Ingénierie des Systèmes d'Information
Vol. 28, No. 2, April, 2023, pp. 419-424
Journal homepage: http://iieta.org/journals/isi

Internet of Things Based Secured Data Transmission Protocol for Agriculture Application

Pallavi Sunil Bangare*, Kishor P. Patil

Department of E&TC, Sinhgad Academy of Engineering, Savitribai Phule Pune University, Pune 411048, India

Corresponding Author Email: psbangare.sae@sinhgad.edu

https://doi.org/10.18280/isi.280217

Received: 27 September 2022
Accepted: 2 April 2023

Keywords:
communication system, IOT, security, MQTT, agriculture, SMO, AES

ABSTRACT

In this research, we proposed a protocol for information transmission in a communication system. The protocol consists of three parts: Publisher, Broker, and Subscriber. The main problem in the transmission is the reliability of the broker. It is very difficult to get the status of the broker whether it is active or not. Secondly, we also worked on the part of security. Here by employing a Watchdog timer to determine whether the broker is active or not. To make the system more secure AES algorithm is incorporated into it. To validate the suggested protocol hardware setup is built and performance is tested in various conditions. Performance tests show that our proposed system outperforms the current system when compared to the existing system. The suggested system architecture's temporal and spatial complexity are also presented in this research.

1. INTRODUCTION

Multiple devices can communicate with one another using the lightweight messaging protocol MQTT. It utilizes the publish-subscribe method for communication and is a TCP-based protocol. Data communication between devices with limited resources and minimal power requirements is made possible by this protocol. As a result, the IoT Framework frequently uses this message protocol for communication. MQTT is a publish-and-subscribe protocol, so client devices and applications interact with topics managed by a broker rather than a server. MQTT uses several bi-directional transports in addition to IP (Internet Protocol) as its primary mode of transport. The MQTT broker is computer software that can be either self-created or a third-party host. There are both open source and proprietary options. Under this strategy, several clients interact with one another, but there is no established relationship between them. Every client communicates with every other client via a Broker, a third-party middleman.

In a way, the broker functions like a post office. Instead of using the intended recipient's direct connection address, MQTT clients use the "Topic" topic line. A copy of every message associated with a topic will be sent to anyone who subscribes to it. While a single broker can subscribe many clients and a client can do the registration with multiple brokers. (One to many capabilities) (many to one). The TCP/IP layered protocol paradigm can be viewed of as an extension of the stack of IoT protocol, which comprises of the physical layer, network layer, link layer, transport layer, application services layer and application protocol layer. The idea behind the Internet of Things (IoT) is to link common household appliances to the web. Even though communication is crucial to the IoT, the variety of IoT use cases makes it one of the trickiest issues to solve. It might be challenging to identify the optimal protocol for a specific solution because there are so numerous network technologies available to suit communication needs.

The data are analyzed using a Merkle Tree. An extension of the hash list, as a hash-based data structure, a Merkle tree. Non leaf node represents a hash of a node's children, and every leaf node represents a hash of a data block. Merkle trees can contain two children per node due to their two-fold branching factor. A protocol is a set of guidelines or a language that various entities can use to communicate or interact with one another. The Internet of Things (IoT) ecosystem is now used by household appliances, manufacturing equipment, vehicle parts, and other products. This environment has consequently had an impact on a wide range of locations, including households, car manufacturers, and hospitals, leading to a sharp rise in the variety of connected devices. The Internet of Things has grown in popularity as an outcome. However, system architects and protocol designers have found it challenging to select the appropriate communication protocol for these items or devices in a particular IoT system. The two key components of an IoT system are bidirectional connectivity and security.

2. LITERATURE SURVEY

Calabretta et al. [1] concentrate on MQTT, a message-based protocol for communication built on the MQTT protocol that has been designed for low-power sensors. It utilizes the publish-subscribe model. Before anything else, we'll go over some of the standard security precautions and improvements listed in the There is a ton of information available for MQTT deployments. Then we offer a probable answer. alternative MQTT-based technique to protect particular topics The protocol AugPAKE was created by AugPAKE.

Mukhandi et al. [2] study cyber-attacks might hamper the development and revision of the majority of ROS based robotic systems for Internet-based applications. It's crucial to recognize and reduce security vulnerabilities associated with applications that use ROS. Kertesz and Mishra [3]. Machine to Machine protocol is exhibited. The authors of this research

analyze the development of M2M protocol research over the previous 20 years (MQTT, AMQP, and CoAP), emphasizing how MQTT research is noteworthy [4]. The most well-known M2M/IoT protocol, MQTT, has a wide range of potential applications. The authors evaluate nearly significant MQTT articles published in the last decade using our quantitative analysis.

Vithanage et al. [4] defined the main causes is that it difficult to run complicated security algorithms and impedes security services like authentication and privacy as limited computing power memory and energy. The result is, adopting suitable security and authentication solutions is necessary for a widespread IoT implementation. This research proposes an authentication platform that makes use of MQTT and LDAP technologies to boost the security and effectiveness of data flow between IoT devices in order to achieve that goal.

Malina et al. [5] introduce a special publish/subscribe-based security architecture for the Message Queue Transport Telemetry (MQTT) protocol. In this study to enable secure and private Internet of Things services, as demonstrated by Huo et al. [6]. Thanks to its simple technical requirements and lightweight architecture, MQTT has surged onto the IoT industry. There are three levels of security in our suggested solution.

Calabretta et al. [7] concentrate on MQTT (Message Queue Telemetry Transport), which was created for lightweight machine-to-machine interactions and was defined [8-10]. MQTT is a publish-subscribe message-based communication protocol. Prior to that, it gives a thorough analysis of some of the newest security fixes and MQTT changes made by the literature by Stoev et al. [9]. The solution described in the paper employs a straightforward non-secure class to implement the Wi-Fi protocol and is based on the MQTT protocol for interfacing ESP8266 devices. Oak et al. [11] created 256-bit symmetric encryption using the Advanced Encryption Standard [11, 12] to enable simple, secure communication.

Buccafurri et al. [13] emphases on the MQTT protocol, which is widely used in the IoT and is depicted in [14]. Developers anticipate that this protocol will have natively implemented safe authentication methods. As a result, this article presents a novel authentication scheme i.e., OTP that uses the Ethereum Blockchain to construct a second factor authentication.

Lohachab [15] presents a novel, lightweight authentication and authorization architecture appropriate for remote IoT scenarios using ECC and MQTT. Sanjuan et al. [16] suggest by means of cryptographic smart cards to develop a security scheme for the MQTT protocol that takes care of the issues with trusted data secrecy and integrity as well as the authentication scheme.

There are some previously issued studies related to the safe MQTT protocol for IoT networks and identified firm significant security flaws in the protocol [17-20]. It provides a real-time, secure, and secure MQTT protocol for Internet of Things applications. Baylmş et al. [21] investigated these circumstances, the IoT social class joins the entrances, stages, and little devices of the cloud. Hwang et al. [22] chooses MQTT taking into account how the informative display identifies and depicts the crucial boundaries that reveal the MQTT server grounded on wide implementation and MQTT dispatch characteristics [22, 23].

Hariprasad et al. [24] study on a review place equipped with sensors and hardware [25] connected to a lightweight Message Queue Telemetry Transport (MQTT) display, the organization's preliminary study is conducted. There are three parts to this: The SENMQTTSET dataset is created by (I) gathering sensor usage data for 3 unique leads; (II) multiset branding through the application of a rule scheme to produce a set of measurable Multiview markings; and (IIII) evaluating the dataset using Machin Learning estimations. The SENMQTTSET dataset has been modified to only include three potential clients: attacks on merchants, allies, and conventional clients.

Kegenbekov et al. [26] study MQTT Protocol. Manufacturers have become interested in the use of MQTT emission aimed at telemetry records in transit. They depicted the sort of telemetry data release and transport to gather study, finish the best and most balanced state of the primary MQTTs, and accumulate the proximity of data among the motion server and the utility server to ensure this goal.

Eric Riedel and co. gives the deception of the newest steel parts is certainly justified by the foundry industry and its processes and design requirements. It is crucial to understand the methodology's limitations. Among others, Baccay et al. [27] propose the audit sought to update the nursery's hydraulic system and regulate the environment. The microcontroller has been redesigned to operate the electromechanical valve and fan in their natural environments: (1) The consumer can actually operate using any Internet-connected device via the web (2) a predetermined still around people, (3) a temperature that kills the content of crop's soil soaking. The sensor center's accumulated data was saved in an external device in.csv format so that it could be assembled as support. The message line telemetry transport broadcast was used to transmit data for graphical display [28-30]. The current system is adequate in terms of availability, firmness, comfort, and accessibility. As a result, the final clients were confident that the developed framework could be applied and altered.

Gamess et al. [31] study the term "Internet of Things" (IoT) refers to the network of devices with specific knowledge and bandwidths. IoT-focused social class programmes have gotten older in generating interest because to the reach of IoT devices connected to the internet. Dikii et al. [32] explore the issue of how the Internet of Things can remain secure in the face of DoS assaults on public services and a select few others. Using three classifiers and the qualities listed below—username, gadget ID, and IP address—they created a purposeful condition for the Assault ID device that was equipped. The producers have picked the Neath conditions to give the chosen classifiers the best enchanter for spotting unusual and genuine visitors in MQTT associations [33-35]. The newest CNN version, called a capsule network-based technique by S. Pande et al., has been proposed as the optimal architecture for maintaining links between learned characteristics across the network and the authors also proposed the KNN-based strategy for retrieving medicinal leaf information [36-38].

3. PROPOSED METHODOLOGY AND HARDWARE SETUP

From the literature, it is clear that there is a problem with the reliability and security in the system. To overcome this hardware set along with suggested protocol is implemented. The hardware arrangement transmits sensor data to the server. Then, at the dashboard, data is retrieved from the server as shown in Figure 1.

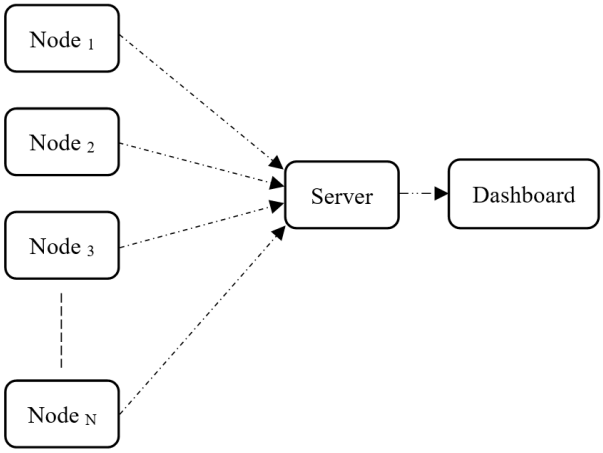

Figure 1. Data communication flow from nodes (sensors) to dashboard via server

These values are then first encrypted along with the device MAC ID and IP address. After Merkle trees spread the data, this system conducts AES on the data. By converting plain text into cypher text, which is made up of seemingly random characters, encryption is able to protect data. Those who possess the unique key are the only ones who can decrypt it. Data must be encoded and decoded using just one secret key when using symmetric key encryption, which is what AES does. The Advanced Encryption Standard is used to achieve asymmetric encryption. AES bits are used to encrypt and decrypt data, and they are available in lengths of 128, 192, and 256 bits. AES employs the symmetric key to safeguard the data once the Merkel tree has processed it. Due to the size of its key length, the three alternatives for AES encryption are 128 bit, 192 bit, and 256 bit, with the latter being the most secure.

1. Throughout the encryption method, the system provides a unique key to the dispersed data before data Byte Replacement (Sub Bytes). In order to create network structures, lines, and sections, the 16 bits of data are finely bowed arrangements.

2. The matrix network moves the rows using circular byte shifts every four lines to the left.

3. Group Columns 16 fledgling bytes are produced by another framework, and this expansion is not repeated in the final cycle.

4. Consist of a round key. Cypher text, a homogenous round of interpreted data of 128 bits and 16 bytes, will be used to store the input matrix, round key, and output.

5. AES cypher text action for decoding in the inconsistency request. The entire procedure is broken down into four parts, each of which is dedicated to the request for a logical discrepancy.

This encrypted data is then sent database. Here, the database is stored in firebase server. On dashboard python script is written which reads the values from the database. Dashboard first try to decrypt the data, once decryption is completed then it checks if received data is from authorized node and from authorized IP address. If yes then and then only the data get reflected on the dashboard otherwise error signal get generated. Agriculture IoT is selected for the testing of proposed algorithm. Node is consisting of the sensor along with Wi-Fi module. Node MCU is the Wi-Fi application board which is selected as it is able to read the value from sensor (Figure 2).

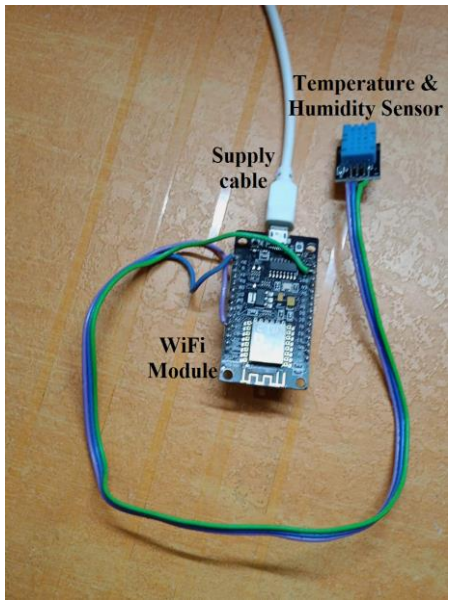

Figure 2. Hardware setup of agriculture IoT

A watchdog timer is a software mechanism that helps ensure the stability and reliability of a broker. It is a timer that monitors the broker's operation and resets the broker if it detects any malfunctions or failures. One of the main advantages of the watchdog timer is that it can help prevent broker crashes and other malfunctions that can result from software bugs, hardware failures, or other issues. By constantly monitoring the broker's operation and resetting it, when necessary, the watchdog timer can help ensure that the system remains stable and reliable.

ESP8266 is a low-cost, low-power, Wi-Fi microchip designed by the Chinese manufacturer Espressif Systems. It can be used as a standalone microcontroller with built-in Wi-Fi connectivity or as a Wi-Fi module to add wireless networking capabilities to other microcontrollers. The use of it provides the low-cost node which allows direct pin to pin connection with DHT11 sensor. The experiments have been conducted on the same hardware and are presented in next section.

4. RESULTS AND DISCUSSION

The received data from the server is decrypted using proposed system architecture. At the dashboard side, the trust and the authenticity are get checked and according to that the data/ notification get reflected on dashboard.

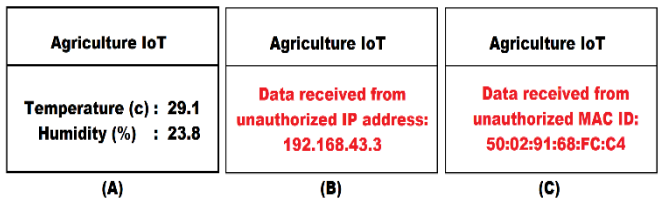

Figure 3. (A) Decrypted data at the dashboard, (B) Notification on dashboard about unauthorized IP address, (C) Notification on dashboard about unauthorized MAC ID

As shown in Figure 3(A), the value of temperature and humidity is displayed on dashboard as this value are sent from

authorized IP address with authorized MAC ID. But in case of Figure 3(B) and Figure 3(C) the received values are from unauthorized IP address and unauthorized MAC ID respectively, so that the instead of showing data from unauthorized device the dashboard shows the notification about unauthenticity. Both the time and the space complexity of the suggested system are tested. By using time stamps at the transmitter and receiver end, the time required for the transmission of data is calculated and tabulated in Table 1. For more clarification, it is plotted in Figure 4.

Table 1. Time required for data transmission

Data size(bytes)	Duration of data transmission (in seconds)
1	0.0001
10	0.0011
100	0.0203
1000	0.0903
10000	0.1518
100000	0.9231

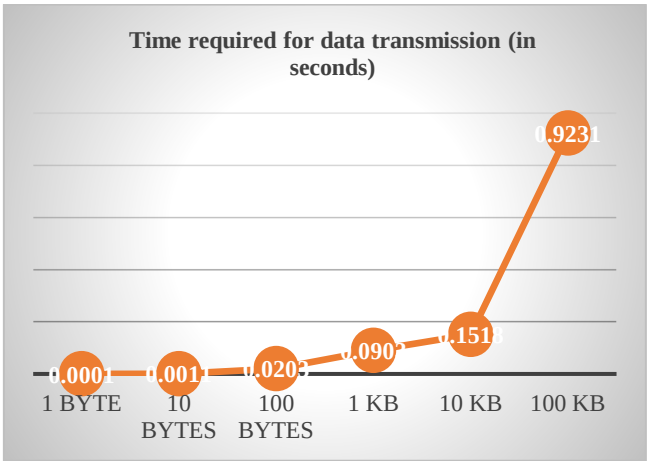

Figure 4. Time required for data transmission from pub to sub

For the added reliability and security in the conventional MPPT the watchdog timer and security protocol are used. For this purpose, broker requires some extra space. The amount of space needed to demonstrate security to data of various sizes is listed in Table 2 and depicted in Figure 5.

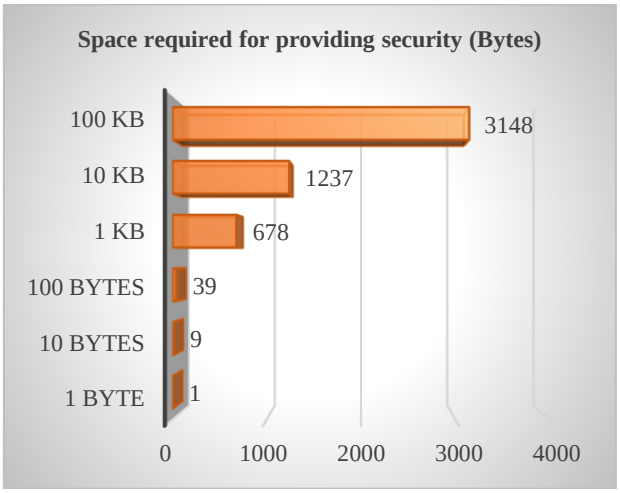

Figure 5. Space required to validate the security for various data sizes

Table 2. Space required to show security for different data sizes

Data size	Space needed for providing security (Bytes)
1 byte	1
10 bytes	9
100 bytes	39
1 kb	678
10 kb	1237
100 kb	3148

The suggested secure system has undergone testing across a wide range of hardware platforms. The suggested protocol's time complexity is tested on several processors because the broker's processing speed depends on the processor [39]. Here, the broker is implemented in different CPUs. The average time required to decrypt data of 1kb of size and display it on dashboard with comparison of several hardware platforms is carried out in Table 3.

Table 3. The amount of time required to transport data using the proposed protocol on various hardware platforms

Platform	Time required to get result (in seconds)
i7 processor, 8GB RAM	0.006
i5 processor, 8GB RAM	0.007
I3 processor, 8GB RAM	0.009

5. CONCLUSIONS

This research mainly focused on the security and reliability. The reliability of the protocol is improved by using watchdog timer into it. For the more secured communication, additional encryption layer is added in conventional MQTT protocol. In the result part, time complexity and space complexity are also calculated. It is observed that proposed MQTT protocol required 2% more time to transmit data than that of the conventional MQTT protocol.

ACKNOWLEDGMENT

We are thankful to Sinhgad Academy of Engineering Management and Savitribai Phule Pune University, for the support of the research work.

REFERENCES

[1] Calabretta, M., Pecori, R., Veltri, L. (2018). A token-based protocol for securing MQTT Communications. 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1-6. https://doi.org/10.23919/SOFTCOM.2018.8555834

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

https://doi.org/10.1109/SII.2019.8700390
[3] Mishra, B., Kertesz, A. (2020). The use of MQTT in M2M and IoT systems: A survey. IEEE Access, 8: 201071-201086. https://doi.org/10.1109/ACCESS.2020.3035849
[4] Vithanage, N.N.N., Thanthrige, S.S.H., Kapuge, M.C.K.P., Malwenna, T.H., Liyanapathirana, C., Wijekoon, J.L. (2021). A Secure corroboration protocol for internet of things (IoT) devices using MQTT version 5 and LDAP. International Conference on Information Networking (ICOIN), pp. 837-841, https://doi.org/10.1109/ICOIN50884.2021.9333910
[5] Malina, L., Srivastava, G., Dzurenda, P., Hajny, J., Fujdiak, R. (2019). A secure publish/subscribe protocol for internet of things. Proceedings of the 14th International Conference on Availability, Reliability and Security - ARES '19 - A secure publish/subscribe protocol for Internet of Things, pp. 1-10. https://doi.org/10.1145/3339252.3340503
[6] Huo, Y.J., Huang, Y.F., Chen, F. (2020). Research on Node Authentication of MQTT Protocol. IEEE 11th International Conference on Software Engineering and Service Science (ICSESS), pp. 405-410. https://doi.org/10.1109/ICSESS49938.2020.9237678
[7] Calabretta, M., Pecori, R., Vecchio, M., Veltri, L. (2018). MQTT-Auth: A token-based solution to endow MQTT with authentication and authorization capabilities. Journal of Communications Software and Systems, 14(4): 320-331. https://doi.org/10.24138/jcomss.v14i4.604
[8] Chen, F., Huo, Y., Zhu, J., Fan, D. (2020). A review on the study on MQTT security challenge. In 2020 IEEE International Conference on Smart Cloud (SmartCloud), pp. 128-133. https://doi.org/10.1109/smartcloud49737.2020.00032
[9] Stoev, I.I., Zaharieva, S., Borodzhieva, A.N., Staevska, G. (2020). An approach for securing MQTT protocol in ESP8266 WiFi module. 2020 XI National Conference with International Participation (ELECTRONICA), pp. 1-4. https://doi.org/10.1109/ELECTRONICA50406.2020.9305164
[10] Hernández Ramos, S., Villalba, M.T., Lacuesta, R. (2018). Mqtt security: A novel fuzzing approach. Wireless Communications and Mobile Computing, 2018: 1-11. https://doi.org/10.1155/2018/8261746
[11] Oak, A., Daruwala, R.D. (2018). Assessment of message queue telemetry and transport (MQTT) protocol with symmetric encryption. First International Conference on Secure Cyber Computing and Communication (ICSCCC), pp. 5-8. https://doi.org/10.1109/ICSCCC.2018.8703314
[12] Ahamed, J., Zahid, M., Omar, M., Ahmad, K. (2019). AES and MQTT based security system in the Internet of Things. Journal of Discrete Mathematical Sciences and Cryptography, 22(8): 1589-1598. https://doi.org/10.1080/09720529.2019.1696553
[13] Buccafurri, F., De Angelis, V., Nardone, R. (2020). Securing mqtt by blockchain-based otp authentication. Sensors, 20(7): 2002. https://doi.org/10.3390/s20072002
[14] Liao, T.L., Lin, H.R., Wan, P.Y., Yan, J.J. (2019). Improved attribute-based encryption using chaos synchronization and its application to MQTT security. Applied Sciences, 9(20): 4454. https://doi.org/10.3390/app9204454
[15] Lohachab, A. (2019). ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. Journal of Information Security and Applications, 46: 1-12. https://doi.org/10.1016/j.jisa.2019.02.005
[16] Sanjuan, E.B., Cardiel, I.A., Cerrada, J.A., Cerrada, C. (2020). Message queuing telemetry transport (MQTT) security: A cryptographic smart card approach. IEEE Access, 8: 115051-115062. https://doi.org/10.1109/ACCESS.2020.3003998
[17] Montella, R., Ruggieri, M., Kosta, S. (2018). A fast, secure, reliable, and resilient data transfer framework for pervasive IoT applications. IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 710-715. https://doi.org/10.1109/INFCOMW.2018.8406884
[18] Laaroussi, Z., Novo, O. (2021). A performance analysis of the security communication in CoAP and MQTT. IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), pp. 1-6. https://doi.org/10.1109/CCNC49032.2021.9369565
[19] Mathews, S.P., Gondkar, R.R. (2019). Protocol recommendation for message encryption in MQTT. International Conference on Data Science and Communication (IconDSC), pp. 1-5. https://doi.org/10.1109/IconDSC.2019.8817043
[20] Muhammad, A., Afzal, B., Imran, B., Tanwir, A., Akbar, A.H., Shah, G. (2019). OneM2M architecture based secure MQTT binding in Mbed OS. In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 48-56. https://doi.org/10.1109/EuroSPW.2019.00012
[21] Bayılmış, C., Ebleme, M.A., Çavuşoğlu, U., Küçük, K., Sevin, A. (2022). A survey on communication protocols and performance evaluations for Internet of Things. Digital Communications and Networks, 8(6): 11. https://doi.org/10.4108/eetiot.v8i4.2691
[22] Hoque, M.J., Rahman, M.A., Uddin, S. (2020). Real time and secure messaging service for IoT applications using MQTT. Journal of Engineering Research and Education, 12: 43-54. https://doi.org/10.3329/iiucs.v17i1.54982
[23] Hwang, K., Jung, I.H., Lee, J.M. (2022). Monitoring of MQTT-based messaging server. Webology, 19(1): 19136. https://doi.org/10.14704/WEB/V19I1/WEB19316
[24] Hariprasad, S., Deepa, T., Chandhar, P. (2022). SENMQTT-SET: An intelligent intrusion detection in IoT-MQTT networks using ensemble multi cascade features. IEEE Access, 10: 33095-33110. https://doi.org/10.1109/ACCESS.2022.3161566
[25] Dinculeană, D., Cheng, X. (2019). Vulnerabilities and limitations of MQTT protocol used between IoT devices. Applied Sciences, 9(5): 848. https://doi.org/10.3390/app9050848
[26] Kegenbekov, Z., Saparova, A. (2022). Using the MQTT protocol to transmit vehicle telemetry data. Transportation Research Procedia, 61: 410-417. https://doi.org/10.1016/j.trpro.2022.01.067
[27] Baccay, J.B., Vıcente, C.P., Bravo, M.T. (2022). IoT-based automated greenhouse with monitoring and control using MQTT protocol. Turkish Online Journal of Qualitative Inquiry (TOJQI), 12(6): 593-609.
[28] Riedel, E. (2022). MQTT protocol for SME foundries: Potential as an entry point into industry 4.0, process

transparency and sustainability. Procedia CIRP, 105: 601-606. https://doi.org/10.1016/j.procir.2022.02.100

[29] Bender, M., Kirdan, E., Pahl, M.O., Carle, G. (2021). Open-source MQTT evaluation. IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), pp. 1-4. https://doi.org/10.1109/CCNC49032.2021.9369499

[30] Borwankar, A.A., Ladkat, A.S., Mhetre, M.R. (2015). Thermal transducers analysis. In National Conference on, Modeling, Optimization and Control, 4th-6th March.

[31] 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, pp. 154-162. https://doi.org/10.1145/3409334.3452067

[32] Dikii, D., Arustamov, S., Grishentsev, A. (2021). DoS attacks detection in MQTT networks. Indonesian Journal of Electrical Engineering and Computer Science, 21(1): 601-608. https://doi.org/10.11591/ijeecs.v21.i1.pp601-608

[33] Surve, J., Umrao, D., Madhavi, M., Rajeswari, T.S., Bangare, S.L., Chakravarthi, M.K. (2022). Machine learning applications for protecting the information of health care department using smart Internet of Things appliances-A review. In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 893-898. https://doi.org/10.1109/ICACITE53722.2022.9823642

[34] Alanya-Beltran, J., Narang, P., Bangare, S.L., Valderrama-Zapata, C., Jaiswal, S. (2022). An empirical analysis of 3D image processing by using machine learning-based input processing for man-machine interaction. In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 2478-2482. https://doi.org/10.1109/ICACITE53722.2022.9823699

[35] Wu, X., Wei, D., Vasgi, B.P., Oleiwi, A.K., Bangare, S. L., Asenso, E. (2022). Research on network security situational awareness based on crawler algorithm. Security and Communication Networks, 2022: 3639174. https://doi.org/10.1155/2022/3639174

[36] Ladkat, A.S., Patankar, S.S., Kulkarni, J.V. (2016). Modified matched filter kernel for classification of hard exudate. In 2016 International Conference on Inventive Computation Technologies (ICICT), pp. 1-6. https://doi.org/10.1109/INVENTIVE.2016.7830123

[37] Ladkat, A.S., Bangare, S.L., Jagota, V., Sanober, S., Beram, S.M., Rane, K., Singh, B.K. (2022). Deep neural network-based novel mathematical model for 3D brain tumor segmentation. Computational Intelligence and Neuroscience, 2022: 4271711. https://doi.org/10.1155/2022/4271711

[38] Shobana, M., Balasraswathi, V.R., Radhika, R., Oleiwi, A.K., Chaudhury, S., Ladkat, A.S., Rahmani, A.W. (2022). Classification and detection of mesothelioma cancer using feature selection-enabled machine learning technique. BioMed Research International, 2022: 9900668. https://doi.org/10.1155/2022/9900668

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