ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/346602846

A Survey on Securing Payload in MQTT and a Proposed Ultra-lightweight Cryptography

Chapter · January 2021

DOI: 10.1007/978-981-15-7062-9_32

CITATIONS
0

READS
17

2 authors:

Edward Nwiah
Sharda University
4 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Shri Kant
Sharda University
34 PUBLICATIONS **54** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Deep Learning for Medical Image Analysis View project

LITERATURE SURVEY ON SECURITY IN INTERNET OF THINGS (IoTs) View project

All content following this page was uploaded by Edward Nwiah on 09 February 2022.

The user has requested enhancement of the downloaded file.

A SURVEY ON SECURING PAYLOAD IN MQTT AND A PROPOSED ULTRA- LIGHTWEIGHT CRYPTOGRAPHY

Edward Nwiah[1] and Shri Kant[2]
[1]M.Tech CSE – Networking & Cybersecurity Department of Computer Science
Sharda University, Knowledge Park III, Greater Noida, Uttar Pradesh 201310, India
2018012616.edward@pg.sharda.ac.in
[2] Department of Computer Science
Sharda University, Knowledge Park III, Greater Noida, Uttar Pradesh 201310, India
shri.kant@sharda.ac.in

Abstract

Internet of Things foresees devices that are connected globally, accessing and sharing pertinent information to make life easier and better. This highly interconnected global network seeks to advance business productivity, government efficiency, and agriculture growth. However, these fantastic opportunities also present a number of significant security challenges..

Quite a number of researches have gone into the domain of Internet of Things (IoT). MQTT which is the short form for Message Queuing Telemetry Transport is an application layer protocol that has been proposed to smoothen publish and subscribe procedures in exchanging data between client and the server. MQTT however, was designed without proper security imbibition. In this paper, recent security mechanisms for enhancing the security of the MQTT protocol have been studied and analysed comparatively. Based on the challenges that surfaced from the survey, this research proposes an ultra-lightweight cryptography, Hummingbird-2 as a novel security solution. This is done to achieve bandwidth and memory efficiency, quality of service of data delivery.

Keywords – Security, cryptography, payload, publisher, subscriber, broker, internet of things, hummingbird, brute force, linear cryptanalysis, differential cryptanalysis, overhead

1 INTRODUCTION

IoT is an emerging technology that extends the power of internet to encompass computers, smartphones other devices, processes as well as the environments. Such connected devices helps in collecting and sending information to and fro. IoT offers a viable means in simplifying forthcoming internet concept, in a way domains which include; smart cities, smart homes, public health, energy management, agriculture, smart transportation, smart grids, waste management, which embed with sensors, actuators, electronics and network connectivity which enables such domains to communicate [1]. Though, the connectivity is capable of transforming various sectors of life, there is still a challenge that potential hackers might cease this opportunity to exploit these technologies in order cause harm with these critical infrastructure. [2].

Gartner mentioned in its report predicting massive sales of IoT devices by 2020 and indicating approximately twenty-one billion devices connecting to each other by same said date which is 2020. The rate at which systems, devices and services are capitalizing on the IoT environment is really creating great opportunities and its relevance to the society

is highly substantial. However, the security aspects is not marching parallel with the innovations it brings on board thereby creating mayhem and economic risk [3]. Security in IoT devices and systems raises concern as developers put much emphasis on customer convenience, functionality, compatibility requirements, etc. rather than security. About 600% attacks were launched against IoT devices from 2016 to 2017 according to Symantec and this indicates that threats and security issues are rising each day [4].

According to the Vice President of Gartner Research, Bob Gill, "By 2020, more than 25% of identified attacks in enterprises will involve the IoT, although the IoT will account for less than 10% of I.T. security budgets". IoT presents variety of challenges which includes; security dangers to IoT devices, operating systems and platforms they are connected to. In this regard, competent technologies are needed to safeguard IoT devices and platforms from the hands of hackers tempering on salient data [5].

Billion devices exchange information through to the internet and is therefore evident that these devices are prone to security attack. Protocols in IoT systems differ from traditional internet protocols and as a result works comfortable with constrained devices. Some of these constraints include low power consumption, limited bandwidth, low computational capabilities, small memory size etc. A lot of protocols have been implemented and are already standardized in the internet of Things.

In view of this Message Queuing Telemetry Transport (MQTT) protocol came into the lime light. The main focus of MQTT was to cater for devices with low bandwidth, high latency or unreliable network. MQTT is entirely lightweight protocol since it offers a lean header structure and also simple to implement. This research therefore proposes Hammingbire-2 to provide extensive security to MQTT since it was not developed with security mechanisms.

1.1 OBJECTIVES

The following objectives have been enumerated by the researcher in this survey:

1. To analyse existing security techniques that have been implemented in securing MQTT protocol.
2. To develop an system to secure payload in an IoT environment using MQTT

1.2 PROBLEM STATEMENT

IoT systems comprises of "things" such as temperature and humidity sensors, Radio Frequency Identification (RFID), motion sensors which are constraint devices with limited memory, low power consumption, limited computational capacity and limited bandwidth. There are various protocols proposed for IoT devices which MQTT is one of them. This protocol is devoid of strong security for transferring messages, the basic authentication mechanism data are transmitted in clear text which is not secure. This protocol depends on another protocol for its security which is Transport Layer Security. This TLS is a weightier and expensive with regards to its computation. Therefore, a lightweight encryption for payload is suggested as optimal option [6]. This paper proposes an ultra-lightweight cryptography to secure payload in MQTT in an IoT based network.

1.3 MQTT PROTOCOL

MQTT is a protocol created and works best for constrained devices due to its lightweight nature. It works on top of transport layer protocol TCP/IP for sending messages. It was proposed to smoothen publish and subscribe procedures in exchanging data between client and server. It was invented by Arlen Nipper of Arcom (now Eurotech) in 1999 and Dr. Andy Stanford Clark of IBM [7]. IBM submitted this MQTT to OASIS specification body in 2013 and its standardization was successfully completed [8]. OASIS in 2014 approved version 3.1.1 of MQTT as a standard application layer protocol. [9]. MQTT possesses versatility features such as simplicity, openness, lightweight, low power usage and again designed to be easily implemented. These features renders it effective in many circumstances, involving constrained environments which includes Machine to Machine communication and IoT contexts where network bandwidth is highly rated.

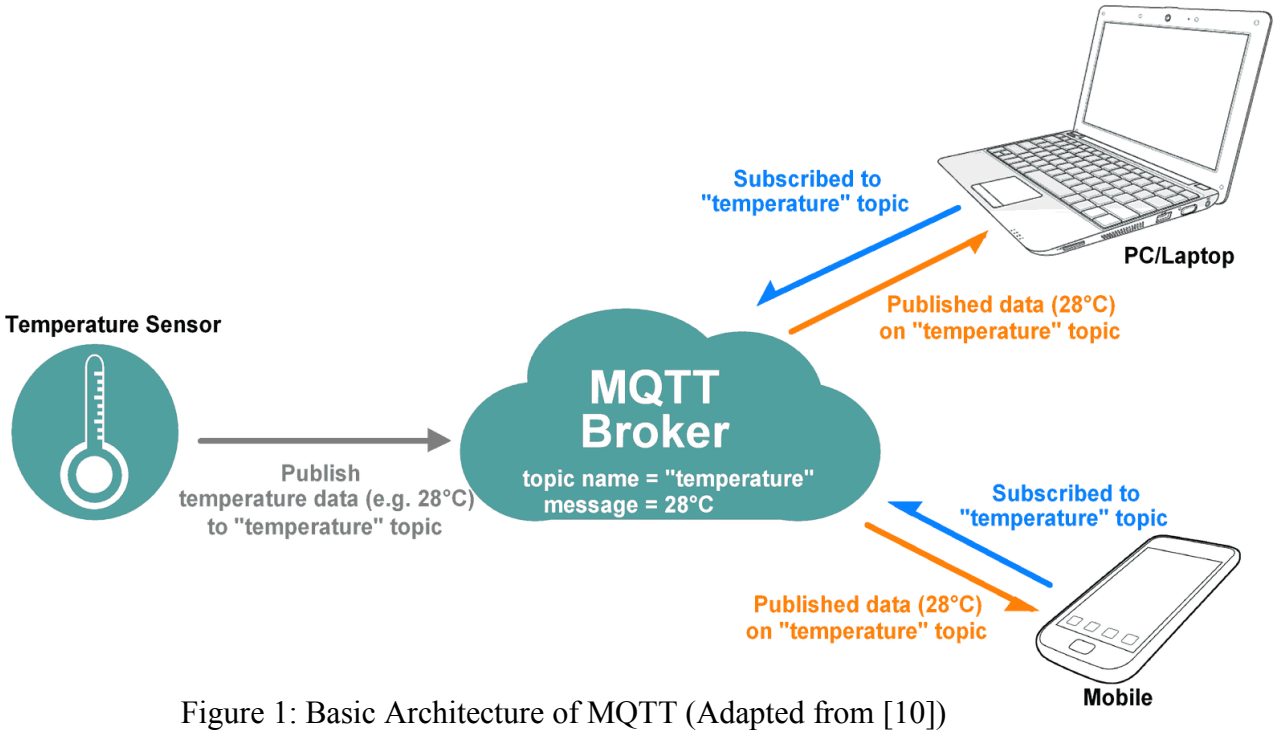

Figure 1: Basic Architecture of MQTT (Adapted from [10])

2 REVIEW OF EXISTING TECHNIQUES

A number of techniques have been proposed by many researchers in securing MQTT. This section presents an analysis of some techniques proposed by other researchers.

L. Bisne and M. Parmar [11] proposed a Composite secure MQTT for Internet of Things by means of dynamic S-box Advanced Encryption Standard (AES) and Attribute – based Encryption (ABE). They presented a key result which offer confidentiality and access control of exchange of information in an MQTT protocol. In their proposed system, access is being provided by an external trusted authority which increases the overhead. Again this approach uses both private key and public key cryptographic solution and as a result doubles the decryption process by the subscriber which in turn increases the overhead.

Singh et al. [12]. In this paper a technique called Key/Ciphertext Policy-Attribute Based Encryption using lightweight Elliptic Curve Cryptography was used. CP/KP-ABE uses the bilinear pairing operations. The use of this scheme is computationally expensive. Again this operations are not appropriate for constrained devices.

Calabretta et al. [13] proposed a technique for MQTT using the AugPAKE. The proposed technique which is uses the AugPAKE algorithm for ensuring confidentiality. In this system two tokens are used which provides authorization in accessing a topic and also authenticate how topics are being used.

Niruntasukrat et al. [14] proposed a mechanism for MQTT-based Internet of Things known as the Authorization mechanism. This ensures the authorization for single topic to be accessed. This security mechanism introduces a fourth element in the MQTT setup and that create an overhead in the process of exchanged messages and the entire communication process.

Shin et al. [15] proposed a security framework for MQTT protocol. The proposed solution make use of Augmented Password-Based Key Exchange (AugPAKE) protocol. It is relatively useful because two separate session keys are used in the negotiation between the publisher and the broker, and the broker and the subscriber. This is done without the need for certificates either for validation or revocation. Their technique does not cater for the confidentiality of the data.

Matischek et al. [16] proposed A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment using Hash and XOR operations. The model is said to have low computational cost, communication and storage overhead, at the same accomplishing common authentication and above all agreement of session key but no mechanism for the data protection.

Almuhammadi et al.[17] in their proposed, common AES modes of operation are analyzed . The comparison was done with regards to time taken for encryption and decryption and throughput with variable data packet sizes. In their analysis they concluded that, for faster modes of operation ECB is considered compared to other modes of operation.

Thatmann et al. [18] the focus of their research was to use encryption for securing MQTT. Attribute-based Encryption technique was used to publish / subscribe message patterns in MQTT. Their security solution was used to compare

different security mechanism previously studied. Their proposed solution is used to mitigate cluster communication security not end-to-end communications. Their work requires another entity called the group controller to communicate with MQTT network across HTTPS RESTful calls which is a tailback.

Peng et al. [19] they used Identity-Based Cryptography (IBC) to develop a secured MQTT protocol. With this cryptography a client, who accesses the public parameters of the system, also encrypt a message using the receiver's key which comprises name or email address. The decryption is derived from a central authority and sent to the receiver. The decryption is trusted because it's also generate a secret for all users resulting several entities, IoT gateways and external administrators, acting as private key generators and administrating distinctive trust areas are introduced. Another shortcoming of this technique is the introduction of IoT gateways and devices which handles two IBC-based private keys, and this in effect generates more overhead.

Upadhyay at al. [20] they proposed a solution that seek to secure MQTT by the use of Access Control Lists (ACLs) included in the Mosquito broker. With this technique different usernames and passwords are needed for different data and which in turn causes more overhead.

Bhawiyuga et al. [21] in their security solution, to authorize access to a specific topic a token is required. To do this, another entity to carry out the access tokens known as the authentication server. The introduction of the authentication server contribute to further overhead both in exchanging message and the management of the server.

S. Katsikeas et al. [22] In their research highlighted appropriate properties of MQTT as a lightweight protocol and its usage for industrial purposes. Different security techniques for MQTT was evaluated, noted among them was payload encryption with AES, payload encryption with AES-CBC, payload authenticated encryption with AES-OCB and link layer encryption with AES-CCM. It was concluded in their evaluation that all the stated techniques are good depending on the purpose.

3 COMPARATIVE ANALYSIS OF LITERATURE REVIEW

SN	AUTHOR	YEAR	TITLE	TOOLS/TECHNIQUES	CONTRIBUTION
1	L. Bisne and M. Parmar	2017	Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES	ABE and dynamic S-box AES	There is confidentiality and access control of data but the introduction of external trusted authority for access policy increases the overhead.
2	Singh et al.	2015	Secure MQTT for internet of things (IoT)	Key/Ciphertext Policy-Attribute Based Encryption using lightweight Elliptic Curve Cryptography.	CP/KP-ABE uses the bilinear pairing operations. The use of this scheme is computationally expensive. This operations are not appropriate for constrained devices.
3	Calabretta et al.	2018	A token-based protocol for securing MQTT communications	AugPAKE security protocol	Their technique ensures confidentiality. In this system two tokens are used which provides authorization in accessing a topic and also authenticate how topics are being used.
4	Niruntasukrat et al.	2016	Authorization mechanism for MQTT-based Internet of Things	OAuth framework	Their system ensures the authorization for single topic to be accessed. Again a fourth element is introduced in the MQTT setup and that create an overhead in the process of exchanged messages and the entire communication process.
5	Shin et al.	2016	A security framework for MQTT	AugPAKE security protocol	Two separate session keys are used in the negotiation between the publisher and the broker, and the broker and the subscriber. Their technique does not cater for the confidentiality of the data.
6	Matischek et al.	2017	A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment	Hash and XOR operations	Their proposal is a lightweight authentication solution which uses only hash and XOR operations.
7	Almuhammadi et al.	2017	A comparative Analysis of AES Common Modes of Operation.		The comparison was done with regards to the time taken for encryption and decryption and throughput with variable data packet sizes and concluded that ECB mode is faster than other modes of operation.

8	D. Thatmann et al	2015	Applying Attribute-based Encryption on Publish Subscribe Messaging Patterns for the Internet of Things	Attribute-based Encryption (ABE)	Technique used to mitigate cluster communication not end-to-end communications. Their work requires another entity called the "group controller" which communicate with the MQTT network through HTTPS RESTful calls which is a tailback.
9	Peng et al.	2016	A secure publish/subscribe protocol for Internet of Things using identity-based cryptography	Using identity-based cryptography	IoT gateways and external administrators are used there by increasing overhead.
10	Upadhyay at al.	2016	MQTT based secured home automation system	Access Control Lists (ACLs)	Access Control Lists (ACLs) included in the Mosquitto broker. With this technique different usernames and passwords are needed for different data and which in turn causes more overhead
11	Bhawiyuga et al	2017	Architectural design of token based authentication of MQTT protocol in constrained IoT device	Token based solution	Different entity to carry out the access tokens known as the authentication server. The introduction of the authentication server contribute to further overhead.
12	S. Katsikeas et al.	2017	Lightweight and secure Industrial IoT Communications via the MQ Telemetry Transport Protocol	Evaluation of different security options	Comparative analysis of different security mechanism to secure MQTT protocol.

4 RESEARCH QUESTIONS

1. What are some of the challenges identified in the existing techniques?
2. Which cryptographic technique can be implemented to address the security challenges of payload being transmitted in MQTT?

5 PROPOSED MODEL

LOGICAL ARCHITECTURE

The logical architecture as seen in Figure 2 depicts a conceptual design of the proposed model which identify the workflow between the components. The components of the architecture includes; Publisher, Key Management System (KMS), Broker and Subscriber. This shows a typical MQTT architecture with its entities communicating through the broker. The role of the publisher is to publish a payload (temperature reading). The Subscriber is the entity that is allowed to receive a payload on topics of interest. KMS is another entity which provides a management service by distributing the secret key to the clients (publisher and subscriber). The Broker then serves as a communication medium between the publisher and subscriber. It receives payload from the publisher and transmit to the authenticated subscriber.

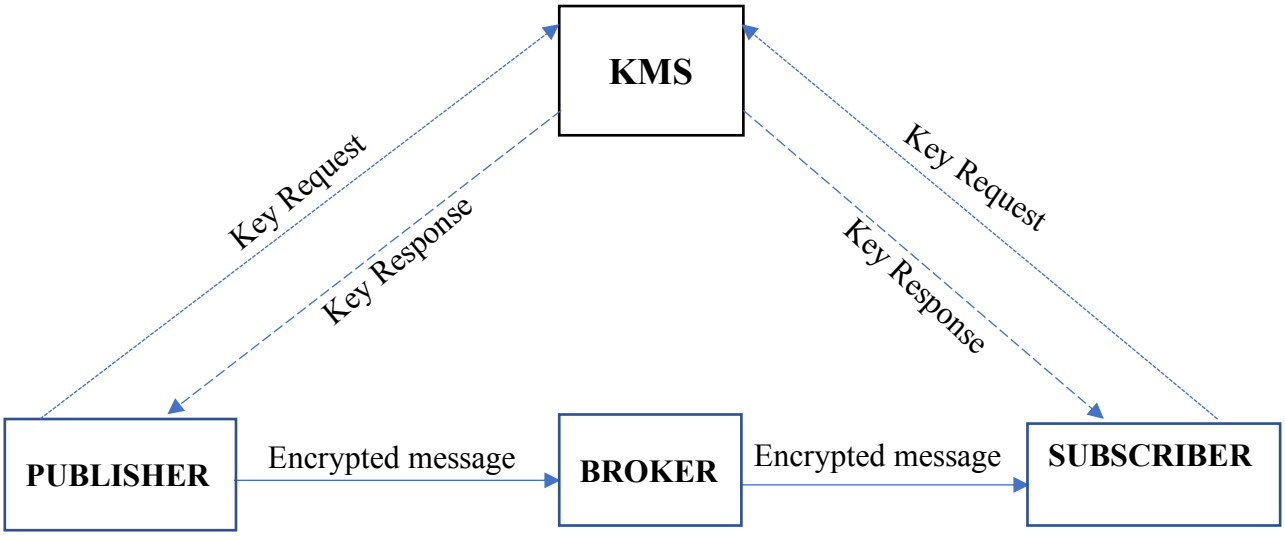

Fig. 2: Logical Architecture of MQTT

The security technique this research is proposing to address the challenges outlined is an ultra-lightweight encryption scheme known as Hummingbird-2. Hummingbird-2 was proposed as an improvement to Hummingbird-1 which combines stream cipher and block structure. It has 256-bit security and can recuperate entire private key with at most 2^{64} off-line computational effort under two related IVs. Nevertheless, Hummingbird-2 incorporate in its design some basic design of Hummingbird-1 [24]**.** This research proposes Hummingbird-2 because it offers privacy-preserving identification and mutual authentication protocol for constrained devices which includes; industrial controllers, smart meters, RFID tags, wireless sensors, etc. Hummingbird-2 has very small hardware as well as software footmark and is convenient for providing security for constraint devices [25]. Hummingbird-2 has a 16-bit block size, 128- bit secret key and a 64-bit initialization vector.

Hummingbird 2 is used in this proposed model to ensure security of payload in an MQTT based IoT system. The focus of this proposed model is payload encryption in MQTT. The payload is encrypted as part of the PUBLISH packets,

which is transmitted to the broker. The Broker then forwards the encoded payload to the Subscriber who has subscribed to the topic. Decryption occurs at the subscriber's end. All other data including client information and topic information are transmitted in a plaintext from the publisher to the subscriber as seen in figure 3.

Fig. 3: Publish Packet. Adapted from [23]

5.1 DISCUSSION, ANALYSIS AND FUTURE WORK

Hummingbird 2 is an ultra-lightweight encryption scheme used in this research. The model will be very difficult for hackers to manipulate the content since the payload is encrypted at the publishers end before transmitting to the broker for onward transmission the subscriber. Decryption is only done at the subscriber's destination. The system read accurately and encrypted temperature readings from three different locations (IoT Lab, Networking Lab and My apartment) which shows good progress of the model.

To ensure eavesdroppers are unable to follow the encryption pattern of plaintext by brute force attack, linear and differential cryptanalysis. The encryption is done in a way that same plaintext gives different ciphertext when encrypted multiple times.

The implementation of the model is at its final stage. We strongly hope, analysis after testing the model will yield great results as expected in the design.

6 CONCLUSION

In this research, a comprehensive comparative analysis was conducted on existing security techniques to secure MQTT protocol. The comparative analysis indicates most techniques focuses on authentication of users and few others on payload being transmitted in an end-to-end communication. Again most of the techniques introduces third parties which to some extent increases overhead depending on their operations.

The propose security technique focuses on securing the payload being transferred from end to end in the MQTT based system using Hummingbird-2 encryption algorithm.

ACKNOWLEDGEMENTS

The work is possible with the help with many people. My sincere gratitude and appreciation to all those who contributed this project possible.

Firstly, I am extremely grateful to my research guide, Prof. Shri Kant Rastogi for his scholarly inputs and consistent encouragement. I could not have imagined having a better advisor and mentor for my project.

Secondly, a special thanks to my family especially Francis Nwiah, Dorothy Nyarko for their love, affection and financial support.

Finally I give thanks to God for taking me through all the difficulties. I have experienced Your guidance day by day. I will keep on trusting You for my future. Thank you, Lord.

REFERENCE

[1] El-hajj, M., Chamoun, M., Fadlallah, A., Serhrouchni, A.: Analysis of authentication techniques in Internet of Things (IoT). In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 18–20 October 2017; pp. 1–3.

[2] Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy, December 2016, 90 pp.

[3] Eddy, N, Gartner: 21 Billion IoT devices to invade by 2020" Information week Nov. 2015.

[4] Internet Security Threat Report (2018), Symantec Corporation, March 2018. https://www.symantec.com/security-center/threat-report

[5] Gartner Insights on How to Lead in a Connected World, "Leading the IoT", https://www.gartner.com/imagesrv/books/IoT/IoTEbook_digital.pdf

[6] Edielson et al. M2M Protocols for Constrained Environment in the Context of IoT: A Comparison of Approaches, Dec. 2015.

[7] Rahul Gupta Banks. Mqtt version 3.1.1. URL: http://docs.oasis-open.org/mqtt/mqtt/v3.3.3/cos02/mqtt-v3.1.1-cos02.html

[8] Oasis. [Online].Available: http://www.oasis-open.org.

[9] ISO/IEC20922, Information technology-Message Queuing Telemetry Transport(MQTT) v3.1.1, ISO, 2016. [Online]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=69466

[10] ElectronicWings. [Online]. Available: http://www.electronicwings.com/nodemcu/nodemcu-mqtt-client-with-arduino-ide

[11] Bisne, L., Parmar, M.: Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES, 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, 2017, pp. 1- 5. doi: 10.1109/IPACT.2017.8245126.

[12] Singh, M., Rajan, M., Shivraj, V., Balamuralidhar, P.: Secure MQTT for internet of things (IoT). In: 2015 Fifth International Conference on Communication Systems and Network Technologies. pp. 746–751. IEEE (2015).

[13] Calabretta, M., Pecori, R., Velti, L.: A token-based protocol for securing MQTT communications. In: 2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM). pp. 1–6. IEEE (2018)

[14] Niruntasukrat, A., Issariyapat, C., Pongpaibool, P., Meesublak, K., Aiumsupucgul, P., Panya, A.: Authorization mechanism for MQTT-based Internet of Things, 2016 IEEE International Conference on Communications Workshops (ICC), Kuala Lumpur, 2016, pp. 290-295. DOI: 10.1109/ICCW.2016.7503802.

[15] Shin, S., Kobara, K., Chuang, C.C., Huang, W.: A security framework for MQTT. In: 2016 IEEE Conference on Communications and Network Security (CNS). pp. 432–436. IEEE (2016)

[16] Matischek, R., Saghezchi, F., Rodriguez, J., Bicaku, A,. Maksuti, S., Tauber, M., Schmittner, C., Esfahani, A., Mantas, G., Bastos, J.: A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment. In: IEEE Internet of Things Journal (2017).

[17] Almuhammadi, S., Al-Hejri, I.: A comparative Analysis of AES Common Modes of Operation. In: IEEE 30th Canadian Conference on Electrical and Computer Engineering(CCECE) (2017).

[18] Thatmann D et al. Applying Attribute-based Encryption on Publish Subscribe Messaging Patterns for the Internet of Things. In: IEEE International Conference on Data Science and Data Intensive Systems (2015).

[19] Peng, W., Liu, S., Peng, K., Wang, J., Liang, J.: A secure publish/subscribe protocol for Internet of Things using identity-based cryptography, 2016 5th International Conference on Computer Science and Network Technology (ICCSNT), Changchun, 2016, pp. 628-634. DOI: 10.1109/ICCSNT.2016.8070234.

[20] Upadhyay, Y., Borole, A., Dileepan, D.: MQTT based se- cured home automation system, 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-4. DOI: 10.1109/CDAN.2016.7570945.

[21] Bhawiyuga, A., Data, D., Warda, A.: Architectural design of to- ken based authentication of MQTT protocol in constrained IoT de- vice, 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-4. DOI: 10.1109/TSSA.2017.8272933.

[22] Katsikeas, S et al. Lightweight and secure Industrial IoT Communications via the MQ Telemetry Transport Protocol. In: (2017).

[22] HIVEMQ. [Online]. Available: http://www.hivemq.com/mqtt-essentials

[23] M.J.O. Saarinen, Cryptanalysis of Hummingbird-1, Fast Software Encryption, FSE'11, LNCS 6733, pp. 328-341, 2011.

[24] Engels, D., Markku-Juhani O. Saarinen, Peter Schweitzer and Eric M. Smith. "The Hummingbird-2 Lightweight Authentication Encryption Algorithm".

View publication stats