scientific reports

Check for updates

OPEN

An IoT based remote medical diagnosis system using one time pad cipher over MQTT protocol

N. Rajesh Kumar[1]✉, R. Bala Krishnan[1], Subramaniyaswamy Vairavasundaram[2]✉, G. Manikandan[3], Indragandhi V[4] & Logesh Ravi[5,6]

Internet of Things (IoT) is an emerging technology that consists of tiny sensors embedded with IoT devices used in e-Health, smart cities and assisted living. IoT devices are equipped with constrained power, memory, and computing capabilities, which creates new security challenges. By integrating sensors and wireless technologies, this cutting-edge technology automates numerous routine tasks in different domains. The main goal of advancing IoT in the existing healthcare system is to automate the monitoring of hospitals and patients' health by spreading goodwill toward the IoT vision. IoT has gained popularity on practically all platforms that are available. This paper presents a remote patient health monitoring and diagnosis system that uses Message Queuing Telemetry Transport protocol (MQTT) and Internet of Things (IoT) devices with one time pad cryptography. The proposed plan offers end-to-end data secrecy for an IoT system using MQTT that enables e-health and mobility. Patients' movements inside nursing homes and healthcare facilities are also managed safely without the need for periodic reconfigurations. Prior to communicating through the MQTT protocol, this secure crypto scheme encrypts the message on both the publisher and subscriber ends. According to the results, the proposed scheme is more efficient than delegation-based architecture in terms of security and lightweight communication. The proposed system established communication between patients and medical experts using IoT technologies to alleviate the hospital strain caused by congestion in medical treatment and enable an expressway of medical responses. According to our results the proposed scheme has low computational overhead compared to other solutions that use conventional encryption to guarantee robust protection against most of the IoT security attacks.

Keywords Internet of things (IoT), MQTT, Smart healthcare, One time pad cipher

Today's generation lives in a highly sophisticated environment with many electronic gadgets that make life easier and more comfortable for day-to-day life. Both physical (such as a smartphone, camera, sensor, car, or drone) and virtual (such as an electronic ticket, agenda, book, or wallet) objects can be considered IoT devices. IoT's rapid development and vast capabilities make it ideal for achieving the objective of a smart environment around us, including smart cities, smart transportation, smart education, smart healthcare, etc. As people's intellectual capacity and level of living improved due to the rapid changes in human lifestyles have led to an increase in demand for quick remedy healthcare services.

The rising cost of healthcare and the prevalence of acute illnesses around the world have led to an increase in healthcare. Healthcare services must be provided at home instead of in hospitals, with a focus on remotely monitoring patient health to enhance quality of life and wellness. Every human being values timely and efficient medical care.

One of the most difficult objectives for many individuals in the current situation is to design an efficient biomedical system for maintaining a secure and rapid healthcare solution. People typically demand high-quality healthcare systems from healthcare facilities. It is challenging to provide patients with high-quality treatment while controlling expenses and addressing the nurse workforce shortage issue. It is a given that these intelligent healthcare systems assist both the sick and the villages. It is essential to create a healthcare system that would

[1]Srinivasa Ramanujan Centre, SASTRA Deemed University, Kumbakonam, Tamil Nadu, India. [2]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. [3]School of Computing, SASTRA Deemed University, Thanjavur, Tamil Nadu, India. [4]School of Electrical Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. [5]Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, Tamil Nadu, India. [6]School of Electronics Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India. ✉email: rajeshkumar.rb@src.sastra.edu; subramaniyaswamy.v@vit.ac.in

benefit everyone. Numerous modifications were made to raise the standards of healthcare systems once a number of technologies entered the field of medicine and healthcare. According to observations, an increase in the senior population is making hospitals more crowded and adding to doctors' workloads. The expense of healthcare services is rising, which is putting pressure on household and national budgets. More doctors, hospitals, laboratories, and pharmaceutical companies may be hired to serve the growing number of people who require healthcare services, or an effective system could be developed to handle all of these demands. In the healthcare industry, making the proper diagnoses and prescribing medications is crucial. Measurements of physiological signals, patient demographics, and patient symptoms all play a role in the diagnosing process. The patient's age, gender, past medical history, and location are all part of their demographic data. The adoption of IOT is currently essential for structuring and creating smart healthcare systems. IoT offers a discrete and affordable answer to e-health, but if the secrecy of Electronic Medical Records (EMRs) is not properly handled, the installation of smart devices in the medical sector is hampered and could result in a dire circumstance. The sensed medical data in a remote healthcare system has to pass across an insecure network architecture. As a result, it is crucial to secure communication in an e-health system.

The protection of sensed medical data of patients from attackers and the authentication of end-users (patients and caretakers) are crucial prerequisites in this respect. Due to their limited processing capacity, memory, battery life, and communication bandwidth, IoT-based e-health systems cannot use traditional security measures. For the implementation of an adaptive e-health system, the proposed model suggested a scheme that uses the MQTT protocol for message exchanges at the application layer, where MQTT is a lightweight messaging protocol that is open source and built on a publish-subscribe architecture. A generic IoT-based publish-subscribe model for the healthcare system is depicted in Fig. 1. The publisher/subscriber area is split up into a number of monitoring regions in this design, with patients at the publisher's end and medical professionals at the subscriber's end. In order to maintain patient monitoring when they are moving around, each location has its own MQTT broker. The stationary MQTT broker has enough power, memory, and communication bandwidth compared to the medical sensors attached to patients, which serve as publishers and have restricted resources. The MQTT broker sends data to the right subscribers (Medical Practitioners) after first sending it over the Internet.

A major focus of the proposed scheme is to implement a resource-effective secure message transmission scheme for e-health systems. In order to accomplish this, healthcare experts analyzed the patient's current health status and medical history using the lightweight messaging protocol, or MQTT. MQTT mostly uses Transport Layer Security (TLS) to shield data from hackers. The MQTT study demonstrates that MQTT is limited in applications due to its reliance on transport layer security standards. The research work's most significant addition may be its presentation of a lightweight mechanism for the aforementioned e-healthcare system, which permits patient mobility while retaining security and privacy in a specific monitoring zone. The research investigation performed for this article is unique and is based on the issue discovered when attempting to protect MQTT connections in an IoT environment. The study highlights the requirement for secure mechanisms to be implemented for MQTT-based e-Health systems. Message Queue Telemetry Transport is a lightweight, straightforward, freely available message communication protocol for networks with limited resources that has

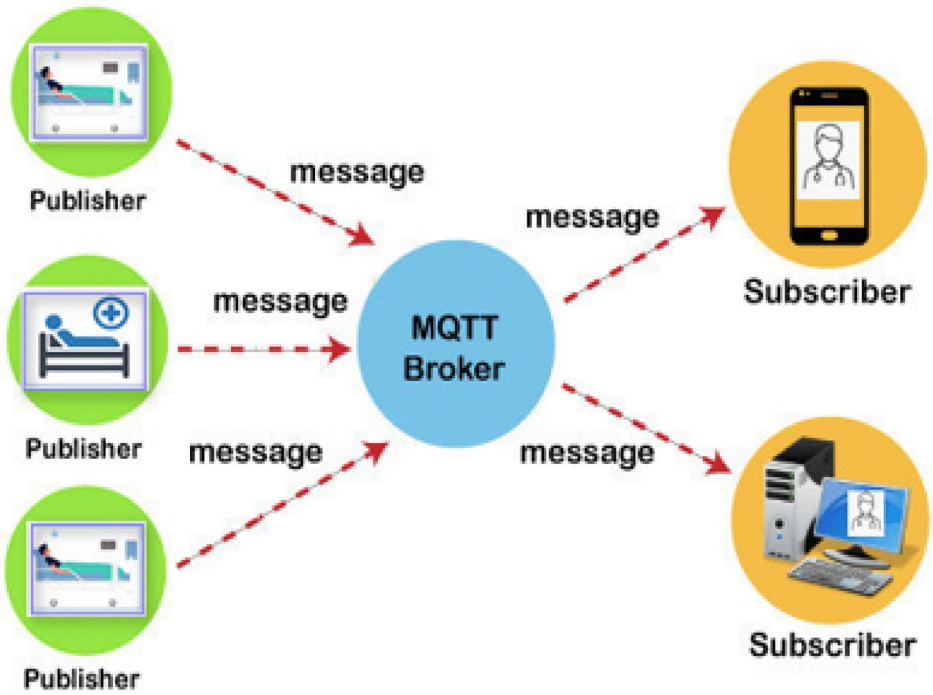

Fig. 1. Architecture of IoT based e-health system with MQTT Broker.

been standardized by OASIS[1]. It relies on publish-subscribe architecture, and a publisher pushes messages on a topic to the brokers and subscriber(s) who have expressed an interest.

The messages are exchanged via an expert node called a MQTT broker. Low power Lossy Networks (LLN) like Wireless Sensor Networks (WSN) based IoT employ a version of MQTT named MQTT-SN (Sensor Networks). Constrained Application Protocol (CoAP), which is used in many IoT applications, is used for message communications at the application layer. However, there are some significant benefits to choosing MQTT-SN versus CoAP. For example, MQTT-SN only requires a 2-byte packet header, but CoAP requires a 4-byte packet header. MQTT-SN performs substantially better than CoAP in terms of average transmission time, outperforming CoAP by 30%[2]. This encourages us to utilize MQTT-SN as the message communication protocol in an Internet of Things-based electronic health system.

The main contributions of the proposed work can be characterised by the following points:

- Development of Secure IoT Framework using One Time Pad cipher using MQTT protocol for remote patient health diagnosis.
- Demonstration of One Time Pad cipher based healthcare message encryption over MQTT protocol.
- Illustration of MQTT broker setup and configuration for handling interaction between patients and medical experts using relevant topics.
- Comprehensive analysis illustrating the superiority of the proposed model over existing approaches in terms of platform performance, security measures and patient mobility.

The rest of this paper is organized as follows. In section "related works", we discuss a detailed literature review on e-health monitoring, importance of secure remote diagnostics systems and effectiveness of IoT based data communication protocols. In section "Proposed Remote Medical Diagnosis System", We present a model of medical image diagnostics using the Internet of Things, as well as a one-time pad cypher to encrypt the message and exchange it through the MQTT. The detailed implementation is given in the section of the "Results and Discussion" along with stringent security analysis of the results and the MQTT-based communication. Section 5 presents the paper's conclusion after all the work has been done.

Related works

The literature review on the solutions of patient monitoring and medical image diagnostics based on Internet of Things is large and diverse. The authors Rathore et al.[3] developed a real-time health care monitoring and response system based on big data analytics. This emergency response tool is suitable for different sectors, such as medical centers, police control rooms, and mobile medical clinics. The authors also evaluate the functionality of this medical response system through high-level computing machines installed with Hadoop tools. A number of health issues patients in the city were tested under a variety of circumstances on their implementation. Zeng et al.[4] proposed a novel solution for monitoring patient health based on ECG signals using IoT technologies. This system mainly used various IoT communication technologies for sensing, communicating, and analyzing the sensor data. WiFi, Bluetooth, and ZigBee are the major standards, and wearable devices are also utilized for the data collection process. Every node is properly set up with web browsers on either end, and they are all connected to other nodes via the HTTP and MQTT protocols. On the other hand, data is kept in different storage servers and visualized from IoT cloud platforms. As a result of this user-friendly approach, medical reports are handled more accurately with a better diagnosis.Park et al.[5] proposed a medical data protection scheme based Shamir's secret sharing scheme. In this method, the participants can choose their things based on authentication and get medical responses securely. Another scheme suggested by the authors Park et al.[6] discusses a number of specific security challenges that are faced by IoT U-healthcare environments, such as the need to protect sensitive patient data and the potential for physical attacks on IoT devices.

Isabel de la Torre Díez et al.[7] provided an excellent summary of the research evidence on the efficacy of IoT-based mental health interventions, as well as an overview of the widely utilized IoT devices and their services being used to support mental health treatment. They also discussed the advantages and difficulties of these approaches. The authors discuss a number of studies that have shown IoT devices can be used to improve monitoring and tracking of mental health symptoms, reduce stress and anxiety, and improve mood and quality of life. Authors Uslu B et al.[2] presented a wide range of factors, including security, privacy, interoperability, scalability, and cost. The strength of the article is to focus on practical aspects of IoT-based smart hospital design. The authors presented concrete guidance on how to select and deploy IoT devices, how to manage data, and how to ensure security and privacy. The authors Sobin C C et al.[8] presented a survey, in which a balanced overview of the pros and cons of different IoT applications including challenges realistically facing on IoT. Another research work stated by the authors Hayek A et al.[9], in which the authors suggested a wearable system for observing vital signs of patients who are affected by epileptic disease in industrial environments. The system is designed to detect seizures and other medical problems early on and to take appropriate action, such as disabling nearby machines and alerting medical personnel. The research work submitted by the authors Kadhim K T et al.[10] suggested different types of smart devices for improving patient health conditions with continuous monitoring and benefits of using IoT for healthcare monitoring, and the challenges that need to be addressed in order to deploy IoT-based healthcare monitoring systems.

A specialized communication system designed by Drăgulinescu, A. M. C et al.[11] for medical services and personal health care usages. This nominated work replaces the current devices with smart IoT devices with low power wide area networks (LPWANs), presenting the advantages and drawbacks of today's systems and technologies. The proposed architecture was implemented in LoPy development boards with IR sensors. The work also discussed in detail about various protection schemes and privacy concerns of the designed architecture. Medical IoT systems are particularly vulnerable to cyber-attacks, so it is important to consider security and

privacy from the design stage. Another research stated by the author Yang X et al.[12], in which an analysis of the research of smart health applications have been presented and a detailed graph has been presented to express the knowledge or capability levels of the available smart Internet of Things based health-care systems.

The research work stated by the authors Muthu B et al.[13] proposed a system using wearable sensors and IoT to predict diseases and analyze symptoms in the healthcare sector. Their intelligence control system gathered data from patients and trained the data using deep learning algorithms for effective prediction. A dedicated cloud-based server is used for data processing, and analyzing for the prediction of patient's risk in developing various diseases. The authors Latif G et al.[14] proposed a healthcare framework named "I-CARES" that minimizes healthcare service delays and the strain that overcrowding in hospitals causes on medical facilities by utilizing smart devices such as Wearable Sensors, Medical dispensers, and a Cloud-based data analysis system.

The research article suggested by the authors Haghparast, M. B et al.[15] proposed a security architecture using the multi-criteria decision-making (MCDM) technique for enabling instance medical services. This new structure dealt with the layers such as network, sensors, service, and application to offer an efficient security scheme for the healthcare application with the help of the fuzzy analytic network process method. Another model suggested by the authors Kalpally, A. T et al.[16] for the attainment of a secured framework for healthcare systems using IoT applications. The proposed scheme supports the model from the architecture level to the application level for achieving the privacy of healthcare communication between the channel partners.

The article stated by the authors Shalaby et al.[17] presented a new approach to iris recognition by incorporating a convolutional neural network (CNN) scheme to obtain deep iris features and encrypt the features using chaotic encryption before transmitting them over the internet. The authors evaluate their approach on two openly available iris databases such as CASIA V4 Interval and Phoenix, and achieve accuracies of 99.24% and 100%, respectively. Another research suggested by the authors Onasanya A. et al.[18] suggested a healthcare solution to improve the life of cancer patients' health conditions. The authors discussed a variety of specific applications, such as remote patient monitoring, wearable devices, and AI-powered decision support systems. The authors Lu, Z. X et al.[19] presented a survey and challenges about the potential applications of the incorporation of IoT technologies with customized clinical settings, including diagnosis, treatment, and medical client monitoring. They also presented the use of IoT to collect and monitor patient data remotely, develop smart medical devices, and create connected healthcare systems. The authors ElRahman, S. A. A. et al.[20] proposed a framework that is designed to address the challenges of sharing healthcare services by providing a secure and privacy-preserving way to store and share patient data. The framework also uses IoT-edge computing to reduce the computational overhead of blockchain technology and improve the performance of the system.

The authors Lavanya M et al.[21] introduced a cloud-based medical assistance system based on hyper ledger fabric blockchain technologies. All transaction details are properly encrypted, validated, and maintained in a general medical repository. This MedSupport system also satisfies various performance evaluation tests and overcomes the limitations of conventional schemes. Another model suggested by the authors, Prasanalakshmi et al.[22], is for the attainment of secure medical content using Hyper Elliptic Curve Cryptography (HECC) on smart devices. The scheme combines steganographic methods with cryptographic algorithms to achieve both security and speed.

S. Balakrishnan et al.[23] attempted to provide a guaranteed healthcare service using IoT development boards with integrated sensors loaded with machine learning techniques. This e-healthcare system observed the patient status with utmost care and gave better suggestions for them. SeSem healthcare system is proposed by Radhika, R et al.[24] using deep recursive feed-forward neural network techniques. The proposed model holds a three-tiered framework for data acquisition, classification, and service delivery. The data processing tier then semantically enriches the data and uses deep learning to predict future health trends. The service delivery tier then provides personalized healthcare services to patients based on the processed data. An industrial IoT health system proposed by Zang[25] incorporates ML models that utilize sensor data to create a novel industrial IoT health system. The scheme is implemented in the Spark platform and tested for industrial big data. The authors Selvarajan S et al.[26] suggested an efficient cyber security model for health care systems. The model deals with quantum trust and consultative transaction principle with block chain scheme for the attainment of secured transmission of health care data between the network channel partners.

With the help of mixed reality and VR technologies, Taghian A et al.[27] implemented clinical applications for automated medical interactions. Through this application, patients and doctors both benefit from AR and VR equipment's rich communication capabilities. Chen X et al.[28] presented a research model, which provides a comprehensive overview of the possible benefits of using IoT and blockchain technologies to enhance the resilience of pharmaceutical supply chains in the post-pandemic period. This scheme maintained an effective way of pharmaceutical supply process using powerful sensors and blockchain technologies. A research survey by the authors Bovenizer W et al.[29], in which a clear overview of bibliometric schemes and their utilization on IoT-based healthcare systems have been presented effectively.

The authors Thakur, D et al.[30] presented a model titled "Deep Think IoT", in which a detailed presentation about the available IoT models on the base of various learning systems has been presented. The article articulates the need for Deep Learning in the implementation of the IoT models for the optimization of real-world requirements. Authors Arunachalam et al.[31] designed a new device for monitoring Alzheimer's disease-affected people using smart technology and enhanced deep learning. This framework used a variety of sensors to collect useful information on the patient's activities, including motion sensors, environmental sensors, and wearable devices, and deep learning-based analysis of medical diagnoses for the patients have been generated. The authors Bhattacharjee P et al.[32] proposed a smart framework for patients who are affected by Parkinson's disease. The model offers a smart IoT based health support system to minimize the fear of falling by observing the movement data of the patients. Nath et al.[33] offered a method to achieve the goal of achieving a privacy framework for point-of-care healthcare apps utilizing IoT devices; a content security model based on blockchain technology

is employed. The model offers a proficient model for the attainment of privacy and security on IoT devices by incorporating blockchain technology. The authors Islam, M. N et al.[34] presented a model of IoT with a machine learning mechanism that effectively predicts the risk level of cardiovascular diseases.

All in all, these studies and proposals indicate the necessity to combine MQTT protocol with a One Time cipher Pad that ensures data security, privacy, and reliability of Internet of Things-based medical diagnosis systems. Therefore the proposed model differs most notably to existing IoT-based healthcare systems using more basic encryption mechanisms by utilizing the information-theoretically provisioned one-time pad cipher to sanction lightweight, low-latency and essentially secure delivery of medical data, using MQTT.

Proposed remote medical diagnosis system

The above literature review section indicating that a secure medical diagnosis system is needed with smart technologies and a new schematic approach has been proposed in the section. The nominated scheme is called a secure, intelligent healthcare system based on one time pad cipher over MQTT protocol. Patients and medical experts communicate using IoT technologies, and healthcare messages are encrypted using one time pad cipher techniques before transmitting via MQTT protocols.

Preliminaries

As part of proposed approach, this sub section presents the preliminary concepts necessary to understand the components and operation of the proposed IoT-based remote diagnosis system.

Message Queue Telemetry Transport (MQTT): OASIS has published a standard for Message Queuing Telemetry Transport (MQTT) on the Internet of Things (IoT). Several big companies, including Amazon and Facebook, are using this protocol extensively to exchange data between resource-constrained devices. The MQTT protocol consists of a lightweight, low-bandwidth publish/subscribe mechanism. There are two components to it: the client, which is a publisher or subscriber, and the broker, which is the middleman. By subscribing to certain topics that are relevant to them, the client receives every message published by the publisher. With MQTT, there is very little overhead, so it only sends the message and very little extra data. Many industries have implemented MQTT, including manufacturing, automotive, sports, energy, military, telecommunications, and healthcare. Working sessions and high packet reprocessing do not break data transfer between the patient devices and healthcare providers. MQTT protocol is efficient in real-time transmission of health data and has a lightweight publish-subscribe model and minimal latency and bandwidth requirements. Its QoS guarantees stable delivery of the most essential medical data, regardless of the network instabilities. MQTT offers three QoS levels: **QoS 0** (at most once, no retries), **QoS 1** (at least once, with possible duplicates), and **QoS 2** (exactly once, highest reliability).

MQTTX client toolbox: It is a versatile and user-friendly desktop application for developers and enthusiasts working with MQTT (Message Queuing Telemetry Transport). Using this software MQTT-based systems can be monitored, debugged, and managed, which features real-time message visualization, topic subscriptions, publications, and advanced filtering.

These levels let IoT health systems balance speed, bandwidth use, and delivery assurance based on the criticality of medical data.

BAN logic: The purpose of a ban logic is to identify and prevent potentially harmful or malicious actions within a protocol through a systematic approach. In this logic, certain actions, nodes, or participants are banned from participating when they violate a set of rules or criteria. In many cases, these rules are based on protocol specifications, consensus mechanisms, or suspicious behavior detection. It protects the integrity and security of the protocol by restricting the offending entity's access or participation when a violation occurs.

Development of one time pad based secure healthcare system

A comprehensive secure healthcare system using Symmetric Cryptosystem over MQTT protocol is primarily the focus of the proposed scheme. It consists of an efficient Internet of Things (IOT) based E-HealthCare Application model with a cryptosystem for offering secure communications to the healthcare clients from their service providers. Table 1 describes symbols used in this secure healthcare system.

Every IoT device would choose a randomly generated, equal-length key with which it would encrypt its content and safely transfers the key to the recipient, using cryptographic schemes such as SMPC or pre-shared secrets. After its usage, the key is thrown away to keep OTP perfect secrecy. This solution was also actually implemented into middleware software such as ZeroC-Ice which is deemed highly lightweight and can be used even on resource-bound IoT devices and was also tested on security threat models such as Dolev-Yao to guarantee its ability to be resistant to cyber security intrusion attacks.

Notation	Description
$Secret\_msg_{p/d}$	Patient/doctor Message
L	Length of Message
$X_0, X_1, X_2, \ldots, X_n$	Generated Random Keys
S_k	Shared_key
$Encrypted\_msg_{p/d}$	Encrypted Message
$Decrypted\_msg_{p/d}$	Decrypted Message

Table 1. Notations and their meanings.

Encryption phase

This secure healthcare system encrypts all healthcare contents before they are sent via MQTT protocols. The sender generates a random key based on length of secret message and XOR operation is performed to obtain the cipher message. With the help of the MQTT protocol powered by MQTTx, encrypted messages are then sent through the communication channel. The following is the comprehensive encryption procedure for medical messages:

(1) First, publishers and subscribers are authenticated, and acknowledgments are sent to each.
(2) The patient(publisher) creates a secret message, $secret\_msg_{p,}$ and passes it to the cryptosystem,
(3) The system computes the length of the message (L) and generate random key based on user choice.
(4) The shared key is obtained using the below expression,

$$X_{n+1} = L\left(Secret_{msg}\right) \tag{1}$$

Where, X_{n+1} = *Random keys* $X_{0,}\, X_{1,}\, X_{2,\ldots,}\, X_{n,}$ for each message

$$If\ session_1 == X_0$$
$$(S_k == X_0)$$
$$else\ if\ \ session_2\left(S_k\right) == X_1$$
$$(S_k == X_1)$$
$$(S_k == X_n)$$

(5) Once shared key is obtained, both Secret message and shared key is converted into binary format to perform encryption.
(6) The cryptosystem performs XOR operation on both secret message and random key using the following equation,

$$Encrypted\_msg_p = E(secret_{msgp} \oplus\ s_k) \tag{2}$$

(7) Finally, encrypted message and keys are shared through the MQTT protocol.

Decryption phase

MQTT brokers provide a well-balanced agent for both publishers and subscribers whenever topics are created and shared. Using the same cryptosystem, subscribers decode the received message from their subscriptions. Following is a detailed explanation of the decryption scheme:

(1) Doctor receives a secret message $secret\_msg_d$ through the MQTT protocol.
(2) Doctor used shared key (one time) S_k to decrypt the message in receiver end.
(3) The cipher message and shared key is transformed into binary format for decryption process.
(4) The cryptosystem performs XOR operation on both cipher message and shared key using the following equation.

$$Decrypted\_msg_d = \left(D(Ciphert_{msg} \oplus\ s_k)\right) \tag{3}$$

(5) Finally decrypted message is dispatched to doctor.

OTP has perfect secrecy where a truly random key the same length as the message is used to encrypt each message; it is proof against brute-force and cryptanalysis. In our application, XOR operations were computationally very cheap in terms of IoT devices, yet, due to the perfect secrecy of OTP, confidentiality is guaranteed in low-resource settings, as proven by Shannon. The following example demonstrates the encryption and decryption process using the OTP scheme.

One time pad cipher based message encryption with SHA-256

Encryption process | sender: Patient_msg |ASCII format
QUERY: BP CHECK OK.
Conversion off Plaintext | Hex Format.
42 50 20 43 48 45 43 4b 20 4f 4b.
Concatenation Result: 425020434845434b204f4b.

One-Time pad (OTP) key generation
Randomly generated using ESP32 hardware RNG and conditioned with SHA-256.
90 B5 15 10 D1 31 90 34 63 7 F 5 F.
Concatenation Result: 90B51510D1319034637F5F.

Cipher text generations process (XOR)
Plaintext : 425020434845434B204F4B.
Key : 90B51510D1319034637F5F.

Ciphertext = Hex (plaintext ⊕ key).
= D2e535539974d37f433014.
Base64 Encoding (for MQTT Transmission):
0UU1U5L0039DMBQ=.

Decryption process | receiver: medical expert
Receive Base64 → Decode to Hex:
0UU1U5L0039DMBQ=.
Ciphertext = D2E535539974D37F433014.

Decrypt with same OTP key (XOR)
Ciphertext: D2E535539974D37F433014.
Key: 90B51510D1319034637F5F.
Plaintext = ciphertext ⊕ key.
= D2E535539974D37F433014 ⊕ 90B51510D1319034637F5F.
= 425020434845434B204F4B.
Hex to ASCII Conversion:
= BP CHECK OK.

Secure message transmission over MQTT protocol

In this subsection, we describe an implementation of secure communication using MQTT, where messages are encrypted using a one-time pad cipher before transmission. The model deals with the publisher-subscriber model, which contains the MQTT Broker with a medical wrapper application for the proficient connection establishment process. The message communication process in the proposed system would be performed between the sender (publisher) and the receiver (subscriber) with the support of MQTT Broker as a mediator. The message exchange process of the nominated framework is presented in Fig. 2.

Before any communication can take place, each client node (Publisher and Subscriber) must register with the online wrapper application (online service provider). Each client node is given a communication key by the online wrapper application, which is used to communicate content (messages) between the online wrapper application and the client nodes. MQTT brokers act as intermediaries between publishers and subscribers, managing messages based on subscribed topics. On both ends, messages are encrypted using one time pad technique.

The extracted data is sent to the Broker via a topic after an effective message exchange between the Online Wrapper Application and the publisher node. In this wrapper application, a communication key is first obtained, and then the broker node sends the data from the sender to the intended clients based on their subscription

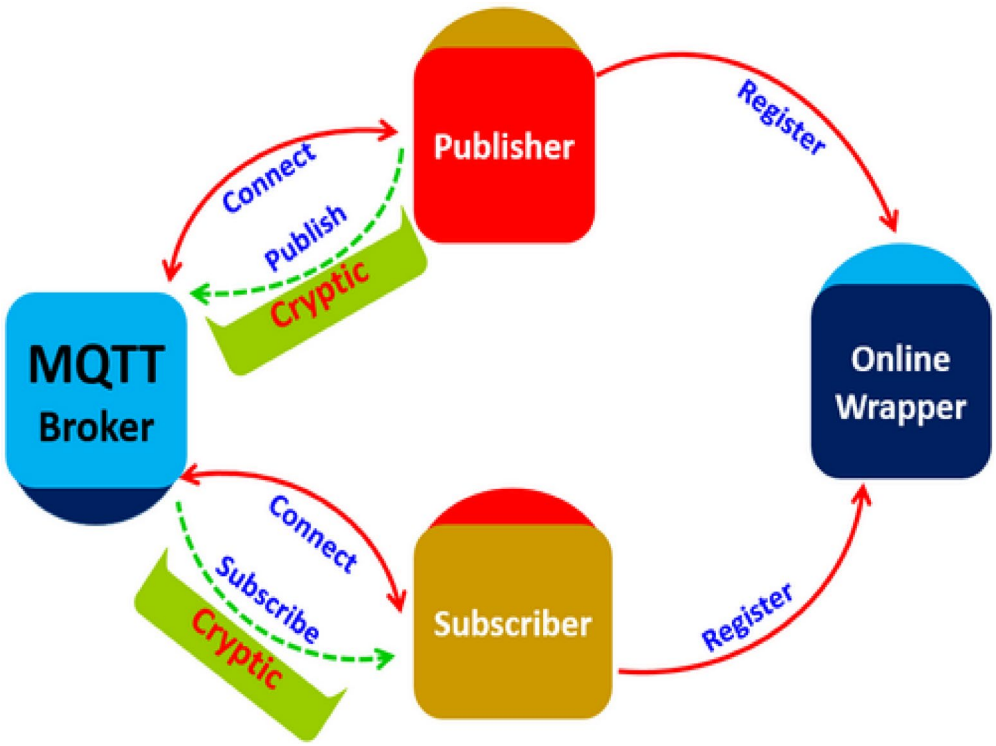

Fig. 2. Proposed message exchange process between subscriber and publisher.

information. The intended subscriber then deals with or responds to the data as received. The overall architecture of the proposed scheme is shown in Fig. 3.

The execution of the proposed system is presented as follows:

(1) Medical clients (publishers) are implanted with sensors during the initial registration process.
(2) A communication key has been generated for the initiated communication by the Online Wrapper Application and the key is shared with the publishers for their subsequent communication.
(3) Medical Service Providers (subscribers) launched their service availabilities from various sources, and it holds an authentication mechanism to detect the valid clients to offer services (services will be offered only to the valid clients, and clients validity would be decided by the Wrapper Application).
(4) Client requests (publishers) are connected with suitable Service Providers (subscribers) over the internet model with the support of MQTT Broker after the authentication process.
(5) The status of the request might be accepted or rejected based on the client load and the success of the authentication procedure at the subscriber's end.
(6) If the request has been accepted, then the communication or service by the subscriber to the publisher would utilize the communication key which the Online Wrapper Application generates.
(7) If the subscriber has not accepted the request, then the request will be forwarded to a suitable subscriber from another location and it is done by the MQTT broker.

The mobility and key advantage of the proposed IOT-based E-health system of the subscriber–publisher model with MQTT broker is that it lets patients move freely throughout the house or hospital without interfering with their ongoing observation. By enabling patients to roam freely around the home or hospital setting, the adoption of a user-friendly health care analysis and response system offers quick medical service. The primary goal of continuous observation in an e-health system is to create electronic health records (EHRs) that enable caregivers to manage illnesses from a distance. In order to accomplish mobility support in an e-health system, we propose broker-broker communication to exchange configuration and authentication information of a mobile node among themselves or to create a handover mechanism among MQTT brokers that reduces the time and effort required for frequent reconfigurations.

In order to prevent delays in transmitting EHRs caused by tasks that must be completed before connecting to the visited broker, the configuration information is transferred from the native MQTT broker of the patient whenever they move between rooms in the home or hospital. When a patient transfers to another broker site, and an emergency arises, this problem becomes more critical. Sensor Motes must immediately publish EHRs in this environment without devoting much time to reconfigurations. A patient monitoring system at a hospital uses multiple MQTT brokers to convey medical information about patients to caregivers in an example mobility scenario. A patient's continuous health observation is interrupted when he changes wards or examination labs (for example, because of medical tests) since he loses connection with the native MQTT broker. When real-time monitoring is required, it is especially critical to provide seamless transfer of sensed medical data during movement.

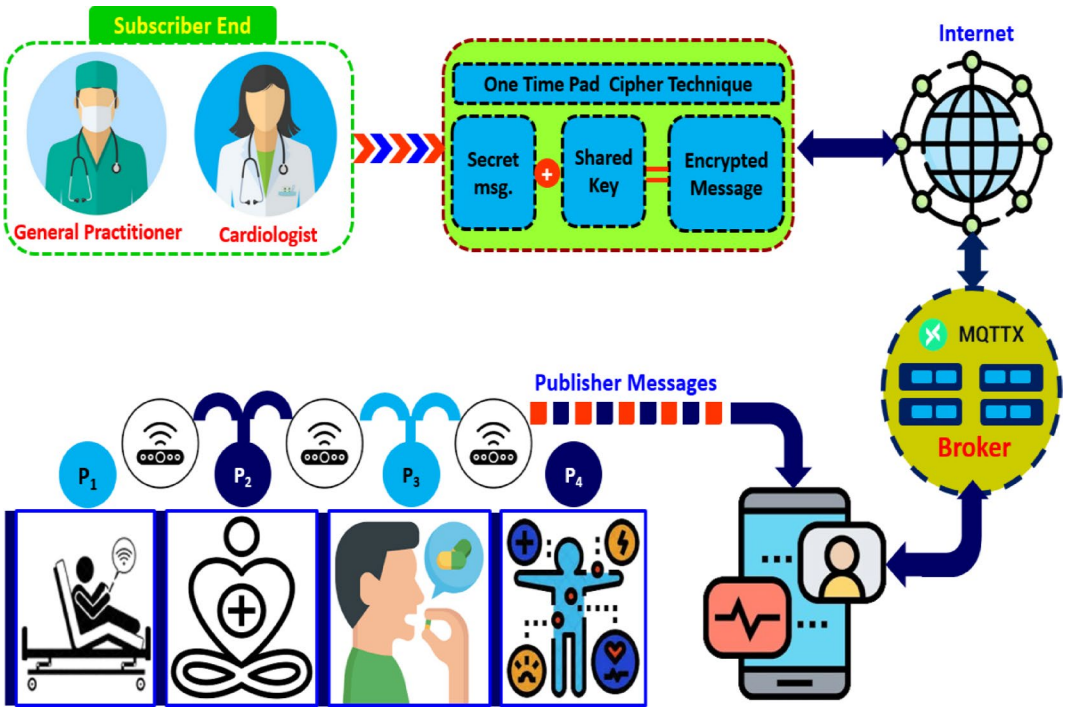

Fig. 3. Overall architecture of proposed health care system.

S. No	Queue Size	Publishers on Queue	Subscribers	Consulting Domain Specialists
1	4	Medical Client 1 Medical Client 4 Medical Client 7 Medical Client 8	Medical Practitioner – 1	Medical Practitioner – 1 Medical Practitioner – 4 Medical Practitioner – 5 Medical Practitioner – 6
2	5	Medical Client 3 Medical Client 5 Medical Client 6	Medical Practitioner – 2	Medical Practitioner – 2 Medical Practitioner – 7 Medical Practitioner – 9
3	4	Medical Client 2 Medical Client 9 Medical Client 10	Medical Practitioner – 3	Medical Practitioner – 3 Medical Practitioner – 10 Medical Practitioner – 11
4	5	Medical Client 11 Medical Client 12 Medical Client 15	Medical Practitioner – 4	Medical Practitioner – 4 Medical Practitioner – 8 Medical Practitioner – 12

Table 2. Evolution of medical clients and medical practitioners' allocation for Consultation.

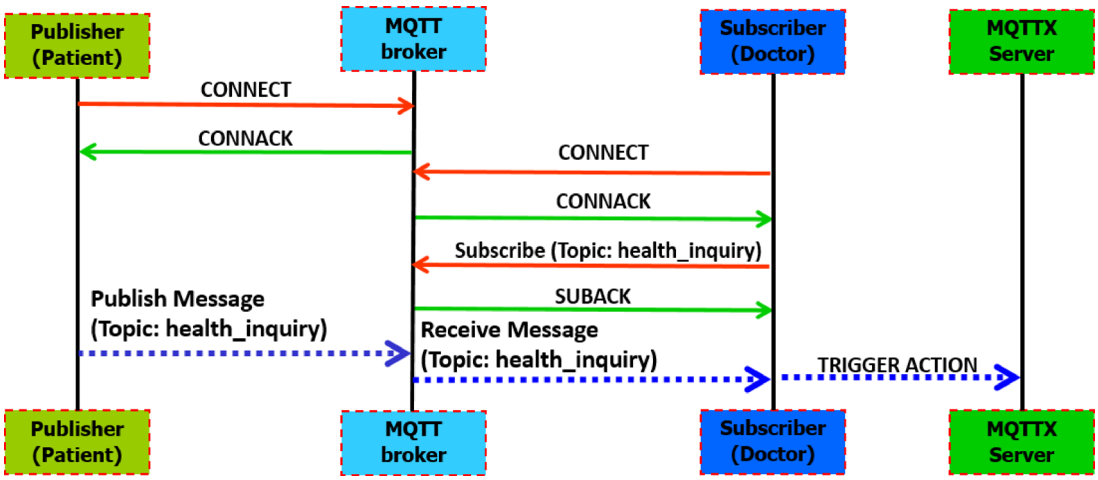

Fig. 4. Implementation of MQTT protocol based health care system.

During the proposed model initiation the Medical Practitioners (MR) are clustered on the basis of their domain or area of specialization for offering efficient services to their remote clients or Medical Clients (MC). For ex, cardiac-related problems will be forwarded to the corresponding cardiac specialists, and the allocation of clients to the practitioners has been done on the basis of the queue size and the availability of the practitioners. A sample of practitioners and their respective client allocations have been depicted in Table 2.

Results and discussion

In this paper, a smart healthcare system is implemented using an ESP32 IoT development board and Arduino Sketch platform. Espressif Systems powered ESP32-DEVKITM-1 with 8 GB RAM and 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40 GHz CPU are used. The prototype is built using the system on chip (SOC) ESP32 with WIFI connectivity as well as the MQTTX cloud platform. MQTT application protocol is also implemented to establish communication between publisher and subscriber. In this framework, medical experts are assigned as subscribers, and patients are publishers to raise medical-related queries. The overall modeling of MQTT protocol-based health care system communication is illustrated in Fig. 4.

In this proposed publish-subscribe model, at first MQTT broker is configured and set up on the MQTTx cloud platform. The broker configuration details are shown in Table 3.

As soon as the broker connection has been established, medical experts can register their domains as subscribers. On the other end, publishers can use brokers to publish the messages through the MQTTX platform. MQTTX broker manages the topics that are subscribed to by doctors, and receives messages from patients about the topics. The setup and monitoring process of MQTTX broker is shown in Fig. 5.

Three main parts comprise an MQTT message's content: a payload, a configurable header, and a fixed header. Every order communication needs to have a fixed header that is two bytes long. The fixed header and the variable header/payload are the two fundamental components of a message. The MQTT message format is summarized in Figs. 6 and 7.

QoS Level: QoS 0, QoS 1, and QoS 2 are the three quality service levels. QoS 0 (00) indicates at most once. QoS 1 (01) indicates at least once. QoS 2 (10) indicates exactly once. The degree of operational overhead increases with the influence of communication efficiency. It is possible to increase the maximum transmission size to 4 bytes, or 256 MB, by including the variable header and payload section.

Configuration	Description
Client_name	Name of the MQTT client
Client_id	Unique ID
Username	MQTTX client user name
Password	MQTTX Password
Keep Alive	Checking the status of TCP/IP connection
Clean Start	Discard existing connection & start a fresh connection
SSID uname & password	Username name & password of hotspot

Table 3. Domain name for MQTT broker connection.

MQTTX Configuration		Message Count		
Connections	espclient@broker.emqx.io	Subscription	Received	Published
Client_ID	mqttx_b6bacfd7	doc/ortho	10	7
Username	emqx	doc/general	12	10
Password	******	doc/neurology	5	4

Fig. 5. MQTT Configuration.

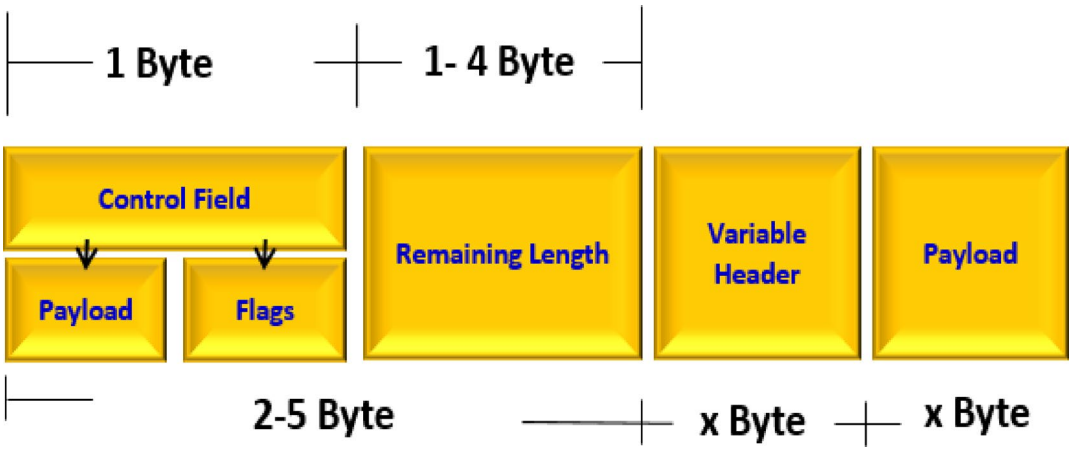

Fig. 6. MQTT message form fixed header.

When a message is transmitted through the message distribution flow in QoS Level 0, it is only sent once and is not verified to have reached its intended recipient. It is, therefore, possible that the message is intended for messages that fall within a specific size range. The MQTT broker manages various topics such as health updates, medical management, appointment, and scheduling, general communication, and emergency alter. The text-based representation of MQTT topics is illustrated in the following Figs. 8 and 9.

In MQTT communication, the message brokers are responsible for managing topics between subscribers and publishers. Figure 10 demonstrates various subscription topics such as health updates, medication details requests, reporting of symptom details, and requesting wellness tips. The broker processes the messages and distributes them to the subscribers after the publisher publishes them. Medical professionals then review the patient report and convey the recommendations to them. Additionally, this communication model is tested

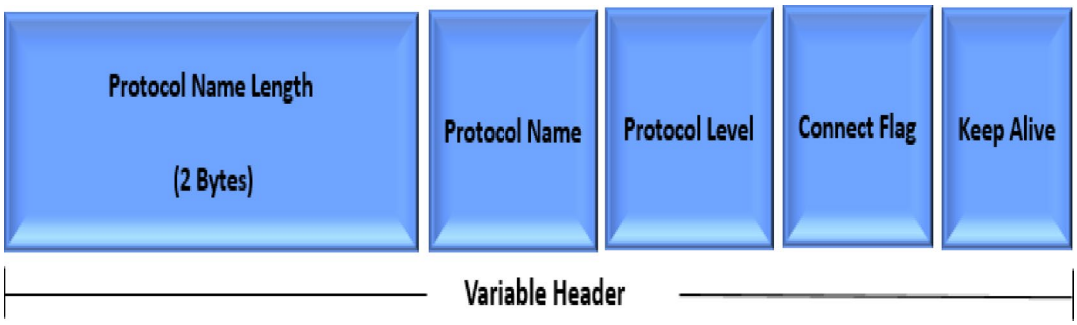

Fig. 7. MQTT message form variable header.

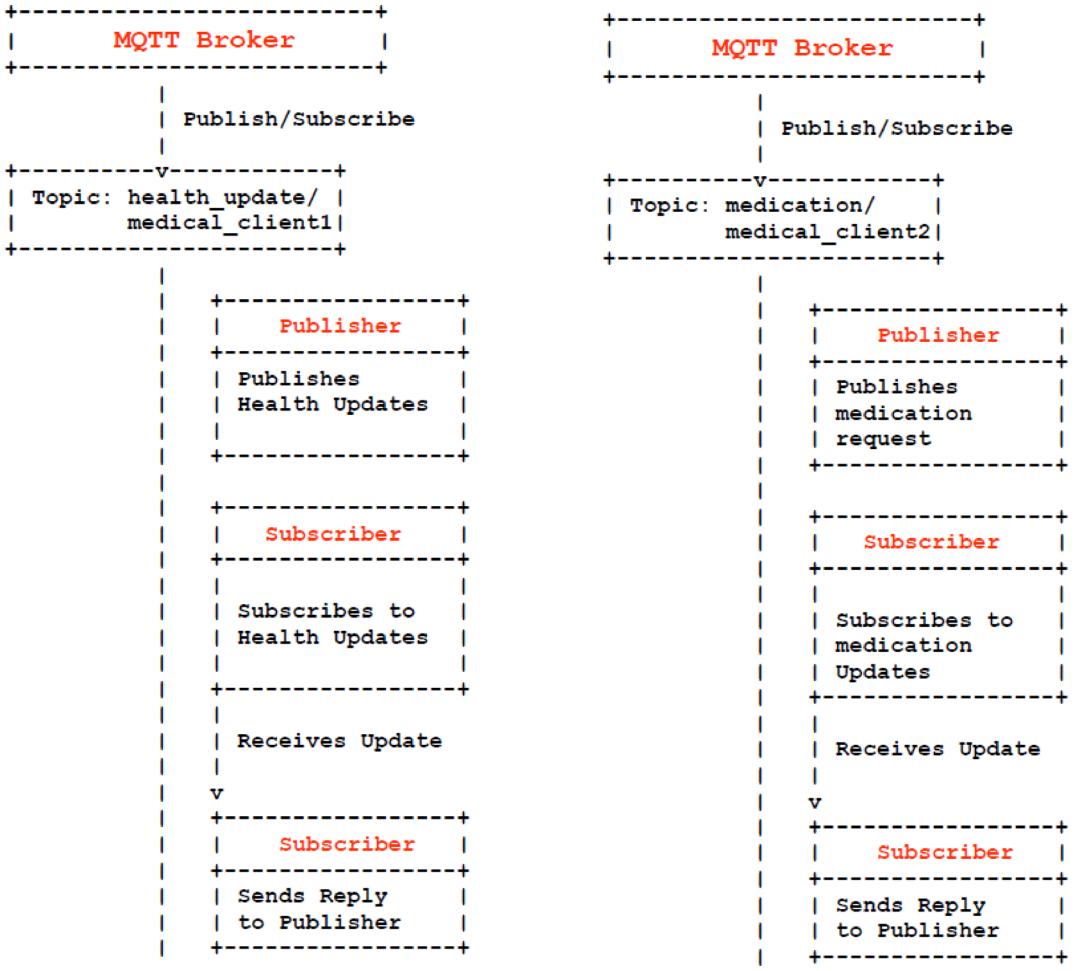

Fig. 8. Text based representation for the topics health update and medication.

using several QOS Levels, including QOS 0 and QOS 1. The relevance of medical communication is taken into account when determining the QOS level in the initial configuration, with at most once (QOS0) and at least once (QOS1) being considered.

Evaluation metrics for platform performance

The scheme IoT-based remote medical diagnosis system using OTP over MQTT utilized various metrics and benchmarks to evaluate the performance of the proposed platform such as system Performance, security Effectiveness and network/Protocol Efficiency. The device layer performance is measured using latency (ms), throughput (messages/sec), CPU utilization (%) and memory usage (MB). All network devices are configured through unified map network and standard connecting interface is used transmit the data packets. The security layer performance is analyzed using various parameters such as computational time, attack resistance score and

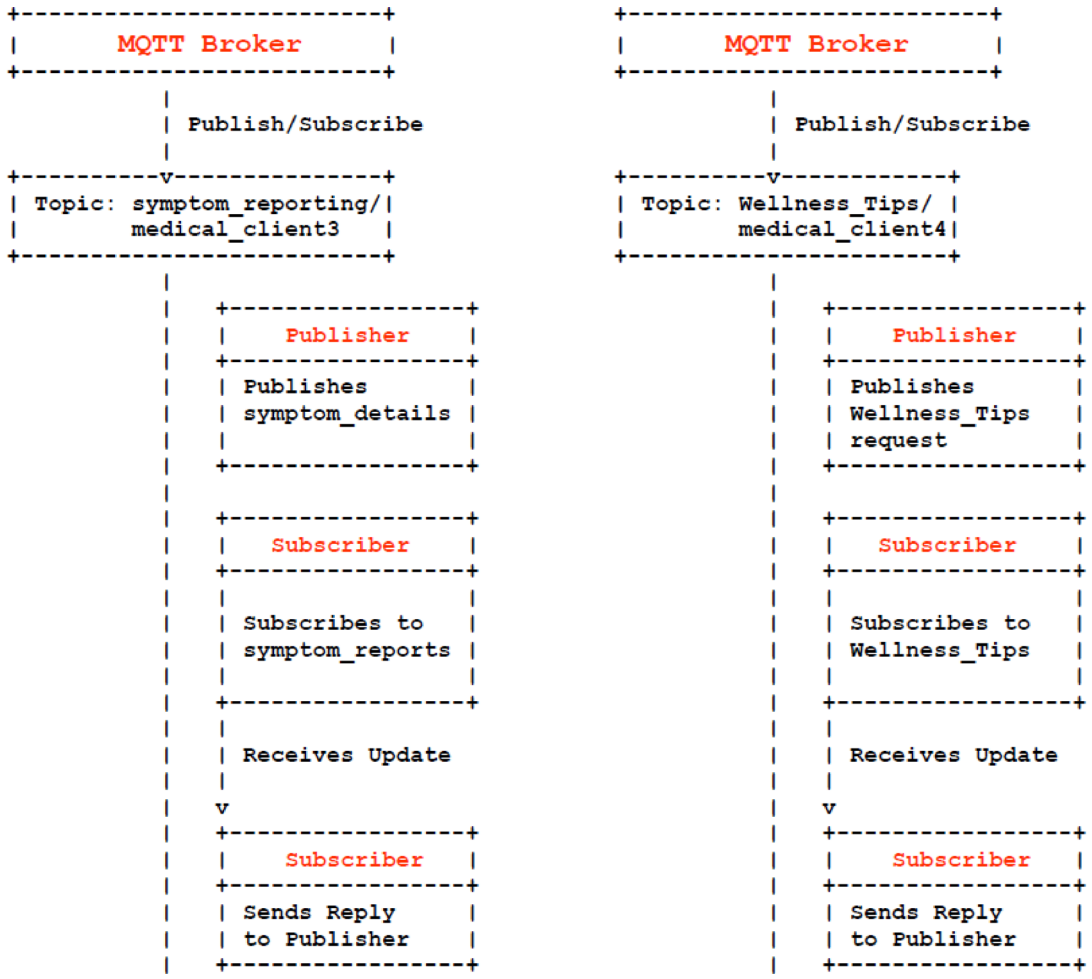

Fig. 9. Text based representation for the topics symptom reporting and wellness tips.

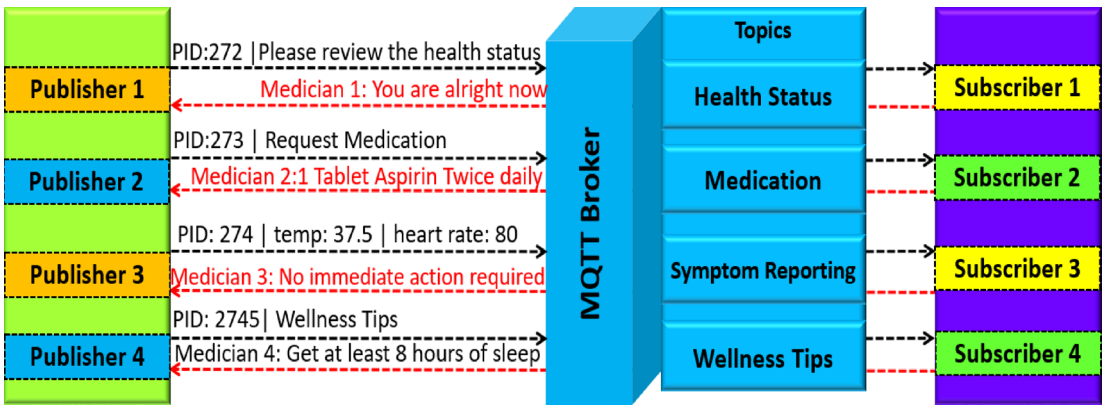

Fig. 10. MQTT Communication with subscriptions.

data integrity. MQTT is the main protocol of this implementation, therefore protocol efficiency is also estimated using packet loss rate, MQTT QoS services, and payload overhead. Table 4 shows that performance evaluation of proposed scheme based on the above metrics.

Security analysis

Access control and authorization for clinicians

MQTT can effectively implement topic-based access control, although the encryption payloads use a one-time pad cipher such that the MQTT broker is not able to read them. This is by way of Access Control Lists (ACLs)

Metric	Proposed system (OTP + MQTT)	Benchmark (AES-128 + MQTT)	Significant improvement
Average Latency (ms)	85 ms	132 ms	35.60%
Throughput (messages/sec)	145 msg/s	112 msg/s	29.5%
CPU Utilization (%)	18%	27%	33.30%
Memory Usage (MB)	22 MB	30 MB	26.70%
Encryption Time (ms)	1.8 ms	6.4 ms	71.90%

Table 4. Overall performance evaluation of proposed IoT based remote medical diagnostics scheme.

Type of the clinician	Subscription details
Cardiologist	Subscribed to health/status and medication/update
General Physician	Subscribed to all four topics
Psychologist	Subscribed to symptom/reporting and wellness/tips
Pharmacologist	Subscribed to medication/update only

Table 5. Mapping topic subscriptions by clinical Role.

Original message	Decimal sequence	Binary conversion	Effect of 1 bit change	Recovered message
REST	82 69 83 84	1,010,010…	83	SEST
WALK	87 65 76 75	1,010,111…	86	VALK
Tab	84 97 98	1,010,100…	85	Uab
DOSE	68 79 83 69	1,000,100…	69	EOSE
CON	67 79 78	1,000,011…	66	BON

Table 6. Differential cryptanalysis.

which are topic-level and not payload visible. Authentication is performed by unique credentials and selective authorization by role or specialization to publish or subscribe to a specific topic.

Our patient-self-published data are structured into four MQTT topics:

- health/status.
- medication/update.
- symptom/reporting.
- wellness/tips.

Patients are publishers and broadcast encrypted health data to such subjects. The medical experts are selectively granted access-subscribers, depending on their specialization and their identity. Table 5 shows clinician-specific subscriptions to health information topics.

Therefore our EMQX based implementation allows a fine-grained configuration of the ACLs and has well-developed authentication controls that allow subjecting topic-level control to secure and scalable access control without viewing the payload.

Cryptanalytic attack techniques

To assess the robustness of the proposed scheme, this section analyzes its security features and examines how it defends against potential attacks. The study of techniques for decrypting encrypted data without requiring access to the secret information needed to do so is known as cryptanalysis. Finding a secret key and understanding how the system works are usually necessary. Cracking or code-breaking is another term for cryptanalysis. The ciphertext is essential to cryptanalysis because it is usually the part of a cryptosystem that is easiest to access. Depending on the information at hand and the kind of cipher being studied, cryptologists can employ one or more attack models to crack a cipher.

Differential attack analysis

One bit in the matrix is toggled using characters that have been translated to ASCII. Different cipher texts are generated when there is a slight difference in the matrix at different places. The Avalanche Effect is seen here. Table 6 displays the length difference between the original and new cipher texts as well as the mismatched bits that result from switching a bit in the matrix.

Ciphertext-only attack analysis

An attack in which the attacker attempts to decrypt encrypted messages without having access to the plaintext or the encryption key is known as a cipher text-only attack. Using just the encrypted ciphertext as a starting point, the attacker in a cipher text-only attack must employ statistical analysis, pattern recognition, and other methods in an attempt to decipher the original plaintext. Since the attacker is unaware of the key or the plaintext, a cipher text-only attack is frequently regarded as one of the most challenging kinds of attacks. It is not impossible, though, particularly if the attacker has access to a lot of ciphertext if the encryption technique is weak. The strong encryption method of the suggested encryption strategy prevents such assaults by generating the cipher text after applying a number of intricate logic operations on the original text.

Known-plain text analysis

An attack in which the attacker has access to both the associated ciphertext and the plaintext is referred to as a known plaintext attack in cryptography. With the use of this data, an attacker can examine how the plaintext and ciphertext relate to one another and possibly figure out the encryption technique or other private information. Because the length of the cipher text generated by encryption is varied and unrelated to the length of the plain text, this assault is thwarted.

Brute-force attack analysis

The length and organization of the plaintext and ciphertext, the complexity of the method, and the structure of the encryption key all affect how strong an encryption technique is against a brute-force assault. Since the length of the ciphertext and the plaintext varies with random keys, the suggested algorithm performs sophisticated logic on the plain text, and there is no relationship between the two texts. Strong encryption algorithms are essential for preventing brute-force assaults. The suggested solution is particularly resilient to these attacks because it primarily targets low-power, lightweight devices. Additionally, it's critical to employ suitable key management and storage strategies to guard against unwanted access to the keys. Randomly generated keys are one way to do this.

Informal security analysis

BAN is a widely recognized formal security model that may be used to analyze and demonstrate the security of our protocol's mutual authentication.

Impersonation attack

Usr_pt and Usr_dr are two authorized users in this system who have registered for MQTT communication using a common key to exchange messages. Any anonymous user attempting to impersonate a valid user must be aware of the shared key and login credentials in order to read messages. This includes Usr_unkown. Due to user_unknown inability to produce legitimate messages, our protocol is resistant to impersonation attempts.

Trace attack

Due to MQTTx authentication and setups, users Usr_unknown, Usr_pt, and Usr_dr cannot be raced in this MQTT-based healthcare system. Furthermore, the MQTT broker takes the lead and only processes publisher messages for particular subscribed topics before sending them to the appropriate subscribers. Users who are not registered are unable to send or receive messages via the MQTT message queue platform. Our protocol offers anonymity and is resistant to trace attacks because of these factors.

BAN Logic Analysis: A commonly used formal security concept is BAN logic. The list of BAN logic's notations is shown in Table 7.

The test is conducted in accordance with the jurisdiction, non-verification, and message meaning requirements that are applicable in BAN logic. The BAN logic test is conducted in four stages, which are as follows:

- Ideal protocol may be altered.
- Assumptions can be made from the ideal protocol.
- Each step in the ideal protocol may be explained.
- Protocol evaluation can be done using BAN logic principles.

Notation	Description
$P \mid \equiv X$	P believes the message from X
#X	The message is newly generated
$P \lhd X$	P sees the message of X
$P \mid \sim X$	P once said X
$P \Rightarrow X$	P monitors and controls message of X
$< X > Y$	Formula X is combined with the formula Y
$\{X\}_k$	Formula X is encrypted by the key *K*
$P \overset{k}{\leftrightarrow} Q$	Players P and Q communication using K as shared key
SK	Session key

Table 7. Notations of BAN Logic.

The following is the format of the MQTT protocol's secure end-to-end encryption communication protocol:

$$P \rightarrow S: E_{Kc}\{M, Nonce_A\}, S, Nonce$$

(1) Ideal protocol.

$$M1\ P \rightarrow S: \left\{\left(P \underset{\Longleftrightarrow}{K_{ab}} S\right), N_A\right\}_{K_{ab}}, \neq \left(P \underset{\Longleftrightarrow}{K_{ab}} S\right)_{K_{ab}}$$

(2) Assumptions can be made from ideal protocol.

A1: $P| \equiv P \underset{\Longleftrightarrow}{K_{ab}} S$

A2: $Q| \equiv P \underset{\Longleftrightarrow}{K_{ab}} S$

A3: $Q| \equiv P \rightarrow P \underset{\Longleftrightarrow}{K_{ab}} S$

A4: $Q| \equiv \left(P \rightarrow \neq \left(P \underset{\Longleftrightarrow}{K_{ab}} S\right)\right)$

A5: $P| \equiv \#(N_A)$

(3) Each step in the ideal protocol may be explained.

E1: $Q \triangleleft \{N_A\}_{K_{ab}}$

(4) Protocol evaluation can be done using BAN logic principles.

Key management

Secure key Escrow and rotation during maintenance

In our implementation, keys are not escrowed, centralized or stored to ensure that there is no point of compromise. Rather, the hardware RNG of the ESP32 produces keys on-demand by means of the SHA-256 conditioning, so that every message uses a new pad segment. On device maintenance or reboot, rotation is accomplished by re-initializing the RNG state and generating a fresh one-time key sequence, and the MQTT session is re-initially flowed without notice. Since the encryption and decryption is stateless and symmetric, previously buffered messages are not lost and no plaintext is revealed. This architecture will ensure smooth rotation of keys without bringing service downtime or a recovery vulnerability.

Incident response and revoking a key

An incident-response plan for a suspected key leak follows the standard phases of a cybersecurity incident response, but with specific actions tailored to the nature of a compromised key. This scheme also actively focused on developing a comprehensive incident-response framework for key management. This includes defining specific metrics for the speed and efficiency of key revocation and re-provisioning at scale. The target performance metrics for the system are detailed in Table 8.

Management of retained messages and persistent sessions

During the testing and validation of our IoT-based remote medical diagnosis system, we have considered and processed both a retained message and persistent session. The primary goal of the paper is on the cryptographic method and its performance evaluation. However, we have conducted an extensive analysis of message queuing and session management. The data was collected during our testing phase and shows how these features were managed. Table 9 highlights the integration of MQTT functionalities into the foundational layer of our system.

Network and protocol efficiency performance analysis

Secure end-to-end encryption for the MQTT protocol is implemented on two Espressif ESP32-DevkitC hardware devices: These pieces of gear are low-power microcontrollers appropriate for Internet of Things uses. The package that is transmitted from publisher to subscriber during the design stage is {, }, , . In order to assess how well the implemented cryptographic algorithms function, , and are disregarded throughout the implementation phase.

S. No	Metric	Target Value	Remarks
1	Time to Detection	< 5 min	Automated monitoring system to flag suspicious activity.
2	Time to Revocation	< 10 min	The duration from detection to the invalidation of the compromised key across all endpoints.
3	Time to Re-provisioning	< 30 min	The time required to distribute and activate new keys to affected devices at a large scale.
4	System Scale (endpoints)	100,000+	The target number of devices for which the system can perform these actions.
5	Rollback Capability	Yes	Ability to revert to a previous state in case of an erroneous re-provisioning.

Table 8. Preliminary key Incident-Response Metrics.

Test case	Scenario	Retained message handled?	Persistent session status	Key consumption & storage
TC-01	Device sends a status message with retain = true	Yes, the broker retains the last known good status.	N/A	No additional key consumption. Key is stored locally on the device until next use.
TC-02	New subscriber connects to a topic with a retained message	Yes, the new subscriber receives the last retained message immediately.	N/A	The subscriber uses its pre-shared key for decryption. No new key is consumed.
TC-03	Device connects with clean_ session = false	N/A	Session resumes; queued messages are delivered.	Decryption keys are managed through the one-time pad sequence. Queued messages consume their corresponding sequence keys.
TC-04	Device reconnects after network drop	N/A	Session resumes seamlessly, maintaining state	The sequence of one-time pad keys is maintained across the session break, ensuring message integrity upon reconnection.

Table 9. Evolution of test case for retained messages and persistent sessions.

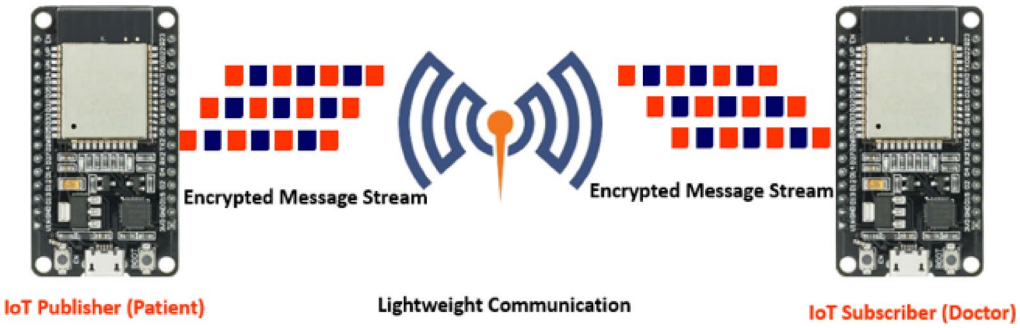

Fig. 11. Lightweight communication on IoT devices.

Communication format	Internet speed	Value
WiFi	Download Speed Upload Speed	7.46 Mbps 5.37 Mbps
Message Type 1	82 bit	Hello doctor
Message Type 2	120 bit	Query on health
Message Type 3	160 bit	Take one dose
Message Type 4	180 bit	Health is normal

Table 10. Message communication.

Message length (characters)	Encryption time (µs)	Decryption time (µs)	Publication time (µs)
10	477	487	495
15	529	540	552
20	688	710	693
25	690	715	697

Table 11. Computation time of cryptosystem.

The communication design that was implemented and shown in Fig. 11.The test is conducted on a WiFi network that meets the requirements listed in Table 10 and computation time is shown in Table 11.

Table 12 illustrates the computation of packet loss and time delay between QOS0 and QOS1. From this tabulation, QOS1 delivers the guaranteed message with some time delay as compared to QOS0. Table 13 illustrates a number of packets on each topic's size with the length between the participants among MQTT users. QoS 0, QOS 1, and QOS 2, in terms of dependability, are offered by the MQTT protocol. Figure 12 illustrates an appropriate time lag between QOS0 and QOS1 for a single transaction.

The security characteristics of our suggested protocol are contrasted with those of other similar protocols in Table 14. Undoubtedly, the current related techniques are unable to withstand different types of attacks, and their protocols are unable to provide mutual authentication and anonymity.

Packet loss rate	Trip time (QoS0)	Trip time (QoS1)
0%	0	0
5%	0.25	0.32
10%	0.29	0.37
15%	0.3	0.4
20%	0.7	0.72
25%	0.8	0.9

Table 12. Packet Loss Rate.

Type of message	No. of packets	Topic length	Message length
MQTT-PUB	41	9	64
MQTT-SUB	30	9	66
MQTT-PUB	51	9	97
MQTT-SUB	72	9	106
MQTT-PUB	21	9	45
MQTT-SUB	56	9	89

Table 13. Number of packets utilized by MQTT Protocol.

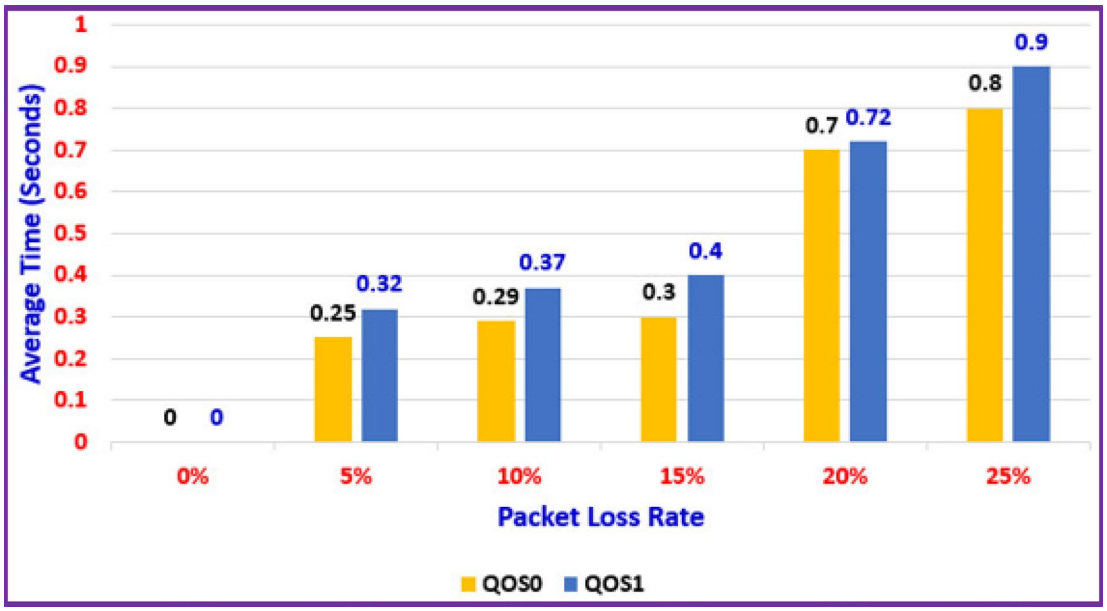

Fig. 12. Time lag between QOS0 and QOS1.

Security property	Choi et l	Xue et al.	Mohit et al.	Proposed scheme
Differential attack	X	✓	✓	✓
Ciphertext-only attack	X	X	✓	✓
Known plain text attack	X	X	X	✓
Brute force attack	✓	✓	✓	✓
Impersonation attack	X	✓	X	✓
Trace attack	✓	X	X	✓

Table 14. Security properties of proposed scheme with other related schemes.✓.

Volume of data estimation and key provisioning overhead

In our proposed model, there is a two-way flow of messages between patient and clinicians on various topics. To estimate the average daily data volume per device, it is essential to determine both the number of message payloads transmitted per message and the frequency of queries generated by each device. The steps in details formula are presented below with examples.

Payload per message

$$msg_{size}\,(bytes) = Payload_{size}\,(bytes) \times \quad Protocol\ overhead\,(bytes)$$

Average daily data volume per device

$$DailyVolume = Total\_no\_msgs_{perday} \quad \times \quad msg\_size\,(bytes)$$

A communication between patient and clinician & calculation of volumetric data daily are as follows:

Patient query: ***Please review the health status*** 31 characters (31 bytes).

Doctor query: **You are alright** 15 characters (15 bytes).

Protocol (MQTT) overhead ~ 20 ~ 30 bytes per message.

We can be conservative and say that each message is **50 bytes** after encoding and headers.

The daily data usage is calculated approximately for 10 messages (5 patient queries + 5 doctor reply).

DailyVolume = Total_no_msgs_perday × msg_size(bytes).

= 10 × 50 bytes = 500 bytes/day.

Thus the average information per day per device is significantly less than 0.01 MB.

The one-time pad is pre-programmed into the ESP32 and is stored safely in flash memory, where each single byte is read out only once using a monotonic index. The short length of every message (50 bytes) means that even a small pad (say 100 KB) can handle thousands of encrypted conversations, after which it is refilled by hand by updating the pad file when setting up the device. The prototype currently being developed does not require the use of such an intensive protocol because the automated replenishment through the secure key distribution can be added to the prototype in the future.

Entropy source validation

In this proposed IoT framework, each ESP32 publisher and the subscriber device use set of System on Chip (SoC's) hardware true random number generator (TRNG). It is accessible through the built-in function esp_random()/esp_fill_random(). The TRNG uses physical noise on the Wi-Fi/Bluetooth RF subsystem (and boot-time oscillator/ADC noise) to generate non-deterministic bits. In order to achieve true-random behavior, Wi-Fi remained on when generating pads and replenishing them on all devices.

Specifically, one-time pad cipher uses directly the random keys produced by the hardware RNG available in ESP32. On Wi-Fi, the RNG is constantly fed with RF and clock-jitter noise, which enhances the quality of randomness. An approximate min-entropy of about 0.94 bits per bit was obtained in the collected bit streams, assessed with NIST SP 800-90B and SP 800 – 22, and all the major statistical tests were passed with all notable failures having been repeated. Table 15 summarizes the entropy estimation results and throughput characteristics of the ESP32 RNG under different conditions.

MQTT QoS retransmission prevention

Each message sent out is given a distinct OTP segment at the time of sending, and a small persistence record (message ID, Ciphertext, key index) is atomically written to non-volatile memory (ESP32 NVS) to ensure the inadvertent reuse of the same OTP key subsequent to a device reboot or subsequent MQTT QoS retransmission. Retransmissions use the same Ciphertext read out of persistent storage; the persisted entry is not removed until the broker acknowledgment is received (the pad bytes are still used up). On reboot the device restores any pending record and republishes the same Ciphertext, so that keys are never reallocated on the same plaintext, maintaining OTP correctness.

Defense-in-depth

Our prototype has not used MQTT using TLS. The justification is that we use the one-time pad (OTP) cipher, with each message XORed against truly random key material, based on the ESP32 hardware RNG. The message is integrity-verified by hashing with SHA-256. This gives information-theoretic confidentiality to the message payloads, stronger than the computational security of TLS. Also, the OTP structure guarantees that retransmissions (MQS QoS 1/2) are sent with the identical Ciphertext, but never with reusing pad bytes, thus leaking information even in case of repeated delivery.

Device role	Entropy source	Environment	Raw min-entropy rate (bits/bit)	Conditioner (type, ratio)	Post-conditioning entropy (bits/bit)	Output bitrate	Entropy throughput
ESP32 Publisher	On-chip TRNG (RF/clock-jitter)	Wi-Fi active	0.94	SHA-256 DRBG, 1:1	0.94*	50.0 Kbps	47.0 Kbps

Table 15. Min-Entropy rate and Validation.

Since MQTT brokers in IoT applications tend to run on resources-constrained machines, TLS introduces a lot of overhead (session setup, certificate handling, RAM/CPU expenses). With our payloads being already flawlessly encrypted prior to transport, TLS would merely be duplicative to its functionality and offer no real additional value. That is, defense-in-depth is not needed here since the fundamental confidentiality assurance is already unconditional with OTP. MQTT over TLS can be used with OTP in later versions. TLS would offer endpoint authentication and identity verification of brokers whereas OTP is lightweight message confidentiality. This multi-tiered strategy would reinforce deployments without making changes to the fundamental security assurances of our scheme.

Secure patient mobility management

Patients have a tendency to come and go among different departments, wards, or monitoring areas within the environment of modern healthcare facilities and still need continuous channeling of medical data. The given proposed system will guarantee safe patient mobility using the persistent session capabilities offered by MQTT protocol, also a unique device identity, which will guarantee continuous communication without reestablishing the connection. One-time pad-based encryption is incorporated into the system such that health information is encrypted and resistant to interception as it becomes mobile. Also, the transition between network access points is verified by the system using device authentication and this has made it both reliable and secure in transferring patient records in dynamic healthcare settings.

Performance under multi-device load

EMQX in a horizontal scaling capacity has the sending of the messages as its foundation backbone and the main scalability limit is OTP key control within the ESP32 nodes given the limited resources available there. We use clustered brokers, partitioning of each topic, adaptive QoS and edge IP aggregation, and a hierarchical key-distribution protocol to generate short-lived session keys generated based on secrets provisioned by the devices (thereby saving key storage per-message). These are done to maintain low per-device overhead on CPU and memory and minimize network contention, but end to end latency and use of EMQX nodes can grow with active concurrent devices, and a monitoring and auto scaling system must be implemented to ensure quality of service at scale. Table 16 shows the scalability of proposed scheme under multiple device communication.

Unique features and contributions of proposed scheme

The unique contributions of this system and their improvements over previous approaches are as follows:

Integration of OTP Cipher in IoT Healthcare: Applies theoretically unbreakable cryptosystem to an MQTT scheme, which is not frequently used because of challenges of key management, hence providing superior confidentiality.

Feasibility on Resource-Constrained Devices: Demonstrates a reasonable implementation of OTP encryption on ESP32 hardware that does not seem to have a major performance penalty, in response to recent criticisms of the computational cost of OTP in limited computing devices.

Secure Key Management Mechanism: It uses time-limited, one-time, encryption keys to help counter replay and key-compromise attacks.

Scalable Multi-Device Communication: Designed to scale, performance is verified up to 20 devices simultaneously which proves that the system is scalable to small-to-medium hospital systems.

Enhanced Data Integrity and Privacy: Integrates MQTT Quality of Service (QoS) levels and OTP encryption in order to provide a combination of reliable delivery and uncompromised security in sensitive medical settings.

Limitations and future work

In the course of development and assessment of the suggested IoT-based remote medical diagnosis system, a number of limitations and challenges were determined. The success of the platform is critical on strong and fast internet connection, and failure to maintain this may lead to a high level of latency and a slow passage of information. The low computing capability and memory capacity of IoT devices make them bound in terms of adopting intensive encryption algorithms and handling huge datasets. The aspect of scalability is also a problem, having a big amount of concurrent connections between patients and doctors might necessitate some further optimization and hardware upgrade. Moreover, real-time key distribution, management, and generation by the One-Time Pad cipher is relatively challenging in the IoT. There is also the interoperability issue of joining incompatible devices and protocols which require an extra layer of adaptation or middleware to achieve easy communication.

Concurrent devices	Aggregate throughput (msg/s)	Avg. end-to-end latency (ms)	EMQX CPU (%)	EMQX memory (MB)	Avg. ESP32 CPU (%)	Key-distribution latency (ms)
5	25	40	12	120	18	12
10	50	55	28	210	20	25
15	75	75	45	360	22	60

Table 16. Scalability analysis.

S.no	Data size (KB)	Encryption time (ms)	Transmission latency (ms)	Decryption time (ms)	Total latency (ms)
1	1	0.5	50–70	0.52	51–71
2	10	5	70–90	5	80–100
3	100	50	100–150	50	200–250

Table 17. Observations on Latency.

This implementation platform requires more smart devices when patients and medical cases are increased. With the increasing number of IoT devices, the secure key distribution and storage are required, and it augments in complexity.

This prototype is implemented based on ESP32 IoT devices and MQTTx cloud platform data management between two parties using MQTT protocol. This environment consist the following resource constraints.

- Computational capacity of the ESP32 is significantly lower for running lightweight cryptosystems.
- Board's limited on-chip memory restricts the storage of cryptographic keys and intermediate data, making efficient memory management critical.
- Energy efficiency during encryption and MQTT-based communication.
- Network bandwidth limitations.

User and clinician feedback was not formally collected due to limited resources; internal testing guided usability improvements. Future work will include structured evaluations with healthcare professionals to enhance practicality.

Clinical risks of data latency and decryption delays

The primary focus of this research was on achieving a high degree of security and data integrity for sensitive medical information transmitted from ESP32.

There is significant clinical risks posed by data arriving too late, especially in scenarios involving critical patient monitoring (e.g., cardiac events, continuous glucose monitoring). While the time taken for data to be encrypted and decrypted is a factor, our primary performance metrics were centered on the computational overhead of the cipher and the transmission latency inherent to the MQTT protocol itself, as these were the core components of our proposed solution. We conducted few initial tests to understand this latency, as shown in the Table 17 below, but determined that a detailed analysis of hard real-time deadlines and their clinical implications was beyond the scope of this specific study.

This data demonstrates that while our model adds a small, predictable amount of latency, the most significant variable is the network transmission time, which is heavily influenced by the underlying communication infrastructure.

Conclusion

This paper presents a remote healthcare communication system between patients (MQTT Publishers) and medical specialists (Subscribers). The proposed scheme used the lightweight communication protocol MQTT to establish the connection between publisher and subscriber. MQTTX acts as an MQTT broker to manage all communications remotely with various quality of services. The scheme also handles multiple topics at the same time and gives quick responses with minimal delay and pack loss based on the QOS levels. A prototype of the suggested system was created and implemented using ESP32 and put into use, and the round-trip time and transaction packet count of the MQTT-based system were evaluated for performance. MQTT protocol yielded good results in terms of time delay, number of lost messages, and amount of bytes used in messages from the practical implementation of these protocols. The described system also represents the first combination of the information-theoretically secure one-time pad ciphering and lightweight MQTT protocols to provide coordinated IoT-based remote diagnosis with low transmission latency, and confidentiality of medical data. As a result, uses less energy and requires less bandwidth. Accordingly, the MQTT message protocol is more appropriate for the design and deployment of e-health platforms over IoT, based on these real-world and simulation results.

Data availability

The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Received: 7 August 2024; Accepted: 27 October 2025
Published online: 26 November 2025

References

1. Bashir, A. & Mir, A. H. Lightweight secure MQTT for mobility enabled e-health internet of things. *Int. Arab. J. Inf. Technol.* **18** (6), 773–778 (2021).
2. Uslu, B. Ç., Okay, E. & Dursun, E. Analysis of factors affecting IoT-based smart hospital design. *J. Cloud Comput.* **9** (1), 1–23 (2020).
3. Rathore, M. M., Ahmad, A., Paul, A., Wan, J. & Zhang, D. Real-time medical emergency response system: exploiting IoT and big data for public health. *J. Med. Syst.* **40**, 1–10 (2016).

4. Yang, Z., Zhou, Q., Lei, L., Zheng, K. & Xiang, W. An IoT-cloud based wearable ECG monitoring system for smart healthcare. *J. Med. Syst.* **40**, 1–11 (2016).
5. Park, Y. & Park, Y. A selective group authentication scheme for IoT-based medical information system. *J. Med. Syst.* **41** (4), 1–8 (2017).
6. Park, Y. J. & Lee, K. H. Constructing a secure hacking-resistant IoT U-healthcare environment. *J. Comput. Virol. Hacking Techniques*. **14** (1), 99–106 (2018).
7. de la Torre Díez, I. et al. IoT-based services and applications for mental health in the literature. *J. Med. Syst.* **43**, 1–6 (2019).
8. Sobin, C. C. A survey on architecture, protocols and challenges in IoT. *Wireless Pers. Commun.* **112** (3), 1383–1429 (2020).
9. Hayek, A., Telawi, S., Börcsök, J., Zeid Daou, A. & Halabi, R. Smart wearable system for safety-related medical IoT application: case of epileptic patient working in industrial environment. *Health Technol.* **10**, 363–372 (2020).
10. Kadhim, K. T., Alsahlany, A. M., Wadi, S. M. & Kadhum, H. T. An overview of patient's health status monitoring system based on internet of things (IoT). *Wireless Pers. Commun.* **114** (3), 2235–2262 (2020).
11. Drăgulinescu, A. M. C., Manea, A. F., Fratu, O. & Drăgulinescu, A. LoRa-based medical IoT system architecture and testbed. *Wireless Pers. Commun.*, **126** (1), 1–23 (2020).
12. Yang, X. et al. Exploring emerging IoT technologies in smart health research: A knowledge graph analysis. *BMC Med. Inf. Decis. Mak.* **20**, 1–12 (2020).
13. Muthu, B. et al. IOT based wearable sensor for diseases prediction and symptom analysis in healthcare sector. *Peer-to-peer Netw. Appl.* **13**, 2123–2134 (2020).
14. Latif, G. et al. I-CARES: advancing health diagnosis and medication through IoT. *Wireless Netw.* **26**, 2375–2389 (2020).
15. Haghparast, M. B., Berehlia, S., Akbari, M. & Sayadi, A. Developing and evaluating a proposed health security framework in IoT using fuzzy analytic network process method. *J. Ambient Intell. Humaniz. Comput.* **12**, 3121–3138 (2021).
16. Kalpally, A. T. & Vijayakumar, K. P. Privacy and security framework for health care systems in iot: originating at architecture through application. *J. Ambient Intell. Humaniz. Comput.* https://doi.org/10.1007/s12652-020-02676-7 1–11 (2021).
17. Shalaby, A. S., Gad, R., Hemdan, E. E. D. & El-Fishawy, N. An efficient CNN based encrypted Iris recognition approach in cognitive-IoT system. *Multimedia Tools Appl.* **80**, 26273–26296 (2021).
18. Onasanya, A. & Elshakankiri, M. Smart integrated IoT healthcare system for cancer care. *Wireless Netw.* **27**, 4297–4312 (2021).
19. Lu, Z. X. et al. Application of AI and IoT in clinical medicine: summary and challenges. *Curr. Med. Sci.* **41**, 1134–1150 (2021).
20. ElRahman, S. A. & Alluhaidan, A. S. Blockchain technology and IoT-edge framework for sharing healthcare services. *Soft. Comput.* **25** (21), 13753–13777 (2021).
21. Lavanya, M. & Kavitha, V. Secure tamper-resistant electronic health record transaction in cloud system via blockchain. *Wireless Pers. Commun.* **124** (1), 607–632 (2022).
22. Prasanalakshmi, B. et al. Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography. *J. Supercomputing*. **78** (1), 361–378 (2022).
23. Balakrishnan, S., Suresh Kumar, K., Ramanathan, L. & Muthusundar, S. K. IoT for health monitoring system based on machine learning algorithm. *Wireless Pers. Commun.* **124**(1), 1–17 (2022).
24. Radhika, R., Bhuvaneswari, A. & Kalpana, G. An intelligent semanticification rules enabled user-specific healthcare framework using IoT and deep learning techniques. *Wireless Pers. Commun.* **122**(3), 1–25 (2022).
25. Zang, J. & You, P. An industrial IoT-enabled smart healthcare system using big data mining and machine learning. *Wireless Netw.* **29** (2), 909–918 (2023).
26. Selvarajan, S. & Mouratidis, H. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. *Sci. Rep.* **13** (1), 7107 (2023).
27. Taghian, A., Abo-Zahhad, M., Sayed, M. S. & El-Malek, A. Virtual and augmented reality in biomedical engineering. *Biomed. Eng. Online*. **22** (1), 76 (2023).
28. Chen, X., He, C., Chen, Y. & Xie, Z. Internet of things (IoT)—blockchain-enabled pharmaceutical supply chain resilience in the post-pandemic era. *Front. Eng. Manage.* **10** (1), 82–95 (2023).
29. Bovenizer, W. & Chetthamrongchai, P. A. Comprehensive systematic and bibliometric review of the IoT-based healthcare systems. *Cluster Comput.* **26**(5), 1–27 (2023).
30. Thakur, D., Saini, J. K. & Srinivasan, S. DeepThink iot: the strength of deep learning in internet of things. *Artif. Intell. Rev.* **56**(12), 1–68 (2023).
31. Arunachalam, R., Sunitha, G., Shukla, S. K., Urooj, S. & Rawat, S. A smart alzheimer's patient monitoring system with IoT-assisted technology through enhanced deep learning approach. *Knowl. Inf. Syst.* **65**(12), 1–39. (2023).
32. Bhattacharjee, P., Biswas, S., Chattopadhyay, S., Roy, S. & Chakraborty, S. Smart assistance to reduce the fear of falling in Parkinson patients using IoT. *Wireless Pers. Commun.* **130** (1), 281–302 (2023).
33. Nath, S. S. et al. B. Block chain-base security and privacy framework for point of care health care IoT devices. *Soft. Comput.* 1–13 https://doi.org/10.1007/s00500-023-07932-4 (2023).
34. Islam, M. N. et al. Predictis: an IoT and machine learning-based system to predict risk level of cardio-vascular diseases. *BMC Health Serv. Res.* **23** (1), 171 (2023).

Author contributions

Conceptualization: [N. Rajesh Kumar, R. Bala Krishnan, G. Manikandan]; Methodology: [N. Rajesh Kumar, R. Bala Krishnan]; Formal Analysis and Investigation: [N. Rajesh Kumar, R. Bala Krishnan, V.Subramaniyaswamy]; Writing — original draft preparation [N. Rajesh Kumar, R. Bala Krishnan, G. Manikandan]; Writing — review and editing [N. Rajesh Kumar, V. Subramaniyaswamy, Logesh Ravi]; Funding acquisition: [V. Subramaniyaswamy, V.Indragandhi, Logesh Ravi]; Supervision: [V. Subramaniyaswamy, V.Indragandhi]. All authors have read and agreed to the published version of the manuscript.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to N.R.K. or S.V.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.