Chapter 63
Analysis of Privacy Preservation Techniques in IoT

Ravindra Sadashivrao Apare
JJT University, Rajasthan, India

Satish Narayanrao Gujar
BSCOER, Pune, India

ABSTRACT

IoT (Internet of Things) is a sophisticated analytics and automation system that utilizes networking, big data, artificial intelligence, and sensing technology to distribute absolute systems for a service or product. The major challenges in IoT relies in security restrictions related with generating low cost devices, and the increasing number of devices that generates further opportunities for attacks. Hence, this article intends to develop a promising methodology associated with data privacy preservation for handling the IoT network. It is obvious that the IoT devices often generate time series data, where the range of respective time series data can be extremely large.

1. INTRODUCTION

The IoT is a compilation of physical objects that are entrenched with software, electronics, together with sensors, which allows objects to be sensed and controlled distantly across the traditional network infrastructure, makes the direct integration feasible among computer communication networks in addition to the physical world, and significantly contributes to enhanced precision, efficiency, and economic compensations (Acemoglu, Makjdoumi, Malekian & Ozdaglar, 2017; Kang, Kim & Choo, 2017; Said, Albagory, Nofal & Raddady, 2017; Shirvanimoghaddam, Condoluci, Dohler & Johnson, 2017). Therefore, IoT is generally applied in numerous applications such as environment monitoring, transportation, medical healthcare systems, building automation, and energy management (G. Sun, Chang, Ramachandran, Z. Sun & Liao, 2017; Lopez, Rios, Bai & Wang). Moreover, IoT is the contemporary web evolution that comprises billions of devices, which are preserved by various association and people who are em-

DOI: 10.4018/978-1-7998-8954-0.ch063

ploying in addition to utilizing them for their own determinations (H. Chen, Beaudoin & Hong, 2017; L. Chen et al., 2017). IoT, in addition, manages with the embarrassment of Cyber Security and privacy intimidations that currently interrupts organizations, in addition, it has the capability to hold the data of entire countries and even industries for payoff just like erstwhile web-dependent information systems potentially (Guliano, Mazzenga, Neri & Vegni, 2017).

IoT must deal powerfully with such intimidations and confidentiality of the information gathered and assure the protection and are distilled from IoT strategies to comprehend its entire potential (Asplund & Nadjm-Tehrani, 2016; Sajid, Abbas & Saleem, 2016). On the other hand, IoT offers several characteristic limitations that make the appliance of traditional privacy methods and security challenges (Xu, Ren, Song & Du, 2016). This is owing to the IoT solutions, which comprise a variety of private security and solutions for defending such IoT data in addition to the store at the layer of the device, the IoT platform and the infrastructure layer or IoT application layer (Zhou, Cao, Dong & Vasilakos, 2017). Subsequently, a magnificent confront in IoT is to guarantee the end-to-end security across the mentioned three IoT layers.

Unsuitably, owing to the resource constrictions of IoT devices, it hands over tremendously multifaceted computation to the energy abundant cloud for significantly improved capability forever (Tiburski, Amaral, de Matos, de Azevedo & Hessel, 2016). On the other hand, the outputs, inputs, in addition to the role of the fundamental estimation might be intimately related to the privacy of IoT users, which could not be undefended to collusion between malicious IoT users in addition to malicious cloud servers (Hossain et al., 2016; Jacobsson, Boldt & Carlsson, 2016).

2. LITERATURE REVIEW

2.1. Related works

In 2017, Prem Prakash Jayaraman et al. has proposed on IoT for end-to-end cyber security and in addition to prevail over the threats in privacy. This has been attained by initiating novel methods to conserve the IoT data, obtaining IoT architectures and performance of concept systems, which guarantees the confidentiality of IoT data that, was widened for open source platform. The entire data was gathered arbitrarily from the IoT tool and articulated as data addends when accumulating one of the numbers in the component. The effectiveness and presentation were estimated, and applicability and possibility on open platform were confirmed experimentally. The suggested method had improved performance on evaluating the proposed IoT system since it produces the data and conserves the system privacy.

In 2017, Gang Sun et al. has hypothetically evaluated the Attack Dummy Local Selection (ADLS) scheme with their suggested Dummy Local Selection (DLS) algorithm. This was made on the location Based Services (LBS), in which the user privacy was attacked. LBS offer service to the entire users offering improved probability to follow the data of third parties. By means of the offered information and the metric entropy, DLS chooses a dummy location for best privacy level. ADLS scheme has the benefit of recognizing the location of the user from the dummy DLS location. On executing the algorithms, they establish that the implemented algorithm offers data-driven service of IoT with improved effectiveness and reduced performance error defending the user's location.

In 2017, Mujahid Mohsin et al. formed a novel and a comprehensive data-driven service IoT checker that was scalable, interoperable offering enhanced security. The variances of security formation were arrested routinely, and the intimidation vectors were evaluated. Real world IoT commodities were