International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1798-1801 www.ijaem.net ISSN: 2395-5252

Security Implemented For IoT with MQTT

Mrs Punam Lokhande
Alamuri Ratnmala Institute of Engineering And Technology,Shahapur,Thane (West)

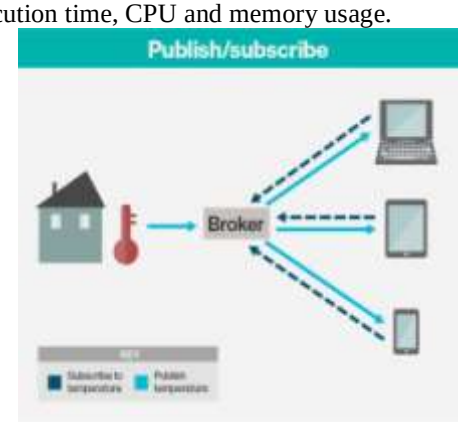
Submitted: 01-07-2021 Revised: 10-07-2021 Accepted: 13-07-2021

ABSTRACT:This research paper is about to implement security protocols in IoT.As IoT devices are tremendously getting popularity and are in used frequently by user.Security is more critical in IoT.Here we are using privacy mechanism approach is Attribute-Based Encryption (ABE). A public key encryption approach that enables smooth access control, scalable key management and flexible data distribution. We concern with two types of ABE,B Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE)is the best for secured use of IoT.
The main focus of this implementation is to applying security to the pub-sub architecture using KP-ABE. KP-ABE mechanism. We are implementing AES cryptography on the payload. By use of cipher key to generate dynamic S-Box which is changing with every changing of cipher key. That results into cryptographic strength.
KEYWORDS: IoT, Attribute-Based Encryption (ABE)., cryptography, pub-sub architecture dynamic S-Box.

I. INTRODUCTION

Traditional Client/Server communication model employs RPC, message queue, shared memory etc. Synchronous, tightly-coupled request invocations. Very restrictive for distributed applications, especially for WAN and mobile environments. When nodes/links fail, system is affected. Fault Tolerance must be built in to support this. Require a more flexible and decoupled communication style that offers anonymous and asynchronous mechanisms.

The publish/subscribe pattern (pub/sub) is an alternative to the traditional client-server model, where a client communicates directly with an endpoint. However, Pub/Sub decouples a client, who is sending a particular message (called publisher) from another client (or more clients), who is receiving the message (called subscriber). This means that the publisher and subscriber don't know about the existence of one another. There is a third component, called broker, which is known by both the publisher and subscriber, which filters all incoming messages and distributes them accordingly. In this existing system, They presented a new security solution to MQTT by using ABE in combination with Dynamic S-Box AES.
The contribution of this system was
(i) to enable security feature for MQTT,
(ii) to use hybrid or composite security for MQTT payload encryption and
(iii) to study the feasibility of our proposed methodology through simulation. We implemented and evaluated our proposed solution in Java and performance evaluation parameter includes execution time, CPU and memory usage.



Proposed System Archetecture

II. AES ENCRYPTION ALGORITHM

The Cipher is described in the algorithm.
STEP 1 : START
STEP 2: Input a new word.
STEP 3: Input is copied to State aray.
STEP 4: Perform initial Round Key addition.
STEP 5: Repeat Round function N times (depending of key length).
STEP 6: End Of Loop with the final round differing slightly from the first Nr-1 rounds.
STEP 7: The final State array is copied to the Output.
STEP 8 : END

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1798-1801 www.ijaem.net ISSN: 2395-5252

III. DYNAMIC S-BOX GENERATION FROM CIPHER KEY ALGORITHM

STEP 1: We need primary S-Box to generate dynamic S-Box, We use S-Box generation algorithm that introduced in AES, to create primary S-Box as follows. Take the multiplicative inverse in the finite field GF(28); the element {00} is mapped itself.

STEP 2: In this step, rows swapped with columns of primary S-Box in GenerateDynamicSbox(cipherKey) function. This function guarantees new S-Box remain one-for-one.

This routine get cipher key as input and generate dynamic S-Box from cipher key. Note that in this paper if cipher key has 192 or 256 bits size, we use only first 128 bits of cipher key.

We used an algorithm to generate dynamic S-Box from cipher key. The quality of this algorithm tested by changing only two bits of cipher key to generate new S-Boxes.

For that purpose we are testing difference of S-Box element by many intervals. This algorithm will lead to generate more secure block ciphers, solve the problem of the fixed structure S-Boxes and will increase the security level of the AES block cipher system. The main advantage of this algorithm is that many S-Boxes can be generated by changing Cipher key.

IV. KP-ABE algorithm:

KP-ABE Access Control:

KP-ABE scheme consists of the following four algorithms:

1. Setup: This algorithm takes as input a security parameter κ and returns the public key PK and a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the Authority.

2. Encryption: This algorithm takes a message M, the Public key PK, and a set of attributes as input. It outputs the ciphertext E.

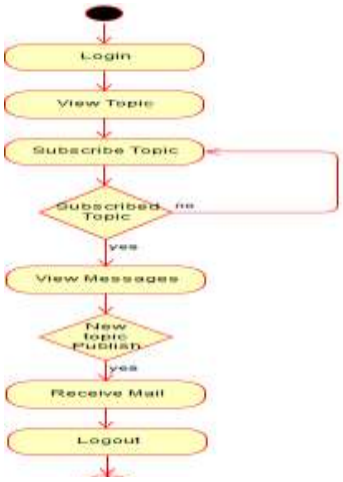
3. Key Generation: This algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key SK that permits the user to decrypt a message encrypted under a set of attributes if and only if equals T.

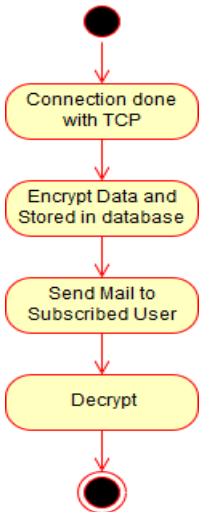
4. Decryption: It takes as input the user's secret key SK for Access structure T and the ciphertext E, which was encrypted under the attribute set. This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure T.

V. ACTIVITY DIAGRAM

Publisher:

Subscriber:





International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1798-1801 www.ijaem.net ISSN: 2395-5252

VI. IMPLEMENTATION DETAILS

Fig. Home page

Fig. Selection of Topics And Publish Page(2)

Fig. Log In page

Fig.Insertion of Topics And Publish Page

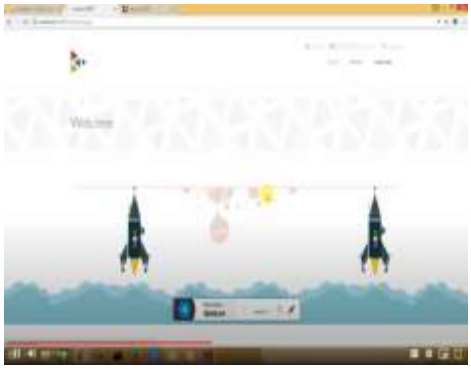


Fig. Selection of Topics And Publish

Fig.Subscribe Page

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1798-1801 www.ijaem.net ISSN: 2395-5252

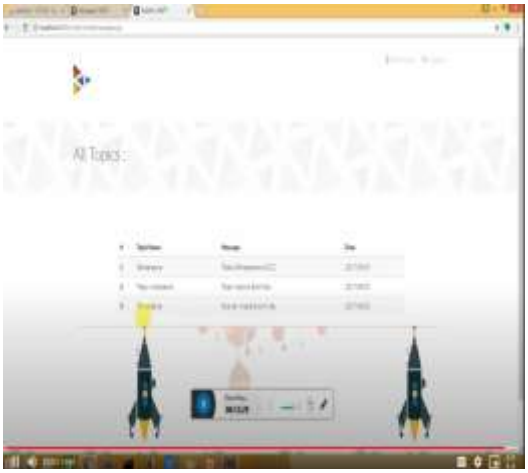


Fig. All Topics With Messages Page

VII. CONCLUSION

By implementing KP-ABE using dynamic s box AES encryption standards the project is helping making a security structure on the public-subscribe architecture used in the MQTT.

Future Scope: Implementing strong guarantee on broker to deliver content to subscriber. After a publisher publishes the event, it assumes that all corresponding subscribers would receive it. Solving Potential bottleneck in brokers when subscribers and publishers overload them by load balancing techniques Encryption hard to implement when the brokers has to filter out th events according to context.

REFERENCES

[1]. A. Carzaniga, D.S. Rosenblum and A.L.Wolf, "Design and evaluation of a wide-area event notication service," ACM Transactions on Computer Systems (TOCS), vol. 19, no. 3, pages 332-383, 2001.

[2]. P.T. Eugster, P.A. Felber, R. Guerraoui and A.M. Kermarrec, "The many faces of publish/subscribe," ACM Computing Surveys (CSUR), vol. 35, no. 2, page 131, 2003.

[3]. M.Ion, "Security of Publish/Subscribe Systems," Ph.D. Thesis, University of Trento, 2013. http://eprints-phd.biblio.unitn.it/993/.

[4]. M. A. Tariq, "Non-functional Requirements in Publish/Subscribe Systems," Ph.D. dissertation, University of Stuttgart, Germany, August 2013.

[5]. M. Ambrosin, M. Conti, T. Dargahi, "On the feasibility of attributebased encryption on smartphone devices", IoT-Sys 2015, 2015.

[6]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. of ACM CCS, pp. 89–98, 2006. [7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. of IEEE SP, pp. 321–334, 2007.