NVE
Natural Volati
Essentia

An End-to-End AES Based Cryptographic Authentication Mechanism for Communication on Internet of Things (IoT) Using MQTT

Mohammad Reza Hosenkhan[1], Binod Kumar Pattanayak[2]

[1]Faculty of Information and Communication Technology, Universite des Mascareignes, Mauritius
[2]Department of Computer Science and Engineering, Institute of Technical Education and Research, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha, India

Abstract

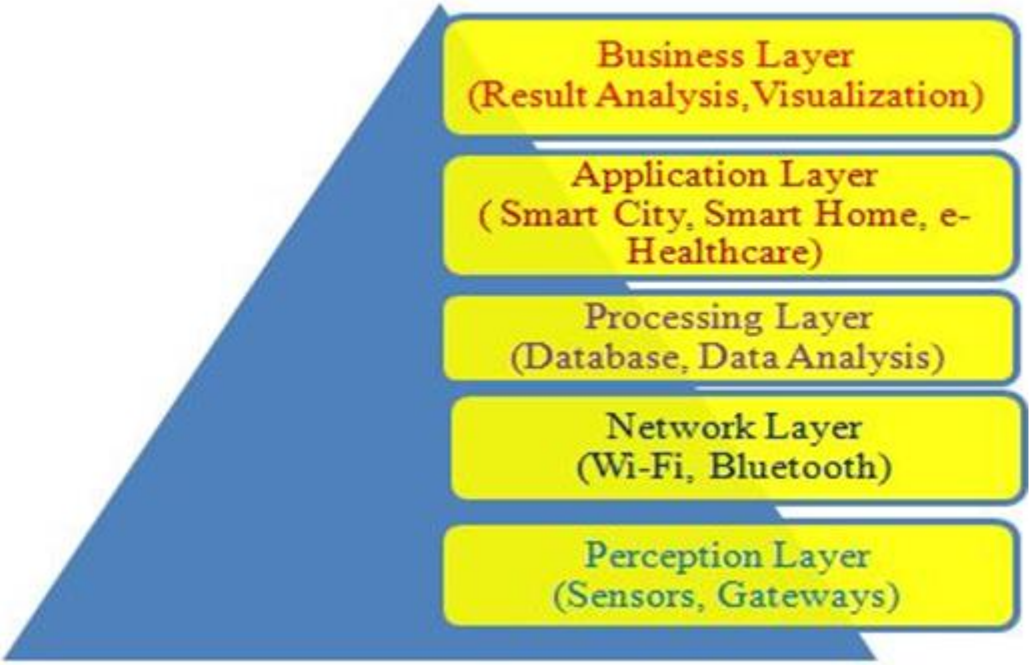
Global Internet has been a revolutionary innovation in the field of global communication across the world that has been usefully serving to the human society for last few decades. Applications of Internet include every field relating to human society. Researchers as well as scientists are immensely involved in bringing in innovations into this communication methodology everyday. However, the traditional Internet is limited in the fact that it is capable of facilitating human-to-human communication only and devices can communicate on the Internet with human intervention only. Further innovation in traditional Internet has led to emergence of Internet of Things (IoT) that could overcome this limitation thereby facilitating device-to-device (D2D) or also referred to as machine-to-machine (M2M) communication wherein smart devices can communicate autonomously via Internet without any human intervention. However, most of the smart devices can be connected to the IoT environment via wireless channels which makes it vulnerable to various security threats to the communication. IoT security has been a major point of focus these days for researchers and scientists across the world. In this paper, we propose as end-to-end AES based cryptographic authentication mechanism for secure communication between the IoT devices using Message Queue Telemetry Transport (MQTT) protocol. Experimental results justify the improved performance of communication protocol MQTT.

Keywords: IoT, MQTT, AES, Security, Cryptography

1. Introduction

In recent years, a significant improvement has been observed in global communication. Emergence of global Internet has facilitated worldwide communication and it is applied in almost all fields of human society. But, this traditional Internet is limited with the fact that it supports human-to-human communications only. Further enhancement of it that is regarded as Internet of Things (IoT), which is capable of facilitating device-to-device (D2D) or machine-to-machine (M2M) communication to overcome the limitation of traditional Internet [Safeipour S. et al., 2018]. Devices can communicate on IoT among themselves autonomously without any human intervention. Smart devices connect to IoT via wireless channels through gateways. Every device on IoT is assigned with a unique identifier, referred to as Radio frequency Identifier (RFID) [Al-Sarawi S. et al., 2017]. As of today, as many as 30 billion of wireless devices are connected to the IoT. As experts reveal, this number may grow up to 75 billion by the year 2025. Since most of the wireless devices that are connected to the IoT are resource constrained devices, security concerns present a major challenge to their operation. A 5-layer IoT protocol stack is presented in Figure 1. As shown in Figure 1, the perception layer comprises of various sensors for capturing information from the environment and gateways for the wireless devices to connect to the network. The network layer here holds responsibility of communicating the information captured from the environment to the network. The devices can connect to the network via a wireless channel such as Wi-Fi, Bluetooth etc. At the processing layer, the received data thus are analyzed and further communicated to the application layer. Specific user applications make use of the received thereby data for necessary computation and then sent to the business layer [Hosenkhan R. et al., 2019]. The business layer manages and provides a wide spectrum of services to the lower layers in the protocol stack. It also employs various technologies such as cloud computing big data analytics. As a whole, this layer manages the IoT system in its entirety thereby ensuring the user's privacy too. It also deals with the analysis of data having been processed as well as the visualization of such results thereby.

Figure 1. IoT Architecture



Billions of wireless devices connect to the IoT environment via wireless channels and such devices are limited with resources which leads to various concerns relating to their successful operation on the iot environment. IoT is capable of supporting a wide range of real life applications. IoT technology is being successfully implemented in the fields of healthcare, education, environmental monitoring and industrial applications [Rath M. et al., 2019; Ramlowat D. D. et al., 2019; Biswal A. K. et al., 2021; Pattanayak B. K. et al., 2021]. In this paper, we have made an attempt to address the issue of authentication for connected devices and propose an end-to-end AES based cryptographic mechanism for the same.

The rest of the paper has been organized as follows. Security issues along with various challenges pertaining to the devices on the IoT environment are covered in Section 2. In section 3, we elaborate the MQTT protocol along with its architecture. Section 4 includes the related work pertaining to secured IoT communication protocols. The proposed model is described in Section 5. Section 6 includes the conclusion along with possible extensions to the current research work in future.

2. IoT Security Issues and Challenges

As elaborated above, the majority of wireless devices that are connected to the IoT are small and resource constrained. Each device connected to the IoT environment is allocated with a unique identifier called radio frequency identifier (RFID) tag that is necessary for the unique identification of the device within the network. Furthermore, as such devices usually operate on wireless media, they are frequently vulnerable to various threats leading to security issues. Various security issues and challenges related to operations on IoT are elaborated as follows.

2.1. Perception Layer Attacks

Several security issues related to the perception layer are elaborated below [8].

i) Unauthorized Access: As explained earlier, every devices on IoT is assigned with a unique RFID tag by virtue of which the device is uniquely identified in the network. The attackers may try to delete/modify the respective RFID tag of a device and as a result, it becomes practically impossible to authenticate the device. Resolution to this can be achieved using HASH Algorithm for authentication of an IoT device in the network.

ii) Tag Cloning: In this case, the attacker duplicates the RFID tag of a device which makes the authentication unachievable. Again, HASH Algorithm can be useful to overcome this issue.

iii) Eaves Dropping: Here, an attacker may tend to access the confidential information that is meant for a specific device which results in breach of privacy and it can be overcome making use of cryptosystems such as Data Encryption Standard (DES) or Blowfish.

iv) Spoofing: A malicious device that is identified with a valid RFID tag may tend to generate false information that creates an illusion for the receiver which assumes the information to have been generated by an authentic device and it can be prevented using the above mentioned cryptosystems.

v) RF Jamming: In case the wireless channel through which a device connects to the IoT environment is overloaded, dynamic risk assessment methods can be used to alleviate this problem.

vi) Physical Damage: An attacker can damage the IoT device physically that are deployed in remote locations and in order for overcoming this problem, the device must be damage-proof packed.

2.2. Network Layer Attacks

Major security issues at the level of IoT network layer are described as follows.

i) Sybil Attack: A malicious node can reveal its fake identity to all other nodes in the network as a result of which nodes tend to communicate with an invalid node which consequently leads to loss of relevant data. End-to-end encryption must be implemented in order for authentication that can resolve this issue.

ii) Sinkhole Attack: In case of occurrence of such an attack, confidentiality as well as privacy can be severely affected and in order to get away with it, hop-by-hop or source initiated routing need to be conducted.

iii) Malicious Attack: Malicious codes may be generated to the network by the attacker which results in paralyzation of the entire network which needs strong authentication mechanism in order to overcome this problem.

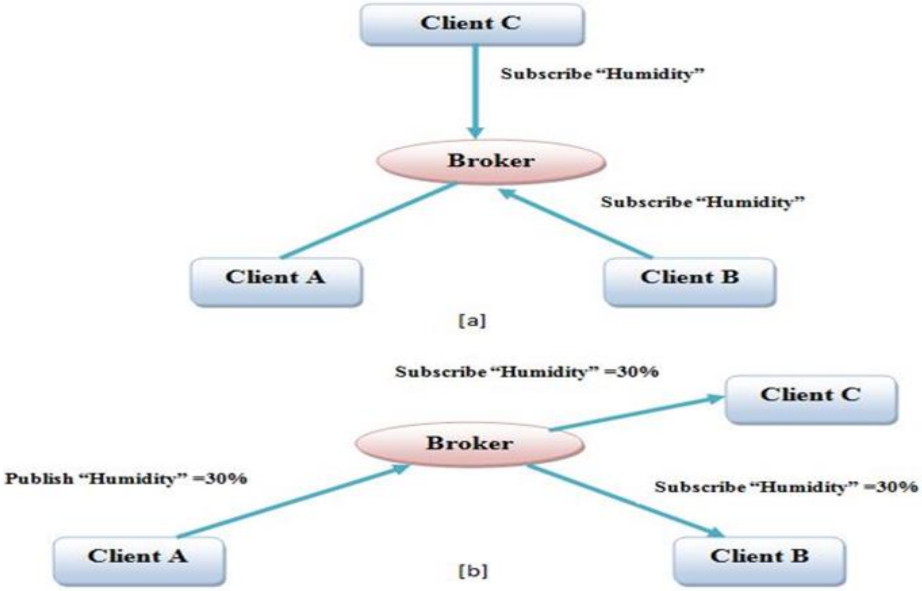
2.3. Application Layer Attacks

Mostly occurred application layer attacks fall into the categories such as malicious code injection and Denial of Service (DoS) attacks.

3. Message Queue Telemetry Transport (MQTT) Protocol

Message Queue Telemetry Transport (MQTT) protocol represents an open standard for communication of lightweight machine-to-machine (M2M) massages on an IoT environment that operates in publish/subscribe strategy. It supports a client/server network model wherein clients refer to various sensors deployed in the environment and the server, also called as broker that is responsible of communication of messages among various clients. The underlying architecture of MQTT is depicted in Figure 2. Some of the clients can be publishers of various topics and some other may be the consumers/subscribers of those topics. As shown in Figure 2 (a), clients B and C subscribe to the topic “Humidity”. After sometime, client A publishes this topic to the broker (Figure 2 (b)). The broker then communicates the topic to the subscribers and most importantly, the contents of the topic appear to be opaque to the broker. The publish/subscribe model here allows the MQTT clients to communicate in one-to-one, one-to-many and many-to-many patterns . The topics in MQTT are entirely hierarchical similar to a file system on a computer. In order for registration of a subscription, clients are provided with wildcards that allow the clients to observe the hierarchies. The wildcard “+” refers to a single directory name whereas wildcard “#” refers to multiple directories of any name. Three Quality of Service (QoS) levels are supported by MQTT: Fire and forget, delivered at least once and delivered exactly once. As a matter of security, brokers need username and password authentication for clients to connect to it. In order for ensuring the privacy, the TCP connection need to be encrypted using Source Sockets Layers (SSL)/Transport Layer Security (TLS).

Figure 2. MQT Protocol Architecture



4. Related Work

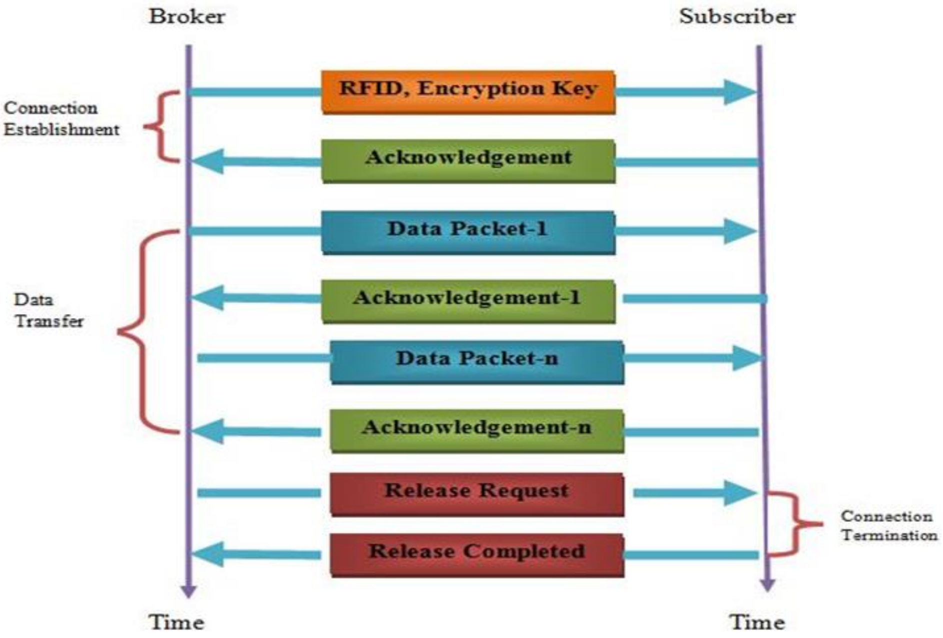
Security provisioning in IoT devices represents an important aspect in communication for the reason that most of the devices on IoT are resource constrained, small and handheld devices. A fair amount of research work has been conducted by several authors worldwide pertaining to secured IoT communication protocols.

Authors in [Su W. et al., 2019] have proposed an extensible as well as transparent MQTT protocol with thing-to-thing security enhancement which as claimed by the authors, prevents from data leakage on IoT thereby providing the extendibility for inclusion of necessary security mechanisms in order to satisfy various security requirements as desired. A symmetric encryption mechanism for assessment of MQTT protocol has been proposed by the authors in [Oak A. et al., 2018]. In this work, the authors have conducted the performance evaluation of MQTT protocol having implemented three separate block encryption mechanisms such as DES, AES and Blowfish that are used for communication of the desired information between the publisher and subscriber through the broker. By virtue of the experimental results, the authors have claimed the suitability of lightweight ciphers in order for provisioning the security features in MQTT protocol. A novel multi-key/multi-password based mutual authentication technique for the devices on IoT has been addressed wherein the secret key between the IoT server and the IoT device is termed as secure vault that encompasses a number of keys of the same size [Shah T. et al., 2018]. Here, the initial contents of the secure vault are shared between the IoT sever and the IoT device that keep on changing with every successful session of communication. The authors claim this technique to be feasible especially for resource constrained IoT devices. In order to achieve secure communication using unreliable Constrained Application Protocol (CoAP), compressed Datagram Transport Layer Security (DTLS) can be added to it as claimed by the authors in [Premalatha T. et al., 2017]. In addition to this, the authors here employ a certification based authentication mechanism in order to prevent from Denial of Service (DoS) attacks. The authors in [Miyazaki Y. et al., 2018] have developed a Network Traversal with Mobility (NTMobile) protocol for direct communication between IoT devices that employs a direct encryption key exchange technique between communicating devices making use of the technology of Public Key Infrastructure (PKI) and as claimed by the authors, it necessarily supports secure communication. An encrypted communication technique for communication between IoT cloud and embedded systems is proposed by the authors in [Nikolov N. et al., 2019] that uses MQTTS with SSL/TLS certificate. Here, the authors have relied on JavaScript Object Notation (JSON) data type that is used between cloud structure and the IoT device. The IoT embedded system here has been used for measuring the temperature with the help of the sensor DTH22. As claimed by the authors, the encrypted thus messages cannot be listened in by an unauthorized user. A model for secure communication between embedded systems via IoT has been proposed by the authors in [Peniak P. et al., 2018] by virtue of using MQTT application protocol and new cryptographic techniques have been employed by the authors in this work along with some additional measures brought in at the level of the application layer. With experimental observations, the authors have claimed to have achieved the required level of secure communication thereby. An information-theoretically secure key management protocol has been devised by the authors in [Mustafa U. et al., 2019] that is suitable for resource constrained IoT devices. The proposed here protocol reduces computational complexity as revealed by the authors. A self-healing group key distribution protocol has been proposed in order for provisioning the security aspects of the vulnerable wireless channel connecting IoT devices by the authors in [Dhanujalakshmi R. et al., 2019] that according to the authors enhances communication efficiency. In addition, lost sessions keys can be recovered as well using this approach. A Heterogeneous Communication (HeComm) architecture for communication between IoT devices has been proposed that relies upon Fog computing [Winderickx J. et al., 2018]. The proposed architecture comprises of two parts: HeComm protocol and HeComm communication. The HeComm protocol here permits the network manager to create a secret key that is utilized for HeComm communication. By virtue of using object security, the HeComm communication is capable of securing the comunication among various IoT devices that ensures end-to-end protection of data communicated rather than totally relying on the Fog computing environment. The authors have evaluated this architecture with the implementation of proof-of-concept that connects two nodes namely, one node from the 6 LoWPAN network and the second one is from LoRaWAN network. Experimental results reveal that the nodes in the HeComm architecture meet the Class 1 constrained nodes. A secure routing protocol has been proposed for heterogeneous networks on IoT that empowers authentication of devices thereby ensuring the integrity of the data communicated between devices [Jerbi W. et al., 2020]. This secure multicast routing protocol, named as Crypto-IoT that has been designed taking into consideration the constraints of wireless sensor networks (WSN) and IoT. With comparative experimental results, the authors claim to have achieved the desired level of efficiency of this protocol that is robust as well. A hybrid approach using authentication along with data confidentiality for securing the communications between IoT devices has been proposed by the authors in [Bhatt J. et al., 2017]. A lightweight secure transport-layer protocol named iTLS has been proposed by the authors in [Li P. et al., 2020] that is capable of delivering protected data with perfect forward secrecy thereby ensuring implicit mutual authentication of devices on IoT without the need of any certificates. It generates dynamically the early keys based on the identity of the IoT device prior to receiving any response from the server thereby allowing the client systems to send encrypted data without additional round trips. As claimed by the authors, the proposed here protocol, iTLS, is capable of reducing the traffic overhead by at least 61.2% and handshake latency by at least 60%. In order to withstand a large spectrum of common Denial-of-Service (DoS) attacks for ensuring reliable operation thereby achieving low latency for dissemination of desired information, a secure as well as lightweight multi-hop communication protocol called LIDOR has been proposed by the authors in [Stute M. et al., 2020] that ensures as per the authors, the reliability of operation under DoS attacks, by 91%.

5. Proposed Model

In our proposed model, we address the issue of secure authentication of IoT devices during communication using MQTT protocol. As depicted in Figure 2, the broker needs to deliver the information to the authentic subscribers. Here, we propose a lightweight AES based cryptographic approach for authentication of devices on the IoT. The authors in [Pattanayak B. K. et al., 2020] have proposed an AES based cryptographic approach for key generation. AES 128 encrypts and decrypts the communicated data blocks in 10 rounds by virtue of using a128-bit cryptographic key. We implement this approach for communication between the broker and the subscriber. The communication procedure between the broker and the subscriber is carried out in the phases: key generation, connection establishment, data transfer and connection termination (Figure 3). In the beginning, the broker sends a control packet to the subscriber incorporating its RFID and the encryption key. The subscriber on receiving this control packet, caches the encryption key and acknowledges back to the broker. Thus, a secure connection between the broker and the subscriber has been established. Then, the broker starts sending the data packets and on receiving each data packet, the subscriber sends an acknowledgement back to the broker. This handshaking procedure continues until entire data are exchanged between the broker and the subscriber. After sending all the data packets that are acknowledged, the broker sends a control packet RELEASE REQUEST to the subscriber. On receiving this control packet, the subscriber acknowledges back to the broker with a control packet RELEASE COMPLETE. When this control packet is received by the broker, the connection is terminated.

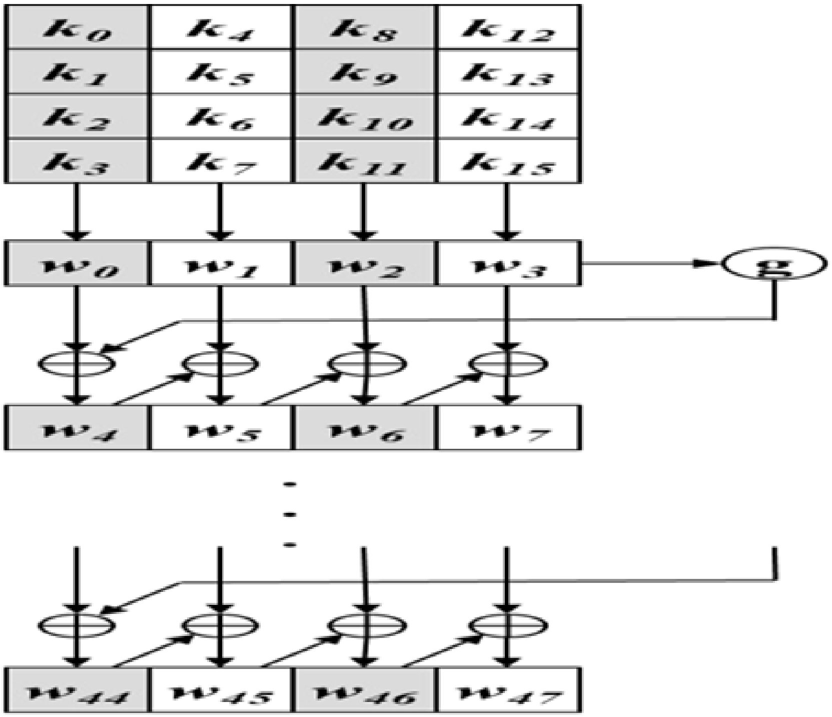
Figure 3. Secure Communication between Broker and Subscriber



5.1. Key Generation

We have implemented a symmetric key encryption mechanism that facilitates faster communication as the same key is used for both encryption as well as decryption. We have used here AES 128 block cipher for key generation. Encryption and decryption of data using AES 128 is carried out in 10 rounds making use of a 128-bit encryption key. Here in each of the rounds, newly generated round key is XOR-ed with the state that is the data block. The round key here is generated from the original key using key expansion (Figure 4).

Figure 4. Key Expansion



The key (K_0, K_1,........., K_{15}) is transformed to 44 separate words where each word comprises of 4 bytes. The procedure of key expansion is depicted in the following pseudo-code.

```
{
    word temp
    FOR i ← 0 TO 3
        w[i] ← (key[4*i], key[4*i+1],
                key[4*i+2],
                key[4*i+3])
    ENDFOR
    FOR i ← 4 TO 43
        temp ← w[i-1]
        IF i mod 4 = 0
            temp ← g(temp)
        ENDIF
        w[i] ← w[i-4] ⊕ temp
ENDFOR
}
```

The AES key expansion algorithm is developed in such a way that it should be resistant to known cryptographic attacks always. The g function used in this algorithm is depicted in Figure 5. As suggested by the authors Daemen J. Et al., 2002. The design criteria taken into consideration while developing this procedure are

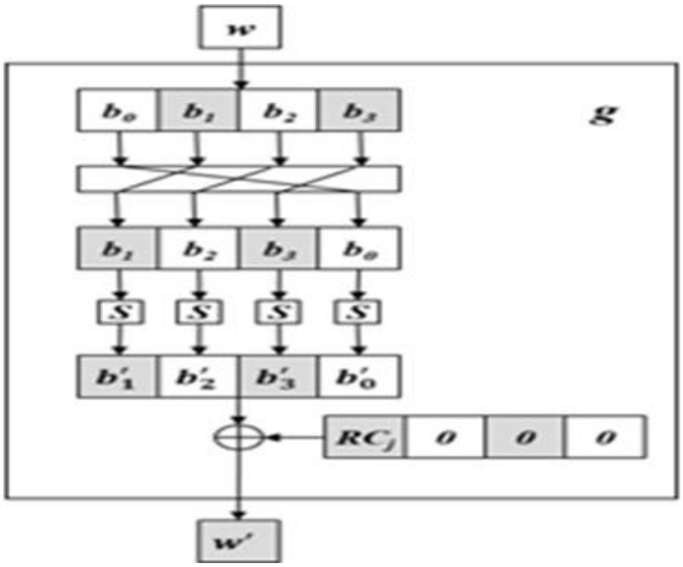
a) Memory Efficiency;

b) Fast on a wide range of processors;

c) Non symmetric and non linear;

d) High diffusion;

Figure 5. The g Function



5.2. Experimental Result Analysis

The experiment is carried out on SimpleIoTSimulator using MQTT communication protocol. AES 128 has been used for encryption/decryption as we use here symmetric encryption/decryption mechanism. A mobile device was connected to the IoT broker via bluetooth. The observations show that 98% of data packets exchanged between the broker and the mobile device are securely communicated between the two ends with the data integrity maintained. The proposed encryption/decryption mechanism appears to be robust in all circumstances.

6. Conclusion and Future Work

Security issues in IoT communication imposes major challenges to efficient implementation of

IoT applications considering that most of the IoT devices are wirelessly connected to the IoT environment and are resource constrained. In this paper, we propose an AES based encryption/decryption mechanism for secure communication between the broker and the subscriber using MQTT IoT communication protocol. We have focused on authentication of devices as the major security issue. Experimental observations show that this authentication mechanism ensures optimal secure communication with data integrity being preserved. However, AES 128 is a heavyweight block cipher that may not be often suitable for small resource constrained IoT devices. Hence, in future, lightweight block ciphers can be used for IoT encryption/decryption that can significantly improve the efficiency of communication.

References

Safeipour S. and Golpira H., The Internet of Things: A State of the Art of Applications, Proceedings of the First International Conference on Modern Approaches in Engineering Sciences, pp.1-9, 2018.

Al-Sarawi S., Anbar M., Alieyan K. and Alzubaidi M., Internet of Things (IoT) Communication Protocols: Review, Proceedings of the 2017 8th International Conference on Information Technology (ICIT), pp.685-690.

Hosenkhan R. and Pattanayak B. K., A Secure Communication Model for IoT, Information Systems Design and Intelligent Applications, pp.187-193. 2019.

Rath M. and Pattanayak B. K., Technological Improvement of Modern Health Care Applications Using Internet of Things (IoT) and Proposal of Novel Health Care Approach, International Journal of Human Rights in Healthcare, Vol.12, No.2, pp.148-162, 2019.

Ramlowat D. D. and Pattanayak B. K., Exploring the Internet of Things (IoT) in Education: A Review, Information Systems Design and Intelligent Applications, pp.245-255, 2019.

Biswal A. K., Singh D., Pattanayak B. K., Samanta D. and Yang M-H, IoT Based Smart Alert System for Drowsy Driver Detection, Wireless Communications and Mobile Computing, Vol.2021, pp.1-13, 2021.

Pattanayak B. K., Nohur D. Cowlessur S. K. and Mohanty R. K., An IoT Based System Architecture for Environmental Monitoring, Progress in Advanced Computing and Intelligent Engineering, pp.507-514, 2021.

Pattanayak B. K. and Amic S., Modified Lightweight AES Based Two Level Security Model for Communication on IoT, TEST Engineering and Management, Vol82, No.1, pp.2323-2330, 2020.

https://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php

Su W., Chen W. and Chen C., An Extensible and Transparent Thing-to-Thing Security Enhancement for MQTT Protocol in IoT Environment, 2019 Global IoT Summit (GioTS), pp.1-4, 2019.

Oak A. and Daruwala R. D., Assessment of Message Queue Telemetry and Transport (MQTT) Protocol with Symmetric Encryption, Proceedings of the 2018 First International Conference on Secure Cyber Computing and Communication (ICSCC), pp.5-8, 2018.

Shah T. and Venkatesan S., Authentication of IoT Device and IoT Server Using Secure Vaults, Proceedings of the 2018 17th International Conference on Trust, Security and Privacy in Computing and Communications, pp.819-824, 2018.

Premalatha T. and Duraisami S., A Certificate Based Authorization and Protected Application Layer Protocol for IoT, Proceedings of the 2017 International Conference on Computer Communication and Informatics (ICCCI-2017), pp.1-5, 2017.

[14] Miyazaki Y., Naito K., Suzuki H, and Watanabe A., Development of Certificate Based Secure Communication for Mobility and Connectivity Protocol, Proceedings of the 2018 15th IEEE Annual Consumer Communications and Networking Conference (CCNC), pp.1-4, 2018.

Nikolov N. and Nakov O., Research of Secure Communication of Esp32 IoT Embedded System to .NET Core Cloud Structure Using MQTTS SSL/TLS, Proceedings of the XXVIII International Scientific Conference Electronics (ET-2019), pp.1-4, 2019.

Peniak P. and Franekova M., Extended Model of Secure Communication for Embedded Systems with IoT and MQTT, Proceedings of the 2018 International Conference on Applied Electronics, pp.1-4, 2018.

Mustafa U. And Philip N., Group-Based Key Exchange for Medical IoT device-to-Device Communication (D2D) Combining Secret Sharing and Physical Layer Key Exchange, Proceedings of the 2019 IEEE International Conference on Global Security, Safety and Sustainability (IGS3), pp.1-7, 2019.

Dhanujalakshmi R. And Kartheeban K., Smart and Secure Group Communication in IoT Using Exponential based Self Healing Group Key Distribution Protocol, Proceedings of the 2019 IEEE International CONference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), pp.1-4, 2019.

Winderickx J., Singelee D. and Mentens N., HeComm: End-to-End Secured Communication in a Heterogeneous IoT Environment via Fog Computing, Proceedings of the 2018 15th IEEE Annual Consumer Communications and Networking Conference (CCNC), pp.1-6, 2018.

Jerbi W., Guermazi A. and Trabelsi H., A Secure Routing Protocol for Heterogeneous Networks for Internet of Things, Proceedings of the 2020 International Conference on Wireless Communications and Mobile Computing (WCMC), pp.571-576, 2020.

Bhatt J., Joshi A., Bisht S. and Purohit K. C., Hybrid Approach for Securing IoT Communication Using Authentication and Confidentiality, Proceedings of the 2017 3rd International Conference on Advances in Computing, Communication and Automation (ICACCA), pp.1-6, 2017.

Li P., Su J. and Wang X., iTLS: Lightweight Transport-Layer Security Protocol for IoT with Minimal Latency and Perfect Forward Secrecy, IEEE Internet of Things Journal, Vol.7, No.8, pp.6828-6841, 2020.

Stute M., Agarwal P., Kumar A., Asadi A. and Hollick M., LIDOR: A Lightweight DOS-Resilient Communication Protocol for Sefety-Critical IoT Systems, IEEE Internet of Things Journal, Vol.7, No.8, pp.6802-6816, 2020.

Daemen J. and Rijmen V., The Design of Rindael, Newyork, 255, 2002.

Bangar, Ashwini, and Swapnil Shinde. "Study and comparison of cryptographic methods for cloud security." Int J Comput Sci Eng Inf Technol Res 4.2 (2014): 205-213.

Wadhwani, Priyanka, Akanksha Gaur, and Vipin Jain. "Cryptanalytic JH and Blake Hash Function for Authentication and Proposed Work Over Blake-512 on C Language." International Journal of Computer Science Engineering and Information Technology Research 4.3 (2014): 187-198.

Dureja, Ajay, and Vandna Dahiya. "Comparative Study Of Collaborative Attacks & Security Mechanisms

In Manet." International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) 4.3, Jun 2014, 139-148

Swamy, Srinadh, Pavan Kumar, and Vasu Dev. "Impr Oved Authentication Technique To Protec T Web Applications." International Journal of Computer Science and Engineering (IJCSE) ISSN (P): 2278-9960.

Gedam, Mrunali T., and Vinay S. Kapse. "Authentication By Color Visual Cryptography Using Visual Information Pixel Synchronization And Error Diffusion." International Journal of Electronics and Communication Engineering (IJECE) 2.4, Sep 2013, 59-66

Sherasiya, Tariqahmad, Hardik Upadhyay, and Hiren B. Patel. "A survey: Intrusion detection system for internet of things." International Journal of Computer Science and Engineering (IJCSE) 5.2 (2016): 91-98.