Privacy preserving fall detection using homomorphic encryption

Domen Vake[a], Niki Hrovatin[bc], Aleksandar Tošić[bc], Jernej Vičič[ab]
[a]University of Primorska Faculty of Mathematics, Natural Sciences and Information Technologies, Glagoljaška 8, 6000 Koper
[b]Research Centre of the Slovenian Academy of Sciences and Arts, The Fran Ramovš Institute, Novi trg 2, 1000 Ljubljana, Slovenia
[c]Innorenew CoE, Livade 6, 6000 Izola, Slovenia
domen.vake@famnit.upr.si, niki.hrovatin@famnit.upr.si, aleksandar.tosic@upr.si, jernej.vicic@upr.si

Accidental falls pose a risk to the health and independence of older adults. According to the World Health Organization's report titled "Fall Prevention in Older Age" [7], around 30 % of individuals aged 65 experience falls annually, and this risk rises for those above 70 years old. Despite various factors contributing to fall prevention (World, 2008), falls can sometimes result from underlying health issues, making them difficult to prevent entirely. Hence, timely detection of fall incidents is crucial to averting severe consequences stemming from fall-related injuries and other hazardous situations.

Tošić et al. [5] present a non-intrusive fall detection solution based on the smart floor, the same setting can be extended into an indoor location system and authors also argue a vast spectrum of possible applications. Hrovatin et al. [4] present local computation obscured by onion routing so only results of the computation leave the nodes ensuring the data privacy by never moving the data from the nodes. An additional possible way to deal with the privacy problems (preserving privacy) is the to use machine learning approaches/algorithms on specially encrypted data using homomorphic encryption [6].

The machine learning algorithm used in this experiment was Random forest [2], more precisely its evolved Python implementation in Catboost [3] library due to expected low discrepancy of the algorithm on encrypted data. The algorithm is supposed to perform

within marginal differences on the encrypted data as concluded in a recent study by Matias et al. [1].

We report acceptable results on our test-setting both from the accuracy (performance) view point and fro the time complexity point of view.

References

[1] Clayton Matias and Naghmeh Ivaki and Regina Moraes, Exploring the Impact of Homomorphic Encryption on the Performance of Machine Learning Algorithms, 12th Latin-American Symposium on Dependable and Secure Computing, 120–125 (2023)

[2] Tin Kam Ho. Random Decision Forests. Proceedings of the 3rd International Conference on Document Analysis and Recognition, Montreal, QC, 278—282 (1995)

[3] Prokhorenkova, Liudmila and Gusev, Gleb and Vorobev, Aleksandr and Dorogush, Anna Veronika and Gulin, Andrey, CatBoost: unbiased boosting with categorical features, Advances in neural information processing systems, 31, 120–125 (2018)

[4] Niki Hrovatin and Aleksandar Tošić and Michael Nicolas Mrissa and Jernej Vičič, A general purpose data and query privacy preserving protocol for wireless sensor networks. IEEE transactions on information forensics and security, 31, 4883-4898, (2023)

[5] Aleksandar Tošić and Niki Hrovatin and Jernej Vičič, Data about fall events and ordinary daily activities from a sensorized smart floor. Data in brief, 37, Elsevier, (2023)

[6] Craig Gentry, A fully homomorphic encryption scheme, Stanford university, ProQuest LLC, 789 East Eisenhower Parkway, 1–210 (2009)

[7] World Health Organization, WHO global report on falls prevention in older age, World Health Organization, 1–48 (2008)