ELEC 599 Abstract

Kai Malcolm
Advisor: Dr. Momona Yamagami
Title: Biosignal Data Privacy For Machine Learning and Co-adaptation Algorithms
Deadline: 15 December 2022

Co-adaptive and personalized algorithms offer an exciting opportunity for high-performing, individualized biosignal interfaces; however, data privacy concerns for these systems are particularly acute given the degree of personalization, the sensitivity of our biosignals, and the increased attack risk for record linkage or membership inference. This work will survey and implement prominent privacy-preserving mechanisms (such as differential privacy, homomorphic encryption, federated learning, etc.) to evaluate performance and privacy for fine-grained, non-IID (independent and identically distributed) applications.

This work aims to show that the decoder (matrix which decodes user EMG data to the machine input) personalizes to the user over time, implying that without taking additional precautions for privacy-preservation, these systems pose a serious threat due to the exceedingly unique personalizations, thus resulting in critical linkability risks. Therefore, a focus of this work is to maintain decoder accuracy while limiting the capabilities of an adversary. Results will be compiled to provide recommendations for practitioners working with biosignals for optimal methods, security, and trade-offs between data privacy and utility, as optimal privacy-utility balances remain a key issue. If successful, this work could be extended to protect underrepresented and thus more vulnerable groups (for instance, people with uncommon, sensitive medical conditions), preventing both linkability and attribute inference. Furthermore, user trust is an especially valuable resource in embedded applications involving data collection and machine learning: being able to provide robust privacy guarantees may help alleviate user concerns and encourage both participation in research studies as well as adoption of medical/assistive technology.

Schedule:

(1) 01/09/22 - Start of Spring 2023 Semester
(2) 01/17/22 - Literature review presentation
(3) 01/31/22 - Report effects of filtering / Windowing on privacy
(4) 04/15/22 - Implement, test, and compare the most promising the privacy mechanisms identified in the literature review
(5) 04/21/22 - Determine recommendations for privacy-preserving data-processing for practitioners
(6) 05/01/22 - Defend to committee