2015 Fifth International Conference on Communication Systems and Network Technologies

Secure MQTT for Internet of Things (IoT)

Meena Singh, Rajan MA, Shivraj VL, and Balamuralidhar P

TCS Innovation Labs, Bangalore, 560066, India, Email:{meena.s1, rajan.ma, shivraj.vl, balamurali.p}@tcs.com

***Abstract*—Rapid innovations in the area of digital things and Information Communication Technology are driving rapid deployment of Internet of Things (IoT) around the globe. Device to Device communications (D2D) in IoT are envisaged through various protocols such as Constrained Access Protocol (CoAP), Message Queue Telemetry Transport (MQTT) and MQTT-SN (for sensor networks). One of the major concerns in the deployment of IoT is to ensure the security of devices and D2D communications. Besides, existing communication protocols for IoT are devoid of security features. To address this, we propose a secure version of MQTT and MQTT-SN protocols (SMQTT and SMQTT-SN) in which security feature is augmented to the existing MQTT protocol based on Key/Ciphertext Policy-Attribute Based Encryption (KP/CP-ABE) using lightweight Elliptic Curve Cryptography. Further we demonstrate feasibility of SMQTT and SMQTT-SN protocols for various IoT requirements through simulations and evaluate their performance.**

I. Introduction

Innovations in the area of 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 [1]. 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 [2]. To enable the integration and management of heterogeneous IoT devices, architectures such as Ubiquitous Sensor Network (USN), Sensor Web Enablement (SWE), etc., are proposed [2]. 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 [3]. To address this cryptography techniques based on Public Key Infrastructure (PKI), Identity based encryption (IBE), etc., are proposed for secure IoT communication [1], [3], [4]. 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., [4], [5], 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 [6]. Hence in this paper we study 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 for MQTT 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) [7], [8] over elliptic curves [1]. 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 (KP-ABE). 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.

The main contribution of this paper is to: (i). Study the feasibility of enabling security using CP/KP-ABE for MQTT and MQTT-SN. (ii). Design, implement and evaluate performance analysis of SMQTT and SMQTT-SN protocols for IoT. This paper is organized as follows. Section II describes a brief survey on the existing IoT protocols and security schemes. An overview of MQTT protocol is described in Section III. Proposed Secure MQTT protocol is described in Section IV. In Section V, we describe MQTT-SN protocol. Robustness of proposed SMQTT against various attacks are analysed in Section VI. Implementation methodology and performance analysis of proposed SMQTT are discussed in Section VII. We conclude the paper in Section VIII.

II. Related Work

In [3], ABE is applied to ensure privacy for IoT based on generic Publish-Subscribe (Pub-Sub) architecture. Here payload is encrypted using symmetric Advance Encryption System (AES) cryptography and AES key is encrypted using ABE scheme which ensures that ciphertext size and payload size is same. Here we argue that, IoT devices generate only few bits of data and to perform encryption on few bits of data both AES and ABE encryption techniques prove to be computational overhead for IoT devices. Thus we aim at optimizing complex arithmetic operations of ABE by using suitable cryptography parameters rather than performing double encryptions. Authors

978-1-4799-1797-6/15 $31.00 © 2015 IEEE
DOI 10.1109/CSNT.2015.16

designed a middleware based on Pub-Sub architecture in [9]. Here privacy of subscriber's interest and confidentiality of published content is protected by enabling CP-ABE and Predicate Based Encryption (PBE). Similarly in [4], [10], authors designed a scheme for Pub-Sub architecture using KP/CP-ABE schemes. Here every subscriber defines a filtering condition as an access policy in KP-ABE and based on this, Broker performs filtering of messages by performing encrypted search on encrypted attributes. Subsequently it forwards message to intended subscribers. To ensure message confidentiality Publisher encrypts message using CP-ABE and publishes it. In [11], Tariq designed security schemes using IBE and ABE to enable confidentiality and authentication. Here it allows publishers to sign and encrypt events simultaneously by using IBE and thus enable efficient routing of encrypted events (from publishers to subscribers) by Searchable Encryption. Further Subscribers verify the signatures associated with all the attributes (of an event) using CP/KP-ABE.
Most of these schemes described are suitable for generic Pub-Sub architectures. Thus a detailed study is required for feasibility of adapting these schemes for IoT. Hence in this direction, we propose and implement optimized ABE schemes for secure MQTT, which enables secure IoT.

III. Proposed Secure MQTT

For the sake of completeness, we describe MQTT protocol which is used for communication between the IoT devices [5]. It is a Pub-Sub protocol for device (publisher: sending device) to device (subscriber: receiving device) communication based on Transmission Control Protocol (TCP) through a broker. In this protocol, a Publisher publishes message under a topic name. Subsequently, all the subscribers under the topic name receives the message through a broker. Various message types are used in this protocol and are distinguished by message type in MQTT message header (cf. Table I). Message type '0000' is reserved for future. Variable Header contains username and password flag (can facilitate user authentication), upon setting them, corresponding values are also included in payload. However, these values are not encrypted in the message and hence not secure. Thus we propose SMQTT protocol which augments security feature to the existing MQTT. To enable this, we propose a new MQTT Publish message *Spublish* with reserved message type '0000'. Detailed implementation of the scheme is described in subsequent sections.

TABLE I: MQTT Header

bit	7	6	5	4	3	2	1	0
byte 1	Message Type				DUP Flag	QoS Level		Ret
byte 2	Remaining Length							
Variable Header								
Payload								

A. Proposed Secure MQTT Protocol Architecture

We propose secure MQTT (SMQTT) based on ABE (cf. Fig.1). In this protocol, a new publish service 'Spublish' is proposed which uses message type '0000', wherein the message is encrypted using ABE [12]. To make it lightweight and suitable for IoT, we adapt ABE scheme based on lightweight Elliptic Curve Cryptography (ECC) [1], [13]. Here Publisher uses Spublish command to publish an encrypted message using ABE. Hence, Subscribers who satisfy the access policy are capable of decrypting the message.

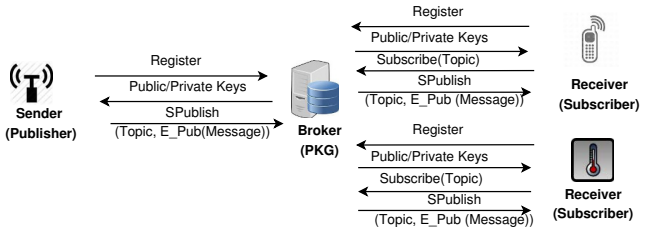

Fig. 1: Architecture of the scheme

B. Proposed Attribute Based Encryption for SMQTT

In ABE technique, sender device encrypts data based on set of conditions in terms of access policy and subsequently receiver device is able to decrypt the ciphertext, if it satisfies access policy. This access policy is expressed in terms of conditions containing the user attributes (can be feature, property, role, etc). Typically, access policy is expressed as a predicate with set of attributes and boolean constructs (OR, AND, NOT). Further in KP-ABE and CP-ABE encryption and decryption depends on key based access policy [7], [14] and ciphertext based access policy [8] respectively. Generally access policy is described as a n-ary access tree. For instance, Fig.2 represents a snapshot of an access tree. According to this access policy, a temperature sensor device publishes temperature data under Smart Home topic through 'Spublish'. A subscriber device who is a controller for Air conditioner or Heater and co-located in the same Location ID of the sensor or a fire alarm device can decrypt the temperature data for the smart home application.

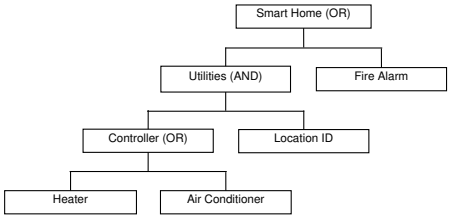

Fig. 2: Access Tree

In this paper, we augment MQTT protocol with KP-ABE and CP-ABE scheme mentioned in [7], [8] based on lightweight ECC [1], [13]. To enable ABE, setup, encryption and decryption operations needs to be performed. During setup phase, Broker (trusted third party) renders the function of a Public Key Generator (PKG) generates the master secret key and access policy (cf. Fig.1 for the scheme). It publishes the public parameters for each attribute of the access policy. Each device must register itself with an Identity and set of attributes with the PKG. PKG verifies attributes and other details given by the device. It sends public parameters to sending device to encrypt the data. Private key for each attribute are sent to receiver by PKG. Further, sending device encrypts the data using the public parameters given by the PKG and access policy. Receiver device decrypts the ciphertext using private key corresponding to the attributes encapsulated in the policy.

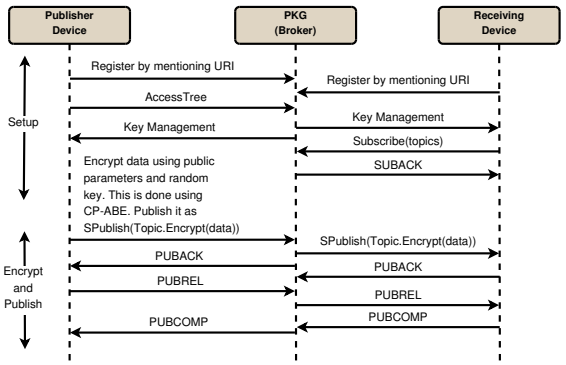

Fig. 3: Proposed SMQTT Protocol

IV. Proposed Secure MQTT Protocol

Proposed secure MQTT protocol is described in Fig.3. In this protocol there are three entities: (i) Publisher device publishes the data under the given topic. (ii) Subscriber device receives the data under the same topic through a Broker. (iii) PKG or broker is the trusted third party. There are four phases in the protocol. In setup phase, registration and key management are done. During encrypt phase, data is encrypted and in publish phase, Publisher publishes encrypted data under the given topic name and sends it to the broker. In decrypt phase, data is decrypted by subscribed devices.

(i). Setup Phase

- Publisher and Subscriber devices register with the PKG by providing unique identity such as Universal Resource Identifier (URI) along with its attributes. Note that all these attributes are subset of universal attribute set $U = \{A_1, A_2, ..., A_n\}$.
- PKG generates Master Secret key set and public parameters according to the CP/KP-ABE scheme and publishes public parameters along with the universal attribute set U [7], [8]. For CP-ABE, all devices, which own the attributes receive the key set from PKG.

(ii). Encrypt Phase

- Publisher device designs an access policy based on the access tree (cf. Fig.2) from the set A and logical connectors. In case of KP-ABE scheme, publisher sends the access tree to PKG and PKG generates key policy and generates the keys accordingly. This scheme is useful, wherein the topics and group of subscribers who access the topics are known a priori and also the standard set of access policies are also determined and all the subscribers get their set of keys for all the required access policies a priori. For CP-ABE scheme, Publisher generates the access tree and access policy.
- In CP-ABE, publisher encrypts the payload and provides the additional information to facilitate decryption along with the policy.
- Publisher device encrypts data using public parameters and generates ciphertext according to KP/CP-ABE.
- Broker sends SUBACK to receiving device.

(iii). Publish Phase

- Publisher embeds encrypted data as payload in SPublish command. It sets topic name accordingly in variable header. Then SPublish packet is sent to Broker.
- Broker responds with PUBACK packet.
- Publisher sends PUBREL packet to Broker.
- Broker forwards message to all Subscribers of topic including receiver.
- Broker deletes data and sends PUBCOMP packet to Sender.

(iv). Decrypt Phase

- Subscriber device decrypts the ciphertext using its private attribute keys, if it satisfies access policy.
- In case of KP-ABE, Subscriber device verifies whether it satisfies the access policy or not. If it satisfies, then it requests PKG to issue corresponding key set and PKG validates the request and sends keys to the subscriber.
- For CP-ABE, subscriber who satisfies access policy decrypts ciphertext using its private key set and information provided in the policy and thus scheme enables non-interactive and offline requirement of PKG. MQTT system works without the intervention of PKG. Once the setup and extraction phase is completed, requirement of PKG no longer exists. Thus this scheme is more generic and suits the requirement of scalability for IoT, but complexity of scheme is high w.r.t storage and computation than that of KP-ABE.

V. MQTT For Sensor Networks (MQTT−SN)

MQTT−SN [15] protocol is designed for Sensor Networks based on UDP to envisage communication for power constraint devices. It consists of MQTT-SN client which is a Publisher device which sends the messages to a Gateway which inturn converts the MQTT-SN message to a MQTT message and forwards it to Broker. Subsequently, Broker delivers message to the MQTT-SN clients (which are Subscribers from another Gateway). Here Gateway acts as a protocol converter from MQTT to MQTT-SN and vice versa (cf. Fig.4) [15].

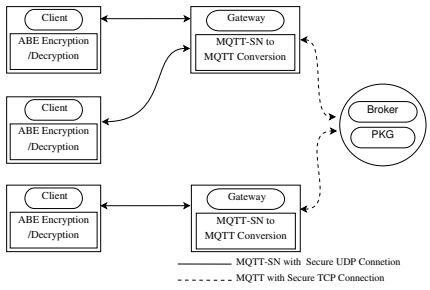

Fig. 4: MQTT−SN Architecture

MQTT-SN protocol message consists of two or four octets of Message Header and n octets of Variable Header (cf. Table

II). Message Header contains Length and Message Type fields. MQTT-SN supports 256 message types. In this, message types (MsgType) ranging from $0X1E - 0XFD$, $0X19$ and $0XFF$ are reserved for future use.

TABLE II: General Message Format for MQTT-SN

Message Header		Message Variable Part
Length (1 or 3 octets)	Message Type (1 octet)	n octets

In this paper, we propose secure version of publish command for the MQTT-SN protocol $SecureMQTT - SN$, underneath our proposed secure MQTT protocol with Spublish command $0X00$. In this scheme, without loss of generality, we utilize reserved messages with its MsgType field equal to $0X1E$ and $0X1F$ as CPPublish and KPPublish (cf. Table III) secure publish commands based on CP-ABE and KP-ABE respectively.

TABLE III: Variable Message Header for Publish command of MQTT-SN

Length (octet 0)	MsgType (1)	Flags (2)	TopicId (3-4)	MsgId (5-6)	Data (7:n)

For the sake of completeness, we explain Secure MQTT-SN protocol. Publishing device encrypts the message using the CP/KP-ABE scheme and sets the message type appropriately and send it to a gateway. Now gateway converts CP/KPPublish command to Spublish command (cf. Section IV) MQTT message and send it to Broker (as discussed in Section IV). Broker forwards packet to all the gateways which are subscribed under topic name using MQTT protocol. Then Gateways converts the Spublish message to CP/KPPublish command (cf. Section IV) and send it to the intended subscribers. Finally, subscribers who satisfy the access policy are able to decrypt the ciphertext successfully.

A. Internetworking of the Brokers

As discussed earlier, smart city or infrastructure demands deployment of large number of IoT devices over a large area and hence topology of the IoT is large. Here we consider a cluster based topology wherein devices are grouped under different clusters with gateway as the cluster head and these gateways are connected to the central broker. Further, gateway acts as a broker (to envisage Pub-Sub protocol) for the devices of the cluster it manages. In this context, establishing secure communication for Pub-Sub is challenging. To leverage this, we address secure Inter-Broker communication (cf. Fig.5). In this setup, a Publisher belonging to one cluster can publish a message wherein Subscribers that are part of other clusters are allowed to subscribe. This can be achieved by configuring the address of all the Brokers that are present in the different cluster in the configuration file of the source Broker. Thus, Inter-Broker communication is achieved. In this setup, Publisher encrypts a message using public key governed by access policy. The role of Local PKG is to enable cryptography primitives for its devices through Global PKG while the Global PKG does the key management. Publisher sends encrypted message to the Broker of the cluster it belongs. Then Broker of that cluster forwards encrypted message to all the Subscribers in the same cluster as well as Broker of other clusters. All the intended Subscribers decrypt message using the keys provided by the Global PKG of the cloud. Hence security is realised in an end-to-end basis rather than hop-to-hop basis.

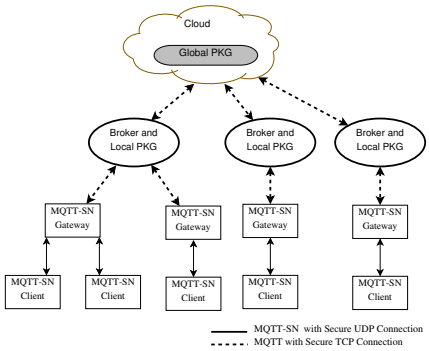

Fig. 5: Inter-networking of the Brokers in MQTT−SN

VI. Security Analysis

We describe robustness of security of our proposed scheme under various attacks. Underlined cryptography schemes for secure MQTT using CP/KP-ABE are based on bilinear pairing and ECC which are efficient and lightweight. Hence, they are preferable for IoT devices. In case of Broker hijacking, message confidentiality is assured as data is encrypted based on an access policy and all the stake holders who are eligible can only decrypt ciphertext. Hence, any malicious Broker cannot decrypt ciphertext, as it does not have the keys which satisfy the access policy. In our scheme, message confidentiality is realised in an end-to-end basis rather than hop-to-hop basis. This is realised from the following arguments. Publisher device encrypts the data using ABE and sends it to Broker which then forwards it to Subscribers. Each Subscriber can be a device, connected to a platform in the same cluster or a different cluster as that of publisher. In this process, though Broker is privileged to access the message, it cannot decrypt the data. In a nutshell, only a valid Subscriber can decrypt the data using its keys that satisfy a policy. Thus, end-to-end security is realised. Our proposed protocols are secure under chosen plain text attack (CPA), chosen ciphertext attack (CCA), man in the middle and collusion attacks.

Lemma 1. *Secure MQTT protocol is secure under CPA and CCA*

Proof: Encryption scheme used in protocol is KP/CP-ABE. According to the security analysis in [7], [8] security of the scheme is based on the intractability assumption of Decisional Bilinear Diffie-Hellman (DBDH) problem. ■

Lemma 2. *Secure MQTT protocol is secure under man in the middle attack*

Proof: Encryption scheme used in protocol is KP/CP-ABE. Any eavesdropper will not be able to decrypt the message based on the intractability assumption of Decisional Bilinear Diffie-Hellman (DBDH) problem. ■

Lemma 3. *Secure MQTT protocol is secure under collusion attack*

Proof: According to the result in [7] if users collude and reconstruct the secret key it is like breaking the Decisional Bilinear Diffie-Hellman (DBDH) problem. ■

VII. Performance Analysis

We evaluate and compare the performance of SMQTT based on our proposed scheme and technique described in [3] based on KP/CP-ABE scheme. Note that as discussed earlier in [3], data is encrypted using 128 bit AES key and this key is encrypted using KP/CP-ABE. In the following subsections, we describe the test bed for the experimentation and analyse results.

A. Experimental Setup

Test bed for evaluating the performance of the secure MQTT and MQTT-SN protocols are described in Table IV. We implemented SMQTT with our proposed scheme and also with the scheme described in [3] based on Java Platform. Publisher and Subscriber clients are implemented using Eclipse Paho client and open source Mosquitto broker. KP-ABE and CP-ABE schemes are implemented using the approach proposed in [7], [8] respectively. We applied lightweight ECC scheme [1], [13] to envisage bilinear operations (which is required to realize ABE) with different key sizes (256, 512 bits) with cryptography parameters described in Table V. In the Setup/Extraction phase, we assume that, PKG distributes keys to Sender and Receiver devices in a secure manner. PKG and Broker are separate entities but in the current implementation they are the same. Broker can connect to another Broker using a Bridge to envisage internetworking of the different Brokers. Thus we can realise security on an end-to-end basis. Due to the paucity of space, we omitted performance results of inter-broker scenarios and also MQTT-SN. As discussed to envisage secured MQTT-SN, underlying SMQTT is required and thus performance analysis of proposed SMQTT is also applicable to secure MQTT-SN.

TABLE IV: System Details

Hardware	Intel Core DUO CPU@3Ghz
Primary Memory capacity	2 GB
Operating System	Windows 7, 32bit, Linux Mint 13
Java version	1.6
MQTT version	3.1
Broker version	Mosquitto Broker 1.2
Client (Publisher and Subscriber)	Eclipse Paho client 0.9

TABLE V: Elliptic Curve Cryptography Parameters

curve	$y^2 = x^3 + x$
p	94856879503209427290989350919117134113398771438092750061123652819282435801122338 3
q	11857109937901178411373668864889641764174846429761593757640456602410304475140292 3

B. Results

We evaluated and compared performance of our proposed secure MQTT protocol in terms of the time taken to perform encryption, decryption, key generation and validation against number of attributes with different key sizes (256, 512 bits) and also its effect on MQTT payload when compared to the scheme in [3]. For the worst case analysis, we considered only AND logical connect in the predicate of access policy. We conducted and repeated the experiment with three laptops connected in 802.3 network and simulated as IoT devices for three iterations. In Table VI, we tabulated setup time (average time for three iterations) by PKG for KP-ABE (which includes key generation and access tree generation) and CP-ABE (includes only one time key generation) for five attributes. Note that as expected, set up time is more for CP-ABE than KP-ABE. Fig.6 describes the impact of SMQTT protocol based on our proposed scheme and technique described in [3] using KP/CP ABE in terms of packet overhead and the number of attributes for a data of three bytes. For both the schemes as the number of attributes increases the payload size of the packet also increases. But size of the ciphertext in CP-ABE is large when compared to KP-ABE. This is due to the additional information that needs to be provided in the policy to facilitate the decryption. Further, packet size in our proposed scheme is smaller than that of [3] for both KP/CP-ABE.

TABLE VI: Set up Time for KP/CP-ABE

Key Size	KP-ABE (ms)	CP-ABE (ms)
256 bits	187	588
512 bits	4307	19177

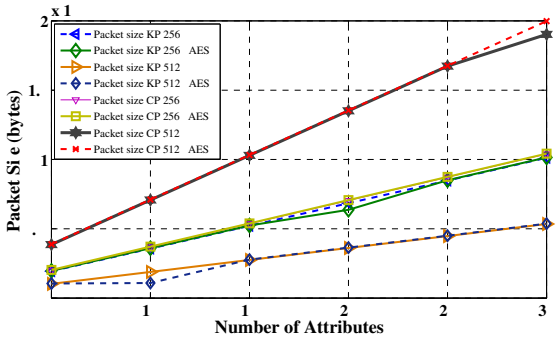

Fig. 6: Packet Overhead versus Number of Attributes

Performance of encryption and decryption algorithms of our proposed scheme and technique described in [3] for KP/CP-ABE are depicted in Fig.7 and Fig.8 respectively with key sizes (256, 512 bits) and varying number of attributes in the access policy. Encryption and decryption time for CP-ABE is more when compared to KP-ABE scheme, since additional information needs to be computed and provided in the access policy in case of CP-ABE. During decryption in case of CP-ABE more number of Tate pairing and complex multiplicative inverse operations needs to be performed than in KP-ABE. Thus major chunk of time is spent in computing these operations. Moreover our proposed scheme consumes less time for encryption and decryption when compared with the scheme described in [3]. Note that we repeated above experimentations on a data size of 64 bytes and the results of the experimentation correlates with the previous experimentation results w.r.t packet overhead, encryption and decryption time (Due to paucity of space, we are unable to include the results in the paper).

Hence by looking at these performance analysis, SMQTT based KP-ABE scheme is suitable wherein the access policies

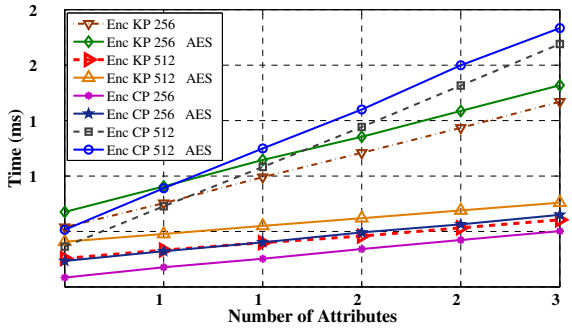

Fig. 7: Performance of ABE Encryption

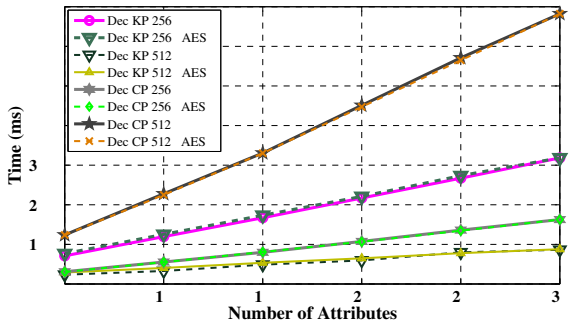

Fig. 8: Performance of ABE Decryption

are fixed and known a priori and requirement of interactive PKG is feasible. SMQTT based on CP-ABE scheme is suitable for those kinds of deployment in which the devices with more computing power and storage and requires dynamic access policies. Further SMQTT based CP-ABE scheme is more generic, dynamic and non-interactive (w.r.t PKG) and enables less communication overhead. Note that it is evident from both theoretical and experimental analysis is that SMQTT based on our propose scheme performs better than that of the scheme described in [3] based on KP/CP-ABE and thus can be a candidate for envisaging secure Pub-Sub architecture for IoT.

VIII. Conclusion and Future Work

In this paper, we analysed the feasibility of CP/KP-ABE to enable communication security for IoT devices based on Pub-Sub architecture. As part of this we proposed, designed and implemented secure MQTT protocols (SMQTT, SMQTT-SN) with new secure publish command "SPublish" which publishes encrypted data based on CP/KP-ABE scheme using lightweight ECC techniques by optimizing parameters and computation algorithms over the elliptic curve [1], [13]. Further security analysis of SMQTT under different attack scenarios are studied and also feasibility of SMQTT for distributed Pub-Sub architecture is proposed on end-to-end basis. Through analytical and simulation analysis, we demonstrate the application of SMQTT based on CP/KP-ABE for various requirements (such as static/dynamic access policy, interactive/non-interactive with PKG by devices, etc) of IoT. Further, we show that, both theoretically and experimentally our proposed SMQTT based CP/KP-ABE scheme performs better than that of the technique proposed in [3].

As part of our future work, we continue to work on security aspects of SMQTT such as key revocation, group publish/subscribe for distributed SMQTT. Further we deploy and evaluate performance of SMQTT and SMQTT-SN protocols on a real IoT platform.

References

[1] B. S. Adiga, P. Balamuralidhar, M. A. Rajan, R. Shastry, and V. L. Shivraj, "An Identity Based Encryption 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. Díaz Pardo de Vera, Á. Sigüenza Izquierdo, J. Bernat Vercher, and L. A. Hernández Gómez, "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 evaluation of 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) V3.1 Protocol Specification," http://www.ibm.com/developerworks/library/ws-mqtt/, 2010.

[6] Davis, Ernesto García and Calveras, Anna and Demirkol, Ilker, "Improving packet delivery performance of publish/subscribe protocols in wireless sensor networks," vol. 13, no. 1. Multidisciplinary Digital 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 13th International 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, Universität Stuttgart, Fakultät 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.