PRIVACY PRESERVING ARRYHTMIA DETECTION WITH NEURAL NETWORKS

Melek Önen

EURECOM, Sophia-Antipolis, France

Artificial intelligence and machine learning have gained a renewed popularity thanks to the recent advances in information technology such as the Internet of Things that help collect, share and process data, easily. This powerful technology helps make better decisions and accurate predictions in many domains including healthcare. In particular, Neural Networks (NN) can support medical workers to analyse patients data and quickly diagnose a particular disease such as heart arrhythmia. Nowadays, heart arrhythmia can be detected at early stages with the help of smart wearable devices that can record electric heart activities using Electro-Cardiograms (ECG) data.

Nevertheless, ECG data is considered as very sensitive. Given the recent data breach scandals, stakeholders face increasing challenges with ensuring data privacy guarantees and compliance with the General Data Protection Regulation (GDPR). A study[1] concludes that in 2018, the global average cost of a data breach is 3.86 million dollars and the healthcare sector is the first sector facing huge costs. Therefore, there is an urgent need for tools enabling the protection of such data while still being able to launch predictive analytics and hence improve individuals lives.

Under the PAPAYA project[2] we aim at addressing privacy concerns when data analytics tasks are performed by untrusted third-party data processors. Since these tasks may be performed obliviously on protected data (i.e. encrypted data), the PAPAYA project develops dedicated privacy preserving data analytics modules that enable stakeholders to extract valuable information from this protected data, while being accurate [1, 2]. Among the analytics operations, we focus on Neural Network classifications and aim at addressing privacy concerns raised by the analysis of the ECG data for arrhythmia classification. Our goal is to enable service providers (data processors) perform classification without discovering the input (the ECG data). On the other hand, we also look into the problem from the service providers point of view as they care about keeping the design of their services confidential from the users (data subjects or data controllers). Users (such as doctors, pharmacists) using these systems/solutions should not be able to discover the details about the underlying system (such as the Neural Network model). The challenge often manifests as a choice between the privacy of the patients and the secrecy of the system parameters. We propose to combine the use of neural networks with secure two-party computation (2PC). Since 2PC protocols cannot efficiently support all kinds of operations, we propose to revisit the underlying neural network operations and design a new, customized neural network model that can be executed to classify arrhythmia accurately, and this, without disclosing neither the input ECG data to the service provider nor the neural network parameters to the users. The solution is implemented. Experimental results show an accuracy of 96.34% which outperforms existing solutions (for a full description of the solution, please see [3]).

This research study was conducted retrospectively using human subject data made available in open access by (https://www.physionet.org/physiobank/database/mitdb). Ethical approval was not required as confirmed by the license attached with the open access data.

1. REFERENCES

[1] E. Ciceri, M. Mosconi, M. Önen, and O. Ermis, "PAPAYA: A platform for privacy preserving data analytics," *ERCIM News*, , no. 118, July 2019.

[2] M. Azraoui, M. Bahram, B. Bozdemir, S. Canard, E. Ciceri, O. Ermis, Masalha R., M. Mosconi, M. Önen, M. Paindavoine, B. Rozenberg, B. Vialla, and S. Vicini, "SoK: Cryptography for Neural Networks," in *IFIP Summer School on Privacy and Identity Management*, 2019.

[3] M. Mansouri, B. Bozdemir, M. Önen, and O. Ermis, "PAC: Privacy-preserving ArrhythmiaClassification with neural networks," in *12th International Symposium on Foundations and Practice of Security(FPS*, 2019.

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

[1] https://www.ibm.com/security/data-breach

[2] www.papaya-project.eu