Enhancing Data Integrity, Confidentiality and Authenticity with Digital Envelopes and Federated Learning

Mario Alberto da Silveira Dib[1*], **Pedro Prates**[2,3], **Bernardete Ribeiro**[4]

[1] Centre for Informatics and Systems of the University of Coimbra (CISUC), Polo II – Pinhal de Marrocos, 3030-290 Coimbra, Portugal
[2] Department of Mechanical Engineering, University of Aveiro, 3810-193 Aveiro, Portugal
[3] CEMMPRE, Department of Mechanical Engineering, Univ Coimbra, 3030-788 Coimbra, Portugal
[4] Centre for Informatics and Systems of the University of Coimbra (CISUC), Department of Informatics Engineering, Polo II – Pinhal de Marrocos, 3030-290 Coimbra, Portugal

* mariodib@outlook.com

Recent concerns with data privacy in machine learning have led to the development of privacy-preserving machine learning methods, such as Federated Learning [1]. This method involves multiple parties to privately train local machine learning models with their own data, sharing with the global server only the models' parameters that will be averaged to update the global model. Such environments are constantly at the risk of suffering cyber-attacks that can compromise the information used in the process and/or the complete machine learning training. One of those attacks are known as data poisoning [2], which is a threat to most machine learning models, in particular for the federated learning method, because of the communication design and the different nodes participating in the training. In this work, it was investigated the application of Digital Envelopes [3] combined with Federated Learning, to improve data integrity and authenticity in order to prevent the machine learning models to be training with poisoned data. Also, this combination improves the confidentiality by assuring the information is not made available or disclosed to unauthorized individuals or entities. The proposed approach was able to identify when the dataset was compromised by a corrupted agent, that impacted the results of the machine learning and prevented the specific dataset to participate in the training process.

References

[1] H. B. McMahan & E. Moore & D. Ramage & S. Hampson & B. A. Arcas (2016) Communication-Efficient Learning of Deep Networks from Decentralized Data. arXiv https://arxiv.org/abs/1602.05629

[2] G. Sun & Y. Cong & J. Dong & Q. Wang & J. Liu (2020) Data Poisoning Attacks on Federated Machine Learning. arXiv. https://arxiv.org/abs/2004.10020

[3] S. Pérez & J. L. Hernández-Ramos & D. Pedone & D. Rotondi & L. Straniero & A. F. Skarmeta (2017) A digital envelope approach using attribute-based encryption for secure data exchange in IoT scenarios. Global Internet of Things Summit (GIoTS), Geneva, pp. 1-6. https://doi.org/10.1109/GIOTS.2017.8016281.