Project Number: P1

Project Title: Trajectory Recovery from Ash: In the Age of AI

Project Clients: Prof. Salil Kanhere and Erik Buchholz, School of Computer Science and Engineering

Project Specializations: Software Development/Engineering, Algorithms, Machine Learning, Deep Learning, Data Science

Background:

Location trajectories collected by smartphones and other devices represent a valuable data source for applications such as location-based services. Likewise, trajectories can potentially reveal sensitive information about individuals, e.g., religious beliefs or sexual orientations. Consequently, safeguarding trajectory datasets becomes imperative.

A prevalent approach to address privacy concerns involves releasing solely aggregated data. For instance, one might release the count of users connected to a specific mobile phone antenna at a given time. While this might appear reasonably secure, the widely cited paper "Trajectory Recovery from Ash: User Privacy Is NOT Preserved in Aggregated Mobility Data" exposed that aggregation offers a false sense of privacy. The paper demonstrated the possibility of recovering user trajectories with remarkably high accuracies of 73-91%.

This work was published over six years ago. Since then, machine and deep learning rapidly progressed in performance, usability, and capabilities. This raises the intriguing question of to what extent deep learning further increases the risk of user re-identification from aggregated location data. Previous research [2] has already shown that the privacy provided by traditional mechanisms can be significantly reduced through deep learning-based attacks.

This project's objective is to ascertain whether AI also poses a threat to the privacy of aggregated location data. The primary research question is: "Can deep learning be harnessed to re-identify users from aggregated location data with greater accuracy than the attack outlined in the paper 'Trajectory Recovery from Ash [1]'?"

Notably, the original paper reports remarkably high accuracies, reaching 90%. However, these figures are anticipated to be lower for alternative datasets with differing properties, such as higher user numbers. Hence, there exists ample room for enhancement.

Requirements:

In the following, we concisely outline the goals of this project.

1. Develop a functional implementation of the attack described in [1]. The implementation should closely adhere to the description in [1].

2. Reproduce the results on (at least) two suitable open-source datasets of choice. Suitable here means that the datasets should be similar in terms of properties to the datasets used in [1]. Evaluation should employ the same metrics as [1].

3. Implement a deep-learning-based alternative to the attack from [1]. (Main contribution)

4. Construct a framework to compare the original attack (as per Goal 1) with the novel deep-learning model (as per Goal 3) across the chosen datasets. The comparison should meet the criteria specified in Goal 2.

The project's **scope** is adaptable to the student's progress and challenges encountered during the baseline implementation.

Scaling Option: If implementing the baseline approach becomes overly demanding due to insufficient or inaccurate information in the original paper, the project scope can be refined to Goals (1) + (2) exclusively. In this scenario, students would replicate the original paper's outcomes on two selected datasets. This focused approach ensures the successful completion of the project. In this case, the results would pave the way for future students to extend the project's progress by addressing subsequent goals."

Required Knowledge and skills:

- Practical deep learning skills: Students should be able to craft an original deep learning model or adapt an existing one for the specific application. Therefore, familiarity with one of the major deep learning frameworks (PyTorch, TensorFlow, or JAX) is required.
- Python Experience: Intermediate to advanced Python skills are prerequisites. The students must implement a baseline model based on the given research paper and develop a deep-learning model for comparison.
- Academic Reading: The skill to comprehend academic literature is crucial, as this project extensively relies on a foundational research paper (Xu et al., 2017. See above)
- While a theoretical understanding of deep learning is advantageous, it's not obligatory. This project centres on hands-on deep learning applications.

Expected outcomes/deliverables:

The project's outcomes will encompass the following deliverables:

Source Code:

- Implementation of the Baseline Model (Xu et al., 2017).
- Creation of a Novel Deep Learning model accomplishing the same objective.
- A Comparative Framework for evaluating both models based on the metrics detailed in the original paper.
- Pre-processing code tailored for at least two suitable datasets of choice.

Project Report:

- Outlining the findings. Artificial Intelligence (Machine/Deep Learning, NLP).

Reading Materials

[1] F. Xu, Z. Tu, Y. Li, P. Zhang, X. Fu, and D. Jin, “Trajectory Recovery From Ash: User Privacy Is NOT Preserved in Aggregated Mobility Data,” in Proceedings of the 26th International Conference on World Wide Web, Perth Australia: International World Wide Web Conferences Steering Committee, Apr. 2017, pp. 1241–1250. doi: 10.1145/3038912.3052620.

[2] E. Buchholz, A. Abuadbba, S. Wang, S. Nepal, and S. S. Kanhere, “Reconstruction Attack on Differential Private Trajectory Protection Mechanisms,” in Proceedings of the 38th Annual Computer Security Applications Conference, in ACSAC ’22. New York, NY, USA: Association for Computing Machinery, December 2022, pp. 279–292. doi: 10.1145/3564625.3564628."