Dissertation Defense
Doctor of Philosophy in Computer Science

OPTIMIZING UTILITY, PRIVACY, AND ENERGY IN IOT SYSTEMS
by Henrique Potter

Date: July 20, 2023
Time: 11:00AM – 1:00PM
Place: Elly Lille / 6145 Sennott Square, Pittsburgh PA 15260

Committee:
- Daniel Mossé, Ph.D., Department of Computer Science
- Stephen Lee, Ph.D., Department of Computer Science
- Adam J. Lee, Ph.D., Department of Computer Science
- Daniel G. Cole, Ph.D., Swanson School of Engineering

Abstract:
This dissertation addresses privacy, utility, and energy consumption challenges in the increasingly ubiquitous Internet of Things (IoT) domain. The central concern revolves around IoT devices that provide connectivity, frictionless interaction, and automation, often inadvertently exposing sensitive user data. Given the risk of data breaches, the novelty of our primary defense strategy lies in emphasizing data minimization exposure through adaptive information filtering mechanisms beyond anonymization schemes.

We first extend IoT's utility-privacy (UP) tradeoffs by introducing energy consumption into our analyses. Through this exploration, we devised a framework to enable users to analyze the energy costs of privatizing data, the effect on data utility, and the achieved privacy levels for different protection techniques. To this end, we proposed a characterization scheme for privacy-preserving functions within the broader context of Utility, Privacy, and Energy (UPE) tradeoffs in IoT applications. The effectiveness of the UPE framework is evaluated on audio and image classification tasks and executed on resource-constrained devices, where it showed to facilitate the selection of privacy-preserving techniques to reduce energy consumption while retaining the user's chosen UP tradeoff point.

Furthermore, we investigate the privacy risks inherent in energy data collection from smart meters. Recognizing that federated learning, while being a promising privacy-preserving solution, is susceptible to attacks, we explore differentially private federated learning (DPFL). We developed an open-source framework to train Non-Intrusive Load Monitoring (NILM) models in a privacy-preserving, federated manner that uses other metrics to judge the efficacy of differential privacy noise addition. We presented the utility and privacy tradeoffs for different levels of noise addition tuned with the differential privacy epsilon value.

Finally, considering IoT devices’ resource constraints and the need for adaptive privatizers, we propose a third piece of work, PrivSpeech, a lightweight and customizable utility and privacy preservation framework focused on human-voice classification tasks. PrivSpeech works on the insight that intelligently obfuscating selected privacy-sensitive attributes can disrupt the latent variables related to the sensitive information while maintaining those related to the utility of the data, which allows a better balance of the utility-privacy tradeoff. We demonstrate its effectiveness in voice-based applications in three different datasets.
Our research extends the current understanding of privacy in the IoT landscape, offering new tools, frameworks, and privacy metrics to manage privacy risks while balancing utility and energy by introducing new privacy metrics and frameworks to help users control and have a better understanding of the risks. We expect our contributions to provide value to IoT systems designers, assisting in making informed decisions to ensure secure, efficient, and privacy-preserving data processing.