International Journal of Software Science and Computational Intelligence
Volume 13 • Issue 1 • January-March 2021

Using Clustering for Forensics Analysis on Internet of Things

Dhai Eddine Salhi, LIMOSE Laboratory, M'hamed Bougara University, Boumerdes, Algeria
https://orcid.org/0000-0002-4025-2806

Abelkamel Tari, LIMED Laboratory, University Abderrahmane Mira, Bejaia, Algeria

Mohand Tahar Kechadi, Insight Centre for Data Analytics, University College Dublin, Dublin, Ireland

ABSTRACT

In the world of the internet of things (IoT), many connected objects generate an enormous amount of data. This data is used to analyze and make decisions about specific phenomena. If an object generates wrong data, it will influence the analysis of this collected data and the decision later. A forensics analysis is necessary to detect IoT nodes that are failing. This paper deals with a problem: the detection of these nodes, which generate erroneous data. The study starts to collect in a cloud computing server temperature measurements (the case study); using temperature sensors, the communication of the nodes is based on the HIP (host identity protocol). The detection is made using a data mining classification technique, in order to group the connected objects according to the collected measurements. At the end of the study, very good results were found, which opens the door to further studies.

KEYWORDS

Arduino, Clustering, Data Mining, Digital Forensics, HIP Protocol, Internet of Things

1. INTRODUCTION

In the next few years, 75% of the world's population will live in cities, which means that reach an average of 20 million people per city. The concept of smart cities is one of the solutions to the urbanization explosion. Smart cities are managed by computers running artificial intelligence algorithms. Smart cities are becoming a necessity for better life, and management future population growth. These are managed by Internet Of Things (IoT) devices, which are connected and remotely controlled to provide efficient services in terms of energy and comfort to the people. If an example of an intelligent public bin is taken that has sensors, once it is full it contacts an information center in order to be emptied as soon as possible.

The communication of connected objects is composed in three layers: The perception layer where the "sensors" layer is equivalent to the physical layer of the TCP model. The purpose of this layer is to gather the data at the sensor level (short range or extended language). The next layer is the network layer; the most important training is Internet routing with gateways and Cloud Computing servers. The last layer is the application layer that guarantees the authentication, integrity and confidentiality of data to create a smart environment.

Our system consists of analyzing the connection between the objects via a network where the five essential factors of security is ensured, which are discussed later in this paper. The proposed solution intervenes at the application layer by developing a new analysis system between the connected

DOI: 10.4018/IJSSCI.2021010104

nodes and a storage server that has the role of keeping the details of the collected data (Data, IP address, time of passage, certificate of confidence and utility level of data) and assesses the quality of communication between these objects.

2. BACKGROUND

The term Internet of Things (IoT) was first introduced as an idea in 1999 by Kevin Ashton (Leo et al., 2014), which has now evolved into a reality that interconnects real world sensors, electronic devices and systems to the Internet, such as:

- Consumer services, smart houses, and smart objects, Smartphones and Tablets;
- Smart energy; smart meters and grids;
- Wearable devices; health and fitness monitoring devices, watches, smart clothing, pets smart collars or implanted RFIDs, and even human implanted devices;
- Wireless sensor networks; weather measuring, health care monitoring, industrial monitoring, data loggings, environmental monitoring (water quality, earth sensing fire detection, air pollution monitoring) etc.

2.1. IOT Architecture

In IoT, each layer is defined by its functions and the devices that are used in that layer. There are different opinions regarding the number of layers in IoT. However, according to the literature (Zhao & Ge, 2013; Atzori et al., 2012; Leo et al., 2014), the IoT mainly operates on three layers termed as Perception, Network, and Application layers (Tewari & Gupta, 2018). Each layer has inherent security issues associated with it. Figure 1 shows the basic three the layers of the IoT framework with respect to the devices and technologies that encompass each layer:

1. **Perception Layer:** The perception layer is also known as the Sensors layer in IoT. The purpose of this layer is to acquire the data from the environment with the help of sensors and actuators. This layer detects, collects, and processes information and then transmits them to the network layer. This layer also performs the IoT node collaboration in local and short range networks (Atzori et al., 2012);
2. **Network Layer:** The network layer of IoT serves the function of data routing and transmission to different IoT hubs and devices over the Internet. At this layer, cloud computing platforms, Internet gateways, switching, and routing devices etc. operate by using some of the very recent technologies such as Wi-Fi, LTE, Bluetooth, 3G, Zigbee etc. The network gateways serve as the mediator between different IoT nodes by aggregating, filtering, and transmitting data to and from different sensors (Leo et al., 2014);
3. **Application Layer:** The application layer guarantees the authenticity, integrity, and confidentiality of the data. At this layer, the purpose of IoT or the creation of a smart environment is achieved.

2.2. Communication Architecture

A good functioning of the IOTs requires good communication architecture in order to exchange data between Things, but also to store, encrypt and analyze these data generated by sensors. An IoT project is composed of four main parts:

- **Things:** These are the connected objects;
- **Infrastructure:** The servers that will communicate with Things, in the Cloud or elsewhere;