World Academy of Science, Engineering and Technology
International Journal of Law and Political Sciences
Vol:19, No:07, 2025

Open Science Index, Law and Political Sciences Vol:19, No:07, 2025 publications.waset.org/abstracts/192534.pdf

Re-identification Risk and Mitigation in Federated Learning: Human Activity Recognition Use Case

Authors : Besma Khalfoun

Abstract : In many current Human Activity Recognition (HAR) applications, users' data is frequently shared and centrally stored by third parties, posing a significant privacy risk. This practice makes these entities attractive targets for extracting sensitive information about users, including their identity, health status, and location, thereby directly violating users' privacy. To tackle the issue of centralized data storage, a relatively recent paradigm known as federated learning has emerged. In this approach, users' raw data remains on their smartphones, where they train the HAR model locally. However, users still share updates of their local models originating from raw data. These updates are vulnerable to several attacks designed to extract sensitive information, such as determining whether a data sample is used in the training process, recovering the training data with inversion attacks, or inferring a specific attribute or property from the training data. In this paper, we first introduce PUR-Attack, a parameter-based user re-identification attack developed for HAR applications within a federated learning setting. It involves associating anonymous model updates (i.e., local models' weights or parameters) with the originating user's identity using background knowledge. PUR-Attack relies on a simple yet effective machine learning classifier and produces promising results. Specifically, we have found that by considering the weights of a given layer in a HAR model, we can uniquely re-identify users with an attack success rate of almost 100%. This result holds when considering a small attack training set and various data splitting strategies in the HAR model training. Thus, it is crucial to investigate protection methods to mitigate this privacy threat. Along this path, we propose SAFER, a privacy-preserving mechanism based on adaptive local differential privacy. Before sharing the model updates with the FL server, SAFER adds the optimal noise based on the re-identification risk assessment. Our approach can achieve a promising tradeoff between privacy, in terms of reducing re-identification risk, and utility, in terms of maintaining acceptable accuracy for the HAR model.

Keywords : federated learning, privacy risk assessment, re-identification risk, privacy preserving mechanisms, local differential privacy, human activity recognition

Conference Title : ICLSPI 2025 : International Conference on Legal, Security and Privacy Issues

Conference Location : Cannes, France

Conference Dates : July 12-13, 2025