Privacy Preserving Neural Network Classification: A Hybrid Solution

Gamze Tillem[1], Beyza Bozdemir[2], Melek Önen[2], and Orhan Ermis[2]

[1] Delft University of Technology, Delft, The Netherlands
G.Tillem@tudelft.nl
[2] EURECOM, Sophia Antipolis, France
{Beyza.Bozdemir, Melek.Onen, Orhan.Ermis}@eurecom.fr

Despite the advantages of big data technologies in extracting valuable information from data, the continuous increase in the amount of big data brings out a burden of dealing with high storage cost and computationally intensive tasks for the organizations. Although cloud computing-based solutions provide services for outsourcing this large amount of data and delegating computation to powerful servers, organizations face another challenging issue: ensuring the privacy of the outsourced data. Advanced privacy enhancing technologies (PETs) can help overcome this issue and enable third parties to execute data analytics over the encrypted version of the outsourced data. Particularly, classification using neural network (NN) models that adopts advanced cryptographic techniques such as homomorphic encryption (HE) [1] or secure two-party computation (2PC) [2] schemes are instrumental examples for integrating PETs in data analytics. HE-based schemes are suitable for standalone execution of outsourced data; Yet they suffer from high computational cost and degraded prediction accuracy. On the other hand, 2PC-based schemes are able to operate with low computational cost and better prediction accuracy when compared to HE-based schemes. However, they imply additional a bandwidth usage. The idea is therefore, to come up with a combination of these two schemes to achieve a good balance between computational and communication costs while providing better prediction accuracy. In this work, we propose a privacy preserving NN classification protocol to securely compute NN predictions using an additive HE scheme (Paillier cryptosystem [3]) and 2PC in a harmony. The proposed protocol is able to operate in two different scenarios, namely the client-server and the non-colluding two-server scenarios, where they both provide security under the semi-honest model. Moreover, the empirical results show that our protocol outperforms state-of-the-art HE-based [1] and 2PC-based [2] protocols.

Keywords: Privacy · Neural Network · Homomorphic encryption · Secure two-party computation.

Acknowledgment

This work was partly supported by the PAPAYA project funded by the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no. 786767.

References

1. Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K.E., Naehrig, M., Wernsing, J.: Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In: Proceedings of the 33nd International Conference on Machine Learning, ICML, New York City, USA. pp. 201–210 (2016)
2. Liu, J., Juuti, M., Lu, Y., Asokan, N.: Oblivious neural network predictions via minionn transformations. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, USA. pp. 619–631. ACM, New York, NY, USA (2017)
3. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic. pp. 223–238 (1999)