Abstract

Internet of Things (IoT) generates, connects and shares collected data from smart devices with various independent parties. With the increasing number of connected devices, its wide deployment is revolutionizing the modern world by covering almost every aspect of an individual's life. In this context, it is in the best interest of the community to successfully motivate users to share their IoT data with the rest of the environment, to allow the emergence of new services in different fields such as healthcare, education, or industrial manufacturing. However, requesting data to be able to extract valuable information from it can be a sensitive matter to approach. Therefore, framing requests and providing clarity on how this information will be used is necessary for building trust and credibility in connected environments. More precisely, when data providers decide to share their data with the community, they have little control over how their information are being used and in which context. In parallel, data consumers don't have the ability to trace back the different nodes by which the available data went through and its processing history to determine, for example, if it meets the technical and legal requirements of a given activity.

Our research focus on three main challenges: (i) the definition of a semantic layer that handles the security requirements in the context of IoT data sharing, (ii) the enforcement of a context-aware security policy that matches both the data provider's preferences and the data consumer's usage, and (iii) the establishment of an end-to-end security solution that manage the sharing of IoT data in a decentralized architecture while eliminating the need to trust any involved IoT parties.

To address these issues, we first present a context-aware IoT data Sharing Management ontology called IdSM-O, to establish a shared security vocabulary and handle the interoperability of IoT environments. Following that, we introduce a three-layer automatic semantic rule manager, that collects data provider's security policies requirements and automatically translate them to semantic rules ready for reasoning. Those contributions are the basement of IdSM, an end-to-end security framework for data sharing management during the phases of collection, transmission, and processing. Using this framework, we aim at addressing user's control enforcement over the owned smart devices, information security requirements, and obligation compliance between various parties in the IoT environment. Finally, we design, implement, and develop a prototype of the the proposal in order to prove its feasibility and analyze its performances.

Keywords : Security, Internet of Things (IoT), semantic web, usage control, data provenance.