Secure MQTT using AES for Smart Homes in IoT Network

B.K.S.Rajaram, Krishna Prakash N

Abstract: ***The privacy and security have been becoming the most exigent tasks in the Internet of Things (IoT) network. The worst enemy could be the IoT without the security and privacy policies. MQTT depends on TCP as per the transport protocol, and by default the encrypted communication is not being utilized by the connection. This paper investigates the approach of applying Advanced Encryption Standard (AES) for smart home communication in MQTT based IoT network. A prototype of network of smart homes is implemented and the data transmission reception is done using MQTT protocol. AES payload encryption with MQTT is done and the network is analysed for privacy and efficiency. Brute force attack is considered for testing the confidentiality and integrity of the data. The hardware setup of the network is implemented using Raspberry pi.***

Keywords: Internet of Things, Message Authentication Codes, Cyclic Redundancy Check, Advanced Encryption Standards, MQTT protocol, Security, cipher text, plain text

I. INTRODUCTION

The major concerns in the IoT network are the security and privacy. The security and privacy is required in the network because there could be a chance of the misconfiguration of the users. With the improper isolation and security [2] shield we would be side-lined for the use of IoT in high-end applications. There are eaves dropping attacks which capture few types of information like Brute force attack (trial and error method for eaves dropping the message). The communication happens more frequently in the network between the end devices in smart homes and therefore there is a more chance for eaves dropping. The devices in the network should not respond to such eaves dropping attacks. So a new security algorithm for smart homes with wireless nodes to demonstrate secured communication has been developed [5]. The properties for which the network will be secured are confidentiality, integrity and authenticity [4]. Confidentiality is the ability to restrict the eaves droppers or the attackers from discovering the original plain text message that has been transmitted by the sender. Integrity is the ability to restrict an active attacker from modifying the message without the notice of the legitimate user. Authenticity is the assurance that a message, communication of the information via source, it entitles from authenticity which encompasses an evidence of uniqueness.

Revised Manuscript Received on March 08, 2019.

B.K.S.Rajaram, Department of Electrical and Electronics Engineering Amrita School of Engineering, Coimbatore , Amrita Viswa Vidyapeetham, India.

Krishna Prakash N, Department of Electrical and Electronics Engineering, Amrita School of Engineering, Coimbatore, Amrita Viswa Vidyapeetham, India.

Many researches have been done in the area of secured communication for IoT applications. Internet of Things is evolving and getting advanced [9], [10] and there is also a need for security. IoT is widely used in smart home applications to control any appliance in the house. Generic design of smart home systems considering the major challenges of privacy and efficiency are discussed in [1], [3], [6]. Classification of different types of attacks, future challenges related to security along with the directions that need to be focused concerning enhancement of security [2]. Different types of attacks like low level attack, medium level attack, high level attack are the major security threats in IoT networks. IoT systems have become vulnerable on the hardware due to malicious insertions of designs causing a catastrophic damage to the system [4], [5].

An efficient protocol [11], [12], [14] has to be used for building any smart applications considering the security issues in the network. If the network gets subjected to the attacks then the protocol would not be serviceable .So first the threats for the network should be identified [5]. So a security algorithm [13] for IoT application calls a need for development for the purpose of providing securities for data considering the confidentiality, integrity and authenticity. The IoT protocol that has been used alone couldn't be enough in order to maintain the security. So a secure encryption algorithm is applied on the data that has been sent using the IoT protocols [8] in order to facilitate for prevention of data loss in the network.

II. BACKGROUND STUDY

Message Authentication codes (MACs) are required to authenticate the message between the sender and receiver. It involves a pseudo random function (PRF) in order to maintain the secured communication between the nodes in the network. The message is sent using the secured PRF because there will be a probability or the threat that the eaves droppers or the attacker might hack and tamper the data. The general attack that an attacker does in this message authentication codes is the chosen message attack which is a method of sending random message instead of the original message. In order to resist such an attacks, there is a requirement of key in the pseudo random function which maintains the confidentiality and integrity between the sender and receiver.

Cyclic Redundancy Check (CRC) is a classic check sum algorithm to detect the error in the transmitted message .The CRC is used to detect the random errors in the message. This algorithm doesn't use any key, so there will be a threat by the attacker for malicious attacks. The limitation in CRC is that it checks the random errors but not malicious errors.

Advanced Encryption Standard (AES) is used to encrypt the plain text [7], [12], [13]. The encrypted data that will be generated after the encryption is known as the cipher text. AES performs all its operations on bytes rather than bits. This comprises a series of linked operations like Add-round key, Substitute byte(s-box), Shift-rows as well as Mix-columns as shown in the Figure 1. The plain text is processed in terms of blocks [8].The text which is encrypted with the sequence should not be repeated. To achieve that the initialization vector (IV) is used. So this IV creates the cipher text in such a way that it will not be responding to any kind of dictionary attacks. The number of rounds of linked operations on a plain text depends on whether it is AES -128, AES-192 or AES-256. This AES algorithm is considered as secured because it is resistant the attacks done by the eaves droppers.

Add round key: In this add round key operation the plain text will be added with the initial key. For the next round key will be generated using the key scheduling algorithm. The output of this operation is 128 bit as the plain text is 128 bits and the key also is 128 bits.

Substitute byte operation or s-box operation: An S-box is a 16*16 matrix through which selection of values has been done depending on the inputs of the new values that are generated by the add round key operation. Each element in the state array matrix constitute a byte or 8 bits. So using the element of size 1 byte in the matrix we select the element from the s-box thus forming a new state array matrix.

Shift rows: After the S-box operation a new state array matrix will be generated. The shift rows

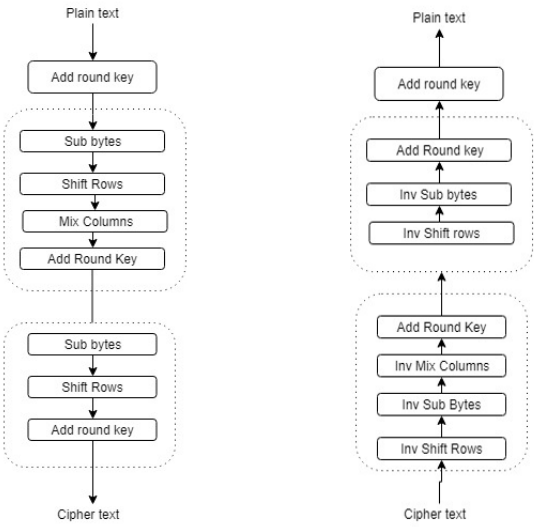

Fig. 1 Linked operations for AES encryption and decryption

operations has to be performed on the newly generated matrix. This operation is performed on each row. The left shift operation is performed on the each row. If it is zeroth row the left shift operation is performed zero times, for the first row the shift operation is performed one time and similarly for the second and the third.

Mix column operation: The array that has been generated after the shift row operation is stored in state array. This state array is then subjected to mix column operation. In this mix column operation there will be a predefined matrix. This predefined matrix is multiplied with the each column of the state matrix. The result will be replaced with the old column.

III. METHODOLOGY

Secured algorithm for smart homes in IoT applications is implemented in this paper. The system consists of network of smart homes and is considered sending the data to the server using a gateway node as shown in Figure 2. The data sent from the sender to the receiver should be secured. So before transmitting the data using some protocol, encryption has to be done in order to maintain the security. The server or the receiver end has to decrypt the data. Encryption and decryption was done so that no other third party can see the data except the sender and the receiver. The data from the smart home are considered to be energy consumption readings. Encryption keeps the data away from the eaves droppers by providing confidentiality. MQTT protocol is used for communication between the device and a server in the IoT network.

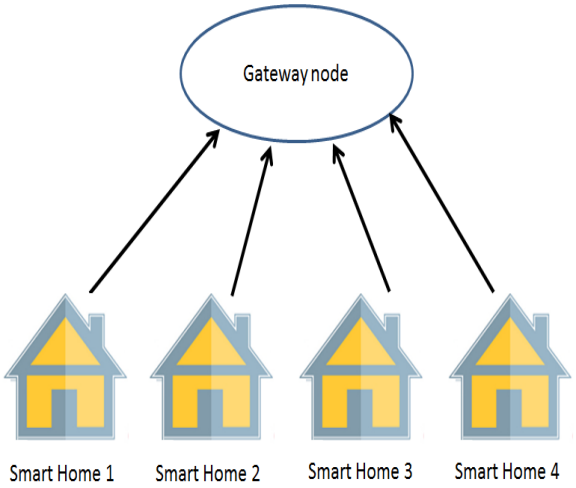

Fig. 2 System Overview

IV. IMPLEMENTATION AND RESULTS

The hardware setup of the network of smart home is implemented using Raspberry Pi. The energy meter readings from smart home are considered as the data to be sent to the gateway node. The data at the sender node (smart home) is encrypted before sending to the network.

AES algorithm is used as the secured Pseudo Random Function than CRC. The block size used in

AES is 128 bits and the mode used is AES-CBC (Cipher Block Chaining). The MQTT protocol is used for communication between the device and a server.

The sample message and the cipher text after encryption is shown in Figure 3 and Figure 4.

```
msg = '1000'

b'37QoPAcalyrP/g246/mxpbakKZQ9hFSvY1T+PS74Ml0='
Ciphertext: b'37QoPAcalyrP/g246/mxpbakKZQ9hFSvY1T+PS74Ml0='
```

Fig. 3 Sample message and cipher text

```
msg = '798.5'

b'aMKImey1NDe+0FsgGGd5JAaCWA/Su5cDA/AnmhMEzDc='
Ciphertext: b'aMKImey1NDe+0FsgGGd5JAaCWA/Su5cDA/AnmhMEzDc='
```

Fig. 4 Sample message and cipher text

The cipher pattern that is generated will not be same all the time as randomization is done using the Initialization Vector. So this maintains the confidentiality of the data or the message. The decryption is done using the same password that has been used by the sender. The decryption happens at the central entity which acts as a receiver. The encrypted and decrypted data is shown in the Figure 5 and Figure 6.

```
('plaintext:', u'1000')
('encryptedtext:', u'37QoPAcalyrP/g246/mxpbakKZQ9hFSvY1T+PS74Ml0=')
47d68207642117056 8d057e408c77ee
('plaintext:', u'1000')
('encryptedtext:', u'37QoPAcalyrP/g246/mxpbakKZQ9hFSvY1T+PS74Ml0=')
47d68207642117056 8d057e408c77ee
('plaintext:', u'1000')
('encryptedtext:', u'37QoPAcalyrP/g246/mxpbakKZQ9hFSvY1T+PS74Ml0=')
47d68207642117056 8d057e408c77ee
```

Fig. 5 Encrypted and Decrypted data

```
('plaintext:', u'798.5')
('encryptedtext:', u'aMKImey1NDe+0FsgGGd5JAaCWA/Su5cDA/AnmhMEzDc=')
47d68207642117056 8d057e408c77ee
('plaintext:', u'798.5')
('encryptedtext:', u'aMKImey1NDe+0FsgGGd5JAaCWA/Su5cDA/AnmhMEzDc=')
47d68207642117056 8d057e408c77ee
```

Fig. 6 Encrypted and Decrypted data

The results show that the confidentiality and security of the information has been maintained between the sender and the receiving parties. There are a lot of attacks done by the eaves droppers on the cipher text. One of the popular attack is the brute force attack which is a method of trial and error in order to obtain passwords. An automated software has been used to make a large number of consecutive guesses until the desired data is achieved. The AES is computationally secure against the brute force attack because it is practically not possible to acquire 128 bit key to get attacked by it.

V. CONCLUSION

The security has become the major challenge in the IoT network. The IoT protocols that are used in the network should be resistant to the attacks. The network should consider the major challenges of data integrity, confidentiality and efficiency. In order to maintain data integrity, confidentiality and efficiency of the system proper cryptographic schemes have to be introduced to the network. Considering the major challenges of security in the IoT network a prototype has been implemented with secure MQTT using AES algorithm.

REFERENCES

1. T. Song, R. Li, B. Mei, J. Yu, X. Xing and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844-1852, Dec. 2017.
2. I. Andrea, C. Chrysostom and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," *2015 IEEE Symposium on Computers and Communication (ISCC)*, Larnaca, 2015, pp. 180-187.
3. R. K. Kodali, V. Jain, S. Bose and L. Boppana, "IoT based smart security and home automation system," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, 2016, pp. 1286-1289.
4. A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," in *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586-602, Oct.-Dec. 1 2017.
5. A. Syed and R. M. Lourde, "Hardware Security Threats to DSP Applications in an IoT Network," *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, Gwalior, 2016, pp. 62-66.
6. Muneer Bani Yassein, Yaser Khamayseh and Maryan Yatim, "NISHA: Novel Interface for Smart Home Applications for
7. Arabic Region subtitle as needed" International Journal of Advanced Computer Science and Applications (ijacsa), 7(5), 2016.
8. D. M. Alghazzawi, S. H. Hasan and M. S. Trigui, "Advanced Encryption Standard - Cryptanalysis research," *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2014, pp. 660-667.
9. S. Kulkarni, S. Durg and N. Iyer, "Internet of Things (IoT) security," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 821-824.
10. R. Román-Castro, J. López and S. Gritzalis, "Evolution and Trends in IoT Security," in *Computer*, vol. 51, no. 7, pp. 16-25, July 2018.
11. D.Yogavani, N.Krishna Prakash, "Implementation of wireless sensor network based multi-core embedded system for smart city", *International Journal of Control Theory and Applications*, 2017, 10 (2), 119-123.
12. M. V. Ramesh *et al*., "Water quality monitoring and waste management using IoT," *2017 IEEE Global Humanitarian Technology Conference (GHTC)*, San Jose, CA, 2017, pp. 1-7.
13. Polamarasetty Anudeep, N. Krishna Prakash, Intelligent Passenger Information System Using IoT for Smart Cities, Advances in Intelligent Systems and Computing, Springer, Vol.851, pp.67-76, 2019.
14. F. J. D'souza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," *2017 International Conference on Computing, Communication and Automation (ICCCA)*, Greater Noida, 2017, pp. 647-652.
15. S. C. V. Bhaskar and V. R. Rani, "Performance analysis of efficient routing protocols to improve quality of service in Wireless Sensor networks," *2017 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, 2017, pp. 0006-0009.
16. Wong Seng Yue, "Application of Energy Conservation Techniques in Industries and Institution", International Innovative Research Journal of Engineering and Technology, Vol: 4, No: 2, p. 7-16, Dec 2018.