Chapter 8
Lightweight Secure Architectural Framework for Internet of Things

Muthuramalingam S.
Thiagarajar College of Engineering, India

Nisha Angeline C. V.
Thiagarajar College of Engineering, India

Raja Lavanya
Thiagarajar College of Engineering, India

ABSTRACT

In this IoT era, we have billions of devices connected to the internet. These devices generate tons of data that has to be stored, processed, and used for making intelligent decisions. This calls for the need for a smart heterogeneous network which could handle this data and make the real-time systems work intelligently. IoT applications leads to increasing demands in high traffic volume, M2M communications, low latency, and MIMO operations. Mobile communication has evolved from 2G voice services into a complex, interconnected environment with multiple services built on a system that supports innumerable applications and provides high-speed access. Hence the sustainability of the IoT applications do rely on next generation networks. Due to the significant increase in the network components, computational complexity, and heterogeneity of resources, there arise the need for a secure architectural framework for internet of things. For this, the authors propose a secure architectural framework for IoT that provides a solution to the lightweight devices with low computational complexity.

DOI: 10.4018/978-1-5225-8241-0.ch008

INTRODUCTION

The novel communication frameworks Next Generation Networks (NGN) is the one that transports all information and services by packets. One of the next generation networks is the Internet of Things. The term Internet of Things has emerged from the concept of a network of objects. These devices are capable of sensing the various factors of the environment and collecting the data. It is one among the next generation networks which are going to interact without human intervention. IoT framework has various heterogeneity levels and desired connectivity among the billions of uniquely identifiable objects. A variety of applications such as healthcare, industrial surveillance with a number of techniques such as intelligent sensors, wireless communication, networks, data analytics, and cloud computing are developed. The biggest obstacles in IoT is security which can be of any type such as communication network security, application security, and general system security.To provide a solution to security issues of IoT we need to develop a secure architectural framework for IoT which encompasses the different network layers. The rise of new applications and wireless devices on fixed and mobile terminals led to the need of secure network architecture. (Massimo, 2016). The communication among the networks devised a strategic evolution of growth of the information to be communicated on the Internet. IoT includes light weight devices such as sensors and actuators. The security threats to IoT includes authentication failure and leakage of data. Since every device is light weight the solutions should also be simple. Traditional security mechanisms like Firewalling, Intrusion Detection and Prevention Systems are deployed at the Internet edge. Those mechanisms are used to protect the network from external attacks which are not sufficient to secure the Internet. IoT architecture does not provide enough security for the wireless network.

Security is the process of protecting a device or an object against all kinds of active and passive attacks. It also prevents from physical damage and unauthorized access of data thus providing authentication and authorization. Leakage of information is also to be prevented thus ensuring confidentiality and data integrity. Ensuring IoT security is not different from other networking environments. It requires to maintain the communication and data management inside and outside the network.

In the rest of the part section 2 describes the different types of protocols of IoT. Section 3 describes the security requirements of IoT which includes the various goals of security. Section 4 describes the lightweight security framework for IoT which addresses all the above described protocols and security requirements to be incorporated in the IoT architecture which is described in section 5. Section 6 focuses on the applications of IoT which can use the described architecture. Section 7 concludes the chapter with enhancement of future work for the architectural framework.