Towards Scalable, Efficient and Privacy Preserving Machine Learning

Rania Talbi, Sara Bouchenak

To cite this version:


HAL Id: hal-01956155
https://hal.science/hal-01956155
Submitted on 14 Dec 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Context and Motivation

- Minimize the computational costs incurred by privacy preservation.
- Provide an end-to-end privacy preserving outsourced data classification service.
- Enable a set of mutually untrusted data owners to have a global vision on the union of their data without breaching the privacy of each one of them.
- Enable dynamic data model updates when new training data samples are available.

Objectives

- We have used a synthetic dataset for fraud detection in a B2B network.
- This dataset contains 1000 bank transactions with 9 attributes each.
- We compare our work to the Ciphermed framework [8].

Related work

Different ML algorithms
- Clustering
- Classification
- Association Rule Mining
- ML output protection
- Original data protection

Different Privacy-preservation objectives
- Cryptographic techniques (SMC/HE, GC, OT)
- Non-cryptographic techniques (PP-Data Publishing techniques)

Design principles

- Cryptographic based protection (data model, training data, classification queries and responses)
- Partial homomorphic encryption (PHE) based building blocks
- Combine PHE with cryptographic blinding (DTPKC cryptosystem [6])
- We implemented the VFDT incremental decision tree learning algorithm [7]

References

3. Liu et al.: Privacy-Preserving Mining of Association Rule on Outsourced Data from Multiple Parties. NDSS 2018: 413-415
8. R.Bast et al.: Machine Learning Classification over Encrypted Data. NDSS 2015