Vol. 5 , Issue. 3, 2018, ISSN 2349-0780

Design and Implementation of SMQTT for IoT Applications

Dhanshri Kolhe
dhanshrikolhe5@gmail.com
Department of computer science
Yeshwantrao Chavan College of Engineering, Nagpur

Prof. Smita Kapse
kawadesmita@gmail.com
Department of computer science
Yeshwantrao Chavan College of Engineering, Nagpur

Abstract:

In the IoT world, establishing a strong mobile network architecture will be critical for organizations to bring together people, processes, data and things. Among the various available protocols and standards to network IoT entities, the Message Queue Telemetric Transport (MQTT) is already a reference solution. It provides a publish/subscribe messaging transport specifically designed to be used in devices with limited resources over constrained networks. A message broker is an imperative component in IoT systems, and it works as a gateway between IoT devices and application platforms. With the growth of IoT devices today, these systems can easily overwhelm message brokers unless the software can fully utilize hardware resources such as multi-core facility. In this paper proposed system is designed to Implement the SMQTT protocol for secure data transfer between entities. Using IomaTic as a development platform system demonstrate the proof of concept and its implementation.

Keywords: *MQTT, D2D, IoT, Cryptography, IomaTic*

I. INTRODUCTION

Innovations in digital things, Information Communication Technology and IPV6 (Internet protocol) are enabling rapid deployment of Internet of Things (IoT) around the globe. It is estimated that trillions of IoT devices are going to be deployed in next five years. IoT Applications are immense in number and utilized to provide solutions for multitude of diversified problems. Though IoT has lot of potentials in the digital world, during its deployment, it encounters several issues with respect to (w.r.t) heterogeneity of devices, device identity, device management, secure device to device communication (D2D), etc. To enable the integration and management of heterogeneous IoT devices, architectures such as Ubiquitous Sensor Network (USN), Sensor Web Enablement (SWE), etc., are proposed. Here, security of devices (such as identity theft, data integrity), D2D communication, etc., are not addressed rigorously. Further most of the privacy and security features proposed by them are at a nascent level. To address this cryptography techniques based on Public Key Infrastructure (PKI), Identity based encryption (IBE), etc., are proposed for secure IoT communication. Though current techniques serve the purpose of basic security primitives for D2D communications, they do not address at the protocol level. Communication protocols exists such as Constrained Application Protocol (CoAP, UDP based), Message Queue Telemetry Transport (MQTT, TCP based), MQTT-SN (UDP based), etc. which are deployed for IoT at different layers have limited or devoid of security features. Hence these protocols need to address security issues for IoT.

Moreover, MQTT and MQTT-SN are more prevalent than CoAP and find applications in the area of social networks, Vehicle to Vehicle communication (V2V) and sensor networks. Hence in proposed work MQTT and MQTT-SN for IoT w.r.t security. Note that it is the user's responsibility to address security issues for MQTT and MQTT-SN.

In this direction, it is suggested to enable security forMQTT by envisaging SSL/TLS with certificates and session key management. However, for IoT due to multitude of heterogeneous devices, storing and managing the certificates and key exchanges for every session is cumbersome and also

SSL/TLS suffers from attacks such as BEAST, CRIME, RC4, Heartbleed, etc. Thus, a scalable, lightweight and robust security mechanism is required for MQTT and its variants for deploying in IoT.

Hence in this direction, we propose a Secure MQTT (SMQTT) which augments security feature for the existing MQTT protocol and its variants based on lightweight Attribute Based Encryption (ABE) over elliptic curves. The advantage of using ABE is because of its inherent design which supports broadcast encryption (with one encryption, message is delivered to multiple intended users) and thus suitable for IoT applications. ABE are of two types: (i). Ciphertext Policy based ABE (CP-ABE) and (ii). Key Policy based ABE (KPABE). In general, each of these schemes are different w.r.t the access policy, key management and are suitable for different kinds of applications. Thus as part of our study, we analyse suitability of these schemes for SMQTT from IoT perspective. To the best of our knowledge, we have not seen any security requirements and solutions of secure MQTT for heterogeneous IoT devices. The proposed security feature is efficient, robust and scalable.

II. PROBLEM STATEMENT

The main objective of proposed work is to develop a mechanism that allows the system to transfer information between multiple IoT devices or between device to server in secure way using modified version of MQTT protocol called secure MQTT. Below points describes the different objective considerations.

- To deploy a MQTT server and create a web communication between IoT board server.
- To develop a MQTT protocol in embedded environment for rapid communication.
- Design an application to monitor and control the things through MQTT protocol.
- Modifying the communication by securing the MQTT communication using encryption methods.

Proposed system is also to adopt new advancing technology, “Lightweight Cryptography”, in the IoT. System describes two reasons that support this proposal. In order to achieve end-to-end security, end nodes have an implementation of a symmetric key algorithm. For the low resource-devices, e.g. battery-powered devices, the cryptographic operation with a limited amount of energy consumption is important. Application of the lightweight symmetric key algorithm allows lower energy consumption for end devices.

The footprint of the lightweight cryptographic primitives is smaller than the conventional cryptographic ones. The lightweight cryptographic primitives would open possibilities of more network connections with lower resource devices. A comparison of the lightweight properties with the conventional cryptographic primitives is shown in Appendix. The comparison in Appendix focuses on hardware properties. Some end nodes might be able to embed general-purpose micro-processors and software properties are considered important in such platforms. However, lowest cost devices can embed only application-specific ICs due to limited cost and power consumption, where hardware properties are crucially important.

III. METHODOLOGY

Proposed system has been designed by keeping temperature sensor monitoring and remote home appliances control over TCP/IP network. System has been designed in three different modules.

3.1 Client / Publisher Hardware:

A IomaTic Development board-based implementation which use ESP8266 as a wi-fi communication module, DHT11 as a temperature monitoring system, relay switching unit for appliances tripping, LCD screen for information monitoring and finally Atmega328P as a microcontroller for logic processing. This part connects to broker as a client and send temperature information to server secondly it accepts from server to operation appliances connected to the relay unit. It also utilizes the

encryption algorithms to securely transmit the messages.

3.2 Broker / Server:

This is a TCP/IP based MQTT broker or server which is responsible to accept network connection request from publisher and subscriber. This will transmit messages between connected client either as a publisher or the subscriber. It mainly works as a post master between subscriber and publisher.

3.3 Client / Subscriber:

A client program which connect to server and subscribe itself to receive temperature in formation and graphically display it to user. It also allows user to control connected appliances using graphical user interface.

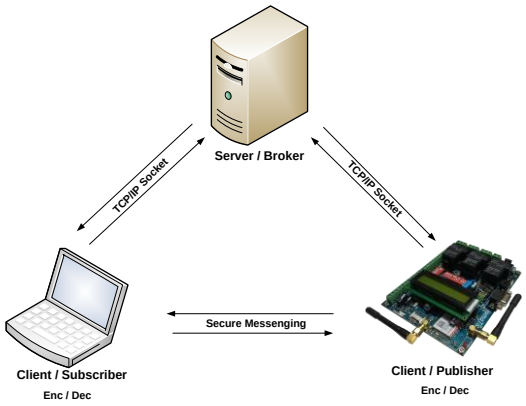

Fig. 3.0 Proposed architecture

Fig. 3.0 describes the overall system architecture of the implementation. MQTT is mainly used for unidirectional communication that is to publish the information to multiple channels at a time over TCP/IP Communication. In proposed system bidirectional Communication is established over TCP/IP socket connection in order to fetch the topic information and send the control command to the hardware or publisher.

Proposed system implemented over IomaTic where, IomaTic is first of its kind, complete IoT application development platform. It takes the ease of Arduino programming IDE and the power of open source Arduino Uno board, clubbed together with tons of on-board component and modules makes it perfect solution for the beginners who are willing to learn IoT and the experts who are ready to deploy IoT as applications or product.

Fig. 3.1 IomaTic Development Board

Unique Arduino and Atmega328p based development board having on-board components like SIM 808 with SIM slot, GPS, Bluetooth, ESP8266, DHT11, buzzer, 16x2 and 16x4 LCD support, 30amp. Relay, serial interface, mini USB programming port, connectors for different configurable IOs, multilevel voltage out like 12v, 5v, 3.3v so you can connect any sensor directly to board, configuration DIP switches to control components or modules power state and LED indications for different modules. To control these entire modules and to develop IoT applications, IomaTic board comes up with different sample codes and almost 40+ ready to deploy application where at single click IomaTic board can be converted in to real life applications that to free of cost.

IV. IMPLEMENTATION

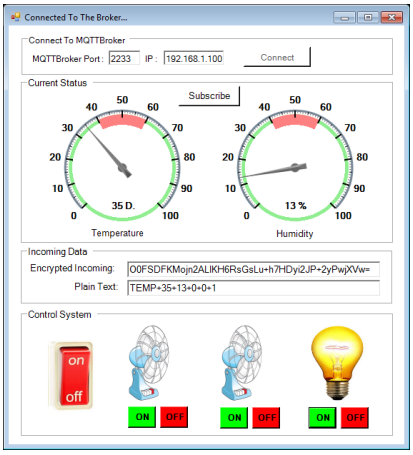

Fig 4.1 (A) Subscriber

Fig. 4.2 (B) Hardware

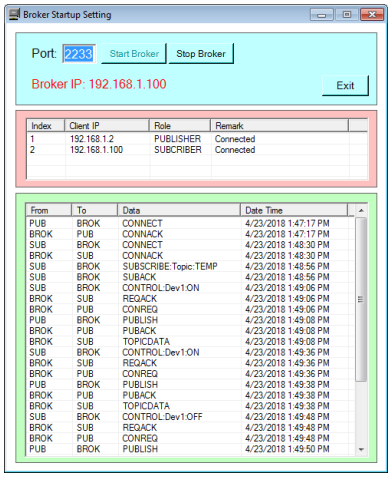

Fig. 4.3 (C) Server /Broker

Fig. 4.1 (A), (B), (C) shows the real time communication and execution result between all entities in proposed system. Subscriber show the received information form hardware, hardware publisher shows the temperature information and control the devices and finally server shows overall information exchange and packet detail.

V. CONCLUSION

Since MQTT, the lightweight messaging publish/subscribe protocol can be used to share any dynamic data, the sharing of data, e.g., flood monitoring data, earthquake data, or traffic data via MQTT protocol, can be used to improve the way of human life. However, there are variety of topic naming when the publishers shared their data over the MQTT protocol. To create the standard of topic naming MTNC was proposed in our previous work. In this work we implement the secure MQTT and tested it over wi-fi network using IomaTic development platform. With the help of socket programming in TCP/IP mode system generates the result as expected

References:

[1] B. S. Adiga, P. Balamuralidhar, M. A. Rajan, R. Shastry, and V. L.Shivraj, “An Identity Based weEncryption Using Elliptic Curve Cryptography for Secure M2M Communication,” in Proceedings of the First International Conference on Security of Internet of Things, ser. SecurIT’12. ACM, 2012, pp. 68–74.

[2] D. D´ıaz Pardo de Vera, A´ . Sigu¨enza Izquierdo, J. Bernat Vercher, andL. A. Hern´andez G´omez, “A Ubiquitous sensor network platform for integrating smart devices into the semantic sensor web,” vol. 14, no. 6. Multidisciplinary Digital Publishing Institute, 2014, pp. 10 725–10 752.

[3] X. Wang, J. Zhang, E. Schooler, and M. Ion, “Performance evaluationof Attribute-Based Encryption: Toward data privacy in the IoT,” in Communications (ICC), 2014 IEEE International Conference on, June 2014, pp. 725–730.

[4] M. Ion, "Security of Publish/Subscribe Systems," Ph.D. dissertation, University of Trento, Italy, May 2013.

[5] D. Locke, "MQ Telemetry Transport (MQTT) V3.1Protocol\Specification,"http://www.ibm.com/developerworks/library/ws-mqtt/, 2010.

[6] Davis, Ernesto Garc´ıa and Calveras, Anna and Demirkol, Ilker, "Improving packet delivery performance of publish/subscribe protocols in wireless sensor networks," vol. 13, no. 1. Multidisciplinary Digit Publishing Institute, 2013, pp. 648–680.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, 2006, pp. 89–98.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute- Based Encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy, ser. SP '07, Washington, DC, USA, 2007, pp. 321–334.

[9] P. Pal, G. Lauer, J. Khoury, N. Hoff, and J. Loyall, "P3S: A Privacy Preserving Publish-subscribe Middleware," in Proceedings of the 13thInternational Middleware Conference, ser. Middleware '12, pp. 476–495.

[10] M. Ion, G. Russello, and B. Crispo, "Supporting Publication and Subscription Confidentiality in Pub/Sub Networks," in Security and Privacy in Communication Networks, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 50, 2010, pp. 272–289.

[11] M. A. Tariq, "Non-functional Requirements in Publish/Subscribe Systems,"Ph.D. dissertation, Universit¨at Stuttgart, Fakult¨at Informatik, Elektrotechnik und Informationstechnik, Germany, August 2013.

[12] A. Sahai and B. Waters, "Fuzzy Identity-based Encryption," in Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, ser. EUROCRYPT'05, Berlin, Heidelberg, 2005, pp. 457–473.

[13] B. S. Adiga, M. A. Rajan, R. Shastry, V. L. Shivraj, and P. Balamuralidhar,"Lightweight IBE scheme for Wireless Sensor nodes,"in Advanced Networks and Telecommuncations Systems (ANTS), 2013 IEEE International Conference on, Dec 2013, pp. 1–6.

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based Encryption with Non-monotonic Access Structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 195–203.

[15] A. Stanford-Clark and H. L. Truong, "MQTT For Sensor Networks (MQTT-SN) Protocol Specification,"http://mqtt.org/documentation, 2013.

[16] Zaidi, Syed Ali Raza, et al. "Enabling IoT empowered smart lighting solutions: A communication theoretic perspective." Wireless Communications and Networking Conference Workshops (WCNCW), 2014 IEEE. IEEE, 2014.

[17] Zhang, Yuejun, Ping Zhou, and Mingguang Wu. "Research on DALI and Development of Master-Slave module." 2006 IEEE International Conference on Networking, Sensing and Control. IEEE, 2006.

[18] Alkar, Ali Ziya, and UmitBuhur. "An Internet based wireless homeautomation system for multifunctional devices." IEEE Transactions on Consumer Electronics 51.4 (2005): 1169-1174.

[19] Kovatsch, Matthias, Markus Weiss, and Dominique Guinard. "Embedding internet technology for home automation." Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on. IEEE, 2010.

[20] Zaheeruddin and Munish Manas, "A New Approach for the Design and Development of Renewable Energy Management System through Microgrid Central Controller", Energy Reports, vgt5Elsevier Inc., vol. 1, pp. 156-163, 2015.