Chapter 2
Encryption Principles and Techniques for the Internet of Things

Kundankumar Rameshwar Saraf
Dr. D. Y. Patil College of Engineering Lohegaon, India

Malathi P. Jesudason
Dr. D. Y. Patil College of Engineering Akurdi, India

ABSTRACT

This chapter explores the encryption techniques used for the internet of things (IoT). The security algorithm used for IoT should follow many constraints of an embedded system. Hence, lightweight cryptography is an optimum security solution for IoT devices. This chapter mainly describes the need for security in IoT, the concept of lightweight cryptography, and various cryptographic algorithms along with their shortcomings given IoT. This chapter also describes the principle of operation of all the above algorithms along with their security analysis. Moreover, based on the algorithm size (i.e., the required number of gate equivalent, block size, key size, throughput, and execution speed of the algorithm), the chapter reports the comparative analysis of their performance. The chapter discusses the merits and demerits of these algorithms along with their use in the IoT system.

DOI: 10.4018/978-1-5225-5742-5.ch002

INTRODUCTION

By using the Internet of Things, physical objects can communicate with each other over the Internet. Therefore, there is a strong need to define and implement security mechanisms which can ensure security and privacy of data that passes through the Internet of Things. The security algorithm used for IoT should follow many constraints of IoT. Hence, lightweight cryptography is the optimum security solution for securing IoT devices.

Simon, KATAN, and LED are optimized for hardware implementations while as Speck and Scalable Encryption Algorithm (SEA) ciphers are optimized for software implementations. Simon and Speck algorithms have been developed by the National Security Agency (NSA). Canniere et al. designed KATAN, and LED was designed by Guo et al. Low performing small computers can use the TEA encryption algorithm invented by David Wheeler and Roger Needham. PRESENT algorithm, invented by Andrey Bogdanov et al. is compact (occupies only 40% of space as compared to that of AES). Scalable Encryption Algorithm has been designed for software implementations in smart cards, processors, and controllers. This chapter provides a detailed description of all these algorithms along with their benefits and drawbacks and concludes with the comparison of all algorithms based on specific common metrics.

BACKGROUND

Encryption is a method of concealing the sensitive information and substituting it by other numbers, letters or symbols which can hide its meaning and readability. The cipher formed by encryption is used to protect the original word or plaintext from any possible third-party attacks. Cipher is of two subtypes, namely classical and modern. A classical cipher, in turn is of two types namely substitution and transposition ciphers. Substitution cipher may be monoalphabetic or polyalphabetic. Presently, modern ciphers are in practice. Symmetric and asymmetric key are the two types of modern ciphers. Symmetric ciphers are further classified into block and stream ciphers. Various modern cipher encryption algorithms and standards that are prominent include AES, DES, 3DES, RC4, SEAL, RSA, DSA and DH. A partial classification of ciphers is shown in Figure 1.

In the Internet of Things, physical devices embedded with sensors, software and connectivity enable data exchange and communication between devices. To secure communication in such environments, i.e., constrained physical devices, the implementation of new lightweight encryption algorithms which can replace the existing modern unconstrained encryption algorithms becomes highly essential.