IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Special Issue 1, April 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Federated Concept Based Machine Learning Technology

Eega Varnika[1], Dr.G.Madhavi[2]

Department of Computer Science, Chaitanya Deemed to Be University, Warangal, Telangana, India[1]

Assistant Professor, Dept. of Computer Science, Chaitanya Deemed to Be University, Warangal, Telangana, India[2]

ABSTRACT*:* in this paper discus the based on AI still faces two major challenges. One is that, in most industries, the data exists in the form of isolated islands. The other is strengthening data privacy and security. We propose a possible so solution to these challenges: secure federated learning. Beyond the first proposed federated learning framework by Google in 2016, we introduced a comprehensive and secure federated learning framework, including horizontal federated learning, vertical federated learning, and federated transfer learning. We provide definitions, architectures and applications for the federated learning framework, and provide a comprehensive survey of the existing works on this topic. In addition, we propose to build data networks between organizations based on federated mechanisms as an effective solution to allow knowledge to be shared without compromising user privacy

I. INTRODUCTION

To be more specific, traditional data-processing models in AI often involve simple datatransaction models, with one party collecting and transferring data to another party and the otherparty being responsible for cleaning and fusing the data. Finally a third party will take the integrated data and build models for still other parties to use. The models are usually the final productsthat are sold as a service. This traditional procedure face challenges with the above new data regulations and laws. As well, since users may be unclear about the future uses of the models, thetransactions violate laws such as the GDPR. As a result, we face a dilemma that our data is in theform of isolated islands, but we are forbidden in many situations to collect, fuse, and use the datain different places for AI processing. How to legally solve the problem of data fragmentation andisolation is a major challenge for AI researchers and practitioners today.

In promoting federated learning, we hope to shift the focus of AI development from improving model performance, which is what most of the AI field is currently doing, to investigating methods for data integration that are compliant with data privacy and security laws.

Literature Survey: To extend the concept of federated learning to covercollaborative-learning scenarios among organizations, we extend the original "federated learning" to a general concept for all privacy-preserving decentralized collaborative machine-learning techniques. We have given a preliminary overview of the federated-learning and federatedtransfer-learning technique. In this article, we further survey the relevant security foundations andexplore the relationship with several other related areas, such as multiagent theory and privacypreserving data mining. In this section, we provide a more comprehensive definition of federatedlearning that considers data partitions, security, and applications. We also describe work flow andsystem architecture for the federated-learning system.

Federated learning enables multiple parties to collaboratively construct a machinelearning modelwhile keeping their private training data private. As a novel technology, federated learning hasseveral threads of originality, some of which are rooted on existing fields. Below, we explain therelationship between federated learning and other related concepts from multiple perspectives.

II. PROPOSED FEDERATED METHOD

Privacy-Preserving Machine Learning: Federated learning can be considered as privacy-preserving, decentralized collaborative machinelearning. Therefore, it is tightly related to multiparty, privacy-preserving machine learning. Manyresearch efforts have been devoted to this area in the past.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 11, Special Issue 1, April 2022
9th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '22)
28 th -29 th April 2022
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Federated Learning versus Distributed Machine Learning: Horizontal federated learning at first sight is somewhat similar to distributed machine learning.Distributed machine learning covers many aspects, including distributed storage of training data,distributed operation of computing tasks, and distributed distribution of model results.
Federated Learning versus Edge Computing: Federated learning can be seen as an operating system for edge computing, as it provides thelearning protocol for coordination and security.As in distributed machine-learning settings, federated learning will also need to address non-IID data. The non-IID local data, performance can be greatly reducedfor federated learning. The authors in response supplied a new method to address the issue similarto transfer learning.
Federated Learning versus Edge ComputingFederated learning can be seen as an operating system for edge computing, as it provides thelearning protocol for coordination and security. The authors of considered a generic class ofmachine-learning models that are trained using gradient descent–based approaches. They analyse the convergence bound of distributed gradient descent from a theoretical point of view, based onwhich they propose a control algorithm that determines the best trade-off between local updateand global parameter aggregation to minimize the loss function under a given resource budget.Federated Learning versus Federated Database Systems: Federated database systems are systems that integrate multiple database units and manage theintegrated system as a whole. The federated database concept is proposed to achieve interoperability with multiple independent databases.

IV. CONCLUSION

In this paper, recently, the isolation of data and the emphasis on data privacy became the next challenges for AI,but federated learning has brought us new hope. It could establish a united model for multiple enterprises while local data is protected so that enterprises could work together on data security. Thisarticle generally introduces the basic concept, architecture, and techniques of federated learning,and discusses its potential. It is expected that, in the near future, federatedlearning would break the barriers between industries and establish a community where data andknowledge could be shared with safety and the benefits would be fairly distributed according tothe contribution of each participant. The bonus of AI would finally be brought to every corner ofour lives

REFERENCES

1. Le Trieu Phong, and Lihua Wang. 2016. Scalable and secure logistic regression viahomomorphic encryption. ACM Conference on Data and Application Security and Privacy, 142–144.
2. Yehuda Lindell, Ariel Nof, and Kazuma Ohara. 2016. High-throughput semi-honest se-cure three-party computation with an honest majority. In Proceedings of the 2016 ACM SIGSAC Conference on Computerand Communications Security . ACM, New York, NY, 805–817. Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. 2018. How To BackdoorFederated Learning.
3. Guillaume Scerri, andBogdan Warinschi. 2017. Secure multiparty computation from SGX. Financial Cryptography. 477–497.
4. Dan Bogdanov, Sven Laur, and Jan Willemson. 2008. Sharemind: A framework for fast privacy-preserving com-putations. In Proceedings of the 13th European Symposium on Research in Computer Security: Computer SecuritySpringer, Berlin, 192–206.
5. Yang Liu And Tianjian Chen,Federated Machine Learning,ACM Transactions on Intelligent Systems and Technology, January 2019.
6. Aaron Segal, and Karn Seth. 2017. Practical secure aggregation for privacy-preserving machine learning.In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details