Challenges of Trustable AI and Added-Value on Health
B. Séroussi et al. (Eds.)

doi:10.3233/SHTI220436

Federated Learning in Healthcare: A Privacy Preserving Approach

K NARMADHA[1] and P VARALAKSHMI
Department of Computer Technology, Anna University, MIT Campus, Chennai, India

Abstract. A need to enhance healthcare sector amidst pandemic arises. Many technological developments in Artificial Intelligence (AI) are being constantly leveraged in different fields of healthcare. One such advancement, Federated Learning(FL) has acquired recognition primarily due to its decentralized, collaborative nature of building AI models. The most significant feature in FL is that, raw data remain with the data sources throughout the training process and thus preventing its exposure. Hence, FL is more suitable and inevitable in healthcare domain as it deals with private sensitive data which needs to be protected. However, privacy threats still exist in FL, necessitating a requirement for further improvement in privacy protection This paper discusses about the concepts and applications of FL in healthcare and presents a novel approach for enhancing privacy preservation in Federated Learning.

Keywords. Artificial Intelligence, Federated Learning, decentralization, privacy

1. Introduction

The COVID-19 pandemic has stressed the need to improve our healthcare systems throughout the world. Many innovations in Artificial Intelligence (AI), mainly in Machine Learning (ML) and Deep Learning (DL) are being extensively applied in various domains of healthcare like disease diagnostics, drug discovery, clinical data prediction, patient monitoring, genome sequencing etc. Federated Learning (FL) is the latest development in AI which is related to building ML/DL models in a distributed, collaborative manner among participating entities without sharing their own raw data [1] [2]. The entities can be organizations like hospitals, banks, research centers, industries etc. or smart devices like sensors, wearables, mobile phones, laptops, tablets etc. FL has gained a lot of attention nowadays as it preserves data privacy and can be used to build AI applications in healthcare, smart manufacturing, computer vision, autonomous driving etc. The application of Federated Learning in healthcare is more relevant and necessary as it deals with private sensitive data of individuals which needs to be protected from unauthorized exposures. Many real-world projects of FL models in smart healthcare have been implemented worldwide and are expected to grow in coming years [5]. Even though FL preserves data privacy by inhibiting movement of raw data, some sensitive information can still be leaked from the exposure of parameters that are exchanged among participating entities. Therefore, a simple yet robust privacy preserving approach

[1] K Narmadha, Corresponding author, Department of Computer Technology, MIT Campus, Anna University, Chennai – 600044, India; E-mail: narmk27@gmail.com

for FL is proposed in this paper. Our proposed approach uses differential privacy in which noise is added to the data to hide its originality.

Section 2 gives introduction on the concepts of Federated Learning. A discussion on leveraging FL in healthcare is described in section 3. The proposed algorithm is presented in section 4. Finally, the paper ends with a conclusion in section 5 highlighting the directions which need more study and research.

2. The rise of Federated Learning

There has been an unprecedented growth of Big Data in recent years and it has further exploded due to the COVID - 19 pandemic. This has led to the growing demand for AI particularly ML and DL, in which computers are trained to process this enormous amount of data to derive meaningful information from it. In traditional method of building ML/DL models, the entire data from all data generating entities will be transmitted to the service provider's or server's location which is usually in a cloud. The complete process of training and building the model will take place only at the server's place. This method has a few challenges. The data which is needed to build a ML model comes from various scattered and geographically distributed sources. Often, it is tough to integrate this fragmented data from isolated remote locations due to factors like limited network connectivity etc. Moreover, a major part of the data involves private sensitive data of individuals. So, transmitting the private data across geographical boundaries in a secured manner and without violating privacy rights of the users is quite difficult. Also, transmitting huge amount of data to a single central location from sources across the world will increase the cost and choke the network bandwidth. On the other hand, higher the amount of data that is fed to a ML model, the accuracy of the model will be better. Thus, to overcome the challenges of data migration and integration as well as maintaining privacy of sensitive data, an alternate method called Federated Learning has attained importance in recent years.

Federated Learning is a type of distributed ML where the model is being collaboratively trained and built by the data generating entities (clients) which are either smart devices or organizations along with servers who act as coordinating entities [1] [2]. In FL, each client's raw data is used locally and not exchanged or transmitted to a server. All participating clients train a local ML model with their own data for a particular number of rounds until a qualifying criterion is met. After each iteration, they transmit the updated ML model parameters to the server for aggregation. The aggregated model parameters are transmitted back to all clients from the server which are used in the next iteration by the clients. This iterative process gets repeated until the model converges or the desired accuracy is obtained. This training process which takes place with one server and *n* clients is explained in the following steps:

- **Step 1:** Server initializes a global model GM and distributes to *n* clients.
- **Step 2:** Each client (C_i) initializes its local model (LM_i) as GM in first iteration.
- **Step 3:** Each client (C_i) trains its local model (LM_i) with its own data and transmits the model parameters to server.
- **Step 4:** Server does a weighted average of the local model parameters of all *n* clients and updates GM [10].

$GM = \sum_i^n (W_i LM_i)$ where W_i - Weight of ith client based on its dataset size

- **Step 5:** Server sends the updated GM to all *n* clients and the local models are modified with updated GM.
- **Step 6:** Each client (C_i) calculates the accuracy of the local model (LM_i) and verify whether the model has converged.
- **Step 7**: If the clients obtain desired accuracy or the local models have converged, the training process is stopped else the process continues from step 3 as next iteration.

Federated Learning (FL) preserves user data's privacy by default as the raw data does not leave the data sources. The domains like healthcare, military etc. which deals with sensitive data can make use of FL to reap AI benefits. Computational power needed for training a model is also shared among the clients instead of relying entirely on a server. Also, the organizations who do not have sufficient training data to build a standalone ML model can leverage FL to build a joint ML model. Moreover, network bandwidth consumption is significantly reduced in FL as huge amount of raw data is not transmitted to the server.

3. FL in healthcare

Federated Learning in healthcare is getting significant attention because of the need to build privacy-preserving and more accurate ML/DL models. FL in healthcare can be used for tasks such as to improve the prediction of diseases at an early stage, give best available treatment to patients, fasten drug discovery process etc. [8]. A handful of articles on FL in healthcare have been published by many authors [5][6][7][8][9]..

Federated Learning in smart healthcare can be used in three different scenarios depending on the type of participating clients.

- **Scenario 1**: Clients are organizations like hospitals, medical research centers, pharmaceutical companies, government medical bodies, genome sequencing labs etc. This type of FL is known as cross-silo FL [1]. For instance, two or more hospitals can collaborate and build a ML model with the help of a government medical body who can act as a server.
- **Scenario 2:** Clients are smart healthcare devices like wearables, smart patient monitors, sensors etc. This type of FL where the clients are smart devices used by individuals is known as cross-device FL [1]. For example, health parameters from wearables of thousands of users can be used to jointly train a ML model without moving the data out from the devices [7].
- **Scenario 3:** In this case, the clients can be either a healthcare organization or a smart healthcare device. This can be called as hybrid FL, where a collaboration between different hospitals and many standalone individuals is made to train and build a ML model.

The data partitioning among the clients can be horizontal or vertical. Two or more diabetes hospitals at different places can collaborate to train a ML model to predict the early stage of diabetes. In this scenario, all the hospitals share the same feature space and different sample space, which is known as horizontal FL [1]. There can also be a collaboration among a diabetes hospital, an eye hospital and a cardiology clinic at a same place. In this case, all the hospitals share different feature space and same sample space, which denotes a vertical partitioning of training dataset and is known as vertical FL [1].

This model can be used to find the relationships between diabetes, eye disorders and cardiac diseases. Federated transfer learning can be applied if a hospital and a pharmaceutical company want to jointly build a ML model to assess the side effects of drugs. Here, both the feature space and sample space differ among the clients.

The main advantage of using FL in healthcare is improved privacy protection of patients' sensitive data. Also, smaller hospitals who do not have sufficient training data and computational power can benefit from a joint collaboration. Moreover, accuracy of the model will definitely improve when the model is being trained in a federated manner as training takes place with huge amount of data.

3.1 Privacy in FL

Federated Learning preserves privacy of user's raw data, however some private information can still be exposed through model parameters that are exchanged between server and clients [4]. It is possible to extract raw data through model inversion attacks. Moreover, curious or malicious server and clients can try to infer other entity's information by analyzing the model parameters. So, different privacy-preserving mechanisms need to be applied to further improve the privacy preservation in FL. The three most popular methods that are used for privacy preservation in FL are homomorphic encryption, secure multiparty computation and differential privacy [4]. Among the three approaches, differential privacy is widely used in real-time applications as it is scalable and involves less overhead compared to the other two.

Differential privacy is a mechanism in which a little amount of random noise is added to any data to perturb its value. The amount of noise to be added depends on the sensitivity of the data. More amount of noise will reduce the utility of data as it leads to higher perturbation. On the other hand, it also achieves higher privacy protection. So an optimal amount of noise needs to be added to balance the trade-off between data utility and privacy. The noise value(N) is calculated from the Gaussian distribution.

$$N = (c.s) / \varepsilon \text{ where } c^2 \geq 2 \log(1.25/\delta) \text{ for } \varepsilon \in (0,1) \quad (1)$$

In the above equation (1), ε denotes the privacy budget and helps to control the level of noise added [4]. δ denotes the probability by which the ε-differential privacy is violated. Sensitivity(s) is calculated based on the maximum difference obtained on the model parameters when the model is trained on two neighboring datasets.

4. Proposed Algorithm

Server initializes a global model GM, ε, δ and distributes to *n* clients. Each client (C_i) initializes its local model (LM_i) as GM in first iteration. Each client (C_i) trains its local model (LM_i) with its own data, calculates the noise(N_i) based on equation (1), adds it with LM_i to get NLM_i, and transmits NLM_i to the server.

$$NLM_i = LM_i + N_i \quad (2)$$

Server does a weighted average of the noise added local model parameters of all *n* clients, updates GM [10] and sends back to all n clients.

$$GM = \sum_i^n (W_i NLM_i) \quad (3)$$

where W_i - Weight of ith client based on its dataset size

Each client(C_i) subtracts its added noise(N_i) from GM and updates its local model for next iteration. Since the local noise is subtracted before proceeding with the next

iteration, the utility of the model parameters increases. Hence, our proposed approach produces better model accuracy.

5. Conclusion

Federated Learning in healthcare will see a tremendous growth in coming years. Some of the areas which need more study are vertical FL, decentralized topology in FL and privacy-preserving FL. Vertical FL in healthcare needs more concrete research as it can be used to find complex relationships among various diseases. Also, more research needs to be done for decentralized FL, which eliminates the requirement for a trusted server and thus improving the privacy preservation in FL. Technologies other than blockchain need to be explored in this type of FL. Effective and efficient privacy preserving mechanisms need to be studied to implement them in future real-world projects of FL.

References

[1] Qiang Y, Yang L, Tianjian C, Yongxin T. Federated Machine Learning: Concept and Applications, ACM Trans. Intell. Syst. Technol., 2019, Jan; vol. 10, no. 2, pp. 12:1–12:19.
[2] Li T, Sahu AK, Talwalkar A, Smith V. Federated Learning: Challenges, Methods, and Future Directions, IEEE Signal Processing Magazine, 2020, May; Volume: 37 Issue: 3, Page(s): 50 - 60.
[3] Kairouz P, et al. Advances and Open Problems in Federated Learning, 2019; Available: https://arxiv.org/abs/1912.04977.
[4] Wei K, et al., Federated Learning With Differential Privacy: Algorithms and Performance Analysis, IEEE Transactions on Information Forensics and Security, 2020, April; Volume: 15, Page(s): 3454 – 3469.
[5] Nguyen DC, et al. Federated Learning for Smart Healthcare. ACM Comput. Surv. 2021;Vol. 1.
[6] Pfitzner B, et al. Federated Learning in a Medical Context: A Systematic Literature Review. ACM Transactions on Internet Technology. 2021 May; Vol. 21, No. 2, Article 50.
[7] Yuan B, Ge S, Xing W. A Federated Learning Framework for Healthcare IoT devices. 2020, May; arXiv:2005.05083v1 [cs.LG].
[8] Brisimi TS, et.al. Federated Learning of predictive models from federated Electronic health records. International journal of Medical Informatics. 2018. Jan.
[9] Xu J, et.al. Federated Learning for Healthcare Informatics. Journal of Healthcare Informatics Research. 2020. November.
[10] McMahan HB, et.al. Communication – Efficient Learning of Deep Networks from Decentralized Data. 2017, Feb; arXiv:1602.05629v3 [cs.LG].
[11] Yu Y, et.al. Blockchain and Federated Learning for Privacy-preserved Data Sharing in Industrial IoT. IEEE Transactions on Industrial Informatics. 2020. June.
[12] Li X, et al. On the Convergence of FedAvg on Non-iid Data. 2020, June; arXiv:1907.02189v4 [stat.ML].