# Computer Science<br>Defense

## *Robust Crowdsourcing and Federated Learning under Poisoning Attacks*

Farnaz Tahmasebian
Emory University

**Abstract:** Crowd-based computing can be described in a way that distributes tasks among multiple individuals or organizations to interact with their intelligent or computing devices. Two of the exciting classes of crowd-based computing are crowdsourcing and federated learning, where the first one is crowd-based data collection, and the second one is crowd-based model learning. Crowdsourcing is a paradigm that provides a cost-effective solution for obtaining services or data from a large group of users. It has been increasingly used in modern society for data collection in various domains such as image annotation or real-time traffic reports. Although crowdsourcing is a cost-effective solution, it is an easy target to take advantage of by assembling great numbers of users to artificially boost support for organizations, products, or even opinions. Therefore, deciding to use the best aggregation method that tackles attacks in such applications is one of the main challenges in developing an effective crowdsourcing system. Moreover, the original aggregation algorithm in federated learning is susceptible to data poisoning attacks. Also, the dynamic behavior of this framework in terms of choosing clients randomly in each iteration poses further challenges for implementing the robust aggregating method in federated learning. In this dissertation, we devise strategies that improve the systems robustness under data poisoning attacks when workers intentionally or strategically misbehave. https://zoom.us/j/9828106847

Tuesday, March 30, 2021, 1:00 pm
https://zoom.us/j/9828106847

Computer Science
Emory University