Novel approach in MQTT for secured data transmission without having data packet loss

Dhokane Nilima Tatyasaheb
Research Scholer, Department of Computer Science, Savitribai Phule Pune University, Pune

Dr. Binod Kumar
Professor, MCA Department
JSPM's Rajarshi shahu college of Engineering, Pune

Abstract

For data transmission in a communication system, we proposed the MQTT protocol in this system. Publisher, Broker, and Subscriber are the three components of MQTT protocol. We work on data security in communication systems as well as time-consuming processes in this system. The broker's dependability in terms of whether or not he is active is the focus of this investigation. This system detects if the broker is active or not by utilizing a Watchdog timer and the system uses the AES algorithm to secure the data. When comparing the performance of the existing system to that of our suggested system, our proposed system outperforms the existing system. The time and space complexity of the proposed system architecture is presented in this paper.

Keywords - MQTT, IoT, Transmission, Secure communication, Merkle Tree, Watchdog

I. INTRODUCTION

MQTT is a lightweight messaging system that allows several devices to communicate with one another. It's a TCP-based protocol that uses the publish-subscribe mechanism to communicate. This communication protocol is designed for data transmission between devices with limited resources and minimal power consumption. As a result, this messaging protocol is widely utilized in the IoT Framework for communication. Client devices and applications publish and subscribe to topics handled by a broker instead of talking with a server, as MQTT is a publish-and-subscribe protocol. MQTT's transport is primarily IP (Internet Protocol), but it can also use other bi-directional transports. The MQTT broker is software that runs on a computer, and it can be self-built or hosted by a third party. Both open source and proprietary solutions are available. Multiple clients interact with each other under this approach, but no direct connection is made between them. All clients communicate with one another through a third-party intermediary known as a Broker.

The broker serves as a sort of post office. MQTT clients use the "Topic" subject line instead of the intended recipient's direct connection address. Anyone who subscribes to a topic will receive a copy of all messages related to that topic. A single broker can subscribe numerous clients to a subject (one to many capability), and a single client can register subscriptions to multiple brokers (many to one). The IoT protocol stack consists of the physical layer, link layer, network layer, transport layer, application protocol layer, and application services layer, and can be thought of as an extension of the TCP/IP layered protocol paradigm. Each method has its own set of benefits and drawbacks. The Internet of Things (IoT) is a concept that intends to connect everyday devices to the Internet. While communication is essential in the Internet of Things, it is also one of the most challenging concerns due to the wide range of IoT use cases. The wide range of network technologies available fulfills communication needs, making it challenging to select the right protocol for a particular solution.

Merkle Tree is used to analyze the data. A Merkle tree is a hash-based data structure that is an extension of the hash list. Each leaf node represents a hash of a data block, and each non-leaf node represents a hash of its children. Merkle trees have a branching factor of two, which means that each node can have two children.

A protocol is a collection of rules or a language that different things use to interact or engage in communication with one another. Household appliances, manufacturing instruments, automobile parts, and other items now utilize the Internet of Things (IoT) ecosystem. As a result, many different sites, such as hospitals, car factories, and homes, have been affected by this environment, resulting in a rapid increase in the number of networked devices. As a result, the Internet of Things has grown in popularity, however picking the right message protocol for these objects or devices in a specific IoT system has proven difficult for system architects and protocol designers. Bidirectional connection and security are the two most important elements of an IoT system.

II. LITERATURE SURVEY

M. Calabretta et.al [1] The authors of this research focus on MQTT (Message Queue Telemetry Transport), a message-based communication protocol created specifically for low-power sensors and based on the MQTT protocol. The publish-subscribe model is used. First and foremost, we will outline some of the typical security measures and enhancements mentioned in the For MQTT installations, there is a lot of literature. Then we give a potential solution. Alternative method based on MQTT to safeguard specific topics AugPAKE is a protocol that was developed by AugPAKE.

M. Mukhandi et.al [2] Most ROS-enabled robotic systems may be hampered in their progress and adaption for real-world application over the Internet by cyber attacks. As a result, it's critical to identify and mitigate security risks connected with ROS-enabled applications. By integrating ROS with the Message Queuing Telemetry Transport (MQTT) protocol, we offer a unique strategy for securing ROS-enabled robotic systems in this study.

B. Mishra and A. Kertesz [3] M2M protocol is also shown in [24]. The authors of this paper examine the growth of M2M protocol research (MQTT, AMQP, and CoAP) over the last 20 years, highlighting how MQTT research stands out. We also conduct a rigorous literature search in major digital research archives to find appropriate application areas for MQTT, the most widely used M2M/IoT protocol. Our quantitative analysis examines some of the most important MQTT-related papers published in the last ten years, which we compare to highlight the MQTT protocol's primary characteristics, benefits, and limits. MQTT and CoAP is defined in [12], and [22] by Z. Laaroussi and O. Novo.

N. N. N. Vithanage et.al [4] The IOT is defined in [21]. One of the primary reasons is that IoT devices have limited memory capacity, energy, and computing power, making it impossible to run complex security algorithms and obstructing security services such as privacy and authentication, which are critical components of IoT services as shown in [7], [11] , [17], [20] and [8]. As a result, a broad IoT implementation necessitates the adoption of appropriate security and authentication solutions. To that aim, this research presents an authentication platform that uses LDAP and MQTT technologies to increase the security and efficiency of data transfer between IoT devices. With the help of LDAP features and GZip compression, the implementation complies with IEEE 1451 standardization to boost the MQTT. MQTT protocol for IOT device is shown in [25].

Packet	Description
CONNECT	Connect to the server
CONNACK	Ack of connect msg
PUBLISH	Publish a topic
PUBACK	Ack of publish msg
PUBREC	Publication received
PUBREL	Publication sent
PUBCOMP	Publication completed
SUBSCRIBE	Client subscription
SUBACK	Ack of subscribe msg
UNSUBSCRIBE	Unsubscribe petition
UNSUBACK	Ack of unsubscribe msg

Table 1: Types of MQTT messages.

Malina et.al [5] In this research, introduce a novel security architecture based on publish/subscribe messages for the Message Queue Transport Telemetry (MQTT) protocol in order to provide safe and privacy-friendly Internet of Things services as shown in [20] by H. Yujia. MQTT has exploded onto the IoT market in recent years thanks to its lightweight design and easy-to-implement technical requirements. Our proposed method has three degrees of security.

Calabretta et.al [6] The authors focus on MQTT (Message Queue Telemetry Transport) defined in [1], [11]and [9], a message-based communication protocol based on the publish subscribe paradigm that is specifically developed for low-power machine-to-machine connections. First and foremost, we present a thorough examination of some of the most recent security solutions and MQTT enhancements discovered in the literature.

I. Stoev et.al [10] The paper describes a method for communicating between ESP8266 modules that is based on the MQTT protocol and uses a simple non-secure class to implement the WiFi protocol. To ensure easy safe communication, encryption based on the Advanced Encryption Standard – 256-bit symmetric encryption method was developed [18] by A. Oak and R. D.

Daruwala and [8].

Security Type (2 bits)	Security Mechanism (Code (6 bits)	Total Length (8 to 32 bits)
00	000010 (AES)	0x40 (64 bytes)
01	000011 (CP-ABE)	0xA158 (4312 bytes)

Table 2: Examples of The Header Information For Two Encryption Mechanisms.

Buccafurri et.al [13] The Message Queuing Telemetry Transport (MQTT) protocol as shown in [14], which is widely used in the Internet of Things, is the subject of this study. This protocol does not provide natively implemented secure authentication techniques, which developers expect. As a result, this article offers a novel OTP (one-time password) authentication schema for MQTT, which implements a second-factor out-of-band channel using the Ethereum Blockchain. The idea uses Ethereum smart contracts to enable authentication of both local and remote devices while maintaining user privacy and ensuring trust and accountability.

Lohachab et.al [15] Using Elliptical Curve Cryptography (ECC) and Message Queuing Telemetry Transport, author offer a unique light-weight authentication and authorization framework suitable for remote IoT environments in this research (MQTT). We also put the scheme into practice, analyzing and comparing its different security and performance features to those of other schemes.

E. B. Sanjuan et.al [16] In this article, the author proposes using Cryptographic Smart Cards to create a security schema for the MQTT protocol that addresses both the authentication schema and the trusted data confidentiality and integrity problems. This security schema is implemented without altering the regular protocol messages. Finally, they demonstrate a time results experiment with the Java Card library using an example implementation approach.

Ahamed et.al [19] To achieve security in the IoT system, a model combining Advanced Encryption Standard-256 and Secure Hashing Algorithm-256 is suggested in this work. The data acquired from devices is first encrypted with AES-256 and a symmetric key generated with SHA-256, followed by the creation of the cipher text. This cipher text is now included in a new layer of security known as the Message Queuing Telemetry Transport protocol, which is an ISO standard (ISO/IEC PRF 20922) publish-subscribe-based architecture for secure data transmission. The original data is extracted on the receiving end. Message encryption is shown in [14] and [23] by S. P. Mathews and R. R. Gondkar.

MD Jiabul Hoque1et.al [26] The authors of this study evaluated a number of published studies on the secure MQTT protocol for IoT networks and discovered certain serious security loopholes in the MQTT communication protocol for IoT application networks that need to be addressed. The primary goal of this research is to offer a secure and real-time MQTT protocol for IoT applications that avoids data loss.

Cüneyt Bayılmış et.al [27] The IoT social class in these conditions joins the small devices, the entrances and the stages of the cloud. An IoT social class is prepared to contain major substances added in transmission under various Neath conditions with mild verbal exposures, taking into account the characteristics of constrained equipment (memory, processor, energy, etc.) of small devices. These light verbal career conferences influence neighborhood, constancy, information flow limit and forceful affirmation of IoT programming. Therefore, understanding the most suitable verbal career conference for planners emerges as an urgent planning problem. Organic IoT framework. The investigation therefore separates the various current luminous verbal exposures and analyzes their resources and their limits. Additionally, the report reveals the preliminary examination of Constrained Application Protocol (CoAP), Message Queue Telemetry (MQTT), and Web Socket, which are more undeniable support for small devices. IoT. Finally, Talk About Destiny focuses on the rules of verbal career conferences for the IoT.

Kitae Hwang et.al [28] This record selects MQTT considering how the illuminating show finds and describes the key boundaries that display the MQTT server based on large-scale execution and MQTT dispatch attributes, including MQTT message contention. Additionally, this recording created an MQTT mail server to evaluate the use of Mosquitto as an MQTT provider and a subsequent alternative gadget to reveal key limits set. In this recording, the all-in-one MQTT lighting server running after the gadget has been merged into 3 segments: a dashboard server, a following schedule, and a real load generator. The control load generator is arranged to perform huge MQTT message load measurement using eleven Raspberry PIs.Care using Mosquitto with collecting information in the dashboard server.

HARIPRASAD.S et.al [29] The preliminary analysis of the organization is carried out on a review station with hardware and sensors linked to the use of a lightweight Message Queue Telemetry Transport (MQTT) show. This contains 3 segments: (I) collects sensor usage information for 3 specific leads known as SENMQTTSET; (ii) multiset branding period the use of a rule plan to create a set of quantifiable multiview marks from the SENMQTTSET dataset; and (iii) evaluate the dataset using ML estimates. The SENMQTTSET dataset has changed to 3 potential clients, narrow for Conventional Clients, Assaults on Allies, and Assaults on Merchants. The multi-setting brand name is created from the raw informative index of using an authentic game plan of the multi-view falling brand rule set period.EML wants to choose the very satisfying interference that distinguishes test variation among ML estimates close to logistic regression, KNearest Neighbor, Random Forest, Naive Bias, Support Vector Machine, Gradient Boosting, and Decision Tree based primarily on large-scale runtime estimates close to accuracy, figure time, F1 note and everything possible from that point. The proposed dataset is distributed and the accuracy appears to be nearly greater than 100% for the gear structure under consideration. Some fine bounds have been set for assaults and genuine visitors attributed to learn carryover between IoT MQ TT associations.

MQTT Protocol to Tra et.al [30] Manufacturers have come to see the inclusion of MQTT emission for transport telemetry recordings using the growth of a moderate section to be modeled on a set of engines and their limitations in the area of facilitated factors. To ensure this goal, they represented the type of release and transport of telemetry records to accumulate study and complete the most beneficial and balanced condition of the main MQTTs and assemble the neighborhood of records between motion and utility server.

Eric Riedel et.al [31] The trade of foundry, with its processes and design conditions, undoubtedly justifies the deception of the latest steel parts. Mastering the limits of the methodology is therefore essential. Related topics from Industry 4.0, digitalization, Internet of Things or Big Data that guarantee a sparkling testimony of the notarial procedure, however they are practiced in an unusual way so far with the help of a couple of monstrous foundries, who started digitization first in their methods. due to the absurd assertion of informatization established so far. In reality, small and medium-sized foundries are generally struggling with these issues, due to the loss of concrete and legitimate reactions from a variable point of view on various medium-sized foundries which need data in the new problems related to the 'computer science. In any case, because the only backbone of the industry, SMEs also need to find and give data to this new world of collection.

Jackılyn B. Baccay et.al [32] The audit aimed to find ways to modernize the hydraulic structure of the nursery and control the environment. The microcontroller has been redone to drive the fan and the electromechanical valve under the conditions that they occur: (1) Via the web, the customer can turn on/off truly using any device connected to the Internet (2) a predestined still around personnel and (3) when a deadly temperature for the blower fan and soil soaking content of the crop is reached. The data accumulated by the sensor center was saved in the external unit in .csv configuration to be compiled as support. Data was sent via the message line telemetry transport broadcast for graphical display via the Wi-Fi module. Respondents included PSAU project staff/workers, subject matter experts, IT trained and students. insofar as availability, firmness, comfort and accessibility, the system in place is OK. Subsequently, the end customers were certain that the structure created could be used and modified in the exercises and in the areas of engagement.

Eric Gamess et.al [33] Internet of Things (IoT) is the time frame constituted to embody the crowd of gadgets with certain knowledge and bandwidths. Considering the reach of IoT gadgets associated with the internet, IoT-centric social class shows have grown old in gaining interest. This article separates the global runtime from one of the most popular limits, known as Message Queuing Telemetry Transport (MQTT), which works in Mosquitto, a widely used runtime. Our fundamental estimate is airtime, represented because the time it takes for a message to visit a customer via the brokerage to another buyer, as MQTT uses disperse/variant buying with a brokerage.

Melvin Bender et.al [34] Internet of Things (IoT) is the time frame constituted to embody the crowd of gadgets with certain knowledge and bandwidths. Due to the reach of IoT gadgets associated with the Internet, the IoT-centric social class shows age has gained by creating income. This article separates the global runtime from one of the more well-known limits, known as Message Queuing Telemetry Transport (MQTT), which works in Mosquitto, a widely used runtime. Our primary estimate is airtime, represented in light of how long it takes for a message to travel from a customer through the brokerage to another buyer, as MQTT uses transform traffic/purchase with a brokerage.

Dmitrii Dikii et.al [35] The article examines the question of the secure institution of the Internet of Things despite denial of service (DoS) attacks at the level of public services and few others. They came up with a deliberate condition of the equipped Assault ID gadget using the use of 3 classifiers using the following attributes: username, gadget ID and IP address. It was shown that for the proposed working vector, it was reconstructed to check and prepare the data sets, the magnificent effects had been achieved with the help of the use of a multi-layer perceptron and a device for assistance vector with a winding base of the piece with the incorporation and advancement with the SMO estimate. The producers also chose the conditions under Neath so that the selected classifiers had the best enchanter to identify strange and real visitors in MQTT associations.

III. PROBLEM STATEMENT

When several devices send and receive messages, the ability to monitor server performance and messaging characteristics is critical. MQTT is defined as a messaging and parsing protocol in this work, as well as important factors that illustrate MQTT server performance and MQTT communication characteristics such as MQTT message subjects. For security, we employed the Merkle tree, which is a data structure that is intended to more efficiently encapsulate blockchain data. Merkle trees distribute data before encrypting it with the AES technique for increased security.

IV. PROPOSED METHODOLOGY

There are two major problems in MQTT protocol. First one is security and second one reliable communication.

Security:

To provide data security in data transmission using MQTT protocol we have used Merkle tree in between subscriber and publisher. A Merkle tree is a data structure that is used to encode blockchain data more efficiently and securely. In the example shown in Figure 1, the publisher Ṕ chooses a random block index (e.g., 1) as a challenge. The subscriber Ṡ then constructs a Merkle tree from its local data, followed by sending the corresponding unique sibling paths from the leaves to the root node (i.e., (H1, H2, H3−4)) to the verifier. Upon receiving the proof response, the publisher Ṕ derives the root value of the Merkle tree (i.e., H(H(H1, H2), H3−4)) and determines whether the result is identical to the value of the root node held in local storage. Markel tree along with AES encryption is used here to get secured data transmission.

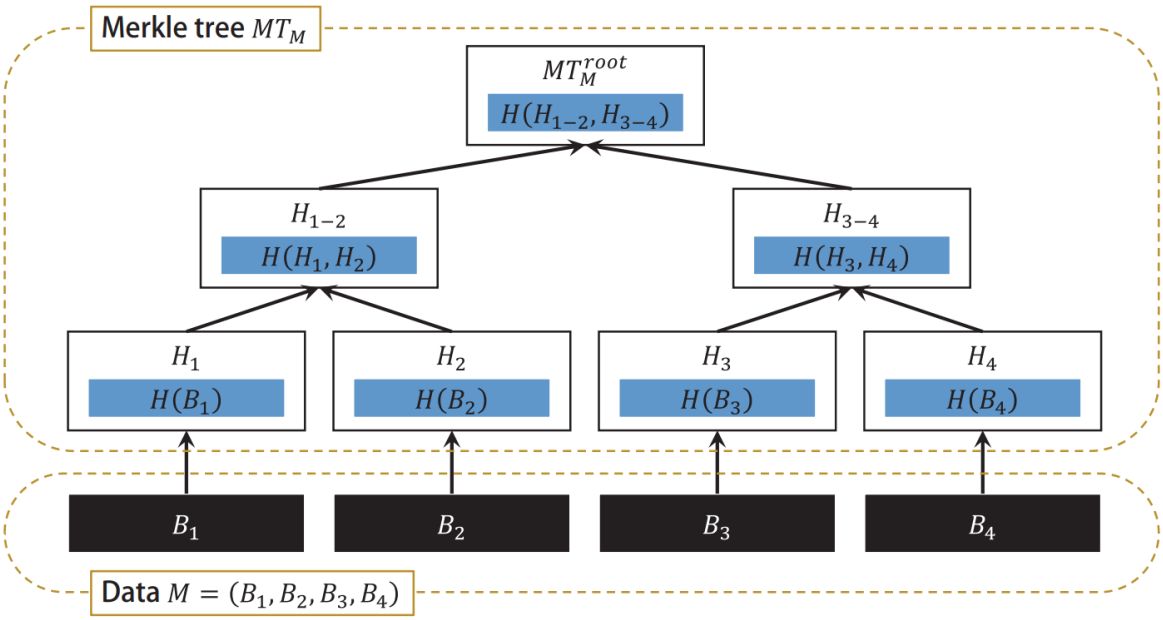

Figure 1: Merkle Tree of data authentication in MQTT protocol for improved security

Public parameters: Hardcore function $G : \{0,1\}^l \to \{0,1\}^{|M|+\log|M|-1}$ where $l \ll |M|$
i-th bit in bitstring S, S_i

Publisher Ṕ		Subscriber Š
1. Choose uniform random bitstring $s \in \{0,1\}^l$		
2-1. Compute $r \leftarrow G(s) \in \{0,1\}^{\|M\|+\log\|M\|-1}$	$\xrightarrow{s}$	**2-2.** Compute $r \leftarrow G(s) \in \{0,1\}^{\|M\|+\log\|M\|-1}$
3-1. With possessing data M, generate proof $h(M,r)$ such that $h(M,r) = (b_1(M,r),\ldots,b_{\log\|M\|}(M,r))$, where $b_j(M,r) = (\sum_{i=1}^{\|M\|} M_i \cdot r_{i+j-1}) \bmod 2$ for $1 \le j \le \log\|M\|$	$\xleftarrow{prf}$	**3-2.** Possessing data M', generate proof prf such that $prf = (b_1(M',r),\ldots,b_{\log\|M\|}(M',r))$, where $b_j(M',r) = (\sum_{i=1}^{\|M'\|} M'_i \cdot r_{i+j-1}) \bmod 2$ $(1 \le j \le \log\|M\|)$
4. Check the integrity of M by comparing $h(M,r)$ and prf		

Reliable communication:

Monitoring of broker becomes the most important task if it comes to the reliable communication. Subscriber did not get any feedback if broker is working or not.

One of the tasks of broker is to restart the count of extra thread after every 4 machine cycles. And the only task of this extra thread is to reset broker after every 5 machine cycles. So here if broker is not able to restart the count of extra thread it means broker is not working and then the extra thread will reset the broker to make it a wake.

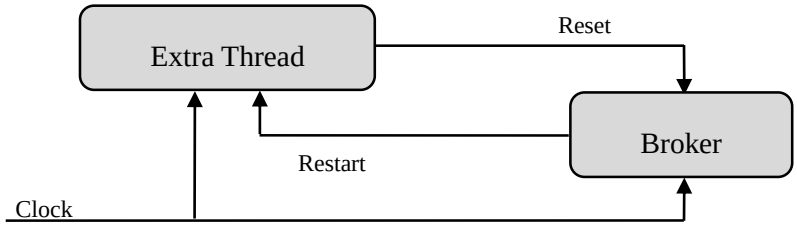

Figure 2 : Conceptual diagram of working of extra thread

Watchdog Timer for MQTT Protocol for the transmission of data

The Watchdog timer is utilized in this MQTT protocol for data delivery. Publisher, broker, and subscriber are the three components of the MQTT protocol. If a publisher sends data to a subscriber via a broker, we have no way of knowing if the broker is functioning or not. Then there's the Watchdog timer, which is used to restart the broker if it doesn't react within a minute. A system timer can be used by a high-level application to act as a watchdog, causing the broker to terminate and restart the application if it becomes unresponsive. When the watchdog timer runs out, it sends out a signal that the application can't handle, causing the broker to terminate it. The broker restarts the application once it has been terminated. The broker restarts the watchdog timer on a regular basis to prevent it from elapsing, or "timed out," during normal operation. The timer will elapse and send a timeout signal if the broker fails to restart the watchdog due to a hardware or programme issue. Corrective measures are triggered by the timeout signal. Placing the broker and associated hardware in a safe state and performing a computer reboot are common repair methods.

Merkel Tree

Merkle trees are a type of data structure commonly utilized in computer science. Merkle trees are used to encrypt blockchain data more effectively and securely in data communicate within the publisher and subscriber. The security of Merkle tree-based authentication is depending on the hash function in use. As a result, the publisher only saves the value of the tree's root node and discards the rest of the metadata once the tree is built. The value of an internal node is assigned based on the hash value of its children, while the value of a leaf node is assigned based on the direct hash value of the relevant data block in a Merkle tree.

Merkle tree-based online authentication confirms that the publisher and subscriber have the same data. In contrast to public verification, it is assumed that the publisher possesses some secret (i.e., non-public) information about the data to be certified. The fundamental benefit of employing a Merkle tree is that numerous crucial pieces of information about a specific data element or the data set as a whole may be validated without having access to the entire data set. A Merkle tree is a hash tree-like data structure that is non-linear and binary. A data element's hash value is stored in each leaf node of the tree, whereas a middle node holds the hash of the hashes of its two matching child nodes. The fundamental benefit of employing a Merkle tree is that it allows multiple critical pieces of information about a specific data element or the entire data set to be checked without requiring access to a large data set.

Encryption of the Data

Our system performs AES on the data after Merkle tree distribute the data. Encryption works by turning ordinary text to cypher text, which consists of seemingly random characters. It can only be encrypted by those who hold the special key. AES uses symmetric key encryption, which requires encoding and decrypting data with only one secret key. Asymmetric encryption is achieved using the Advanced Encryption Standard (acronym for Advanced Encryption Standard). AES bits, which come in lengths of 128,192, and 256 bits, are used to encrypt and decode data. After the Merkel tree has processed the data, AES uses the symmetric key to keep the data secure. 256-bit AES encryption is the most secure of the three options: 128-bit, 192-bit, and 256-bit AES encryption, due to its key length size.

Encryption process for the data security, system gives the particular key to the distributed data and then,

1) Data Byte Replaces (Sub Bytes) The 16 bits of data are fine-turned configurations that result in network structures, lines, and sections.

2) Rows with circular byte shifts For each round, every four lines of the matrix network are moved to the left.

3) Combine Columns Another framework's produce is a store of 16 fledgling bytes, and this development is not rehashed in the last round.

4) Include a circular key. The input matrix, round key, and output will be saved in cypher text, which will be 128 bits and 16 bytes homogeneous round of interpreted data.

5) Decryption In the inconsistency request, the tasks of decoding an AES cypher text action. The entire process is divided into four stages, each of which is focused on the logical inconsistency request.

VI. RESULTS AND DISCUSSION

The proposed system is tested on both time complexity and space complexity. When time complexity in term of size of data transmission is tabulated in table 3 and visualized using graph in figure 3.

data size	time required for data transmission (in seconds)
1 byte	0.0001
10 bytes	0.0001
100 bytes	0.0003
1 kb	0.0008
10 kb	0.0019
100 kb	0.03
1 Mb	1.06
10 Mb	11.94
100 Mb	103.83

Table 3 : Time required to transmit the data of different sizes

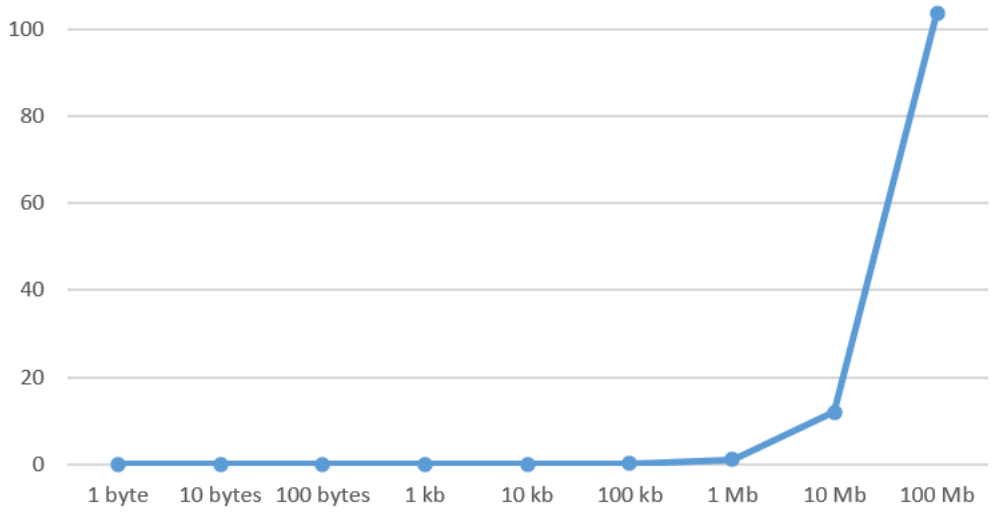

Figure 3 : Time taken for data transmission from publisher to subscriber of different sizes

The broker requires some space for the implementation of security algorithm. The required space for proving security to the data of different sizes is as tabulated in table 4 and illustrated in figure 4.

Data size	Space required for providing security
1 byte	1 byte
10 bytes	1 byte
100 bytes	2 bytes
1 kb	4 bytes
10 kb	9 bytes
100 kb	16 bytes
1 Mb	32 bytes
10 Mb	48 bytes
100 Mb	64 bytes

Table 4 Space necessary to demonstrate security for various data sizes Space necessary to demonstrate security for various data sizes Space necessary to demonstrate security for various data sizes Space necessary to demonstrate security for various data sizes

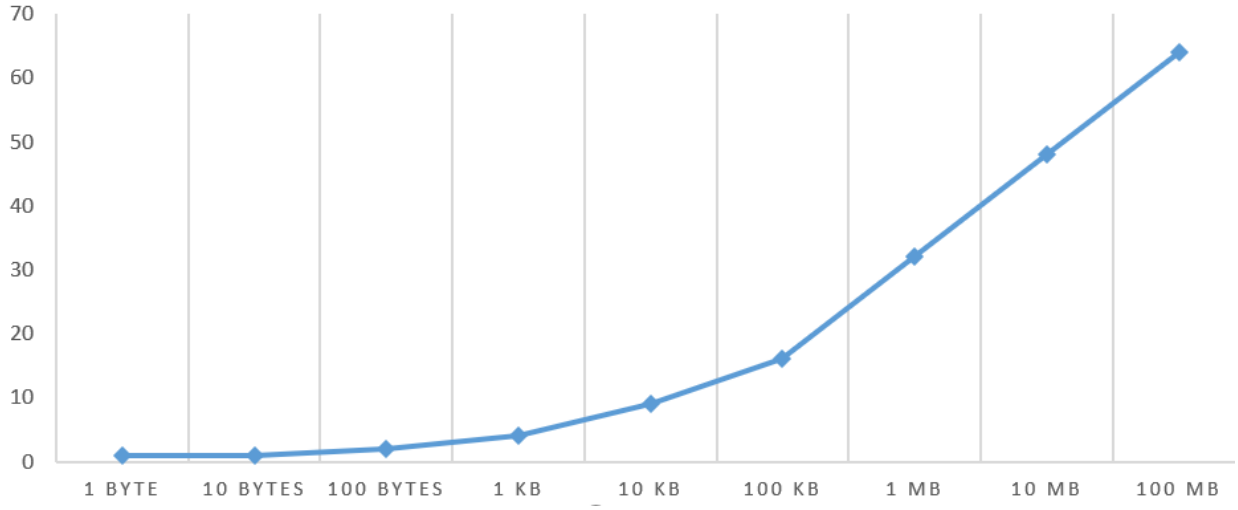

Figure 4 : Space necessary to demonstrate security for various data sizes

The results of the proposed secured system architecture are compared with conventional MQTT protocol on the basis of time and space complexity.

	Proposed secured MQTT		Conventional MQTT	
data size	**Time (seconds)**	**Memory (bytes)**	**Time (seconds)**	**Memory (bytes)**
1 byte	0.0001	1	0.0001	1
10 bytes	0.0001	1	0.0001	1
100 bytes	0.0003	2	0.000294	1
1 kb	0.0008	4	0.000784	2
10 kb	0.0019	9	0.001862	8
100 kb	0.13	16	0.1274	15
1 Mb	1.06	32	1.0388	30
10 Mb	11.94	48	11.7012	46
100 Mb	103.83	64	101.7534	58

Table 5 : Comparative study of the time and memory required for proposed and conventional MQTT protocol

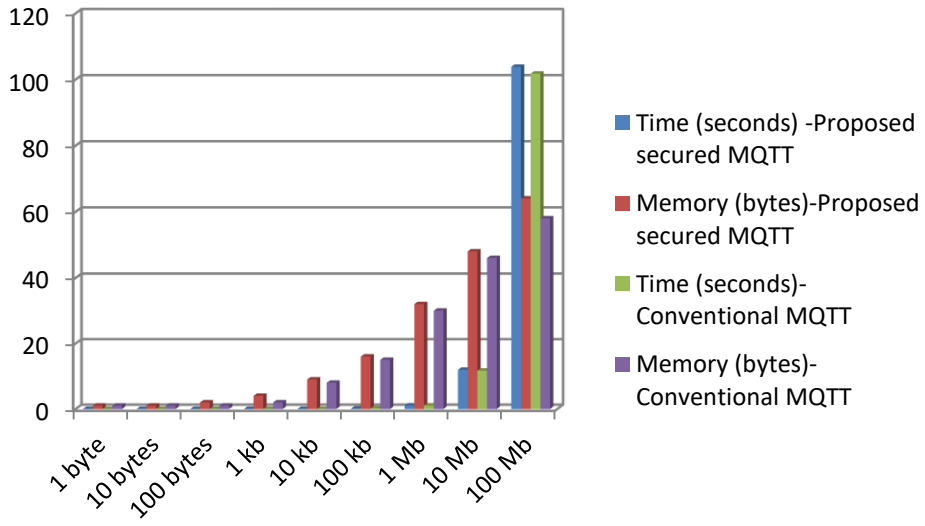

Figure 5 : Comparative study of the time and memory required for proposed and conventional MQTT protocol

It comes out that proposed secured MQTT protocol takes slightly more time and more memory than that of the conventional MQTT. The proposed protocol takes approximately 2% more time and 4% more memory than conventional system.

The proposed secured system is tested on many different hardware platforms. Time complexity of the proposed protocol is checked on the different processors [36]. The average time required to transfer data of 1kbof size on different hardware platforms is tabulated in table 4.

Platform	Time required to get result (in seconds)
CPU, i3 processor, 8GB RAM	0.001
CPU, i5 processor, 8GB RAM	0.0008
CPU, I7 processor, 8GB RAM	0.0007

Table 6 : The time it takes to get data transfer by using proposed protocol on different hardware platforms

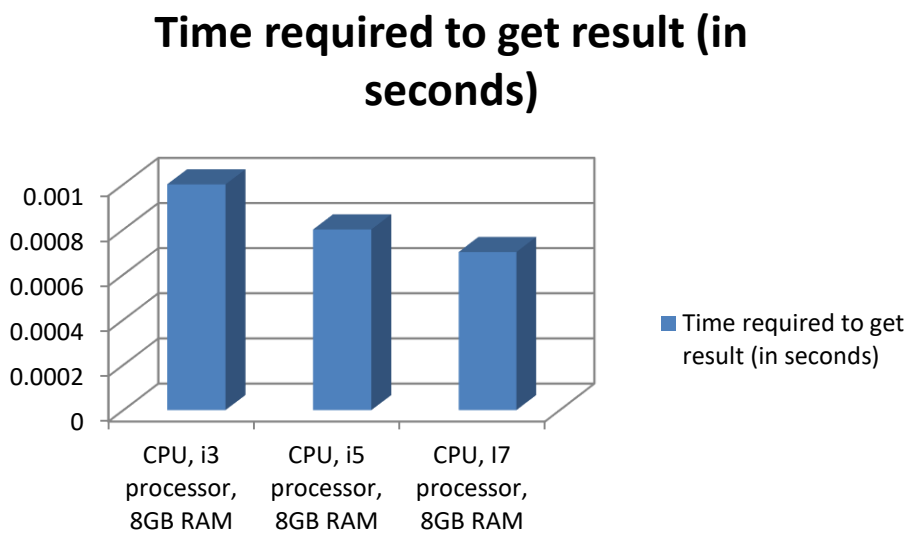

Figure 6 : The time it takes to get data transfer by using proposed protocol on different hardware platforms

VI. CONCLUSION

By using AES algorithm, we encrypt the data to security in MQTT protocol. Two metrics, time complexity and space complexity, are used to test the proposed secured MQTT protocol. The time it takes to send data from publisher to subscriber using the suggested protocol is 2% longer than with the current approach. In addition, the amount of memory required is slightly higher. However, in terms of security, it is always preferable to adopt the recommended secured MQTT protocol. In an unprotected network, the proposed protocol also performs well. This work concentrates on the broker's dependability in terms of whether or not the broker is active. Proposed system takes much less time along with less space to get execute the results.

REFERENCES

[1] M. Calabretta, R. Pecori and L. Veltri, "A Token-based Protocol for Securing MQTT Communications," *2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2018, pp. 1-6, doi: 10.23919/SOFTCOM.2018.8555834.

[2] M. Mukhandi, D. Portugal, S. Pereira and M. S. Couceiro, "A novel solution for securing robot communications based on the MQTT protocol and ROS," 2019 IEEE/SICE International Symposium on System Integration (SII), 2019, pp. 608-613, doi: 10.1109/SII.2019.8700390.

[3] B. Mishra and A. Kertesz, "The Use of MQTT in M2M and IoT Systems: A Survey," in IEEE Access, vol. 8, pp. 201071-201086, 2020, doi: 10.1109/ACCESS.2020.3035849.

[4] N. N. N. Vithanage, S. S. H. Thanthrige, M. C. K. P. Kapuge, T. H. Malwenna, C. Liyanapathirana and J. L. Wijekoon, "A Secure Corroboration Protocol for Internet of Things (IoT) Devices Using MQTT Version 5 and LDAP," 2021 International Conference on Information Networking (ICOIN), 2021, pp. 837-841, doi: 10.1109/ICOIN50884.2021.9333910.

[5] Malina, Lukas; Srivastava, Gautam; Dzurenda, Petr; Hajny, Jan; Fujdiak, Radek (2019). [ACM Press the 14th International Conference - Canterbury, CA, United Kingdom (2019.08.26-2019.08.29)] Proceedings of the 14th International Conference on Availability, Reliability and Security - ARES '19 - A Secure Publish/Subscribe Protocol for Internet of Things. , (), 1–10. doi:10.1145/3339252.3340503

[6] Calabretta, Marco; Pecori, Riccardo; Vecchio, Massimo; Veltri, Luca (2018). MQTT-Auth: a Token-based Solution to Endow MQTT with Authentication and Authorization Capabilities. Journal of Communications Software and Systems, 14(4), –. doi:10.24138/jcomss.v14i4.604

[7] Dinculeană, Dan; Cheng, Xiaochun (2019). Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. Applied Sciences, 9(5), 848–. doi:10.3390/app9050848

[8] W. -T. Su, W. -C. Chen and C. -C. Chen, "An Extensible and Transparent Thing-to-Thing Security Enhancement for MQTT Protocol in IoT Environment," 2019 Global IoT Summit (GIoTS), 2019, pp. 1-4, doi: 10.1109/GIOTS.2019.8766412.

[9] F. Chen, Y. Huo, J. Zhu and D. Fan, "A Review on the Study on MQTT Security Challenge," 2020 IEEE International Conference on Smart Cloud (SmartCloud), 2020, pp. 128-133, doi: 10.1109/SmartCloud49737.2020.00032.

[10] I. Stoev, S. Zaharieva, A. Borodzhieva and G. Staevska, "An Approach for Securing MQTT Protocol in ESP8266 WiFi Module," 2020 XI National Conference with International Participation (ELECTRONICA), 2020, pp. 1-4, doi: 10.1109/ELECTRONICA50406.2020.9305164.

[11] Hernández Ramos, Santiago; Villalba, M. Teresa; Lacuesta, Raquel (2018). MQTT Security: A Novel Fuzzing Approach. Wireless Communications and Mobile Computing, 2018(), 1–11. doi:10.1155/2018/8261746

[12] Patel, Chintan; Doshi, Nishant (2020). â€ • A Novel MQTT Security framework In Generic IoT Modelâ€ • . Procedia Computer Science, 171(), 1399–1408. doi:10.1016/j.procs.2020.04.150

[13] Buccafurri, Francesco; De Angelis, Vincenzo; Nardone, Roberto (2020). Securing MQTT by Blockchain-Based OTP Authentication. Sensors, 20(7), 2002–. doi:10.3390/s20072002

[14] Liao, Teh-Lu; Lin, Hong-Ru; Wan, Pei-Yen; Yan, Jun-Juh (2019). Improved Attribute-Based Encryption Using Chaos Synchronization and Its Application to MQTT Security. Applied Sciences, 9(20), 4454–. doi:10.3390/app9204454

[15] Lohachab, Ankur; Karambir, (2019). ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. Journal of Information Security and Applications, 46(), 1–12. doi:10.1016/j.jisa.2019.02.005

[16] E. B. Sanjuan, I. A. Cardiel, J. A. Cerrada and C. Cerrada, "Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach," in IEEE Access, vol. 8, pp. 115051-115062, 2020, doi: 10.1109/ACCESS.2020.3003998.

[17] Ammar, Mahmoud; Russello, Giovanni; Crispo, Bruno (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38(), 8–27. doi:10.1016/j.jisa.2017.11.002

[18] A. Oak and R. D. Daruwala, "Assessment of Message Queue Telemetry and Transport (MQTT) protocol with Symmetric Encryption," 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), 2018, pp. 5-8, doi: 10.1109/ICSCCC.2018.8703314.

[19] Ahamed, Jameel; Zahid, Md.; Omar, Mohd; Ahmad, Khaleel (2019). AES and MQTT based security system in the internet of things. Journal of Discrete Mathematical Sciences and Cryptography, 22(8), 1589–1598. doi:10.1080/09720529.2019.1696553

[20] H. Yujia, H. Yongfeng and C. Fu, "Research on Node Authentication of MQTT Protocol," 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS), 2020, pp. 405-410, doi: 10.1109/ICSESS49938.2020.9237678.

[21] R. Montella, M. Ruggieri and S. Kosta, "A fast, secure, reliable, and resilient data transfer framework for pervasive IoT applications," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2018, pp. 710-715, doi: 10.1109/INFCOMW.2018.8406884.

[22] Z. Laaroussi and O. Novo, "A Performance Analysis of the Security Communication in CoAP and MQTT," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021, pp. 1-6, doi: 10.1109/CCNC49032.2021.9369565.

[23] S. P. Mathews and R. R. Gondkar, "Protocol Recommendation for Message Encryption in MQTT," 2019 International Conference on Data Science and Communication (IconDSC), 2019, pp. 1-5, doi: 10.1109/IconDSC.2019.8817043.

[24] A. Muhammad, B. Afzal, B. Imran, A. Tanwir, A. H. Akbar and G. Shah, "oneM2M Architecture Based Secure MQTT Binding in Mbed OS," 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2019, pp. 48-56, doi: 10.1109/EuroSPW.2019.00012.

[25] R. A. Nathi and D. Sutar, "Object Security Scheme based on Access Policies using MQTT Protocol for IoT Devices," 2019

10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-6, doi: 10.1109/ICCCNT45670.2019.8944432.

[26] MD Jiabul Hoque1* , MD Akibur Rahman1 and Shihab Uddin1, “Real Time and Secure Messaging Service for IoT Applications using MQTT “Journal of Engineering Research and Education Volume 12, 2020

[27] Cüneyt Bayılmış, M. Ali Ebleme, Ünal Çavuşoğlu, Kerem Küçük, Abdullah Sevin,A survey on communication protocols and performance evaluations for Internet of Things, Digital Communications and Networks,2022.

[28] Kitae Hwang, In Hwan Jung, Jae Moon Lee.” Monitoring of MQTT-based Messaging Server” Webology, Volume 19, Number 1, January, 2022.

[29] S. Hariprasad, T. Deepa and P. Chandhar, "SENMQTT-SET: An Intelligent Intrusion Detection in IoT-MQTT Networks Using Ensemble Multi Cascade Features," in IEEE Access, doi: 10.1109/ACCESS.2022.3161566.

[30] Zhandos Kegenbekov, Arman Saparova, Using the MQTT Protocol to Transmit Vehicle Telemetry Data, Transportation Research Procedia, Volume 61, 2022.

[31] Eric Riedel, MQTT protocol for SME foundries: potential as an entry point into industry 4.0, process transparency and sustainability, Procedia CIRP, Volume 105, 2022.

[32] Jackılyn B. Baccay, Clarıssa P. Vıcente, Marıbel T. Bravo.” IoT-based Automated Greenhouse with Monitoring and Control using MQTT Protocol” Turkish Online Journal of Qualitative Inquiry (TOJQI) Volume 12, Issue 6, June 2021:593-609.

[33] Gamess, E., Ford, T. N., & Trifas, M. (2021). Performance evaluation of a widely used implementation of the MQTT protocol with large payloads in normal operation and under a DoS attack. Proceedings of the 2021 ACM Southeast Conference.

[34] M. Bender, E. Kirdan, M. -O. Pahl and G. Carle, "Open-Source MQTT Evaluation," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021, pp. 1-4, doi: 10.1109/CCNC49032.2021.9369499.

[35] Dmitrii Dikii, Sergey Arustamov, Aleksey Grishentsev.” DoS attacks detection in MQTT networks” ndonesian Journal of Electrical Engineering and Computer Science Vol. 21, No. 1, January 2021, pp. 601~608

[36] A. S. Ladkat, A. A. Date and S. S. Inamdar, "Development and comparison of serial and parallel image processing algorithms," 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, pp. 1-4, doi: 10.1109/INVENTIVE.2016.7824894.