Chapter 57
Applying Security to a Big Stream Cloud Architecture for the Internet of Things

Laura Belli
University of Parma, Italy

Simone Cirani
University of Parma, Italy

Luca Davoli
University of Parma, Italy

Gianluigi Ferrari
University of Parma, Italy

Lorenzo Melegari
University of Parma, Italy

Marco Picone
University of Parma, Italy

ABSTRACT

The Internet of Things (IoT) is expected to interconnect billions (around 50 by 2020) of heterogeneous sensor/actuator-equipped devices denoted as "Smart Objects" (SOs), characterized by constrained resources in terms of memory, processing, and communication reliability. Several IoT applications have real-time and low-latency requirements and must rely on architectures specifically designed to manage gigantic streams of information (in terms of number of data sources and transmission data rate). We refer to "Big Stream" as the paradigm which best fits the selected IoT scenario, in contrast to the traditional "Big Data" concept, which does not consider real-time constraints. Moreover, there are many security concerns related to IoT devices and to the Cloud. In this paper, we analyze security aspects in a novel Cloud architecture for Big Stream applications, which efficiently handles Big Stream data through a Graph-based platform and delivers processed data to consumers, with low latency. The authors detail each module defined in the system architecture, describing all refinements required to make the platform able to secure large data streams. An experimentation is also conducted in order to evaluate the performance of the proposed architecture when integrating security mechanisms.

DOI: 10.4018/978-1-5225-9866-4.ch057

INTRODUCTION

In recent years, the forecast of a worldwide network of pervasively deployed heterogeneous networks is becoming a reality. The Internet of Things (IoT) involves billions of different devices, connected in an Internet-like structure, allowing new forms of interaction between things and people. The actors involved in IoT scenarios have extremely heterogeneous characteristics, in terms of processing and communication capabilities, energy supply and consumption, availability and mobility, spanning from Smart Objects (SOs) - i.e., constrained devices equipped with sensors or actuators, smartphones, wearables and other personal devices - to Internet hosts and the Cloud.

In order to allow heterogeneous nodes to efficiently communicate with each other and with existing Internet actors, shared and interoperable communication mechanisms and protocols are currently being defined and standardized. The most prominent driver for interoperability in the IoT is the adoption of the Internet Protocol (IP), namely IPv6. An IP-based IoT can extend and operate with all existing Internet nodes, without additional efforts. Standardization institutions, such as the Internet Engineering Task Force (IETF), and several research projects are contributing to the definition of new mechanisms to bring IP to SOs (e.g., 6LoWPAN (Kim, Kaspar, & Vasseur, 2012)). This is motivated by the need to adapt higher-layer protocols (e.g., application-layer protocols) to constrained environments. As a result, IoT networks are expected to generate huge amounts of data, which can be subsequently processed and used to build several useful services for final users. The Cloud has become the natural collection environment for sensed data retrieved by IoT nodes, due to its scalability, robustness, and cost-effectiveness. Figure 1 shows the hierarchy of different levels involved in data collection, processing and distribution in a typical IoT scenario.

Figure 1. Different actors and layers involved in IoT scenarios: sensed data are sent from IoT networks to the Cloud, which provides services to consumers. At an intermediate level, preliminary local operations, such as data collection, processing, and distribution, may be carried out