Towards a Provenance-Aware Internet of Things (IoT) System

Ebelechukwu Nwafor

April 10, 2017

Abstract

The Internet of Things (IoT) offers immense benefits by enabling devices to leverage networked resources thereby making intelligent decisions. The numerous heterogeneous connected devices that exist throughout the IoT system creates new security and privacy concerns. Some of these concerns can be overcome through trust, transparency, and integrity, which can be achieved with data provenance. Data provenance, also known as data lineage, provides a history of transformations that occurs on a data object from the its origin to its current state. Data provenance has been explored in the areas of scientific computing, business, forensic analysis, and intrusion detection. Data provenance can help in detecting and mitigating malicious cyber-attacks.

In this research, we explore the integration of provenance within the IoT system. We propose a provenance collection framework for IoT applications. In this framework, trace data is collected from sensors and actuators on an IoT device. Trace data is then mapped into provenance using the Prov-Sensor alignment model to depict relationships between entities contained in an IoT system. Provenance data is stored locally and then transmitted to a cloud backend where it is stored in a graph database in which further data processing and analytics can be performed. Due to the amount of data generated in real time, provenance data generates enormous amounts of data. We overcome the storage challenge of provenance collection by adopting a policy approach for provenance collection and storage which allows flexibility in deciding what provenance data to keep. We evaluate the effectiveness of our framework by looking at an application of provenance data using an intrusion detection system, which detects malicious threats against IoT applications.