# 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 energy besides being vulnerable to Compression Ratio Info-leak Made Easy (CRIME), Heartbleed, Browser Exploit Against SSL/TLS (BEAST), etc., attacks [15, 42]. In this paper, we propose a security mechanism which augments security attribute to contemporary MQTT protocol based on lightweight computations for e-health IoT system. The architecture of the proposed e-health IoT system is shown in Figure 1.

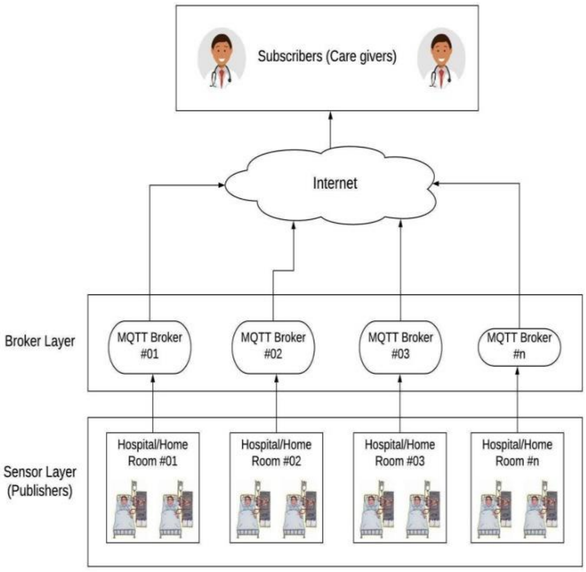

Figure 1. Architecture of IoT based e-health system.

In this architecture, the hospital/home area is divided into a number of monitoring areas and each area is having a separate MQTT broker so as not to disrupt the continuous monitoring of patients during their mobility. The medical sensors attached to patients act as publishers and have limited resources, while as, the MQTT broker being stationary is equipped with sufficient resources in terms of power, memory and communication bandwidth. MQTT broker transfers data through the internet and then to the appropriate subscribers (caregivers).

In healthcare IoT systems, improving patient's quality of life is important to mitigate the negative effects of being hospitalized [34]. Providing patients with the possibility to walk around the medical environments knowing that the monitoring of their health condition is not interrupted is an important feature [34]. Enabling mobility support for patient monitoring system offers a high quality of medical service as it allows patients to move around freely within the premises. In this article, a secure mechanism for mobility enabled e-health IoT system is proposed. The primary focus of this research work is to incorporate resource efficient security scheme for e-health systems. This has been achieved by using lightweight messaging protocol i.e., MQTT for exchanging medical data between patient and caregiver. The literature study on MQTT establishes the fact that MQTT is constrained for use in applications due to its dependence on transport layer security protocols i.e., TLS. In this paper, we addressed this issue by relieving MQTT from resource intensive protocol i.e., TLS in order to achieve the benefits of its usage in terms of low overhead and lightweight features. The main contributions of this article include:

- An end-to-end lightweight security mechanism for IoT based e-health system.
- The proposed scheme facilitates the mobility of patients while maintaining security and privacy intact in a particular monitoring area such as a hospital or home.

The analysis of our scheme depicts significant improvement in saving mote energy for protecting sensed medical data of patients, thereby increasing mote lifetime.

The work done in this research article is original and is based on the problem identified in order to secure MQTT communications in an IoT domain. The paper identifies the need of implementing secure mechanism for MQTT based e-Health systems. The overall scenario of an e-health system has been created in Cooja simulator and the evaluation of the proposed mechanism is compared with existing state-of-the-art mechanisms. The rest of the paper is organized as follows. Section 2 presents the existing work for securing MQTT and e-health systems. Section 3 describes the constructs that have been used to develop the proposed security mechanism. The proposed security concept and algorithm is presented in section 4. The details of implementation are presented in section 5. Section 6 illustrates the implementation results of the proposed security mechanism and its comparison with existing schemes. Finally, the conclusion of the work done in this paper is presented in section 7.

## 2. Related Work

Researchers in [2, 10, 18, 23, 51] have presented and discussed the necessity of addressing security and privacy issues in IoT based healthcare systems and have concluded that because of security and privacy issues in IoT based healthcare systems, many medical consultants and healthcare providers prefer to store Electronic Health Records (EHRs) of patients on local storages which are not connected to internet. An exhaustive literature review on security and privacy concerns in healthcare systems has been presented in [23]. Authors have discussed the blockchain-based solution for security and privacy issues in IoT based healthcare system. The authors illustrated the advantages of addressing security issues and developing of solutions for IoT based healthcare system.

Chen *et al*. [13] proposed a confidentiality scheme for the Publish-Subscribe system using symmetric key cryptography. In this scheme, the publisher is required to distribute a random number and a key to every subscriber. The random number is used by publishers and subscribers to conceal their actual information from brokers by adding a random number to it. The disadvantage of this method is that it needs the publisher to create a connection with every subscriber in order to redistribute random number and keys whenever the subscriber joins back to the system. Jara *et al*. [27] presented architecture for remote healthcare monitoring based on IoT. The proposed architecture appears to be promising in remote monitoring of patients, however, the architecture does not explain the management of emergency situations. Elhoseny *et al*. [20] proposed a secure information transmission system for IoT based e-health systems that provide confidentiality and integrity services. The proposed scheme uses steganography and encryption methods to protect sensitive information from attackers. Since the IoT devices are resource constrained and using both of these security schemes consume significant node resources. The research work in [1] presented a security scheme that offloads the resource intensive tasks to fog node. The proposed scheme employs identity-based encryption, and identity-based signature to provide authentication, non-repudiation and confidentiality services. A secure architecture for e-health IoT system based on certificate-based Datagram Transport Layer Security (DTLS) handshake protocol is proposed in [34]. The proposed architecture uses a secure key management scheme between medical sensors and gateways, therefore, making the architecture more secure than centralized delegation-based architecture. However, the energy consumption of this security scheme is higher and drains the node energy quickly.

A secure mechanism for IoT systems has been suggested in [40] where a node-specific fixed master key is embedded to devices during the initial registration phase. A shuffling algorithm, based on some challenge, is then applied to create dynamic cryptographic keys on the client as well as server-side. However, it is doubtful how the client and server use the same challenge to shuffle the master key by equal shifts. Further, the master key imprinted in the devices is easily accessible to the adversary that can launch a shuffling algorithm and obtain the cryptographic keys, thereby leading to network compromisation. A security mechanism based on Elliptic Curve Cryptography (ECC) algorithm has been proposed in [31]. The proposed mechanism provides authentication service; however, the resource analysis of the proposed mechanism has not been delineated. An ECC based secure mechanism has been proposed in [4] for protecting application layer data from attackers. The proposed mechanism has been evaluated and compared with Rivest-Shamir-Adleman (RSA) algorithm.

An authentication mechanism based on Single-User-Sign-Inpolicy has been proposed for IoT based e-health systems [17]. The proposed mechanism provides better authentication for Cloud connected Medical Things and consumes less computation overhead. Chattopadhyay *et al*. [12] proposed a secure framework for IoT-based e-health systems. The proposed framework contains three communication channels viz a channel from bio-sensor node to the processing unit, another channel from processing unit to the gateway and third channel from gateway to the cloud.

Pasha and Shah [37] proposed a framework for Internet of Things based healthcare system considering the characteristics of interoperability, varied standards and protocols in the framework design. The proposed framework was demonstrated to be secure by security experiments.

It is concluded from the literature survey that the security and privacy concerns of e-health data hinders its usage and widespread adoption. Thus, an efficient and secure scheme for IoT-based healthcare systems is prime requirement.

## 3. Background

This section briefly describes the details of the chosen constructs in the proposed security scheme.

### 3.1. Message Queue Telemetry Transport

It is a lightweight, simple, open source messaging protocol for resource-constrained networks, standardized by OASIS [7]. It is based on Publish-Subscribe architecture where an entity namely publisher pushes messages on a topic that is subscribed by subscriber(s). The messages are exchanged through a specialized node known as MQTT broker [47]. A variant of MQTT known as MQTT-SN (Sensor Networks) is used for Low power Lossy Network (LLN) such as IoT and Wireless Sensor Networks (WSN).

In many applications, Constrained Application Protocol (CoAP) is used for message communications at the application layer in IoT. However, there are certain important advantages of using MQTT-SN over CoAP. For example, packet header size of CoAP is 4 bytes while MQTT-SN needs only 2 bytes for packet header. The message transmission time of MQTT-SN is significantly less than CoAP, outperforming CoAP by 30% for average transmission time [6]. This motivates us to use MQTT-SN as the protocol for message communication in IoT based e-health system.

### 3.2. Pcg-Rand

Random numbers find applications in cryptography with an important requirement that the past sequences must not be repeated nor discovered, which could otherwise ease attackers to break the cryptographic system [29]. Random Number Generators (RNGs) fall into two main categories i.e., True RNG (TRNG) which captures random real-world events to create random sequences. However, implementing TRNG requires additional hardware to capture real-world events, therefore making TRNG more expensive [44]. The second category known as Pseudo-Random Number Generator (PRNG) considers that algorithms with erratic outputs are copious to generate random sequences. However, PRNGs are not cryptographically secure because of their high periodicity and predictability rate that make them unfit for cryptographic applications.

A new class among PRNG known as Cryptographically Secure Random Number Generators (CSRNG) is employed for cryptographic applications as these are statistically efficient with difficult predictability rate. O'Neil [35] presents a list of CSRNGs with their comparative study. It was observed that pcg-family provides excellent statistical quality with challenging predictability, fast time performance and small code footprint [34]. Because of these features, pcg-rand has been used as CSRNG to generate security keys in our proposed security mechanism.

### 3.3. Why Lightweight Cryptography?

IoT consists of devices that are limited in size and constrained in terms of storage, energy and computational capability [48]. The main challenge of embedding security to IoT devices lies in their insubstantial node resources to execute conventional security algorithms [8, 30, 38, 39, 48]. Augmenting security to IoT system is essential as concluded in [47] that "The future of IoT system will depend on our capability to competently secure difficult-to-secure, resource-limited devices".

One of the possible ways to embed security to IoT devices is to tailor existing complex secure algorithms so that they will consume less node energy, but the research work in [9] illustrated that the tailored version of such algorithms still remains complex for IoT devices. The other way is to design lightweight cryptographic protocols that use simple secure components without compromising the security of critical data at nodes which is the primary focus of our research.

## 4. Proposed Mechanism

The proposed mechanism consists of a Trusted System (TS), MQTT Broker, Publisher, and Subscriber. TS, being reliable, is used for handling trust relationships among motes and is responsible for generating key material used for cryptographic operations. During the initial registration phase, TS assigns a Pre-Shared Secret (PSS) to each new device that wants to be added to the IoT network. PSS is assumed to be stored securely during the registration phase using secure bootstrapping (e.g., a technique in [28]). Therefore, the IoT motes and TS are assumed to be in a trust relationship based on PSS. The proposed solution uses MQTT protocol to which security elements are augmented by enciphering MQTT payload using a symmetric cryptosystem. The proposed system employs pcg-rand as a CSRNG because of its properties as defined in section 2. In our proposed system, the encryption keys are valid for each communication session only and are destroyed after session expires. The message exchange process in the proposed system is shown in Figure 2.

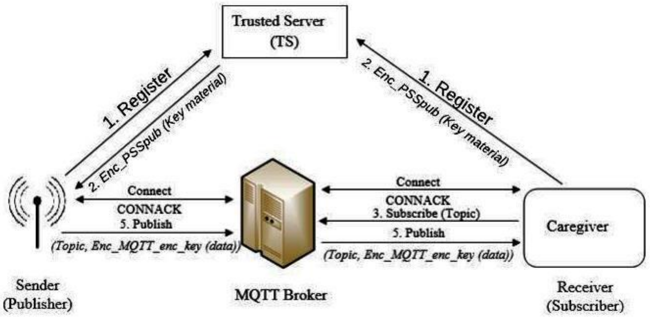

Figure 2. Message exchange.

In Figure 2, each client node (Publisher and Subscriber) has to register itself with TS before any communication can occur. TS assign PSS to each client node which is used to exchange key material between TS and client nodes. After a successful key exchange process between TS and publisher node, the sensed data is encrypted and forwarded over a topic to Broker. Based on the subscription information, the broker node forwards the received encrypted data from Publisher to intended Subscriber which deciphers the received data using the key obtained from TS.

### 4.1. Security System

The proposed security system concept is as follows:

- Medical sensor nodes implanted on patients are embedded with unique PSS during the initial registration process.
- TS sends key material to implanted sensors by encrypting it with PSS$_i$ corresponding to each mote. The message format is as follows:

  Enc_PSS$_i$ (Key material)
- Publisher (sender) performs encryption operation as soon as the data is sensed.
- A simple cryptographic operation is used to encrypt data with a key such as invertible exclusive-OR (XOR). Other lightweight encryption methods such as HIGHT [25], RECTANGLE [50], TWINE [45] can also be used so that the cryptographic computations do not consume much node energy.
- Encrypted data is published to MQTT broker which

forwards it to the appropriate Subscriber (receiver) in the format:

Enc_MQTT_enc_key (data)

- Subscriber launchesdecryption algorithm to decipher the transmitted message and takes appropriate action.
- Both the keys (encryption and decryption) are destroyed after the message is delivered successfully.

### 4.2. Mobility System

The key and congenial feature of an e-health system is to allow patients to walk around the home/hospital rooms without affecting their continuous observation. The use of a portable patient monitoring system provides a high-quality medical service by allowing patients to move freely within home/hospital premises. The main objective of continuous observation in e-health system is to obtain EHRs that allows remote caregivers to discover symptoms and manage ailments. To achieve mobility support in e-health system, we propose broker-broker communication for exchanging configuration and authentication details of a mobile node among themselves i.e., develop handover mechanism among MQTT brokers that saves time and energy spent on frequent reconfigurations.

Whenever a patient walks through different rooms in the home/hospital area, the configuration details are handed over from its native MQTT broker to the visited broker so that there will be no delay in transmitting EHRs, which is caused by reconfiguration tasks to be completed before getting connected to the visited broker. This is more serious issue when a patient moves to other broker site and there occurs an emergency situation. In this scenario, sensor motes must publish EHRs quickly without spending time in reconfigurations. At the same time, the cryptographic operations must not be too complex such that the time for encryption will be more, and accordingly the emergency care will get delayed. Therefore, a lightweight and quick encryption pattern is also provided in this research along with mobility support.

We consider an example mobility scenario, consisting of several MQTT brokers for relaying medical data of patients to caregivers in a patient monitoring system at the hospital. When a patient moves through different wards or examination labs (e.g., due to medical tests), he gets disconnected from the native MQTT broker, thereby halting his continuous health observation. It is particularly important to allow seamless transmission of sensed medical data during mobility in situations where real-time monitoring is needed. Our proposed method provides the solution to this problem in such a way that when a patient moves to a different area, the main broker to which the sensor is authenticated with will update and handover configuration data to visited broker, thereby avoiding reconfigurations which saves its energy and time to forward medical details. However, when a new sensing mote is detected, the registration and authentication must be performed which prevents unauthorized activity.

## 5. Experimentation

### 5.1. IoT Operating System and Motes

We used Contiki Operating System (OS) with z1 motes to create experimental setup. The rationale for using Contiki [14] as a tool for simulation of the proposed mechanism is that it is an open source tool, providing support for many protocols, such as Internet Protocol version 6 (IPv6), CoAP, Routing over Low Power and Lossy Networks (RPL), and MQTT. Contiki uses standard C-language for creating application programs that can be tested in the Cooja simulator prior to burning to IoT motes. The experimental setup consists of four z1 motes, out of which one mote act as TS, two motes are configured as MQTT clients (Publisher and Subscriber) and the fourth mote is set as RPL border router, used to assign IPv6 addresses to MQTT clients and to communicate with external internet.

### 5.2. Performance Metrics

IoT consists of resource-limited devices and require efficient utilization of node resources to provide services for a longer period of time. Therefore, we use energy consumption of IoT devices to assess the performance of our proposed mechanism. Powertrace utility of the Contiki OS is used to evaluate the node energy consumption which gives the count of timer ticks or usage time of processor and radio [19]. The count of timer ticks for processor and radio modes is converted to energyusing the following formula [19]:

$$\text{Energy (mJ)} = \frac{Energest_{Value}\ x\ Current\ (mA)\ x\ Voltage\ (V)}{RTIMER\_ARCH\_SECOND\ X\ Time\_Duration} \qquad (1)$$

Where “*Energest_value*” is the periodic value printed by Energest, “*RTIMER_ARCH_SECOND*” is the number of ticks performed by the internal CPU timer per second, that is 32768 in this case and “*Time_Duration*” is the time in seconds from the previous Energest measurement. To calculate the power consumption of the proposed mechanism on z1 motes, we use current and voltage values of processing and radio as given in the z1 datasheet [46, 52]. The operational voltage in both modes is 3v. We have also measured memory usage with the help of built-in objdump tool of Linux.

## 6. Results and Discussions

In this section, the results of our experiments are presented and compared with other existing schemes for IoT [34, 40, 41].

## 6.1. Energy Consumption

The comparative analysis of energy consumption by IoT motes for cryptographic operations is shown in Figure 3.

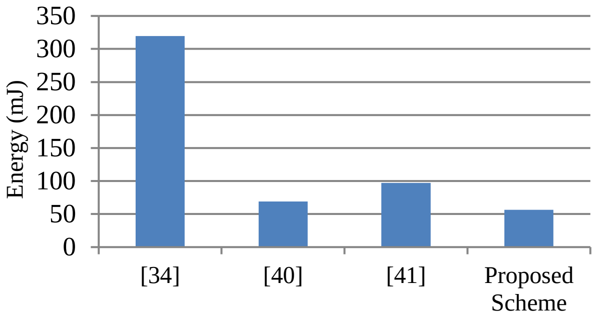

Figure 3. Energy consumption comparison.

It is depicted from Figure 3 that the proposed security mechanism consumes less energy for encryption of sensed data at IoT motes. The reason for consuming less energy is that our proposed mechanism uses lightweight cryptographic operations to scramble the sensed data into intangible data.

## 6.2. Memory Consumption

The implementation of the proposed scheme requires 5608 bytes of memory, which is affordable by IoT motes. For example, z1 mote has 92KB of memory and can surely accommodate our proposed mechanism. The comparison of memory requirements with other schemes is shown in Figure 4.

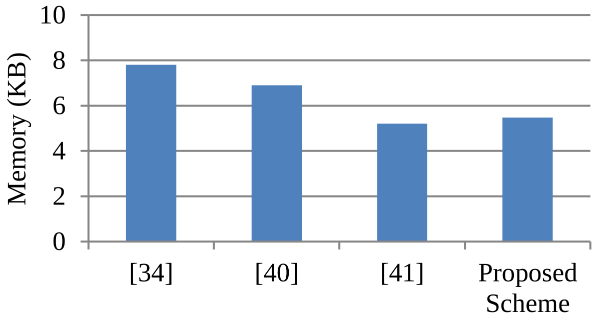

Figure 4. Memory consumption comparison.

## 6.3. Expected Battery Lifetime

Battery lifetime is useful in determining the mote lifetime and is calculated by dividing the total energy of mote with energy consumed in each transaction. Each transaction consists of encryption, transmission/reception and decryption. Suppose the motes are powered with two AA batteries (2800 mAh) and the lifetime of each scheme is calculated on a varied number of transactions per hour as depicted in Figure 5.

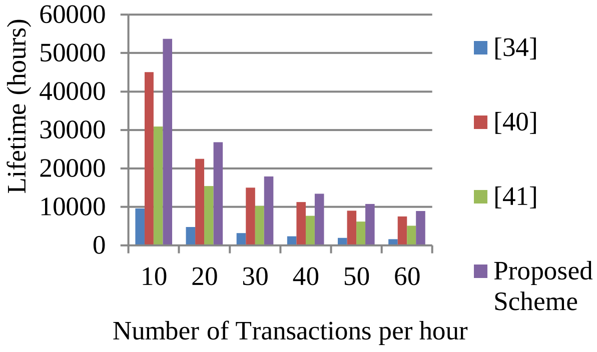

Figure 5. Node lifetime comparison.

Figure 5 presents the lifetime of motes with a varied number of transactions per hour. We observe that the expected lifetime of the proposed scheme is about 53664 hours (corresponding to 10 transactions per hour), approximately 5.6 times the corresponding value for Certificate-Based Datagram Transport Layer Security (CB-DTLS) (9575 hours). Therefore in all usage scenarios, proposed scheme is superior with respect to the expected lifetime.

## 6.4. Security Analysis

### 6.4.1. End-to-End Message Confidentiality

The proposed mechanism provides end-to-end security using a lightweight cryptographic algorithm, thereby providing message confidentiality service among communicating entities. In such a scheme, if an attacker snoops on the transmitted medical data, he cannot access the actual message contents as the message is encrypted with 64-bit dynamic key. A brute force attack on a 64-bit key would require 1.84 x $10^{19}$ years [16].

### 6.4.2. Forward Security

Forward security assures that the disclosure of current enciphered health data should not threaten the security of formerly exchanged data. In our scheme, the key is generated randomly using CSRNG with 64-bit key size, therefore making it difficult for an attacker to get previously encrypted data if, somehow, he gets success in deciphering the current communicated message.

### 6.4.3. Spoofing Attack

Since all the messages exchanged between publisher and subscriber pass through the MQTT broker, therefore if an attacker attempts to hijack the MQTT broker to get access to communicating messages. In such a scenario, an attacker doesn't breach the system as the MQTT broker is itself devoid of cryptographic keys which are possessed by publisher and subscriber only. This makes the attacker unable to see the actual contents of the message.

## 7. Conclusions

In this paper, we presented a lightweight security mechanism for IoT based e-health system. The proposed mechanism uses lightweight messaging protocol for exchanging medical data between client nodes and uses lightweight cryptographic operations to encipher the sensitive data. Results show that our scheme provides efficient utilization of node energy and increases the longevity of medical sensors by a considerable figure. The mote lifetime in our scheme is 5.6 times greater than the method described in [33] consuming only 17.84% of energy than [34]. Along with end-to-end data confidentiality, our scheme provides mobility services for patients by allowing them to walk around hospital wards without affecting their continuous observation by caregivers. Our proposed encryption system is resilient to spoofing attack, brute force attack and provides forward secrecy. Therefore, our scheme, being energy efficient, provides end-to-end data confidentiality and mobility support in IoT based e-health systems. We conclude from the research work in this paper that by consuming less energy in node related operations, we can enhance the lifetime of IoT devices substantially that will allow the IoT sensors to monitor the area under observation for longer period of time.

## References

[1] Abbas N., Asim M., Tariq N., Baker T., and Abbas S., "A Mechanism for Securing IoT-enabled Applications at the Fog Layer," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, pp. 16, 2019.

[2] Abouelmehdi K., Beni-Hssane A., Khaloufi H., and Saadi M., "Big Data Security and Privacy in healthcare A Review," *Procedia Computer Scienc*e, vol. 113, pp. 73-80, 2017.

[3] Ahamed F. and Farid F., "Applying Internet of Things and Machine-Learning for Personalized Healthcare: Issues and Challenges," *in Proceedings of International Conference on Machine Learning and Data Engineering*, Sydney, pp. 19-21, 2018.

[4] Albalas F., Al-Soud M., Almomani O., and Almomani A., "Security-Aware CoAP Application Layer Protocol for the Internet of Things using Elliptic-Curve Cryptography," *The International Arab Journal of Information Technology*, vol. 15, no. 3A, pp. 550-558, 2018.

[5] Alzahrani S., "Sensing for the Internet of Things and its Applications," *in Proceeding of 5th International Conference on Future Internet of Things and Cloud Workshops*, Prague, pp. 88-92, 2017.

[6] Amaran M., Noh N., Rohmad M., and Hashim H., "A Comparison of Lightweight Communication Protocols in Robotic Applications," *Procedia Computer Science*, vol. 76, pp. 400-405, 2015.

[7] Banks A. and Gupta R., MQTT Version 3.1.1., OASIS Standard. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/ mqttv3.1.1-os.html, Last Visited, 2019.

[8] Bello O. and Zeadally S., "Intelligent Device-to-Device Communication in the Internet of Things," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1172-1182, 2016.

[9] Biswas K., Muthukkumarasamy V., Wu X., and Singh K., "Performance Evaluation of Block Ciphers for Wireless Sensor Networks," *in Proceedings of International Conference on Advanced Computing and Communication Technologies*, New Delhi, pp. 443-452, 2016.

[10] Cha S., Hsu T., Xiang Y., and Yeh K., "Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges," *IEEE Internet Things*, vol. 6, no. 2, pp. 2159-2187, 2019.

[11] Chakravorty R., "MobiCare: A Programmable Service Architecture for Mobile Medical Care," *in Proceedings of 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, Pisa, 2006.

[12] Chattopadhyay A., Nag A., Ghosh D., and Chanda K., "A Secure Framework for IoT-Based Healthcare System," *in Proceedings of the International Ethical Hacking Conference*, Kolkata, pp. 383-393, 2018.

[13] Chen W., Jiang J., and Skocik N., "On the Privacy Protection in Publish/Subscribe Systems," *in Proceedings of International Conference on Wireless Communications, Networking and Information Security*, Beijing, pp. 597-601, 2010.

[14] Contiki., "Contiki: The Open Source Operating System for the Internet of Things," http://www.contiki-os.org/, Last Visited, 2017.

[15] Curguz J., "Vulnerabilities of the SSL/TLS Protocol," *Computer Science and Information Technology*, vol. 6, pp. 245-256, 2016.

[16] Daemen J. and Rijmen V., *the Design of Rijndael*, Springer, 2002.

[17] Deebak B. and Al-Turjman F., "Secure-User Sign-in Authentication for Iot-Based Ehealth Systems," *Complex and Intelligent Systems*, pp. 1-21, 2021.

[18] Ding L., Wang Z., Wang X., and Wu D., "Security Information Transmission Algorithms for Iot Based On Cloud Computing," *Computer Communications*, vol. 155, pp. 32-39, 2020.

[19] Dunkels A., Eriksson J., Finne N., and Tsiftes N., "Powertrace: Network-level Power Profiling for Low-Power Wireless Networks," SICS Technical Report T2011:05, 2011.

[20] Elhoseny M., Ramirez-Gonzalez G., Elnasr O., Shawkat S., Arunkumar N., and Farouk A., “Secure Medical Data Transmission Model for IoT-Based Healthcare Systems,” *IEEE Access*, vol. 6, pp. 20596-20608, 2018.

[21] El-Zouka H. and Hosni M., “Secure IoT Communications for Smart Healthcare Monitoring System,” *Internet of Things*, vol. 13, no. 3, 2021.

[22] European Commission Information Society, Internet of Things Strategic Research Roadmap, 2009.

[23] Hathaliya J. and Tanwar S., “An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0,” *Computer Communications*, vol. 153, pp. 311-335, 2020.

[24] Holst A., “Number of IoT Connected Devices Worldwide 2019-2030,” https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, Last Visited, 2021.

[25] Hong D., Sung J., Hong S., Lim J., Lee S., Koo B., Lee C., Chang D., Lee J., Jeong K., Kim H., Kim J., and Chee S., “HIGHT: A New Block Cipher Suitable for Low-Resource Device,” *in Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems*, Yokohama, pp. 46-59, 2006.

[26] Hummen R., Shafagh H., Raza S., Voig T., and Wehrle K., “Delegation based Authentication and Authorization for IP-based Internet of Things,” *in Proceedings of the 11th IEEE International Conference on Sensing, Communication, and Networking*, Singapore, 2014.

[27] Jara A., Zamora-Izquierdo M., and Skarmeta A., “Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 47-65, 2013.

[28] Kang N., Oh S., and Yoon S., “Secure Initial-Key Reconfiguration for Resource Constrained Devices,” IETF draft-kang-core-secure-reconfiguration- 01, 2014.

[29] Kenny C., “Random Number Generators: An Evaluation and Comparison of Random.Org and some Commonly Used Generators, 2005,” http://www.random.org/analysis/Analysis2005.pdf, Last Visited, 2021.

[30] Kent S. and Seo K., “Security Architecture for the Internet Protocol,” RFC 4301, 2005.

[31] Khan S. and Aggarwal R., “Efficient Mutual Authentication Mechanism to Secure Internet of Things (IoT),” *in Proceedings of International Conference on Machine Learning, Big Data, Cloud and Parallel Computing*, Faridabad, pp. 409-412, 2019.

[32] Koop E., Mosher R., Kun L., Geiling J., Grigg E., Long S., Macedonia C., Merrell R., Satava R., and Rosen J., “Future Delivery of Health Care: Cybercare,” *IEEE Engineering in Medicine and Biology Magazine*, vol. 27, no. 6, pp. 29-38, 2008.

[33] Li S., Xu L., and Zhao S., “The Internet of Things: A Survey,” *Information Systems Frontiers*, vol. 17, pp. 243-259, 2015.

[34] Moosavi S., Gia T., Rahmani A., Nigussie E., Virtanen S., Isoaho J., and Tenhunen H., “SEA: a Secure and Efficient Authentication and Authorization Architecture for Iot-Based Healthcare using Smart Gateways,” *Procedia Computer Science*, vol. 52, no. 1, pp. 452-459, 2015.

[35] O’Neil M., “Pcg: A Family of Simple Fast Space-Efficient Statistically Good Algorithm for Random Number Generation. HMC-CS-2014-0905,” Technical Report, Harvey Mudd College, 2014.

[36] Pascu L., “IoT Disrupts Market; could add $14.2 Trillion to Global Economy by 2030,” https://www.bitdefender.com/box/blog/iot-news/iiot-disrupts-market-add-14-2-trillion-global-economy-2030/, Last Visited, 2019.

[37] Pasha M. and Shah S., “Framework for E-Health Systems in IoT-Based Environments,” *Wireless Communications and Mobile Computing*, vol. 18, pp. 1-12, 2018.

[38] Polk T. and Turner S., “Security Challenges for the Internet of Things,” *IETF Security*, 2011.

[39] Rifà-Pous H. and Herrera-Joancomartí J., “Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices,” *Future Internet*, vol. 3, no. 1, pp. 31-48, 2011.

[40] Sahraoui S. and Bilami A., “Efficient HIP-Based Approach to Ensure Lightweight End-To-End Security in Internet of Things,” *Computer Networks*, vol. 91, pp. 26-45, 2015.

[41] Saied Y. and Olivereau A., “D-HIP: A distributed Key Exchange Scheme for HIP-Based Internet of Things,” *in Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, San Francisco, pp. 1-7, 2012.

[42] Saleem W., Ali H., and AlSalloom N., “A Framework for Securing EHR Management in the Era of Internet of Things,” *in Proceedings of 3rd International Conference on Computer Applications and Information Security*, San Francisco, pp. 1-5, 2020.

[43] Sirohi P., Agarwal A., and Tyagi S., “A Comprehensive Study on Security Attacks on SSL/TLS Protocol,” *in Proceedings of 2nd International Conference on Next Generation Computing Technologies*, Dehradun, pp. 893-898, 2016.

[44] Sunar B., Martin W., and Stinson D., "A Provably Secure True Random Number Generator with Built-in Tolerance to Active Attacks," *IEEE Transactions on Computers*, vol. 56, no. 1, pp. 109-119, 2006.

[45] Suzaki T., Minematsu K., Morioka S., and Kobayashi E., "TWINE: A Lightweight Block Cipher for Multiple Platforms," *in Proceedings of International Conference on Selected Areas in Cryptography*, Burnaby, pp. 339-354, 2013.

[46] Texas Instruments., "MSP430F261x MSP430F241x Mixed Signal Microcontroller datasheet," http://www.ti.com/lit/ds/symlink/msp430f2618.pdf, Last Visited, 2019.

[47] The HiveMQ Team, "MQTT Essentials," https://www.hivemq.com/blog/mqtt-essentials-part-3-client-broker-connection-establishment, Last Visited, 2018.

[48] Trappe W., Howard R., and Moore R., "Low-Energy Security: Limits and Opportunities in the Internet of Things," *IEEE Security and Privacy*, vol. 13, pp. 14-21, 2015.

[49] Xu D., He W., and Li S., "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233-2243, 2014.

[50] Zhang W., Bao Z., Lin D., Rijmen V., Yang B., and Verbauwhede I., "RECTANGLE: a Bit-Slice Lightweight Block Cipher Suitable for Multiple Platforms," *Science China Information Sciences*, vol. 58, pp. 1-15, 2015.

[51] Zhou J., Cao Z., Dong X., and Vasilakos A., "Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26-33, 2017.

[52] Zolertia., "Z1 Datasheet," https://github.com/Zolertia/Resources/blob/master/Z1/Hardware/Revision%20C/Datasheets/Zolertia%20Z1%20datasheet%20Revision%20C. pdf, Last Visited, 2019.

**Adil Bashir** received his Bachelor of Technology (B. Tech) in Computer Science and Engineering from Islamic University of Science and Technology, Jammu and Kashmir, India in year 2011. He did his Master of Technology (M. Tech) in Communication and Information Technology and PhD both from National Institute of Technology (NIT) Srinagar, India in the year 2013 and 2021 respectively. Presently, he is an Assistant Professor in the Department of Computer Science and Engineering at Islamic University of Science and Technology, Awantipora, Kashmir. His research interests are Internet of Things, Wireless Sensor Networks, Embedded Systems and Network Security.

**Ajaz Hussain Mir** has done his Bachelor of Engineering (B.E) in Electrical Engineering with specialization in Electronics & Communication Engineering (ECE). He did his Master of Technology (M.Tech) in Computer Technology and PhD both from IIT Delhi in the year 1989 and 1996 respectively. He is Chief Investigator of Ministry of Communication and Information Technology, Govt. of India project: Information Security Education and Awareness (ISEA).

Presently, he is Professor in the Department of Electronics & Communication Engineering at NIT Srinagar, India. He has been guiding PhD and M.Tech thesis in Security and other related areas and has a number of International publications to his credit. His areas of interest are Biometrics, Image processing, Security, Wireless Communication and Networks.