DR, Anusha S (2023) Security and privacy in federated learning: A survey. Trends Comput Sci Inf Technol 8(2): 029-037.
DOI: https://dx.doi.org/10.17352/tcsit.000066

which is of utmost importance for the development of drugs, health care, and public health. However, in addition to the heterogeneous and highly dimensional data characteristics generated by a variety of data formats, varying from free-text clinical notes to specific medical images, inconsistent data sources and concerns related to the protection of health data are also important obstacles to multi-institutional health information research.

Federated learning, a method to train a common global model with a central server while maintaining all the confidential data in the local institutions where the data belongs, is a new attempt to connect decentralized data sources to health care without sacrificing data privacy [18].

The goal of the survey is to provide a valuable tool for health informatics and computational research on current developments in machine learning techniques for heterogeneous data distributed across a broad number of organizations, while taking into account privacy concerns related to data sharing.

Motivation

In our daily lives, we have unlimited access to data (usually) and we can train a machine learning model. This way of working is perfect as long as the safety of the data is not in the way. But let's assume we need to focus on the diagnosis of COVID-19, so we need a large amount of data from clinics or hospitals. And if they don't want to exchange data privacy rules, then we're helpless.

Here comes FL to support us. It's a learning technique that enables us to train a common model across all devices. First of all, some initial training is performed on your local server/machine using some initial data. This kickstarts the training later each target computer in the circuit, downloads the model, and enhances it by using the data (federated data) on the device. So, in this scenario, we're sending the model to the data instead of the other way around, and this frees us from the hassle of aggregating data on a single computer, and we're consistent with data privacy.

Methodology

There are many privacy and security issues in the learning process, and we can usually explain the related protection methods in three categories: protection of privacy on the client side, protection of privacy on the server side, and protection of security on the FL side.

1. Privacy protection on the client side

In FL, clients upload their learning results, including parameter values and weights, to the server, but they might not trust the server because a suspicious server may take a look at the data submitted to infer private information [19]. To resolve this issue, certain privacy-preservation techniques can be used by clients as follows:

- **Perturbation:** The idea of disturbance is to add noise to the client's uploaded parameters. This line of work also uses differential privacy to mask such sensitive attributes until the third party is unable to identify the entity, making it difficult to recover the data in order to protect the privacy of the user. However, the origin of these approaches also requires data to be transmitted elsewhere and typically entails a trade-off between precision and privacy, which needs to be modified.

- **Dummy:** The definition of the dummy method is based on the preservation of the privacy of the venue. Dummy model parameters along with the true one will be sent from the clients to the server, which can mask the client's contribution during training. Due to the aggregation processed on the server, the performance of the device can still be assured.

2. Privacy protection on the server side

After collecting modified parameters from clients, the server will perform a weighted average of these parameters based on the size of the data. However, when the server transmits aggregated parameters to clients for model synchronization, this knowledge can leak as spy agencies can exist. Thus, security on the server side is also important.

- **Aggregation:** The main concept of aggregation is to collect the required data or model parameters from various server-side clients. After aggregation, the opponents or the untrustworthy server cannot examine the client information according to this aggregate data parameter. In addition, in certain cases, sever is free to pick clients with high-quality criteria or non-sensitive specifications. However, the issue of how to build an effective grouping mechanism is still a problem for the current FL.

- **Secure Multi-Party Computation (SMC):** The SMC root uses encryption to make individual system updates uninspected by the server, instead of just disclosing the amount after a substantial number of updates. In-depth, SMC is a four-round interactive protocol that is optionally allowed during the reporting process of the contact round. In each protocol round the server collects messages from all devices, and then uses the user message collection to measure an individual response and transfer to each device. The third round is a commit round, during which devices upload encrypted data-masked model updates to the server. Finally, there is a finalization process in which devices disclose appropriate encryption secrets to enable the server to uncover the consolidated model update.

3. Security protection for FL framework

As far as the security of the entire FL architecture is concerned, it is primarily concerned with model stealing attacks. In particular, any FL participant can implement secret backdoor functionality into a common global model, e.g. to ensure that an image classifier assigns an attacker-chosen label to images with certain features, or that a word predictor finishes certain sentences with an attacker [20]. As a result, certain security design safety mechanisms for FL are also in place.

Citation: Kandati DR, Anusha S (2023) Security and privacy in federated learning: A survey. Trends Comput Sci Inf Technol 8(2): 029-037.
DOI: https://dx.doi.org/10.17352/tcsit.000066

- **Homomorphic Encryption:** Homomorphic encryption is used to secure user data by sharing parameters under the encryption scheme [21]. These parameters are encrypted before uploading, and public-private decoding keys are often needed to be transmitted, which can result in additional communication costs.

- **Back-door defender:** Current backdoor defenses are not successful as most of them need access to training data. In addition, the FL framework cannot ensure that all clients are not malicious and have no knowledge of what the participants are doing locally, and prohibits anyone from auditing participants' changes to the joint model [22].

Construction process of the simulation model using Federation Learning

Here are the seven steps of the construction process of the simulation model using Federation Learning:

Step 1: Picking a model framework.

Step 2: Determining the network mechanism.

Step 3: Building the centralized service.

Step 4: Designing the client system.

Step 5: Setting up the training process.

Step 6: Establishing the model management system.

Step 7: Addressing privacy and security.

Challenges on private and secure FL and future scope

In this sub-section, we discuss three major challenges in the private and safe FL framework and suggest detailed discussions on each issue.

A. **Data poisoning: A security issue:** In FL, clients who recently worked only as passive data providers are now able to examine intermediate model states and can contribute arbitrary updates as part of the decentralized training process [23]. This provides an opening for unethical clients to leverage the training process with few restrictions. In particular, opponents acting as sincere clients may send out incorrect updates that intentionally influence the performance of the training model, a process known as model poisoning.

Common poisoning attacks compromise training data to alter the behavior of the model at inference time. They have shown that an opponent can predict membership as well as the properties associated with a subset of training data. In addition, some harmful clients can update unnecessary parameters which in turn damage the performance of the system. Thus, data poisoning on safety problems can be summarized as follows:

- How to calculate damage performance if a malicious client generates data or model poisoning?

- How do we understand and avoid these poisoning habits from our clients?

- How to increase the degree of protection by avoiding potential attacks during communication?

B. **Scaling up issue: A privacy and security issue:** It is easy to expand the current FL system to a broad one such as hundreds or thousands of customers, due to the availability of high-performance and low-price equipment. However, this large scale will pose a range of practical issues: system availability that interacts with local data delivery in complicated ways (e.g. time zone dependency); unreliable device compatibility and disrupted execution; lock-out synchronization between devices with varying availability; and restricted device storage and processing resources. Many of these issues can be summarized as scaling-up issues and the most critical and urgent problem is what happens if more end-user equipment (UE) is able to participate in FL. In particular, the following challenges need to be resolved:

- If more UEs interact in the FL, they can contribute to fewer interaction rounds thanks to more calculations in each round, which should be an obvious benefit.

- If more UEs interact in the FL, there will be less effect of the data poison attack because it will be difficult for the opponent to manage a large number of UEs.

- If more UEs participate in the FL, can they have better protection of privacy? The idea is that hiding a UE in a larger dataset is better than doing the same thing in a smaller dataset.

C. **Model aggregation: A security issue:** The aggregation is mostly performed on the server after collecting the relevant variables and updating the global model. This method is especially important as it can take advantage of the clients and decide the conclusion of the learning process. If the security method is implemented on the client side, such as the interruption applied prior to the selection of model parameters, the aggregation cannot be simply a traditional averaging operation. The key reasons can be inferred as (i) the noise power of the disturbance is increasing including the number of clients; (ii) the server should know the stochastic information from the clients and the architecture of the aggregation system needs to differentiate the privacy-sensitive clients from the privacy-insensitive ones. Therefore, a more intelligent process of aggregation should be given as follows:

- Intelligent aggregators should consider client variations and use different aggregation techniques.

- Intelligent aggregators can address the noise-added issue of privacy security. For example, the use of the Minimum Mean Square Estimation (MMSE) aggregator can act as an excellent candidate.

Citation: Kandati DR, Anusha S (2023) Security and privacy in federated learning: A survey. Trends Comput Sci Inf Technol 8(2): 029-037.
DOI: https://dx.doi.org/10.17352/tcsit.000066

- Intelligent aggregators can change the parameter weights for interacting with clients during multiple interaction rounds.

FL is a promising area of study in machine learning. Researchers are working hard to further improve the potential of the technique to meet privacy and security needs. For example, the privacy policy discussed above protects privacy at a local or global level with respect to all devices on the network. In practice, however, it may be appropriate to define privacy at a more detailed level, taking into account the fact that privacy constraints may vary across devices or even across data points on a single computer. One idea is to use random sampling privacy assurances instead of user-specific ones, thereby offering a weaker form of privacy in return for more accurate models. Developing strategies for addressing mixed device-specific or sample-specific privacy constraints seems to be promising.

Another example of forthcoming FL trends – allowing the parallel training of deep learning models on distributed data sets while protecting data privacy is complex and challenging. An FL framework, FedF for privacy preservation, coupled with parallel training, has been developed by one group of researchers. The system allows the model to be learned from several economically training data sets (which may belong to different owners) while not disclosing any information on each data set as well as intermediate outcomes.

Results and discussion

In this section, simulations are presented to demonstrate the above issues and to explore some potential solutions. For each experiment, we first partition original training data into disjoint non-iid training sets, locally measure Stochastic Gradient Descent (SGD) updates for each dataset, and then aggregate updates using an averaging method to train a globally shared classifier. The prototype is evaluated on the well-known classification dataset: MNIST, the digit classification problem which distinguishes 10 digital numbers from 0 to 9, and the system fail to achieve the classification when the accuracy cannot reach 10%. The dataset given in MNIST is divided into 60,000 training examples and 10,000 test examples. The global epoch is set to 300 iterations on the server side, while 120 iterations are applied on each client side and the local batch size is set to 1200.

A. Data poisoning

In this subsection, we first set up a CNN framework for 30 clients, and the malicious clients will upload a fake value of the parameters in each contact round. Fake value can be the opposite of true value, or random numbers within (-1, 1).

Technical Problems: Mechanisms for the prevention of data poisoning need to be investigated.

Solution: There are three key ways to avoid data poisoning in a privacy-aware FL environment. The first is to identify malicious clients when the device is set up. ML methods can be used in this case. For example, a supervised learning algorithm can be used to classify malicious clients during each contact round. Another approach focuses on the process of aggregation. After each aggregation, depending on the quality of the client's uploaded learning parameters, the server will change the aggregation weights for each client. In this way, the server is able to place more confidence in clients who are more helpful in achieving rapid convergence and good learning results. Third, social network principles can be used to update the weights of each contact round by leveraging the social relationship of each client to the overall performance of the system.

B. Scaling up issue

In this subsection, we first demonstrate the classification accuracy for different client numbers. We can see from this that with the growing number of clients, output does not show much benefit. However, the overall delay may be greatly decreased if there are more clients. In particular, customers are randomly allocated to a 1 × 1 km2 square area, and we record the amount of the maximum measurement and transmission time as a delay in each contact round for a different number of clients. Then we set the learning stops when the accuracy reaches 90% and record the total contact round and measure the total delay. Note that this result might be different for other delay models.

Technical Problems: In a wide network, the server can have a long wait period and a complicated resource allocation during the upload parameter.

Solution: For the scaling-up problem, one way to fix the long waiting period is to set up a time limit for each client to upload. At each learning period, the server will collect at least the necessary client parameters before running the next round of FL. If the waiting time reaches this deadline, the present learning period will be discontinued. In addition, we can use the idea of user clustering in game theory to deal with a large number of clients. By effectively separating clients into various groups, each group of clients can compete with each other to achieve the learning target. In turn, the server would also have benefits. In this new structure design, a significant number of clients would be divided by their shared interests, identical physical locations, or the same uploading methods.

C. Model aggregation

The model aggregation should be smart. It not only deals with the vast amount of noise when ensuring the efficiency of the device but also applies various aggregation approaches to different clients. In the conventional FL environment, the current aggregation weight approach depends on the size of the training, but a more intelligent aggregator should be built for multiple objectives. In addition, the set of modified parameters may also be changed. For example, the server may choose uploaders with better channel or parameter quality.

Technical Problems: In the current FL environment, we need to build an intelligent aggregator.

Solution: We suggest an intelligent aggregation approach to fix the issue of malicious clients. The proposed algorithm consists of two parts:

Citation: Kandati DR, Anusha S (2023) Security and privacy in federated learning: A survey. Trends Comput Sci Inf Technol 8(2): 029-037.
DOI: https://dx.doi.org/10.17352/tcsit.000066

1) Add the test process to the server side and change the aggregation weight according to the test output of each client's uploaded parameters;

2) Increase the local time for each customer. The proposed algorithm will reduce the transmission loss caused by malicious clients. In addition, more local intervals are required when there are more malicious clients in the FL system.

The use of AI for predicting the outcomes of public health scenarios

The pre-emergency phase in public health issue response refers to the time leading up to the actual disaster. Since the emergence of public health disasters is sometimes sudden and unexpected, it is crucial to monitor and warn of their occurrence. Government efforts at this time are mostly directed toward better monitoring and response to public health disasters. There are two key elements of disaster management preparation for public health disasters: disaster forecasting and disaster instruction and practice [24].

Notification of impending public health issues is a crucial responsibility in the pre-disaster readiness phase. Effective early detection will greatly accelerate the organization's reaction time in the event of a disaster. The governments of many different nations rely mostly on traditional surveillance techniques to create a system for early detection in the event of an epidemic or spreading disease. It's important to note that this monitoring technique isn't without its drawbacks. Monitoring consumes a lot of manpower and material resources, and it covers the entire country, so there is no cross-checking or adjustment for discrepancies; all information is gathered in one place; however, the data is relatively late to be gathered after daily sampling and a weekly summary. Data integrity would be compromised by a failure in even a single node [25]. Government organisations might considerably benefit from AI's ability to analyse social networks, online news feeds, and government information in order to track outbreaks, sensibly allocate healthcare services, and accelerate advancements.

Artificial intelligence for identifying COVID-19 from coughs: Improvements in disease identification and early detection methods have the potential to significantly slow down the development and impact of a disease. Recent efforts to construct advanced deep-learning AI models for cough sound classification as a COVID-19 preliminary screening tool have shown encouraging results [26]. If authorised, a cough-based diagnosis of COVID-19 would be a straightforward, reasonable, and reproducible approach for detecting the virus. Recent research has investigated how cough noises can be used as a pre-screening tool to identify COVID-19 in asymptomatic individuals [27-30]. Using sophisticated algorithms incorporating acoustic signal interpretation and machine learning, this can be detected even in the absence of obvious symptoms since the virus may cause subclinical modifications throughout the body. Especially for asymptomatic individuals, it may be more effective to utilise this approach than a traditional method of pre-screening for COVID-19 based on temperature.

Conclusion

In this paper, we explored possible issues of privacy and security in FL. We also found out that data protection can be offered on the client or server side, and security protection is specifically intended for the device level. In addition, we concluded that the issues considered could be categorized as data poisoning, scaling up, and model aggregation problems. Additionally, we have also presented some potential solutions to protect privacy and security in the design of FL systems. Finally, we have also presented how AI might be useful in analyzing public health data in evidence-based research scenarios.

References

1. Wang X, Han Y, Wang C, Zhao Q, Chen X, Chen M. In-edge Ai: Intelligent zing mobile edge computing, caching and communication by federated learning. IEEE Network. 2019; 33(5): 156-165.

2. Liu B, Ding M, Zhu T, Xiang Y, Zhou W. Adversaries or allies? Privacy and deep learning in big data era. Concurrency and Computation: Practice and Experience. 2019; 31(19): e5102.

3. Li Q, Wen Z, Wu Z, Hu S, Wang N, He B. A survey on federated learning systems: vision, hype, and reality for data privacy and protection. 2019. arXiv preprint arXiv:1907.09693.

4. Shi E, Chan THH, Rieffel E, Song D. Distributed private data analysis: Lower bounds and practical constructions. ACM Transactions on Algorithms (TALG). 2017; 13(4): 1-38.

5. Larson DB, Magnus DC, Lungren MP, Shah NH, Langlotz CP. Ethics of Using and Sharing Clinical Imaging Data for Artificial Intelligence: A Proposed Framework. Radiology. 2020 Jun;295(3):675-682. doi: 10.1148/radiol.2020192536. Epub 2020 Mar 24. PMID: 32208097.

6. Konecný J, McMahan HB, Ramage D, Richtárik P. Federated optimization: Distributed machine learning for on-device intelligence. 2016. arXiv preprint arXiv:1610.02527.

7. Ilias C, Georgios S. Machine Learning for All: A More Robust Federated Learning Framework. 2019.

8. Xu J, Glicksberg BS, Su C, Walker P, Bian J, Wang F. Federated Learning for Healthcare Informatics. J Healthc Inform Res. 2021;5(1):1-19. doi: 10.1007/s41666-020-00082-4. Epub 2020 Nov 12. PMID: 33204939; PMCID: PMC7659898.

9. Pai MM, Ganiga R, Pai RM, Sinha RK. Standard electronic health record (EHR) framework for Indian healthcare system. Health Services and Outcomes Research Methodology. 2021; 21(3): 339-362.

10. Dasaradharami Reddy K, Gadekallu TR. A Comprehensive Survey on Federated Learning Techniques for Healthcare Informatics. Comput Intell Neurosci. 2023 Mar 1;2023:8393990. doi: 10.1155/2023/8393990. PMID: 36909974; PMCID: PMC9995203.

11. Yang Q, Liu Y, Chen T, Tong Y. Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST). 2019; 10(2): 1-19.

12. Geyer RC, Klein T, Nabi M. Differentially private federated learning: A client level perspective. 2017; arXiv preprint arXiv:1712.07557.

13. Shaheen M, Farooq MS, Umer T, Kim BS. Applications of federated learning; Taxonomy, challenges, and research trends. Electronics. 2022; 11(4): 670.

Citation: Kandati DR, Anusha S (2023) Security and privacy in federated learning: A survey. Trends Comput Sci Inf Technol 8(2): 029-037.
DOI: https://dx.doi.org/10.17352/tcsit.000066

14. Asad M, Moustafa A, Ito T. Federated learning versus classical machine learning: A convergence comparison. 2021; arXiv preprint arXiv:2107.10976.

15. Hasan J. Security and Privacy Issues of Federated Learning. 2023; arXiv preprint arXiv:2307.12181.

16. Gosselin R, Vieu L, Loukil F, Benoit A. Privacy and security in federated learning: A survey. Applied Sciences. 2022; 12(19): 9901.

17. Mothukuri V, Parizi RM, Pouriyeh S, Huang Y, Dehghantanha A, Srivastava G. A survey on security and privacy of federated learning. Future Generation Computer Systems. 2021; 115: 619-640.

18. Alam T, Gupta R. Federated learning and its role in the privacy preservation of IoT devices. Future Internet. 2022; 14(9): 246.

19. Blanco-Justicia A, Domingo-Ferrer J, Martínez S, Sánchez D, Flanagan A, Tan KE. Achieving security and privacy in federated learning systems: Survey, research challenges, and future directions. Engineering Applications of Artificial Intelligence. 2021; 106: 104468.

20. Ma C, Li J, Ding M, Yang HH, Shu F, Quek TQ, Poor HV. On safeguarding privacy and security in the framework of federated learning. IEEE Network. 2020; 34(4): 242-248.

21. Ma J, Naas SA, Sigg S, Lyu X. Privacy?preserving federated learning based on multi?key homomorphic encryption. International Journal of Intelligent Systems. 2022; 37(9): 5880-5901.

22. Zhang K, Tao G, Xu Q, Cheng S, An S, Liu Y, Zhang X. Flip: A provable defense framework for backdoor mitigation in federated learning. 2020; arXiv preprint arXiv:2210.12873.

23. Tolpegin V, Truex S, Gursoy ME, Liu L. Data poisoning attacks against federated learning systems. In Computer Security-ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14-18, 2020, Proceedings, Part I 25. Springer International Publishing. 2020; 480-501.

24. Zhang Y, Yang Y. Research on response means of government network public opinion crisis based on 4R crisis management theory. Mod Intell. 2017; 37: 75-80.

25. Imran A, Posokhova I, Qureshi HN, Masood U, Riaz MS, Ali K, John CN, Hussain MI, Nabeel M. AI4COVID-19: AI enabled preliminary diagnosis for COVID-19 from cough samples via an app. Inform Med Unlocked. 2020;20:100378. doi: 10.1016/j.imu.2020.100378. Epub 2020 Jun 26. PMID: 32839734; PMCID: PMC7318970.

26. Wired. Covid-19 Will Accelerate the AI Health Care Revolution. 2020. https://www.wired.com/story/covid-19-will-accelerate-ai-health-care-revolution/

27. Kandati DR, Gadekallu TR. Genetic clustered federated learning for COVID-19 detection. Electronics. 2022; 11(17): 2714.

28. Kandati DR, Gadekallu TR. Federated learning approach for early detection of chest lesion caused by COVID-19 infection using particle swarm optimization. Electronics. 2023; 12(3): 710.

29. Li H, Li C, Wang J, Yang A, Ma Z, Zhang Z, Hua D. Review on security of federated learning and its application in healthcare. Future Generation Computer Systems. 2023; 144: 271-290.

30. Abad G, Picek S, Ramírez-Durán VJ, Urbieta A. On the security & privacy in federated learning. 2021; arXiv preprint arXiv:2112.05423..

Citation: Kandati DR, Anusha S (2023) Security and privacy in federated learning: A survey. Trends Comput Sci Inf Technol 8(2): 029-037.
DOI: https://dx.doi.org/10.17352/tcsit.000066