# Chapter 22
# An Improvised Framework for Privacy Preservation in IoT

**Muzzammil Hussain**
*Department of Computer Science and Engineering, Central University of Rajasthan, Ajmer, India*

**Neha Kaliya**
*Department of Computer Science and Engineering, Central University of Rajasthan, Ajmer, India*

## ABSTRACT

*Data privacy is now-a-days a special issue in era of Internet of Things because of the big data stored and transmitted by the public/private devices. Different types and levels of privacy can be provided at different layers of IoT architecture, also different mechanisms operate at different layers of IoT architecture. This article presents the work being done towards the design of a generic framework to integrate these privacy preserving mechanisms at different layers of IoT architecture and can ensure privacy preservation in a heterogeneous IoT environment. The data is classified into different levels of secrecy and appropriate rules and mechanisms are applied to ensure this privacy. The proposed framework is implemented and evaluated for its performance with security and execution time or primary parameters. Various scenarios are also evaluated, and a comparison is done with an existing mechanism ABE (Attribute Based Encryption). It has been found that the proposed work takes less time and is more secure due to short key length and randomness of the parameters used in encryption algorithm.*

## 1. INTRODUCTION

Evolving technologies are devoting a high rise in of Internet of Things (IoT). This is leading to a huge increase in the count of connected devices and raw data produced by the devices(Gubbi, Buyya, Marusic, & Palaniswami, 2013) . Data generated and collected in one area (for instance- Smart Meter data record in the Energy domain regularly maintains a track of whole household energy usage) is now produced at remarkable frequency that it is susceptible to fetch any private data beyond the premier purpose. Therefore, data privacy is of serious significance (Matharu & Upadhyay, 2014) (Commission, 2015).

DOI: 10.4018/978-1-7998-8954-0.ch022

There exist many privacy preservation mechanisms (Banerjee, Dong, & Taghizadeh, 2014) but they leaked in one or other important issue. In traditional encryption scheme (Ukil, Bandyopadhyay, & Joseph, 2012), it is a pre-requirement for sender to be aware of the details and identity of all known receivers (Ukil et al., 2012). Basically, the main principle to be followed is that a sender will encrypt the data which will only be decrypted and used by the intended receiver. Such encryption schemes will fail in scenarios when systems sender does not know the receivers who will use the data being sent (Sweeney, 2002b) (Sweeney, 2002a).

A framework is proposed which ensures security for data management of IoT. This framework includes Access Control List (ACL) concept and also a data classification model, which classifies data according to its sensitivity and assigns tag value to each category. An access control mechanism which incorporates digital certificate authentication mechanism and secret key encryption mechanism is implemented.

The proposed framework is explained in second module, module 3 describes theoretical evaluation of proposed work, module 4 describes the security analysis of proposed work followed by the implementation and result in next module, module 6 gives the comparison with ABE on the basis of execution followed by conclusion and future work in last module.

## 2. PROPOSED WORK

In the traditional data management framework, the security manager is focusing on data protection and privacy measures (Abu-Elkheir, Hayajneh, & Ali, 2013). Due to massive amount of data available, data classification and accessing with full security and also at the same time, keeping a track to give access rights only to authorized user is a very challenging task. Hence, authors have proposed a module of security framework including different modules leading to successful deployment of IoT. In the data management framework described, the security manager deals with data protection and privacy measures in accordance with some rules of security that are of relevance to both the protected data and to the final users.

Authors designed a framework of security manager with some security components such as access control list (ACL), user authentication mechanism and data classification module.

### 2.1. Data Classification Model

Data classification mechanism must be very easy, and the strategy chosen must classify the data properly. During data classification, confidentiality and security of data is considered at highest priority. While maintaining integrity, low-quality data cannot be trusted. Looking at its availability, high availability needs resilient storage and networking. We need to use an effective metadata strategy to tag the data as well. This model is represented in Figure 1.

Data classification model steps

1. Analyze the source/entities which are generating and transmitting the data.
2. Categorize the data sources on the basis of the type of information they are collecting.
3. If the data sources are public devices, e.g., Wi-Fi etc., they will collect “general data”. Store this data in database after assigning tag value 00 to it.