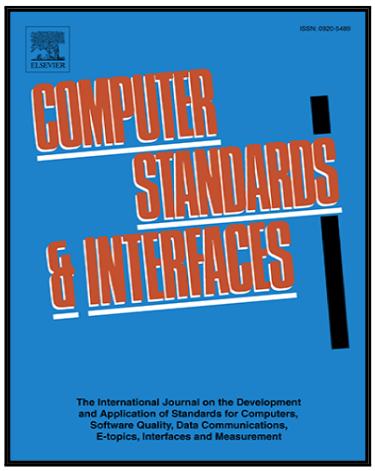

Efficient Machine Learning over Encrypted Data with Non-interactive Communication

Heejin Park, Pyung Kim, Heeyoul Kim, Ki-Woong Park, Younho Lee

PII: S0920-5489(17)30271-4
DOI: 10.1016/j.csi.2017.12.004
Reference: CSI 3258

To appear in: *Computer Standards & Interfaces*

Received date: 12 July 2017
Revised date: 8 December 2017
Accepted date: 8 December 2017

Please cite this article as: Heejin Park, Pyung Kim, Heeyoul Kim, Ki-Woong Park, Younho Lee, Efficient Machine Learning over Encrypted Data with Non-interactive Communication, *Computer Standards & Interfaces* (2017), doi: 10.1016/j.csi.2017.12.004

Highlights

- A privacy-preserving machine learning protocol framework is proposed.
- The proposed protocol preserves the privacy of model, user input, and classification output.
- We realized the Naive-Baysian classification protocol on our framework.
- We utilized Fully Homomorphic Encryption only for implementation.
- The proposed supports higher security and communication efficiency.