PROC. INTERNAT. CONF. SCI. ENGIN. ISSN 2597-5250
Volume 3, April 2020 | Pages: xix-xix E-ISSN 2598-232X

KEYNOTE SPEECH

Techniques and Challenges while Applying Machine Learning Algorithms in Privacy Preserving Fashion

Artrim Kjamilji
Faculty of Engineering and Natural Sciences, Computer Science and Engineering, Sabancı University, Istanbul-Turkey
Email: artrimk@sabanciuniv.edu

Abstract. Nowadays many different entities collect data of the same nature, but in slightly different environments. In this sense different hospitals collect data about their patients' symptoms and corresponding disease diagnoses, different banks collect transactions of their customers' bank accounts, multiple cyber-security companies collect data about log files and corresponding attacks, etc. It is shown that if those different entities would merge their privately collected data in a single dataset and use it to train a machine learning (ML) model, they often end up with a trained model that outperforms the human experts of the corresponding fields in terms of accurate predictions. However, there is a drawback. Due to privacy concerns, empowered by laws and ethical reasons, no entity is willing to share with others their privately collected data. The same problem appears during the classification case over an already trained ML model. On one hand, a user that has an unclassified query (record), doesn't want to share with the server that owns the trained model neither the content of the query (which might contain private data such as credit card number, IP address, etc.), nor the final prediction (classification) of the query. On the other hand, the owner of the trained model doesn't want to leak any parameter of the trained model to the user. In order to overcome those shortcomings, several cryptographic and probabilistic techniques have been proposed during the last few years to enable both privacy preserving training and privacy preserving classification schemes. Some of them include anonymization and k-anonymity, differential privacy, secure multiparty computation (MPC), federated learning, Private Information Retrieval (PIR), Oblivious Transfer (OT), garbled circuits and/or homomorphic encryption, to name a few. Theoretical analyses and experimental results show that the current privacy preserving schemes are suitable for real-case deployment, while the accuracy of most of them differ little or not at all with the schemes that work in non-privacy preserving fashion.