IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, May 2023

Verifiable Secret Sharing Scheme Using Deep Learning Framework In Cloud Environment

Geetha T[1], Hariharan P[2], Matheshwaran K[3], Hariharan B[4], Mohamed Hisham R[5]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4,5]
Dhanalakshmi Srinivasan Engineering College, Perambalur, India

Abstract: *Cross-device federated learning is a machine learning approach that enables multiple devices to collaboratively train a model without sharing their data with each other. This approach is particularly useful in medical settings where data privacy and security are paramount. In this context, medical data is sensitive and protected by law. Federated learning can help to preserve the privacy of medical data while still allowing for the development of models that can be used to improve patient outcomes. One challenge with federated learning is the need to protect the model during training and inference. Model encryption is a technique that can be used to protect the model from unauthorized access. Elliptic Curve Cryptography (ECC) is a form of encryption that is well-suited for federated learning due to its ability to efficiently encrypt and decrypt data. In this project, propose a cross-device federated learning approach that utilizes medical datasets to build a predictive model. We also employ ECC to encrypt the model during training and inference. Divide the medical dataset into subsets that are distributed across multiple devices. Train the model collaboratively across all devices using federated learning techniques. Then use ECC to encrypt the trained model to protect it from unauthorized access. The proposed system also provides a more accurate prediction of disease risk while preserving patient confidentiality. The results show that the SVM-based model can achieve high accuracy in predicting disease risk, and the encrypted data can be used effectively to train the model without compromising patient privacy. Additionally, our use of ECC encryption provides an extra layer of security for the model, ensuring that it remains protected during training and inference.*

Keywords: Federated Learning, Medical Data, Eliptic Curve Cryptography, Security And Privacy

REFERENCES

[1]. Fu, Anmin, Xianglong Zhang, Naixue Xiong, Yansong Gao, Huaqun Wang, and Jing Zhang, (2020) "VFL: A verifiable federated learning with privacy-preserving for big data in industrial IoT." IEEE Transactions on Industrial Informatics 18, no. 5 (2020): 3316-3326.

[2]. Guo, Xiaojie, Zheli Liu, Jin Li, Jiqiang Gao, Boyu Hou, Changyu Dong, and Thar Baker, (2020) "VeriFL: Communication-efficient and fast verifiable aggregation for federated learning." IEEE Transactions on Information Forensics and Security 16 (2020): 1736-1751.

[3]. Lei Yu, Ling Liu, Calton Pu, Mehmet Emre Gursoy, Stacey Truex, (2019) "Differentially Private Model Publishing for Deep Learning"

[4]. Melis, Luca, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov,(2018) "Exploiting unintended feature leakage in collaborative learning." In 2019 IEEE symposium on security and privacy (SP), pp. 691-706. IEEE, 2019.

[5]. Peng, Zhe, Jianliang Xu, Xiaowen Chu, Shang Gao, Yuan Yao, Rong Gu, and YuzheTang,(2021) "Vfchain: Enabling verifiable and auditable federated learning via blockchain systems." IEEE Transactions on Network Science and Engineering 9, no. 1 (2021): 173-186.

[6]. Sav, Sinem, Apostolos Pyrgelis, Juan R. Troncoso-Pastoriza, David Froelicher, Jean-Philippe Bossuat, Joao Sa Sousa, and Jean-Pierre Hubaux,(2021) "Poseidon: Privacy-preserving federated neural network learning." arXiv preprint arXiv:2009.00349 (2020).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, May 2023

[7]. Shai Halevi,NaliniRatha, Sharath Pankanti,Karthik Nandakumar, (2020) "Towards Deep Neural Network Training on Encrypted Data"

[8]. Sheller, Micah J., Brandon Edwards, G. Anthony Reina, Jason Martin, Sarthak Pati, AikateriniKotrotsou, Mikhail Milchenko et al,(2020) "Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data." Scientific reports 10, no. 1 (2020): 1-12.

[9]. Tian L,MaziarSanjabi,AhmadBeirami,Virginia Smith, (2020) "Fair resource allocation in federated learning Fair resource allocation in federated learning"

[10]. Tomer Gafni, Nir Shlezinger, Kobi Cohen, Yonina C. Eldar, and H. Vincent Poor, (2021) "Federated Learning: A Signal Processing Perspective"