Privacy Preserving Yet Verifiable IoT Devices

Ankit Jena
Carnegie Mellon University, Information Networking Institute

Abstract
The advent of the Internet of Things has tilted the technology landscape at an unprecedented scale. As the market for IoT devices grows manifold, home assistants are becoming more and more ubiquitous. While these devices get smarter and enhance user experience, privacy concerns continue to grow. Home assistants like Google Home and Amazon Echo gather massive volumes of potentially sensitive user data. To the average user who seems really impressed by the convenience such devices have ushered in, it is very easy to overlook the fact that the microphone on your favorite home assistant might be eavesdropping on everything you’re saying. What exacerbates the problem is the lack of a legal framework defining ownership of the data collected by these devices. In this work, we intend to redesign and implement a speech recognition cloud application and localize the application logic on the IoT device eliminating the need to send raw user audio to the cloud thereby preserving the user’s privacy. The application runs inside enclaves using Intel Software Guard Extensions (SGX). By leveraging remote attestation capabilities of Intel SGX we allow for verifiability of the IoT service for the cloud service provider.