IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

Review Paper on the uses of Digital Signature in MQTT Protocol

Mr. Pradeep Nayak[1], Ashwini M[2], Monisha N. S.[3], Moollya Gautami[4], Bhaskar Sahana[5]
Assistant Professor, Department of Information Science and Engineering[1]
Students, Department of Information Science and Engineering[2,3,4,5]
Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka, India

Abstract: *The Message Queue Telemetry Transport (MQTT) protocol for publish/subscribe middleware is proposed in this paper as a way to secure messages. In which the end-to-end method employs the Advanced Encryption System (AES) and Secure Hash Algorithm (SHA), and analyses the overhead associated with the usage of digital signatures Because there is no encryption method applied to the payload, MQTT has this drawback. Which enables one to discover the payload content that results in no data privacy. MQTT also has issues with data integrity. This digital signature's function is to confirm the payload's authenticity, that it doesn't alter during transmission, and that the payload is secret.The proposed solution can be evaluated and tested after which the programme can secure the MQTT payload. The addition of a security mechanism to MQTT, such as the encryption and decryption processes and verification outcomes, results in overhead in many areas. The overhead employed in this study is used to calculate the payload size, message sending time, process of digital signature security mechanism, memory consumption, and CPU utilisation. In an overhead analysis, overhead is performed by looking at many AES key types and numerous SHA key types. Upon closer inspection, it is seen that the digital signature system has resulted in a size increase for a number of the previously listed elements.*

Keywords: AES, SHA, digital signature, payload, MQTT, publish, end-to-end, subscription, overhead

REFERENCES

[1]. Syaiful Andy, Budi Rahardjo, and BagusHanindhito. Attack scenarios and security analysis of mqtt communication protocol in iot system. International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), 4(September):600–604, 2017.

[2]. Syed Naeem Firdous, Zubair Baig, Craig Valli, and Ahmed Ibrahim. Modelling and evaluation of malicious attacks against the IoT MQTT protocol. Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThingsGreenComCPSCom-SmartData 2017, 2018-Janua:748–755, 2018. K. Elissa, "Title of paper if known," unpublished.

[3]. Manish Parmar Lochan Bisne. Composite Secure MQTT for Internet of Things using ABE and Dynamic S-Box AES. pages 1–5, 2017.

[4]. Yuri F Gomes, Danilo F S Santos, Hyggo O Almeida, and Angelo Perkusich. Integrating MQTT and ISO / IEEE 11073 for Health Information Sharing in the Internet of Things. 2015 IEEE International Conference on Consumer Electronics (ICCE), pages 200–201, 2015

[5]. Nut Aroon. Study of using MQTT cloud platform for remotely control robot and GPS tracking. 2016 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, ECTI-CON 2016, 2016.

[6]. Yuvraj Upadhyay, Amol Borole, and D. Dileepan. MQTT based secured home automation system. 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016.

[7]. Singh Meena, MA Rajan, VL Shivraj, P Baramuralidhar P. Secure MQTT for Intenet of Things (IoT). 2015 Fifth International Conference on Communication Systems and Network Technologies

[8]. RashiDhagat and Purvi Joshi. New approach of user authentication using digital signature. 2016 Symposium on Colossal Data Analysis and Networking (CDAN), pages 1–3, 2016.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, January 2023
Impact Factor: 7.301

[9]. Muhammad Arif Mughal, Xiong Luo, and A T A Ullah. A Lightweight Digital Signature Based Security Scheme for Human-Centered Internet of Things. 2018.

[10]. Don Jomar S Hombrebueno, Ma Gracia Corazon E Sicat, Jasmin D. Niguidula, Enrico P. Chavez, and Alexander A. Hernandez. Symmetric cryptosystem based on data encryption standard integrating HMAC and digital signature scheme implemented in multi-cast messenger application. 2009 International Conference on Computer and Electrical Engineering, ICCEE 2009, 2:327–334, 2009.

[11]. Sourabh Chandra, SmitaPaira, B Tech Student, SkSafikul, Alam Assistant, and Goutam Sanyal. A comparative survey of symmetric and asymmetric key cryptography. 2014 International Conference on Electronics, Communication and Compytational Engineering (ICECCE), pages 83–93, 2014.

[12]. Alizai, Zahoor Ahmed. Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures. 2018 International Conference on Applied and Engineering Mathematics.