Lightweight Secure MQTT for Mobility Enabled e-health Internet of Things

Adil Bashir[1] and Ajaz Hussain Mir[2]
[1]Islamic University of Science and Technology, Jammu and Kashmir, India
[2]National Institute of Technology Srinagar, Jammu and Kashmir, India

Abstract: *Internet of Things (IoT) is a smart interconnection of miniature sensors, enabling association of large number of smart objects ranging from assisted living and e-health to smart cities. IoT devices are equipped with limited resources in terms of power, memory and processing capabilities, therefore, presenting novel challenges to security. The purpose of this paper is to design energy efficient security mechanism for IoT based e-health system in which medical data is encrypted using lightweight cryptographic operations. The proposed scheme provides end-to-end data confidentiality for mobility enabled e-health IoT system. Our security scheme is simple and can be computed quickly on scarce resourced motes while providing required security services. Further, the mobility of patients is managed securely without the need of frequent reconfigurations during their movement within hospital/home premises. The evaluation results demonstrate that the proposed scheme reduces energy utilization to 17.84% and increases longevity of motes by 5.6 times compared to Certificate-Based Datagram Transport Layer Security (CB-DTLS). Energy consumption in configuration handover during mobility is handled by resource-rich devices, which make this scheme efficient in managing mobility of sensors. This work can be used as a basis for future research on securing patient data in an e-health system using energy efficient cryptographic operations.*

Keywords: *Internet of Things, sensors, MQTT, lightweight security, energy efficiency, e-health.*

Received April 4, 2020; accepted September 27, 2020
https://doi.org/10.34028/iajit/18/6/4

1. Introduction

Internet of Things (IoT) is the interconnection of miniature devices equipped with sensing, actuating, and communication capabilities enabling them to sense environmental or physiological phenomena, share it with other devices and take actions of their own with zero or minimal human intervention [22, 33, 49]. The devices in IoT can be physical objects (smart phone, camera, sensor, vehicle, and drone) or virtual objects (electronic ticket, agenda, book, and wallet). The swift growth of IoT and its enormous capabilities make it useful to realize the goal of smart environment around us such as smart education, intelligent transportation, smart cities, smart healthcare, etc., [5]. It is estimated that 25.44 billion objects will be equipped with sensing, actuating, and communicating capabilities and will be connected to the internet by 2030 [24], resulting in a $14.2 trillion boost in the economy worldwide [36].

The increasing cost of healthcare and the occurrence of acute diseases globally require shifting healthcare services from hospital system to the home system with a focus on monitoring patient health remotely for improving quality of life and wellbeing [21]. It is predicted that the current way of healthcare will be transformed to home-centered by 2030 [32] and IoT plays an important role in bringing this transformation [32]. IoT presents an inconspicuous and cost-effective solution to e-health, however, the application of IoT in the healthcare domain is hindered if security and privacy concerns of Electronic Health Records (EHRs) are not addressed properly which can lead to a disastrous situation [3].

In a remote healthcare system, the sensed medical data has to pass through insecure network infrastructure i.e., internet and is vulnerable to attacks [42]. Therefore, securing communication in an e-health system becomes critical. In this regard, the authentication of end-users (patients and caregivers) and safeguarding sensed medical data of patients from intruders are key pre-requisites [26]. Traditional security mechanisms used for other wireless networks cannot be directly used in IoT-based e-health system [11] because of the limited processing power, memory, battery, and communication bandwidth of IoT devices. In this direction, we propose a lightweight security scheme for e-health system that employs Message Queue Telemetry Transport (MQTT) protocol for message exchanges at the application layer. MQTT is an open source, publish-subscribe architecture based lightweight messaging protocol standardized by OASIS [7, 47]. Besides authenticating publisher and subscriber, MQTT relies mostly on Transport Layer Security (TLS) for protecting data from attackers. However, it is worth mentioning that TLS is not the lightest of the protocols and consumes sufficient mote