A review of Federated Learning

Zargar Danish [1], Dr Ihtiram Raza Khan [2]
{[1] danishzargarr@gmail.com, [2] drihtiramrazakhan2021@gmail.com}

Department of Computer Science & Engineering, Jamia Hamdard,New Delhi. India[1,2]

Abstract: With the fast development of Artificial Intelligence (AI) and Machine Learning (ML), data privacy & security is becoming a serious problem. Since the majority of the Machine Learning Models are centralized in nature which requires sharing the private data to train the centralized ML Model i.e., a model which is stored on a central shared server. In this context, a new approach that is decentralized in nature comes for our rescue, this approach is called Federated Learning (FL). [1] [2] Google is the first company to introduce this concept in 2016. [1] Federated Learning is a decentralized ML technique where different devices or clients in a Federated Network train an ML Model at a central shared Server without sharing their private data. Federated Learning preserves data privacy and gives more control to clients over their data. In this paper, I will give a brief introduction to Federated Learning: its classification, applications, Challenges, Security issues & Future Directions.

Keywords: Machine Learning (ML), Federated Learning (FL), Artificial Intelligence (AI)

1. Introduction

With the advancement in mobile technology, fast connectivity, Artificial Intelligence and Machine learning, there is a generation of massive data, called big data. [1] To manage Big-data, Machine Learning technologies are being used in various domains such as healthcare, finance, smart-assistants etc. Due to the comprehensive and common use of Machine Learning techniques in important fields, it is important to safeguard the privacy and security of users' data. The majority of these Machine learning techniques are Centralized techniques i.e., data of various devices is aggregated into a central server so that the centralized ML algorithm can be trained with this data. This method has some issues such as the violation of the privacy of user data, limiting access to the data for the users, and even leaking some sensitive data of users.

Since the Facebook data breach of 2018 in which data of around 500 million users was leaked, people have become more concerned about the security & privacy of their data. [2] The unlawful use of users' data is a problem for both the users and the companies using the data. [1] As a result of this various countries have made laws for the protection and security of data. In India the "Information Technology Rules, 2011" announced under the "Information Technology Act, 2000" supervise and govern the privacy & security of data. [3] [4]

ICIDSSD 2022, March 24-25, New Delhi, India

DOI 10.4108/eai.24-3-2022.2318998

For example, to develop a Keyboard Text/Emojis detection model, different users share their private data to train and develop a shared Machine Learning Model residing on a Central Server. In this process, the sensitive data of users is being used without their actual consent. This violates the user's privacy which is of utmost importance. The solution to such a problem can be a technique that is decentralized in nature i.e., Federated Learning (FL). [5] FL is a decentralized Machine Learning technique where different clients in a Federated Network train a Shared Machine Learning Model at a central Server without sharing their local private data. Federated Learning was introduced by Google in 2016. FL has the potential to be applied to various domains where data privacy is of much importance such as mobile keyboards, healthcare, speech recognition, blockchain etc.

Although there are various applications of Federated Learning, their implementation has various challenges. Those challenges need to be addressed to successfully implement this technique.

Therefore, in this paper I will try to give a brief introduction of Federated Learning i.e., its classification, applications, Challenges, Security issues & Future Directions.

2. Problems in Centralized Machine Learning Techniques

With the advancement in mobile technology, fast connectivity, Artificial Intelligence and Machine learning, there is a generation of massive data, called big data. [1] This Big-data is managed using ML techniques. But most of these Machine Learning techniques are Centralized techniques i.e., the data of various devices is aggregated into a central server for training the Machine Learning Model. The problems with this approach are as follows:

- The violation of data privacy when exchanging the data with the central server in order to train the Machine Learning Model. [1]
- The users have limited access to their data which is stored at a central server. [1]
- Exchanging large chunks of data for training complex Machine Learning models puts a huge load on the centralized machine learning network. [6]
- A huge processing load is put on a single Central Server during the training of the Machine Learning Model. [6]

3. Working of a Simple Federated ML Model

The solution to the problems of Centralized Machine Learning techniques is the Federated Learning approach, which is a decentralized Machine Learning technique where different devices or clients in a Federated Network train a Shared Machine Learning Model at a central Server by exchanging the 'learning from a locally stored Machine Learning model' rather than 'the data itself' with the Centrally stored Shared Machine Learning Model. Federated Learning addresses the problems associated with centralized machine learning techniques. The Federated Learning works as follows: [7]

Step – 1: A generic Machine learning model is trained at the central server.

Step – 2: From the central server this trained Machine learning model is sent to the users of this federated network. The local models learn with the locally generated data and then get

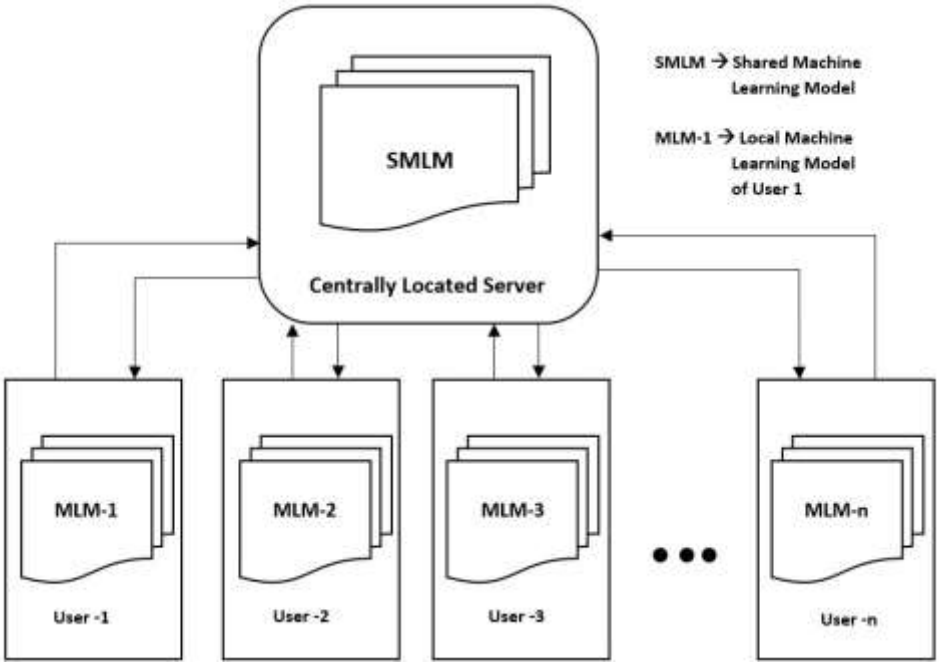

Fig. 1. How FL Works

better with time. See **Figure 1.**

Step – 3: After a certain period of time clients or devices send their learning to a central server instead of the data using homomorphic encryption, which allows the Central machine learning model to perform different computations on this encrypted learning, thus protecting the privacy of the clients' or devices' data.

Step – 4: When new learnings are received from different users of this federated network, the central machine learning model gets updated with these learnings, resulting in an improved central machine learning model.

Step – 5: The updated central machine learning model is again sent to the users of the federated network. This cycle is repeated multiple times.

Federated learning protects the user's privacy by sharing the 'learnings' rather than 'the data itself' with the Centrally stored Shared Machine Learning Model. In the Federated learning approach, the user's data is stored locally thus giving the user more control over the data.

The processing load on a central server is divided among all the clients of the federated network because now the user's data is required to train only a local learning model which is residing on the user's device, then these learnings are sent to a central server. After receiving the learnings or local updates from clients or user's devices, the global or central machine learning model is updated with this local update, instead of training it with the client's data, thus reducing the load on the central server. The users in a federated network send only the learnings rather than the data, thus users don't share large chunks of information with the central server, which results in less load on the federated network.

4. Classification of Federated Learning:

4.1 Horizontal federated Learning: It is utilized in those cases in which the data-set on each user's device in the federated network has a different sample space but the same feature space. For example, two branches of a bank operating in two different regions may have a different set of users, so the intersection of their user space is small (thus different sample space) but the feature space will be the same because of the nature of the business is same. [8]

4.2 Vertical federated Learning: It is used in those cases in which the data-set on each user's device in the federated network has a different feature space but the same sample space. Let us take an example of a bank and a hospital operating in the same region, may have almost the same set of users, so the intersection of their user space is large which results in the same sample space but different feature space because the nature of the work is different in the bank than the hospital. [8]

4.3 Federated Transfer Learning (FTL): It is utilized in those cases in which the data-set on each user's device in the federated network has a different sample space as well as feature space. Let us take an example of a bank and a hospital operating in two different countries, may have an almost different sets of users, so the intersection of their user space is small (thus different sample space) & the different feature space because the nature of the work is different in the bank than the hospital. [9]

4.4 Cross-silo Federated Learning: It is utilized in those cases in which the users or clients in the federated network are a small number of different organizations. In this method, clients have less computing power and can't reliably communicate with the central server. Only a few clients are available at one time. [10, 11]

4.5 Cross-device Federated Learning: It is utilized in those cases in which the clients or users in a federated network are mobile devices or IoT devices. This method is usually used with those data-sets which are either horizontally partitioned or vertically partitioned. In this method, clients have the abundant computing power and can

communicate with central server reliably. Most of the clients are available all the time. [10, 11]

5. Applications of Federated Learning

5.1 Mobile Keyboard Prediction: In 2016, Google developed a Federated Learning technique with the aim of improving prediction in their keyboard while maintaining the privacy of users. [1]

5.2 Object detection: It is used in computer vision and Image Processing to detect different objects in an image or video. It is used in many areas such as object-detection in fire-hazards, object-detection on Roads, etc. Developing an object detection model has privacy concerns so Federated learning can be used to develop it. [12]

5.3 Internet of Things (IoT): All IoT systems have some kind of sensors that generate data for processing at a central server. This involves data privacy and security issues for IoT devices. These issues are handled by using Federated Learning in IoT. [1]

5.4 Smart Healthcare: Federated-learning technique can also be used in Smart healthcare. If an ML model is developed that can detect a disease based on some symptoms of that disease. If that ML model is trained with data of patients of a single hospital, it will make the ML model inaccurate for prediction. Thus, to make the ML model accurate we need to provide data of patients from multiple hospitals, but since patient data is sensitive, it won't be feasible to share it. In this situation, Federated Learning comes to our rescue, it will train the ML model with data of patients from different hospitals while preserving the privacy of the patient's data. [1, 8]

5.5 Speech recognition: Speech recognition is used to interpret and convert spoken words into text. With the advancement in Artificial Intelligence & Machine Learning, it has been used in various applications such as Google translator. [13] In order do this the complete information of speech data is required to train the speech recognition model, this speech data is sent to a central server thus creating security and privacy concerns for this speech data. Federated learning can be a perfect solution to train speech recognition models, without exposing the speech data, thus giving privacy and security the priority. [14]

5.6 Voice recognition: Voice recognition is used to interpret and convert spoken words into commands to be performed. With the advancement in Artificial Intelligence & Machine Learning, it has been used in various devices and applications such as Google Assistant, Amazon's Alexa etc. [15] [16] It helps users to interact with their devices in a hands-free mode to do various tasks. In order to do this the complete information of speech data is required to train the Voice recognition model, this speech data is sent to a central server

thus creating security and privacy concerns for this speech data. Federated learning can be a perfect solution to train such Voice recognition models, without exposing the speech data, thus giving privacy and security the priority. [17]

5.7 Blockchain: "Blockchain is a time-ordered, non-tampering, decentralized distributed account book …". [18, p. 430] The integration of blockchain & federated learning allows training of a machine learning model on user devices (without disclosing the users privacy and security) using the blockchain as a central database, the users will be rewarded based on their contribution towards the training of Federated Learning Model. This has opened up new fields like open banking which connects banks with third-party service providers to share bank data through APIs in an encrypted way, this is done to improve the overall customer experience. [1]

5.8 Transportation: The number of sensors on vehicles and roads has increased greatly with the advancement in technology. These sensors generate a tremendous amount of data from various geographical locations. This huge amount of data can be used for traffic flow prediction or traffic jam prediction in those locations by training a Traffic Prediction Model. But this data is spread across devices and for protecting the privacy of this data it shouldn't be exchanged with an ML model. In such situations Federated Machine Learning comes to our rescue, it will train the Traffic Prediction Model without exposing the privacy of user's data from various geographical locations, thus helping to predict jams, traffic flow and preserving the privacy of users. [8]

5.9 Interest-based advertising (IBA): IBA is a type of advertising which shows ads of interest to a user instead of other less relevant ads because advertisers guess and predict the likely interests of a user based on the information they have collected. IBA requires data of users to make guesses about user's interests, but it violates the privacy of user's data. In such situations, Federated Leaning comes to our rescue. Federated Learning models will predict the user's interest-based ads thus showing ads of interest to a user on his device instead of less relevant ads, without exposing the user's data. [19]

5.10 Sixth Generation (6G) Wireless Networks: For the development of sixth-generation (6G) wireless networks Machine Learning plays an important role. The Centralized machine learning techniques violate data privacy and cause transmission delays for transmitting huge amounts of data. The emerging future applications like self-driving vehicles, unmanned aerial vehicles, smart environments, smart underwater communication, smart automation & manufacturing, Haptic Communication, etc., will require *low latency and privacy features*. Optimising these applications using centralized machine learning techniques will not be possible. So Federated Learning will be a desirable solution to optimise these emerging future applications because it won't transfer any data from these applications to a central server thus getting rid of transmission delays and providing privacy to data of these applications. [20, 21]

6. Challenges of Federated Learning

6.1 Challenge – 1: Expensive Communication

Reason: In a Federated Machine Learning Network we can have millions of devices connected, which increases the size of the network. Since it is a decentralized approach so all the computations on data will be carried out locally. The speed with which the individual computations are done on local data can be faster than the network communication speed itself resulting inexpensive communication. [22]

Possible solutions: These are the possible solutions:

- The information from localized machine learning models should be compressed first and then exchanged with the central machine learning model. [22, 1]
- Reducing the number of times, the learnings from local ML models are exchanged with the central ML model. [22, 1]

6.2 Challenge – 2: System Heterogeneity:

Reason: The Federated network consists of a huge number of varied devices that will have different hardware, power, network connectivity, storage, & computational capabilities. In addition to these differences' other constraints like device drop-outs, unreliable devices also create hurdles for the smooth and proper working of Federated Learning. [1]

Possible solutions: The possible solutions to handles these problems can be:

- Federated Learning models should be tolerant to differences in hardware, power, network connectivity, storage, & computational capabilities of devices in the Federated network. [22]
- Federated Learning models should be "… robust to devices dropping out of the network". [1, p. 12] [22]
- Federated Learning models should be having the information of low participation of devices in a particular round of training. [22]

6.3 Challenge – 3: Algorithm Challenges

Reason: Since the majority of the ML algorithms are of Centralized nature, they won't work with Federated Learning Models because here no data is exchanged with the central server instead the Federating Learning Model is trained locally. [1] [22]

Possible solutions: New algorithms can be developed which will work with Federated Learning Model. [1] [22]

6.4 Challenge – 4: Privacy Concerns

Reason: Federated Learning is a privacy-preserving technique but even it has some privacy issues. Even though it doesn't share data with the central server but it does share the 'learnings or local updates from the training of a local ML model' with the Central server. These learnings can expose sensitive information associated with the users of a Federated Network. [1] [22]

Possible solutions:

While sharing the 'learnings or local updates' with the Central server, *homomorphic encryption* can be used to encrypt this 'learning' so that the computation performed in the central server will be on encrypted 'learning'.

While sharing the 'learnings or local updates' with the Central server, *differential privacy* can be applied to that 'learning' by adding a little noise or disturbance in the learning of each iteration, which means that the central server can't draw any conclusion regarding which sample data has been used to train the local model in that iteration. But adding too much noise can make the model less accurate even though it will improve privacy. So, a balance should be found between differential privacy and the accuracy of the model. [1] [22]

6.5 Challenge – 5: Statistical Heterogeneity

Reason: The Federated network consists of a large number of varied devices that will have different hardware, power, network connectivity, storage, & computational capabilities. These devices generate data that is not distributed identically across these devices. Each device generates data that varies substantially. The data points from these devices vary substantially. Analysing, modelling and evaluating these data points is complex. This affects the overall performance of the model. [1] [22]

Possible solutions: "Both the multi-task and meta-learning perspectives enable *personalized* or *device-specific* modeling, which is often a more natural approach to handle the statistical heterogeneity of the data". [22, p. 4]

7. Security concerns of Federated Learning

Just like any other machine learning techniques Federated Learning can also have security issues.

7.1 Security Concern – 1: Data Poisoning Attacks

These attacks involve an opponent who poisons the local data of some devices which are training their local learning models. After the local training is completed, each device will send its learnings to the central learning model. The accuracy of the central learning model gets compromised because the learnings (from the training of local models) carried the poison to the central model. [8] [1] [22]

Possible solutions:

In each training iteration, identify the poisoned devices based on their learnings/updates before sending their learnings to the Central learning model. [8] [1] [22]

7.2 Security Concern – 2: Model Poisoning Attacks

These attacks involve an opponent who poisons the local models of some devices instead of data. The attacker changes some of the parameters of the local machine learning model. After these devices train their data on these poisoned models, each device will send their learnings to the central learning model. The accuracy of the central learning model gets compromised because the learnings (from the training of poisoned local models) carried the poison to the Central learning model. [8] [1] [22]

Possible solutions: In each training iteration, identify the devices whose local models have been poisoned based on their learnings/updates before sending their learnings to the Central learning model. [8] [1] [22]

7.3 Security Concern – 3: Membership Inference Attacks

These attacks involve drawing conclusions regarding which sample data has been used to train a local model in a particular iteration. The attacker in this way can know about the sample data of a device based on its local model update. This attack is carried out when 'learnings from training a local machine learning model' are shared with the Central learning model. [8] [1] [22]

Possible solutions: When the local learnings are being shared with the Central learning model, apply *differential privacy* on that learning by adding a little noise or disturbance in the learning of each iteration, which means that the attacker can't draw any conclusion regarding which sample data has been used to train the local model in that iteration. Too much noise can make the model less accurate, so a balance should be found between differential privacy and accuracy of the model. [8] [1] [22]

7.4 Security Concern – 4: Backdoor Attacks

While sharing the 'learnings from training a local machine learning model' with the Central learning model, *secure averaging* is used to keep the identity of devices secure.
These attacks involve the attacker using the same *'secure averaging'* to introduce a backdoor into the central learning model. The attacker uses this backdoor to change some task labels without affecting the accuracy of the central learning model. [8] [1] [22]

Possible solutions:

While sharing the 'learnings' with the Central learning model, differential privacy can be applied to the 'learning' of each device by adding a little noise or disturbance in the learnings of each device in each iteration. It can be done at the cost of the performance of the central learning model. [8] [1] [22]

8. Conclusion & Future Directions

Federated Learning being a decentralized Machine Learning technique provides a better way to address the problems of Centralized machine learning techniques. It provides the user's data privacy, direct access to their data, the lesser load on the central server as well as on the communication network. Being a decentralized technique, it faces various challenges during implementation, those challenges are addressed by certain solutions but new research can be conducted to tackle these challenges in a better and more efficient way. Just like any other machine learning technique, it is also prone to attacks, even though some solutions exist that protect against these attacks to some extent but the research area is open in this field to find new ways to tackle these attacks efficiently. Since the future is for Artificial Intelligence & faster networks, Federated Learning will bring most out of these technologies in a privacy-focused way.

Acknowledgement

I contend and am thankful to my supervisor, Dr Ihtiram Raza Khan Assistant (Professor in Jamia Hamdard) for helping, inspiring, & encouraging me in completing my research work on "A review of Federated Learning".

References

[1] D. Jatain, V. Singh and N. Dahiya, "A contemplative perspective on federated machine learning: Taxonomy,threats & vulnerability assessment and challenges," *Journal of King Saud University – Computer and Information Sciences,* 2021.

[2] "What Really Caused Facebook's 500M-User Data Leak?," 04 June 2021. [Online]. Available: https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/. [Accessed 03

December 2021].

[3] "Data Privacy Standards Issued in India – Legal Compliance or New Brand Differentiator?," The National Law Review, [Online]. Available: https://www.natlawreview.com/article/data-privacy-standards-issued-india-legal-compliance-or-new-brand-differentiator. [Accessed 01 December 2021].

[4] "The Information Technology Act, 2000," India Code Digital Repository of All Central and State Acts, [Online]. Available: https://www.indiacode.nic.in/handle/123456789/1999. [Accessed 10 October 2021].

[5] S. Prakash and S. Avestimehr, "Mitigating Byzantine Attacks in Federated Learning," *arXiv preprint arXiv:2010.07541,* 2020.

[6] G. Drainakis, K. V. Katsaro, P. Pantazopoulos, V. Sourlas and A. Amditis, "Federated vs. Centralized Machine Learning under Privacy-elastic Users: A Comparative Analysis," in *IEEE 19th International Symposium on Network Computing and Applications (NCA), 2020, pp. 1-8,*, 2020.

[7] A. Gupta, "How Federated Learning is going to revolutionize AI," towards data science, [Online]. Available: https://towardsdatascience.com/how-federated-learning-is-going-to-revolutionize-ai-6e0ab580420f. [Accessed 10 November 2021].

[8] P. M. Mammen, "Federated Learning: Opportunities and Challenges.," *arXiv preprint arXiv:2101.05428,* 2021.

[9] "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST),* vol. 10, no. 2, pp. 1-19, 2019.

[10] S. Li, J. Xia, W. Wang, F. Yan, Y. Liu and C. Zhang, "Batchcrypt: Efficient homomorphic encryption for cross-silo federated learning.," in *{USENIX} Annual Technical Conference ({USENIX}{ATC} 20)*, 2020.

[11] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji and K. Bonawitz, "Advances and Open Problems in Federated Learning," *arXiv preprint arXiv:1912.04977,* 2019.

[12] M. Aledhari, R. Razzak, R. M. PARIZI and F. SAEED, "Federated learning: A survey on enabling technologies, protocols, and applications.," *IEEE Access,* vol. 8, pp. 140699-140725, 2020.

[13] "Google Translate," [Online]. Available: https://translate.google.co.in/. [Accessed 05 November 2021].

[14] "speech recognition," [Online]. Available: https://searchcustomerexperience.techtarget.com/definition/speech-recognition. [Accessed 05 November 2021].

[15] “Google Assistant,” [Online]. Available: https://assistant.google.com/. [Accessed 05 November 2021].

[16] “Alexa,” [Online]. Available: https://developer.amazon.com/en-US/alexa. [Accessed 05 November 2021].

[17] “voice recognition (speaker recognition),” [Online]. Available: https://searchcustomerexperience.techtarget.com/definition/voice-recognition-speaker-recognition. [Accessed 06 November 2021].

[18] X. Chen, B. Xiao, Q. Xu, C. He and J. Lin, “Block-chain based federated learning for knowledge capital,” *Procedia Computer Science,* vol. 187, pp. 426-431, 2021.

[19] “What is "interest-based" advertising?,” [Online]. Available: https://bbbaccountabilityprogram.freshdesk.com/support/solutions/articles/35000046312-what-is-interest-based-advertising-. [Accessed 10 November 2021].

[20] M. Z. Chowdhury, M. Shahjalal, S. Ahmed and Y. M. Jang, “6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions.,” *IEEE Open Journal of the Communications Society,* vol. 1, pp. 957-975, 2020.

[21] Z. Yang, M. Chen, K.-K. Wong, H. V. Poor and S. Cui, “Federated Learning for 6G: Applications, Challenges, and Opportunities,” *Engineering,* 2021.

[22] T. Li, A. K. Sahu, A. Talwalkar and V. Smith, “Federated Learning:Challenges, Methods, and Future Directions,” *IEEE Signal Processing Magazine,* vol. 37, no. 3, pp. 50-60, 2020.

[23] B. McMahan, E. Moore, D. Ramage, S. Hampson and B. Aguera y Arcas, “Communication-efficient learning of deep networks from decentralized data.,” in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics in Proceedings of Machine Learning Research*, 2017.