Towards Scalable, Efficient and Privacy Preserving
Machine Learning
Rania Talbi, Sara Bouchenak

To cite this version:
Rania Talbi, Sara Bouchenak. Towards Scalable, Efficient and Privacy Preserving Machine Learning, Middleware ’18 Doctoral Symposium, Dec 2018, Rennes, France. <hal-01956155>

HAL Id: hal-01956155
https://hal.archives-ouvertes.fr/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.
Preliminary results

- 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 Ciphered framework [8].

References


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

Related work

Different ML algorithms

- Clustering
- Classification
- Association Rule Mining

Different Privacy-preservation objectives

- ML output protection
- Original data protection

Privacy Preservation techniques

Non-cryptographic techniques (PP-Data Publishing techniques)

Cryptographic techniques (SMC/HE, GC, OT)

Different architectures

- Distributed
- Outsourced

Naive approach: a combination of low level PP-building blocks

1st optimization: use inline building blocks

2nd optimization: Parallel computing