A Successful Key Distribution Technique for Internet of Things Technology

Venkatesh Naramula[1,a)] , Dr. Kadapa Sagar[2]

[1] *Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India.*
[2]*Professor, Dept. of CSE, CBIT, Hyderabad, Telangana, India.*

[a)] Corresponding author: naramula.venky@gmail.com

Abstract: Our lives have significantly transformed as a result of the Internet of Things (IoT). We employ IoT because of our customers, government agencies, and business partners. Security is a major problem when offering a variety of services even if IoT offers new options. Particularly hard is how the statistics are presented. How to secure the flow of information produced by IoT devices while passing through various nodes and gateways may be safeguarded from security threats. In this paper, we propose an effective key management approach that mixes symmetric and asymmetric cryptosystems in order to get the speed of the former and the security benefits of the latter. Our aim is to guarantee the IoT environment's security. Our method takes into account a number of Smart Objects (SO) that can produce, register, and distribute keys for IoT information transfer. We selected the open-source MessageQueuingTelemetryTransport (MQTT) protocol as a solution to help communication between the starting point and target nodes. The proposed approach is tested experimentally, and the results are discussed in terms of key exchange time, algorithm implementation time, number of reprocess connections, and bandwidth consumption.

Keywords: IoT, Group key management, Key Sharing, Authentication, Key distribution.

INTRODUCTION

Nearly every area of a person's life is now impacted by the Internet of Things (IoT). The Internet of Things enables multiple sensors or smart devices to cooperate and provide a variety of services in the context of several applications, such as smart cities, smart agriculture, home automation, healthcare, etc.(Figure 1). In the field of Security, military, etc. An Internet of Things IoT concept enables broad Internet-based communication between smart things. Security threats and dangers are a major issue in this strategy. New methodology, standards, and algorithms for secure key distribution, key generation and key management with high resilience, reliability and accessibility are now being defined by the academic community and standardization bodies.

Information may be secured in a conventional information transmission system by employing a single cryptographic key. However, the conventional single key technique is inappropriate when information is routed via several nodes en route from a source to a destination. The whole communication system may be destroyed if the key is stolen or compromised. Furthermore, there will be a significant risk component since a lot of information is sent in a true IoT system. As a result, real-time confirmation in addition to security is required, which is difficult and time-consuming.

Significant efforts have been made to offer validation and security for IoT information transfers, with a focus on key management. Some examples are the Mutual key management approach [8, GKMP], Elliptic Curve Cryptography (ECC)/Elliptic Curve Diffie Hellman (ECDH) applied key management, and others. a few of these systems employ asymmetric-cryptosystems, whereas remaining use symmetric-key-based-cryptosystems. Although symmetric-key cryptosystems are extra secure, they nevertheless have a high computation cost. We propose a hybrid of symmetric and asymmetric cryptosystems, taking use of both the speed and benefits of the former.