Chapter 4
Analysis of Identity-Based Cryptography in Internet of Things (IoT)

Aravind Karrothu
Vellore Institute of Technology, India

Jasmine Norman
Vellore Institute of Technology, India

ABSTRACT

Fog networking supports the internet of things (IoT) concept, in which most of the devices used by humans on a daily basis will be connected to each other. Security issues in fog architecture are still a major research area as the number of security threats increases every day. Identity-based encryption (IBE) has a wide range of new cryptographic schemes and protocols that are particularly found to be suitable for lightweight architecture such as IoT and wireless sensor networks. This chapter focuses on these schemes and protocols in the background of wireless sensor networks. Also, this chapter analyses identity-based encryption schemes and the various attacks they are prone to.

INTRODUCTION

Recent days, many networking systems are deployed for accessing other real time devices/gadgets to communicate with each other, which is considered as Internet of Things (IoT). This is the biggest step for internet but, at the same time the security concerns need to be addressed for various applications such as smart activities like

DOI: 10.4018/978-1-7998-0194-8.ch004

smart house, transportation, industrial and other smart devices. IoT devices deployed at typical locations are susceptible to attacks like device conciliation and false data modification. At the same time, IoT has to maintain a light-weight security mechanism and thus it becomes a prominent research area for the security researchers.

The IoT architecture is shown in Figure 1 and it is treated as 3-tier construction with every sensor node communicate with each other and transmits the data to a recognized gateway, every gateway again acts as a node and transmits the data to root level node called server. Server handles the data in terms of maintaining and processing with data centres. In 2016, S. Sankaran proposed a framework (Sankaran, 2016) for IoT using IBC and developed the functionality of IoT in a hierarchal manner and it shown in Figure 2. In this figure, every individual node appeared as a leaf node and can access with upper layer using their own IDs, and every node can communicate with other nodes too. Later the data transmits to gateway with the help of same IDs and parallelly root level node can access the data from '*n*' gateway nodes and allocated IDs and communication is done with IDs in between root level node and leaf nodes. In this manner IBC scenario can apply in IoT for providing security. Data centres maintained by server handles data accessing from higher level to lower level, as the server act as third party. Third party also to be maintained in trustworthy manner else there is a chance for vulnerable attacks.

Lightweight security is classified into three categories, symmetric key based, public key cryptography (PKC) and hybrid key cryptography. Malan et al., confirmed that PKC is more applicable for smart world for device authentication in IoT (Malan, Welsh & Smith, 2004). Identity based Cryptography (IBC) is broadly used for many application fields and IoT has one of the parts on this consideration. In any system, IoT devices/entities can allow with proper authenticate accessibility (IDs) and communicate each and also provide secure communication with their identities to make public keys for encryption of the messages, so-called IBC is more reliable

Figure 1. Illustration of Internet of Things