Chapter 23
IoTP an Efficient Privacy Preserving Scheme for Internet of Things Environment

Shelendra Kumar Jain
https://orcid.org/0000-0002-9692-9505
Department of Computer Science, Central University of Rajasthan, NH-8, Bandar Sindri, Ajmer, 305817, Rajasthan, India

Nishtha Kesswani
Department of Computer Science, Central University of Rajasthan, NH-8, Bandar Sindri, Ajmer, 305817, Rajasthan, India

ABSTRACT

Many emerging fields are adopting Internet of Things technologies to incorporate smartness in respective areas. Several IoT based application area produces large volumes of real time data. Data aggregated through sensor nodes may contain highly sensitive information. An effective and successful IoT system must protect sensitive data from revealing to unauthorized persons. In this article, the authors present an efficient privacy-preserving mechanism called Internet of Things privacy (IoTp). The research simulates and analyzes the effectiveness of the proposed data aggregation and data access mechanism for a typical IoT system. Proposed IoTp scheme ensures privacy at data collection, data store and data access phases of the IoT system. The authors have compared proposed work with existing model. Results show that IoTp scheme is efficient and lightweight mechanism for data collection and data access. It is suitable for the resource constrained IoT ecosystems.

INTRODUCTION

Internet of things (IoT) has the capability to connect everything and provide services ubiquitously through the internet. Cities become smart by adapting IoT and other disruptive innovations and services (Al Shidhani, 2019). It has enabled users to perform relevant tasks easily and smartly. Human life is tremendously affected from the smart things and their activities (Choudhary, & Kesswani, 2019). For collection of data,

DOI: 10.4018/978-1-7998-8954-0.ch023

IoT device uses sensor(s), while the collected data may be sensitive or non-sensitive in nature. A smart device in IoT may contain any sensitive data such as name, address, date of birth, financial information, health information, personal activity, location, user behavior, specific patterns, energy consumption, etc. (Corcoran, 2016; Jayaraman, Yang, Yavari, Georgakopoulos, & Yi, 2017). Data sensitivity depends on many factors, like data owner's preferences, a specific time situation, importance of data; public interest in data etc. For instance, revealing information such as health statistics may be sensitive for user X but not for another user Y. There is a constant growth in the amount of sensitive information collected by sensors and devices (Xiong, 2015). Data owner may be unaware of the sensitivity of data which are being collected about him/her. Confidential information of IoT based service user may be collected and sent to the cloud (Pacheco, Alchieri, & Barreto, 2017). The data generated by IoT device is shared with service provider and hosted in the cloud by third parties (Schurgot, Shinberg, & Greenwald, 2015). Often users do not want to reveal their data to third party which is collected by the IoT device (Henze, 2016). Disclosure of sensitive data from any weak point results into serious consequences, for example a patient disease profile data disclosure may affect his/her job opportunity (O'Flaherty, 2015), marriage life, social disrespect, depression level etc. In recent advanced information technology era, there are several cases where sensitive data is disclosed and these types of cases are increasing continuously.

Private information about the computation might be recorded secretly by the cloud server and adversary may try to access this type of information (Kumar & Vardhan, 2018). Privacy issues should be taken into consideration because sensitive information may leak from the device, during storage, communication and processing of the data (Kraijak, & Tuwanut, 2015; Kumar, & Patel, 2014; Chen, & Tian, 2017; Kaur, Verma, Jain, & Kesswani, 2019). Typically, there are three IoT architecture layers: 1. Perception layer: It consists of the sensor nodes and IoT devices that collect data. 2. Middleware: It consists of gateway to upload collected data to data storage such as cloud. 3. Application layer where user devices and applications access IoT data and services from data storage and service providers. These layers are shown in Figure 1 along with the privacy threats that may occur on these layers.

Privacy threats introduce hurdles in the success of Internet of Things vision and can cause disclosure of sensitive information and put the user at a high risk. Some of these threats are as follows:

- **Malicious administrator or hacker:** An insider or malicious attacker may gain control over the entire system;
- **Lack of control over the IoT devices:** Usually the IoT devices are not directly under the control of the user which may affect the privacy of the user;
- **Lack of proper authentication mechanism:** As of now, there is no standard authentication mechanism that is followed by the IoT devices;
- **Lack of end to end privacy:** There is no uniform end-to-end privacy mechanism that can be followed across all the layers;
- **Inferences:** May be drawn from the collected and stored data;
- **Linking data collected from sensors:** To extract patterns of the user habits and many more such kind of other threats;
- **Incorporation of the centralized approaches in IoT:** Can result in the privacy risks due to single point attack.

Privacy preservation is a way of minimizing or eliminating privacy issues and threats in an Internet of Things like ecosystem. Privacy preservation is important in order to achieve the potential of billions