International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

Authentication and Access control Mechanism using Elliptical Curve Cryptography with Message Authentication Code

Sana Fathima

Abstract: ***Nowadays, Internet of Things (IoT) provided smart and inter-connected devices, which are ranging from tiny sensors to complex nodes of Fog and Cloud, communication protocols and several networking technologies. IoT plays a significant role in various application areas such as e-commerce, healthcare, research, governance and so on, and these application easily accessible for end users. Although the IoT has many benefits, there are some security challenges associated with the vulnerabilities presents in this area. This research work introduced a new authentication and access control model using Message Authentication code (MAC) with Elliptical Curve Cryptography (ECC) to address the security issues in Message Queuing Telemetry Transport (MQTT). In cryptography, a message can be authenticated by MAC (i.e. to verify that whether the message came from authenticate sender and the content of the message is changed or not). If any changes occur to the message content, the verifier can able to detect those changes using MAC values, which preserves the authenticity as well as data integrity. The validated results stated that the proposed ECC-MAC-MQTT shows better performance when compared with existing techniques in terms of accuracy, precision, recall and f-measure.***

Index Terms**: *Access Control, Elliptical Curve Cryptography, Internet of Things, Message Authentication Code, Secret Keys, Vulnerabilities.***

I. INTRODUCTION

IoT refers to the emerging concept of computing in which abundant physical objects are connected to the Internet to form a network. This network enables connected objects to access, interpret, exchange and monitor the information of each other [1]. In IoT, the information are shared to make real time decisions, coordinate intelligence and deliver the ubiquitous services to the users by enabling the collaboration of physical objects without human interference [2]. However, major development in the field is facing potential security threats associated with each layer of its framework. To provide efficient security solutions in terms of privacy, confidentiality, authentication, and integrity, researchers have done significant work in the field of cryptographic techniques [3,4]. The traditional existing techniques cannot be developed on the IoT devices due to various constraints and heterogeneity. When compared with traditional techniques, the better security is provided by developing a light-weight cryptographic primitives with limited resources and performed a few computations only [5,6].

While dealing with secure IoT infrastructure, authentication and authorization play an imperative role [7]. One-way authentication is unable to provide security for both the communicating parties. Alternative solution to this problem is mutual authentication in which both the parties get authenticated before the actual transmission. When the resources are limited, ECC is the most suitable asymmetric key cryptographic technique [8,9]. According to ECC, several authentication techniques are proposed and implemented, but some of them does not support authentication at protocol level and some failed to present the mutual authentication [10-13]. To overcome this problem, this research work implements the ECC-MAC-MQTT, which is suitable for resource-constrained IoT networks. The MAC is used to solve the mutual authentication issues provided by ECC, because it uses the center point for sharing the data to end user. Therefore, user can able to predict which sender sends the message and whether it is altered or not. The major contributions of the proposed ECC-MAC-MQTT work are summarized as follows:

- The research work illustrates the efficiency of using MAC with ECC over MQTT with less computation overhead. The data loss is avoided by using the MAC in ECC method.
- Two different tools such as Access Control Policy Testing (ACPT) and Automated Validation of Internet Security Protocols and Applications (AVISPA) are used to validate the correctness of proposed ECC-MAC-MQTT scheme.
- This research work presents a performance analysis to show how the proposed method is better than some of the other related schemes.

The remaining paper is consisting of several parts, where Section 2 describes the survey of related existing works proposed in recent years, Section 3 presents the explanation of proposed ECC-MAC-MQTT protocol. The validation process is conducted and discussed in Section 4, whereas conclusion of the research work with future scope is described in Section 5.

II. LITERATURE REVIEW

In this section, related works on MQTT protocol for IoT networks were reviewed.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Sana Fathima*, Department of Computer Science & Engineering, Sree Chaitanya College of Engineering, Karimnagar, India.

By using the constraint characteristics of IoT devices, the unauthorized access of data was prevented. Because of insufficient storage and devices computation, traditional existing networks were not compatible with IoT. A. P. Haripriya, and K. Kulothungan, [14] addressed the vulnerabilities by developing a lightweight fuzzy logic-based Secure-MQTT, that identified the malicious activity at the time of communication between IoT devices. By using fuzzy rule interpolation, the node's malicious behavior was detected and also the dense rule bases were avoided by generating these rules dynamically. In Secure-MQTT, the exhaustive sets of rules were avoided and protected the low configuration devices from DoS attack. When compared with traditional detection systems, the extensive experiments proved that fuzzy based Secure-MQTT identified many attacks and achieved low error rate. To strengthen the application layer, MQTT messages like PUBREC and PUBLISH, but this method focused on the features of Connect and ConnectAck of CONNECT and CONNACK messages. M. Hasan, et al., [15] predicted the anomalies and attacks on the IoT networks by using various machine learning algorithms such as Decision Tree (DT), logistic regression (LR), Artificial Neural Network (ANN), Random Forest (RF) and Support Vector Machine (SVM). The experiments were carried out on collected micro-services that was communicated using MQTT protocol. The results showed that various cyber-attacks on IoT were accurately predicted by RF technique when compared with other methods. In addition to this, the samples also predicted accurately in the case of DoS and Normal. There may arise various problems in real-time data due to that these approaches were depends on virtual environment data. An anomaly was created because the microservices behave differently at various times that leads to deviations in normal behavior. A. Lohachab, [16] tackled the vulnerabilities associated with security challenges by presenting a light-weight authorization and authentication framework using MQTT and Elliptical Curve Cryptography (ECC). Authorization of devices were approved by using the Usage Control (UCON) based access control, whereas the access control policies were defined for users by developing a Capability Based Access Control (Cap-BAC) model. The analysis of formal and informal security was presented in the ECC to deal with various security attacks. The efficiency of the ECC was poor because the method was unable to handle the dynamic nature of devices, even though it was useful for resource-constrained IoT devices. N. Moustafa, et al., [17] mitigated the malicious events by implementing an ensemble intrusion detection technique against protocols namely MQTT, DNS in IoT networks. According to the analysis of potential properties, the statistics features were generated from the protocols. The effects of these features and events of malicious were effectively predicted by developing the AdaBoost ensemble learning method using ANN, DT and Naive Bayes (NB). By using the correlation and co-entropy coefficient measures, the characteristics of malicious and normal activities were identified. When compared with other classification techniques, the ensemble techniques achieved higher detection rate with lower false positive rate. There were insufficient features presents in the ensemble method, which results that it was unable to build the dynamic profile. D. Yacchirema, et al., [18] integrated the advantages of IoT and ensemble learning algorithms, this work used to identify the fall of elderly people in indoor environments using IoTE-Fall system. The four classifiers such as Deepnets, LR, DT and ensembles were used to achieve high efficiency in detecting the fall using training and testing time. The ensemble-based predictor model was analyzed to accelerate the readings and identified the most appropriate predictor for fall detection. The main advantage of this IoTE-fall system was accurate detection, fast processing and provided the reliability of protocols, while re-creating the machine learning model, the average detection was enhanced at every stage. There were some barriers raised due to the wrong usability of various tri-axial devices in real-time environment, which lead to complexity of elements and high cost for maintenance.

III. PROPOSED METHODOLOGY

In this section, the basic concepts involved in the formulation of this scheme including ECC, MQTT and system models are discussed.

A. Elliptic curve cryptography (ECC)

A Public Key Cryptosystem (PKC) as ECC was implemented by Miller and Koblitz to offer better performance and more security by using small key size, when compared with existing PKC [19]. Therefore, this system is the most appropriate for IoT environment, which consists of resource-constrained devices. Consider the $a,b \in F_p$ a, in an elliptic curve as $E_p(a,b)$ over a finite prime field F_p, is given in Eq. (1) below:

$$E_p(a,b): y^2 = x^3 + ax + b(\text{mod } p) \quad (1)$$

Where $p > 3$ and $4a^3 + 27b^2 \neq 0(\text{mod } p)$. The identity element is considered as a point, which have an infinity values as O. Two common operations on elliptic curves are scalar addition and scalar multiplications. Scalar multiplication uP over an elliptic curve $E_p(a,b)$ is defined as repeated additions, as given in Eq. (2) below:

$$uP = P + + ... + (utimes) \quad (2)$$

Where $u \in F_p *$. The next section shows the basic idea of MQTT protocol.

B. Message queuing telemetry transport (MQTT)

According to publish-subscribe architecture, MQTT protocol is used for Machine-to-Machine (M2M), IoT applications and runs over Transmission Control Protocol (TCP), where Organization for the Advancement of Structured Information Standards (OASIS) standardized these light-weight application layer messaging protocol [20].

The low bandwidth communication channels, unreliable networks and resource-constrained devices are specifically designed by using these MQTT protocol, where the entities are involved as publishers, brokers and subscribers. The data are collected from the surroundings by publishers which contains sensing devices, then forward this data to Cloud Server as broker and sends it to group of target users who are interested in sensed data. The subscribers are authenticated first to obtain the requested data, where the clients established the one connection per session in MQTT protocol. The ECC are integrated with the concept of MQTT and Transport Layer Security (TLS) in this proposed framework. The next section explains the system model of the research work.

C. System Model

The physical devices are entered into the network for data transmission, the manufacturer of the device loads some parameters into the memory of the device that are used for future communications. These devices are then registered into their respective IoT networks based on the nature of application and type of device by sending their identity to the central administrator server of the network. This server is also registered over the Cloud database. Furthermore, the users are also registered over the Cloud by sending their identifying information. The suitable access control policies are decided for the devices and users by using CapBAC and UCON model, once the registration is done successfully. After defining the policies, three cases along with secure authentication are involved in the data exchange phase. Through IoT networks, the cloud obtains the data from the sensors or physical devices in the first case. While storing the data with delay-sensitive applications, the data will be send to Cloud, which is stored for the longer durations. In the next two cases, the data are transformed in two ways, i.e. the target users receive the data once it is received from the sensors in a periodic manner. The other way is that the data broadcast is occurs, when the request is made by the specific user. In addition, users are provided with the facility to change their credentials by providing the old credentials to CAS for verification. User's access rights can also be revoked if they move out of their parent network or they turn out to be rogue ones. The working scheme is divided into 7 phases as shown in Figure 1 and also described below:

1) First Phase (Installation): In this phase, the identity D_ID_i of the device D_i, hash function $h_1(\ )$ and a pseudo-random password pr_i are loaded into the memory of the device by the manufacturer M that are used for later communication are as in Eq. (3):

$$M \rightarrow D_i : \{D\_ID_i, h_i(\ ), pr_i\} \quad (3)$$

Where pr_i is computed using secret parameter s chosen by the manufacturer M as in Eq. (4),

$$pr_i = h_1(D\_ID_i \| s) \quad (4)$$

2) Second Phase (Initial setup): The initial system parameters are decided in this phase, that are used for future computations.

(i) A generator P of an additive group G of order n are selected by Cloud Authentication Server (CAS), that considers an E as an ECC over a finite field F_p, where the large prime numbers are defined as p and n .

(ii) CAS selects a private key $k \in Z_n^*$. From this private key, it computes public key equals to kP .

(iii) Authentication server chooses a secure one-way hash function $h2(\ ): \{0,1\}^* \rightarrow \{0,1\}^n$, which is collision-resistant (based on MD5 or SHA-1) with fixed output.

(iv) The data transmission requests are encrypted and maintained by using a secret key S_key.

3) Third Phase (Registration): The credentials of system entities such as user, IoT network and devices should be registered at the CAS in this phase.

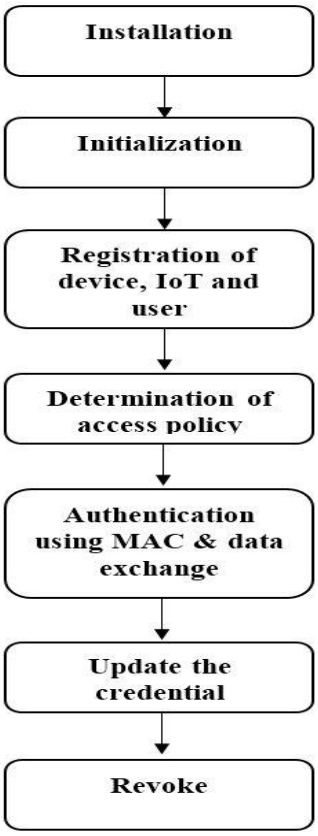

Fig. 1. Working Procedure of proposed ECC-MAC-MQTT method

- **Device Registration**: In this step, the IoT devices or sensor nodes are registered in their respective IoT network based on their functionality by sending identity to the CAS through network layer. In return, the administrator gives the anonymously identified information to the devices.

- **IoT Network Registration:** In this step, the administrator of the IoT network is registered over the Cloud by sending the network identity to the CAS and receiving hashed value of the same.

- **User Registration:** In this step, the user who is going the access the Cloud services and data is registered by sending the anonymous user identity and a pseudo-random password to CAS, which is first checked by the CAS in order to avoid identity collision.

4) Fourth Phase (Access Policy Determination): The data collected from the sensor devices are identified by defining the access policies using UCON model and then it is stored over other nodes or cloud servers. The data which is obtained from an authorized source are ensured by checking the identity of the device. The devices are not compromised and ensured by an integrity of device attributes. Data is send to cloud servers, once the security check is finished, which is depends on the availability of time, bandwidth and security level. Based on the data access requests made by users, the access control policies are defined specifically. According to role and identity of user, the policy enforcement server assigned the capabilities of CapBAC model. The access request is checked by these tokens or assigned capabilities, which is made by users. The user request is considered and served upto successful check.

5) Fifth Phase (Authentication and Data Exchange): In this phase, data are disseminated by IoT network, requested by users and also broadcast the data.

- *Data dissemination step:*

The registered IoT devices or sensor nodes collect data C_DATA from the surroundings and send it for storage over the Cloud. The IoT device generates time stamp t_i and computes and sends the following to CS_j of IoT network IN_j as in Eq. (5):

$$D_i \rightarrow NL \rightarrow CS_j : S\_key\_ \left\{ d_i \| h_2\left(n_j d_i\right) \| C\_DATA \| ti \right\} \quad (5)$$

CAS verifies the identity of the device by computing $h_2\left(n_j, d_i\right)$ and upon successful verification computes as in Eq. (6):

$$M_0 = rP, M_0^{'} = \left(IN\_ID_j \| C\_\text{DATA} \| r \| t_j\right) + rkP, A_j = h_2\left(rkP \| IN\_ID_j\right) \quad (6)$$

Where, r is a random number and sends $\left(M_0, M_0^{'}, A_j\right)$ to CAS as $CS_j \rightarrow NL \rightarrow CAS : \left(M_0, M_0^{'}, A_j\right)$. CAS computes and verifies the identity of CAS by computing A_j in order to accept the collected data.

- *Data Request by Users:*

In this step, the users request for the data R_DATA from the Cloud through MAC, which contains three algorithms:

(i) At random, a key from the key space are selected by using key generation algorithm.

(ii) The message is given by key and tag, which will return by using signing algorithm.

(iii) The message authenticity is verified effectively by using verifying algorithm. i.e. when the tag and message are not tampered with or forged, return will accept, otherwise it will reject.

A given message's valid tag is computed for secure unforgeable MAC without the knowledge of key, which is computationally infeasible. In general, a three type of efficient algorithms (G,S,V) are presents in MAC, that should satisfy:

- On input 1^n, the key k is given by G (key-generator), where, the security parameter is defined as n.
- On the key k, a tag t is defined as output by S (signing) and x is described as the input string.
- The inputs consists of the key k, the string x and the tag t are verified by V (verifying) as outputs accepted or rejected. S and V must satisfy the following equation (7):

$$\Pr\left[k \leftarrow G\left(1^n\right), V\left(k, x, S\left(k, x\right)\right) = accepted\right] = 1 \quad (7)$$

A MAC is unforgeable if for every efficient adversary A as in Eq. (8),

$$\Pr\left[\begin{array}{l} \leftarrow G\left(1^n\right), \left(x, t\right) \leftarrow A^{s(k,.)}\left(1^n\right), \\ x \notin Query\left(A^{s(k,.)} 1^n\right), V\left(k, x, t\right) = accepted \end{array}\right] < negl\left(n\right) \quad (8)$$

Where, oracle $S\left(k;\right)$ is accessed by A, that is denoted by $A^S\left(k;\right)$, and set of queries on S are denoted as $\text{Query}\left(A^S\left(k;\right), 1^n\right)$, which is made by A, and defined as n. The string x on S are not directly queried by any adversary, which is required by MAC. Otherwise, the adversary can easily obtain the valid tag. In existing ECC techniques, the data are shared to end user by using secret keys, which leads to data loss. The key sizes are very large, which consumes more time to transmit message. To overcome this drawback, the proposed method uses the MAC in ECC.

- *In data broadcast step:*

In this step, the data collected by the IoT devices is broadcasted to a target set of users. The subscribers are described as target group of users, broker are presented as cloud server and publisher will act as IoT devices, which is employed in MQTT protocol.

6) Sixth Phase (Credential Update): The user's ID and old password are provided to CAS to change his/her password in this phase. This new password should be matched with the stored one, if it is correct, the new password is promoted and then user sends the same to CAS.

7) Final Phase (Revoke): If an IoT device change to a various network or becomes faulty in this phase, then its registration from the existing IoT network is cancelled. Record of the device identity is removed from the central administrator server. Similarly, a user can be revoked from accessing the Cloud services. The identity is dropped by CAS.

IV. EXPERIMENTAL ANALYSIS

In this section, the implementation of the proposed method using two various tools (i.e. ACPT and AVISPA) are briefly described and the experimental validation of these approach with other existing techniques along with the results are evaluated and discussed.

A. Implementation Tools

In this approach, the implementation of the ECC-MAC-MQTT are carried out by two various tools as AVISPA and ACPT that are explained below:

AVISPA tool: The verification and formalization of security protocols, associate threat models and the security goals are used by AVISPA, which is also defined as automated push-button tool. The protocols are the formal role-based language that are specified in High-Level Protocol Specification Language (HLPSL) and uses the control flow patterns, algebraic properties, data structures and cryptographic operators. The user defined the security problem by using HLPSL2IF Translator, which is translated into Intermediate Format (IF).

ACPT tool: In order to identify and reduce the faults in the policies, the ACPT tools are executed along with static and dynamic verification, which is implemented by National Institute of Standards and Technology (NIST). The ACPT tool performed mainly three functions such as policy analysis, specification of policies and convert the policy into XACML format.

B. Parameter Evaluation

In this section, the various parameters such as accuracy, precision, recall, f-measure and False Positive Rate (FPR). The mathematical explanations for this metrics are given as below:

Accuracy: Accuracy is the ratio of percentage of malicious nodes detected successfully and is determined by the following formula in Eq. (9):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (9)$$

Where, TP refers to True Positive, TN refers to True Negative, FP refers to False Positive and FN refers to False Negative.

Precision: Precision gives the number of malicious nodes correctly identified among the detected malicious nodes, which is defined as follows in Eq. (10):

$$\Pr ecision = \frac{TP}{TP + FP} \quad (10)$$

Recall: Recall gives the percentage of malicious nodes correctly identified among the total detected malicious nodes, which is defined as follows in Eq. (11):

$$\mathrm{Re}\,call = \frac{TP}{TP + FN} \quad (11)$$

F-measure: The performance of the ECC-MAC-MQTT is also measured by F-measure, which is used to weight the average of recall and precision of a model. The mathematical equation is given in Eq. (12).

$$F - measure = \frac{2 * TP}{2 * TP + FP + FN} \quad (12)$$

FPR: The summarization of classifier performance over the possible threshold is defined by FPR graph, where the abnormal nodes are identified by giving the rate of legitimate nodes. The equation for FPR is defined as in Eq. (13):

$$FPR = \frac{Number\ of\ \ false\ positive\ samples}{Total\ number\ of\ \ samples} \quad (13)$$

In next section, the validation for these parameters of proposed method against existing techniques are discussed.

C. Performance Evaluation of Proposed ECC-MAC-MQTT

In this section, the quantitative analysis of proposed method is carried out with existing techniques namely fuzzy based Secure-MQTT [14], several machine learning algorithms [15], ensemble intrusion detection techniques (i.e. NB, ensemble) [17] and ensemble learning algorithm [18] in terms of metrics such as accuracy, F-measure, recall, FPR and precision. Table 1 shows the comparative values of accuracy and precision over proposed method. Figure 2 shows the graphical representation of accuracy over proposed.

Table I. Comparative Analysis of Proposed Method

Methodology	Accuracy (%)	Precision (%)
Fuzzy based Secure-MQTT [14]	Not available	90.90
DT [15]	99.40	99.02
LR [15]	98.30	98.01
ANN [15]	99.40	99.04
SVM [15]	98.20	98.21
RF [15]	99.40	99.0
Ensemble [17]	99.54	Not available
NB [17]	91.17	Not available
IoTE-Ensemble learning [18]	98.72	96.22
Proposed ECC-MAC-MQTT	99.72	99.35

Fig. 2. shows that the proposed method achieved higher accuracy when compared with other existing techniques. The NB achieved low accuracy (i.e. 91.17%), and other existing techniques achieved nearly 99% accuracy.

The proposed method achieved 99.72% accuracy due to the verification of shared messages among end user by using MAC method. By verifying the messages, the error rate is reduced and achieved higher accuracy. Figure 3 shows the graphical representation of precision of proposed method.

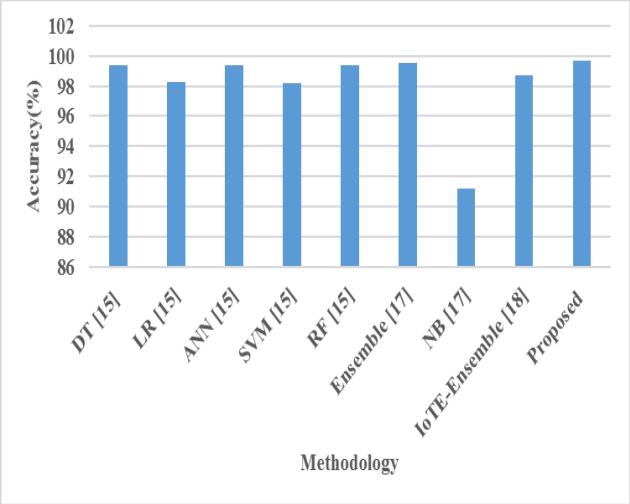

Fig. 2. Comparison of Accuracy over Proposed ECC-MAC-MQTT

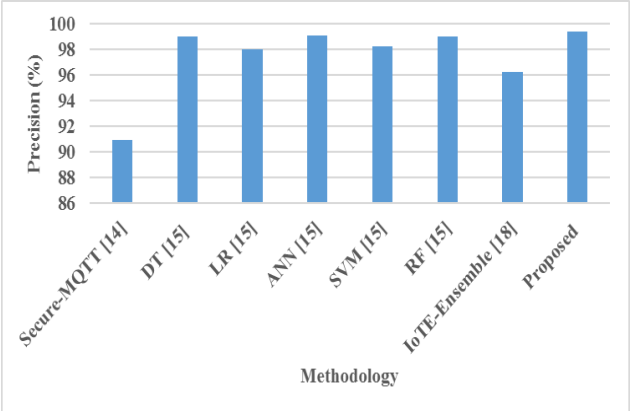

Fig. 3. Precision of Proposed ECC-MAC-MQTT Method

The precision of existing technique Fuzzy based Secure-MQTT achieved very low values (i.e. 90.90), when comparing with other machine learning techniques. The LR and SVM achieved 98% precision, IoTE-Ensemble technique achieved 96.22% precision and other existing techniques such as DT, ANN and RF achieved 99% precision. From the graph, the proposed method shows higher precision value (i.e. 99.35%) because of using MQTT and MAC methods. Table 2 shows the validated values of recall and f-measure over proposed method with existing techniques. Figure 4 shows the performance of recall and f-measure over proposed method.

Table II. Performance Analysis of Proposed over Existing techniques

Methodology	Recall (%)	F-measure (%)
Fuzzy based Secure-MQTT [14]	90.90	90.90
DT [15]	99.00	99.00
LR [15]	98.00	98.00
ANN [15]	99.00	99.00
SVM [15]	98.00	98.00
RF [15]	99.00	99.00
sProposed ECC-MAC-MQTT	99.64	99.45

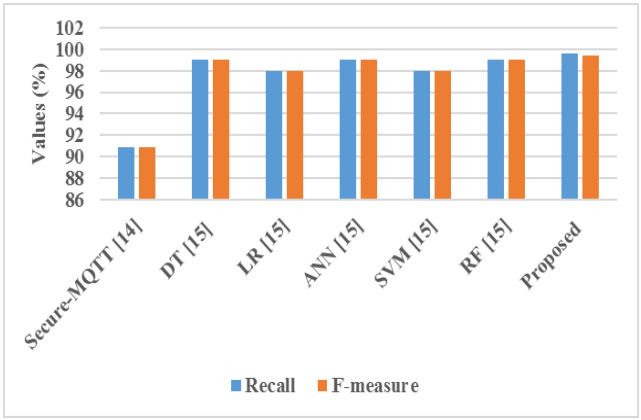

Fig. 4. Comparative Analysis of proposed method in terms of recall and F-measure

From the Table 2 and figure 4, the performance of proposed ECC-MAC-MQTT achieved higher recall and f-measure with machine learning techniques and fuzzy based Secure-MQTT. The results of recall and f-measure are carried out for various positive samples. When the number of positive samples increases, the values of recall and f-measure decreases. Here, the experiments for recall and f-measures are validated by using 20 positive samples. The DT, ANN and RF achieved the recall and f-measures values as 99%, whereas SVM, LR and Fuzzy based Secure-MQTT achieved 98% and 90.90% for both recall and f-measure. The proposed method shows less increase in both the parameters (i.e. 99.64% recall and 99.445% f-measure) due to usage of various end users with single server. Table 3 shows the performance of FPR for various time slots of proposed method with existing methods such as ensemble technique and fuzzy based Secure-MQTT protocol. The number of request messages are varied over several timeslots are shown in Figure 5, which shows the FPR of the proposed ECC-MAC-MQTT, Secure-MQTT and ensemble technique.

Table III. Comparison of FPR over proposed method

Methods	Time Slots (in sec)					
	2	6	10	14	18	20
Ensemble [17]	0.39	0.50	0.52	0.59	0.39	0.40
Fuzzy based Secure-MQTT [14]	0.2	0.35	0.32	0.29	0.30	0.38
Proposed	0.18	0.20	0.17	0.15	0.21	0.19

ECC-MAC-MQTT obtains the least threshold FPR range [0.1–0.37] as compared to the range [0.3–0.59] of existing techniques. The most suitable code for secure message transport is ECC-MAC-MQTT's that gives better results in FPR.

The absence of early detection mechanism in existing techniques increases the FPR. From these results, it can be seen that proposed ECC-MAC-MQTT protocol is secure against different security attacks.

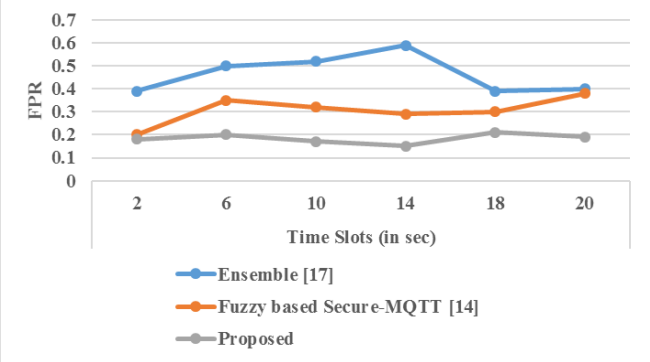

Fig. 5. Comparison of FRP values over Proposed ECC-MAC-MQTT method

V. CONCLUSION

A diverse ecosystem of actuators, nodes and sensors are created by IoT, which also described the large networks of connected devices and shares the data about their environments. However, various levels of IoT architecture and their connected devices faces the security challenges because of their associated vulnerabilities. The networking environments are protected by using authorization and authentication model, which is one of the most technique when compared with other possible traditional methods. This research work provides the strong authorization and authentication framework by developing the light-weight protocol of ECC in MQTT and merged it with MAC mechanisms. The access control policies are defined for the users by using CapBAC model, where the authorization of devices are given by using UCON based access control. To broadcast the data transmission, this research work uses the concept of MQTT protocol. Two different tools namely ACPT and AVISPA are used to implement this scheme and the validation of ECC-MAC-MQTT is carried out by several experiments by parameter metrics such as accuracy, precision, recall, FPR and f-measure. The ECC-MAC-MQTT method achieved 99.72% accuracy, 99.35% precision with 0.15 FPR, when compared with existing techniques such as ANN, Fuzzy based Secure-MQTT and SVM. The key sizes are large in the proposed ECC-MAC-MQTT method, hence the further development of this method is to reduce the size of the key.

REFERENCES

1. K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad. (2016). A lightweight message authentication scheme for Smart Grid communications in power sector. Computers & Electrical Engineering, 52, pp. 114-124.
2. M. Cuka, D. Elmazi, K. Bylykbashi, E. Spaho, M. Ikeda, and L. Barolli. (2019). Implementation and performance evaluation of two fuzzy-based systems for selection of IoT devices in opportunistic networks. Journal of Ambient Intelligence and Humanized Computing, 10(2), 519-529.
3. B. Agyemang, Y. Xu, N. Sulemana, and H. Hu. (2018). Resource-oriented architecture toward efficient device management for the Internet of Things. Journal of Ambient Intelligence and Humanized Computing, pp. 1-13.
4. J. Choi, Y. In, C. Park, S. Seok, H. Seo, and H. Kim. (2018). Secure IoT framework and 2D architecture for End-To-End security. The Journal of Supercomputing, 74(8), pp. 3521-3535.
5. R. K. Lomotey, C. P. Joseph and C. Chai. (2018). Traceability and visual analytics for the Internet-of-Things (IoT) architecture. World Wide Web 21(1), pp. 7-32.
6. T. Malche, P. Maheshwary, and R. Kumar. (2019). Environmental Monitoring System for Smart City Based on Secure Internet of Things (IoT) Architecture, Wireless Personal Communications, pp. 1-30.
7. G. Gardasevic, M. Veletic, N. Maletic, D. Vasiljevic, I. Radusinovic, S. Tomovic, and M. Radonjic. (2017). The IoT architectural framework, design issues and application domains. Wireless personal communications, 92(1), pp. 127-148.
8. Z. Liu, and H. Seo. (2018). IoT-NUMS: evaluating NUMS elliptic curve cryptography for IoT platforms. IEEE Transactions on Information Forensics and Security 14(3), pp. 720-729.
9. A. Luoto, and K. Systa. (2018). Fighting network restrictions of request-response pattern with MQTT. IET Software 12(5), pp. 410-417.
10. I. Goldberg, D. Stebila, and B. Ustaoglu, (2013). Anonymity and one-way authentication in key exchange protocols. Designs, Codes and Cryptography, 67(2), pp. 245-269.
11. D. G. Roy, B. Mahato, D. De, and R. Buyya. (2018). Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT)—MQTT-SN protocols. Future Generation Computer Systems, 89, pp. 300-316.
12. H. Zhu. (2015). A Provable One-way Authentication Key Agreement Scheme with User Anonymity for Multi-server Environment. KSII Transactions on Internet & Information Systems, 9(2).
13. S. Jang, D. Lim, J. Kang, and I. Joe. (2016). An efficient device authentication protocol without certification authority for Internet of Things. Wireless Personal Communications, 91(4), pp. 1681-1695.
14. A. P. Haripriya, and K. Kulothungan. (2019). Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. EURASIP Journal on Wireless Communications and Networking, 1, pp. 90.
15. M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 7, pp. 100059, 2019.
16. A. Lohachab. (2019). ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. Journal of Information Security and Applications, 46, pp. 1-12, 2019.
17. N. Moustafa, B. Turnbull, and K. K. R. Choo. (2018). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 2018.
18. D. Yacchirema, J. S. de Puga, C. Palau, and M. Esteve. (2019). Fall detection system for elderly people using IoT and ensemble machine learning algorithm. Personal and Ubiquitous Computing, pp. 1-17.
19. B. B. Gupta, and M. Quamara. (2018). An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards. Procedia computer science 132, pp. 189-197.
20. H. Urs, H. L. Truong, and A. Stanford-Clark. (2008). MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks.3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08). IEEE, 2008.

AUTHORS PROFILE

Sana Fathima has lived in India since 1994. She received B.Tech and M.Tech degrees from the Jawaharlal Nehru Technological University, Hyderabad, India, in 2015 and 2017, respectively. She was honoured with a scholar award during master's degree by Academy of Computer Science. In Febraury 2018, she became an Assistant Professor at the department of Computer Science and Engineering, where she has established an advanced laboratory, emphasizing the controlling of devices in the network through internet. She teaches several courses on technology in computers to engineering students. She has attended various national workshops for academic and professionals. She is an author and coauthor of other more papers in international refereed journals. She has given invited/plenary talks at national conferences. Her research interest cover several aspects across networking, with a special focus on Internet of Things. She has received several important recognitions to her research career.