Title

A Chaotic Maps-Based Privacy-Preserving Distributed Deep Learning for Incomplete and Non-IID Datasets

Abstract

Federated Learning is a machine learning approach that enables the training of a deep learning model among several participants with sensitive data that wish to share their own knowledge without compromising the privacy of their data. In this research, the authors employ a secured Federated Learning method with an additional layer of privacy and proposes a method for addressing the non-IID challenge. Moreover, differential privacy is compared with chaotic-based encryption as layer of privacy. The experimental approach assesses the performance of the federated deep learning model with differential privacy using both IID and non-IID data. In each experiment, the Federated Learning process improves the average performance metrics of the deep neural network, even in the case of non-IID data.

Authors

Arévalo I.; Salmeron J.L.

Author full names

Arévalo, Irina (56600586400); Salmeron, Jose L. (7005863394)

Author(s) ID

56600586400; 7005863394

Year

2024

Source title

IEEE Transactions on Emerging Topics in Computing

Volume

12.0

Issue

1

Page start

357

Page end

367

Page count

10.0

DOI

10.1109/TETC.2023.3320758

Link

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85174805147&doi=10.1109%2fTETC.2023.3320758&partnerID=40&md5=d651ee42701527d5e4df7e34c6dfe2f0

Affiliations

Universidad Pablo de Olavide, Sevilla, 41013, Spain; CUNEF Universidad, Madrid, 28040, Spain; Universidad Autónoma de Chile, San Miguel, 8910123, Chile

Authors with affiliations

Arévalo I., Universidad Pablo de Olavide, Sevilla, 41013, Spain; Salmeron J.L., CUNEF Universidad, Madrid, 28040, Spain, Universidad Autónoma de Chile, San Miguel, 8910123, Chile

Author Keywords

Federated learning; non-IID datasets; privacy-preserving machine learning

Index Keywords

Chaotic systems; Deep neural networks; Privacy-preserving techniques; Sensitive data; Computational modelling; Differential privacies; Federated learning; Learning models; Machine-learning; Non-IID dataset; Privacy preserving; Privacy-preserving machine learning; Proposal; Computer architecture

References

Abadi M., Et al., Deep learning with differential privacy, Proc. 23rd ACMConf. Comput. Commun. Secur., pp. 308-318, (2016); Acar A., Aksu H., Uluagac S., Conti M., A survey on homomorphic encryption schemes: Theory and implementation, ACM Comput. Surv., 51, (2017); Bagdasaryan E., Veit A., Hua Y., Estrin D., Shmatikov V., How to backdoor federated learning, Proc. 23rd Int. Conf. Artif. Intell. Statist., pp. 2938-2948, (2020); Chen Y., Ning Y., Slawski M., Rangwala H., Asynchronous online federated learning for edge devices with non-IID Data, Proc IEEE Int. Conf. Big Data, pp. 15-24, (2020); Cheng K., Et al., SecureBoost: A Lossless Federated Learning Framework, (2019); Cheng Y., Liu Y., Chen T., Yang Q., Federated learning for privacypreserving AI, Commun. ACM, 63, 12, pp. 33-36, (2020); Dua D., Graff C., UCI Machine Learning Repository, (2017); Duan J., Zhou J., Li Y., Huang C., Privacy-preserving and verifiable deep learning inference based on secret sharing, Neurocomputing, 483, pp. 221-234, (2022); Esteva A., Et al., Dermatologist-level classification of skin cancer with deep neural networks, Nature, 542, 7639, pp. 115-118, (2017); Gao D., Ju C., Wei X., Liu Y., Chen T., Yang Q., HHHFL:Hierarchical Heterogeneous Horizontal Federated Learning for Electroencephalography, (2019); Goodfellow I.J., Bengio Y., Courville A., Deep Learning, (2016); Guerrero-Gomez-Olmedo R., Salmeron J.L., Kuchkovsky C., LRP-based path relevances for global explanation of deep architectures, Neurocomputing, 381, pp. 252-260, (2020); Hu R., Guo Y., Li H., Pei Q., Gong Y., Privacy-preserving personalized federated learning, Proc. IEEE Int. Conf. Commun., pp. 1-6, (2020); Ibitoye O., Abou-Khamis R., El Shehaby M., Matrawy A., Shafiq M.O., The Threat of Adversarial Attacks on Machine Learning in Network Security-A Survey, (2023); Kaissis G., Makowski M., Ruckert D., Braren R., Secure, privacypreserving and federated machine learning in medical imaging, Nat. Mach. Intell., 2, pp. 305-311, (2020); Konecny J., McMahan B., Ramage D., Richtarik P., Federated Optimization: Distributed Machine Learning for On-device Intelligence, (2016); Lecun Y., Bengio Y., Hinton G., Deep learning, Nature, 521, pp. 436-444, (2015); Lee S., Lacy M.E., Jankowich M., Correa A., Wu W.C., Association between obesity phenotypes of insulin resistance and risk of type 2 diabetes in african americans: The Jackson heart study, J. Clin. Transl. Endocrinol., 19, 3, (2020); Liu Y., Kang Y., Xing C., Chen T., Yang Q., A secure federated transfer learning framework, IEEE Intell. Syst., 35, 4, pp. 70-82, (2020); McMahan B., Moore E., Ramage D., Aguera B., Federated Learning of Deep Networks Using Model Averaging, (2016); McMahan B., Ramage D., Google AI Blog, (2017); McMahan H.B., Moore E., Ramage D., Hampson S., Arcas B.A., Communication-efficient learning of deep networks from decentralized data, Proc. 20th Int. Conf. Artif. Intell. Statist., 54, pp. 1273-1282, (2017); Ramos S., Gehrig S., Pinggera P., Franke U., Rother C., Detecting unexpected obstacles for self-driving cars: Fusing deep learning and geometric modeling, Proc. IEEE Intell. Veh. Symp., pp. 1025-1032, (2017); Street W., Wolberg W., Mangasarian O., Breast cancer diagnosis and prognosis via linear programming, Oper. Res., 43, 4, pp. 570-577, (1995); Street W., Wolberg W., Mangasarian O., Nuclear feature extraction for breast tumor diagnosis, Electronic Imaging, (1999); Wang H., Kaplan Z., Niu D., Li B., Optimizing federated learning on non-IID data with reinforcement learning, Proc. IEEE Conf. Comput. Commun., pp. 1698-1707, (2020); Wang Z., Song M., Zhang Z., Song Y., Wang Q., Qi H., Beyond inferring class representatives: User-level privacy leakage from federated learning, Proc. IEEE

Conf. Comput. Commun., pp. 2512-2520, (2019); Wei K., Et al., Federated learning with differential privacy: Algorithms and performance analysis, IEEE Trans. Inf. Forensics Secur., 15, pp. 3454-3469, (2020); Yang Q., Liu Y., Cheng Y., Kang Y., Chen T., Yu H., Federated Learning, (2019); Zhang C., Xie Y., Bai H., Yu B., Li W., Gao Y., A survey on federated learning, Knowl.-Based Syst., 216, (2021); Zhao Y., Suda N., Li M., Civin D., Lai L., Chandra V., Federated Learning with Non-IID Data: A Metric Learning Approach, (2018); Zhu H., Xu J., Liu S., Jin Y., Federated learning on non-IID data: A survey, Neurocomputing, 465, pp. 371-390, (2021); Zia U., Et al., Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains, Int. J. Inf. Secur., 21, 4, pp. 917-935, (2022)

Correspondence Address

I. Arévalo; Universidad Pablo de Olavide, Sevilla, 41013, Spain; email: iarebar@alu.upo.es

Publisher

IEEE Computer Society

ISSN

21686750

Language of Original Document

English

Abbreviated Source Title

IEEE Trans. Emerg. Top. Comput.

Document Type

Article

Publication Stage

Final

Open Access

All Open Access; Green Open Access

Source

Scopus

EID

2-s2.0-85174805147