Mutual authentication and data security in IOT using hybrid mac id and elliptical curve cryptography

Harish Kumar N.[1] & Dr. Deepak G.[2]

[1] Assistant Professor, Department of Computer Science & Engineering, Dayananda Sagar College of Engineering. Bangalore, Karnataka, India.

[2] Assistant Professor, Department of Computer Science & Engineering, PES University, Bangalore, Karnataka, India.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Internet of Things (IoT) is a new emergent technology of the Internet. The Internet that we use today runs with human interposing. The Internet of Things which is the extended version of the internet which aims to offer the machine to machine communication or the device may be referred to as objects we call it object to object communication, which is without the involvement of the humans. With the growth of IOT in the market there are many considerable subjects relating to privacy, authentication, data confidentiality, data protection and other problems where solutions to these issues to be derived. This paper works on providing Mutual authentication and data security. A light weight Approach has been employed by generating Hybrid MAC ID for mutual authentication and using Elliptical Curve for secure data transfer which provides authentication and data confidentiality in the IoT Network.

Keywords : Elliptical Curve, Hybrid MAC, Authentication, IoT.

1. Introduction

Security is the utmost important concern in wireless communications, as the broadcast nature of the wireless structure makes the signals which are transmitted through the medium available to the unauthorized devices or nodes. As the IOT is wireless communication since more number of devices entering to the field of IOT, the security of the devices on the IOT platform becomes the most important thing. The device with the less security becomes the more vulnerable device that may face the cyber-attacks, grabbing the most sensitive data that is already in the connected devices on the internet. Also with the IOT there is a problem with the huge data storage which being is generated by the no of devices that are increasing day by day. Hence there is uplift in physical layer security in the scenario of wireless communication. The physical layer increases the security of the devices on the IOT, so that there will be authentic information is delivered to the desired location.

Security is the main part with IoT concern, due to increase in the more number of devices that are being registered in the network daily. And securing these devices becomes the major concern, since a lot of data is being generated from these devices together. According to the many researches being conducted on the IOT, the major issues on the network of interconnected devices is about the privacy and data security. And the devices with the poor area of defense against the attacking devices will be a way to enter for the attacker onto the distributed network.

This paper focuses on the Mutual authentication technique used in IoT. It is an approach for proving the individuality of an object in IoT or it is the action taken to authenticate the system's exclusive identity. The scenario where two communicating parties prove each other simultaneously is stated as two-way verification or mutual authentication. A reliable communication is delivered to IoT devices existing in remote area. Mutual authentication is supplemented by elliptic curve cryptography to enable the security towards the data communication also certifies openness, optimality and competence of the algorithm. Section 2 is on literature survey carried, Section 3 on System Architecture and methodology, Section 4 discuss on proposed approach, Section 5 on results and performance Analysis followed by Conclusion.

2. Literature Review

A new framework for authentication in IoT infrastructure using a multi-level authentication protocol, which uses Elliptic Chebyshev Session hashing (EcSH) for refining the complete performance and working of IoT network is proposed by Vairagade (2020). A new secure authentication protocol using ECC and ID verifier has been proposed. This allows performing mutual authentication and also fulfils the IoT security requirements (Afroz, *et.al.* 2019). A secure group-based lightweight authentication scheme in E-health applications using ECC has been identified. This aims at providing mutual authentication and energy efficiency in healthcare applications (Almulhim, *et.al.* 2018). An authentication scheme which customs simple algebraic operations like hashing, XORing and make it suitable for IoT in light weight environment has been proposed.

User credentials such as identity of user, biometrics, and passwords are used for user authentication (Gowthami, *et.al.* 2018). A better, lightweight and computationally effective authentication structure for wearable devices has proposed (Hasan, *et.al.* 2019). A scheme has been proposed which attains security necessities such as mutual authentication, the security of a secret key, session key agreement, repels forgery attack etc (Hasan, *et.al.* 2019). A two factor scheme is used for cloud based IoT to provide security and mutual authentication. Kiran *et.al.* (2019) has presented a novel safe mutual authentication system that can be applied in smart homes applications. This technique uses block chain, group signature and message authentication code to audit users access history. Lin *et.al.* (2019) has defined an unique two-factor lightweight mutual authentication approach for IoT objects, that can be positioned at various levels.

Physically Unclonable Function (PUF) is used as first factor which services with a nonce taken from the physical channel. Entity-based fingerprint is the second factor used for getting user specific information. Noura *et.al.* (2019) has worked on an authentication scheme by using the dynamic cipher alongside with the present public key encryption, where the client produces the key dynamically, which can only be cracked by brute force. The key dynamically generated by means of random function is used for encryption and decryption. Added to this, an augmentation to the security is projected by incorporating dynamic cipher based authentication.

Phimphinith *et.al.* (2019) has offered a light weight mutual authentication mechanism grounded on ECC between server and IoT objects. Sachan *et.al.* (2019) worked on the Light Weighted Mutual Authentication and Dynamic Key Encryption for IoT Devices Applications in their research paper. Tewari *et.al.* (2018) worked on the Mutual Authentication Protocol for IoT Devices Using Elliptic Curve Cryptography in their research paper & produced novel results. Similarly, Koblitz (1987) did extensive work on the Elliptic curve cryptosystems. Mathematics of Computation which was extended to the use of elliptical curves in cryptography by Miller *et.al.* (1999).

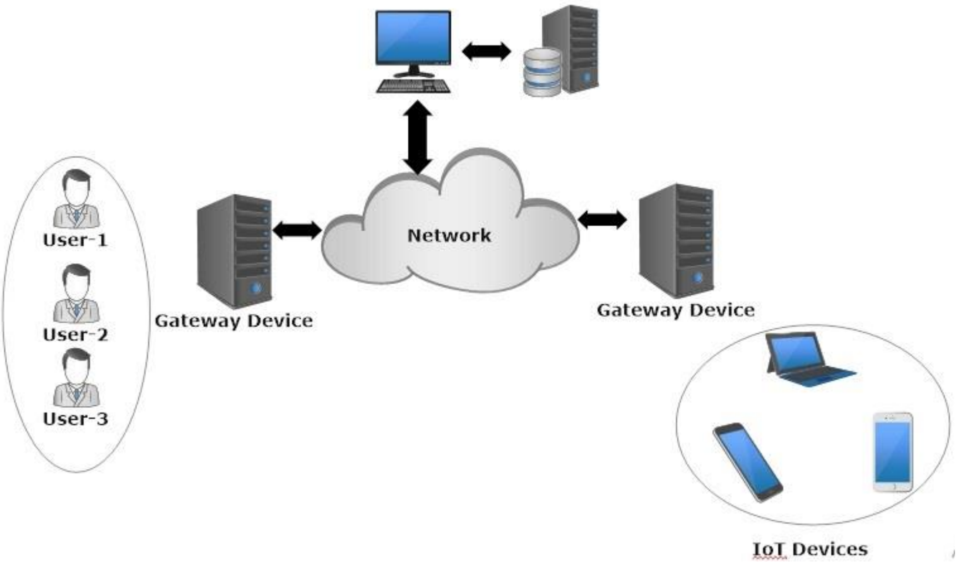

Fig. 1 : System Architecture

Notations	Description
GWD	Gateway Devices
Nj	Node
H (.)	One way hash function
||	Concatenation operation
Sgn	Secret parameter available for GW and Nj
HIi	Hashed Identity
HMC	Hybrid Mac-ID
SER	Server
ACK	Acknowledgement
NACK	Negative Acknowledgement

Table 1 : Notations

3. IoT System Architecture

The system architecture in Figure 1 depicts the arrangement of objects and user interaction with IoT network. Multiple users are connected to IoT network via a gateway device which acts like interface between user and network. IoT gadgets like mobiles, laptops and other devices are connected to the network via a gateway device. In IoT devices network, authentication between the objects has to be achieved to maintain the authenticity of the objects in the communication. Similarly, user has to be validated and authenticated to prove the identity of the person intending to communicate or get the information from the IoT network. In both cases mutual authentication has to be achieved one from devices end and from user perspective.

4. Proposed Mutual Authentication Algorithm

In this section, a Mutual Authentication algorithm is designed which aims at providing authentication of IoT objects by using the MAC-ID of the device along with the MAC-ID of gateway device connected to those IoT objects. Table 1 contains the notations used to illustrate the proposed scheme.

The Algorithm Steps are as follows:

```
Algorithm: Mutual Authentication Using Hybrid MAC-ID
Step 1  :  Device Registration to the IoT network.
           Nj=reg(MAC-ID)
Step 2  :  Hybrid MAC-ID Generation using Device MAC-ID and Gateway device ID.
           HMC = getmac(Nj,24)|| getmac(GWD,24)
           HIi = H(.)HMC
Step 3  :  Mutual Authentication of IoT devices with Server.
           Nj(MAC-ID)->GWD
           Sgn(GWD(Nj 24Bit||GWD 24bit))->SER
           SER->validate ( )
           On success
           Nj(ACK)<-GWD<-SER.
           On Failure
            Nj(NACK)<-GWD<-SER.
Step 4  :  Data Communication between the User and server for accessing the IoT data from devices.
```

Each Step of the proposed scheme is discussed in the following sub sections.

Step 1 : Device Registration

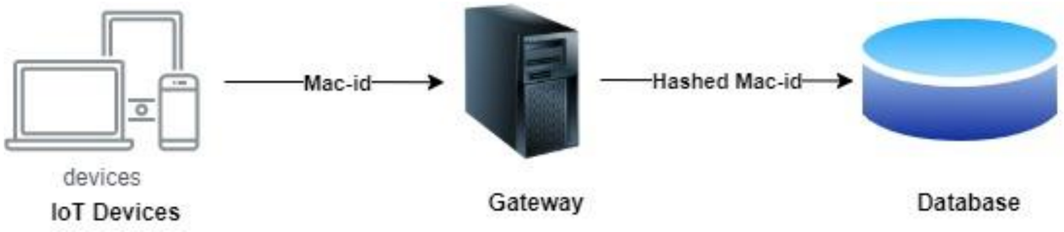

Fig. 2 : Device Registration

Figure 2. shows the process of device registration. At the time of network setup the IoT devices will share their MAC -ID to the gateway devices and they are hashed and stored in the sever database. Devices connected to the network are having 48 bit MAC address and the gateway connecting the objects and IoT network is also having 48 bit MAC address. At the time of registration the first 24 bits of device and last 24 bits of gateway MAC address are taken and performed a 24 bit swap finally resulting in 48 bit value which is hybrid in combination. After the 24 bit swap, the resulting hybrid Mac is hashed using SHA 256 hashing algorithm and a copy is stored locally in the gateway device and another copy in the server database. This can be used as a part of mutual authentication among devices level in the IoT network. Figure 3. Shows the Hybrid MAC generation process. Figure 4. depicts the Hybrid Mac obtained from the above process.

Step 2 : Hybrid MAC Generation

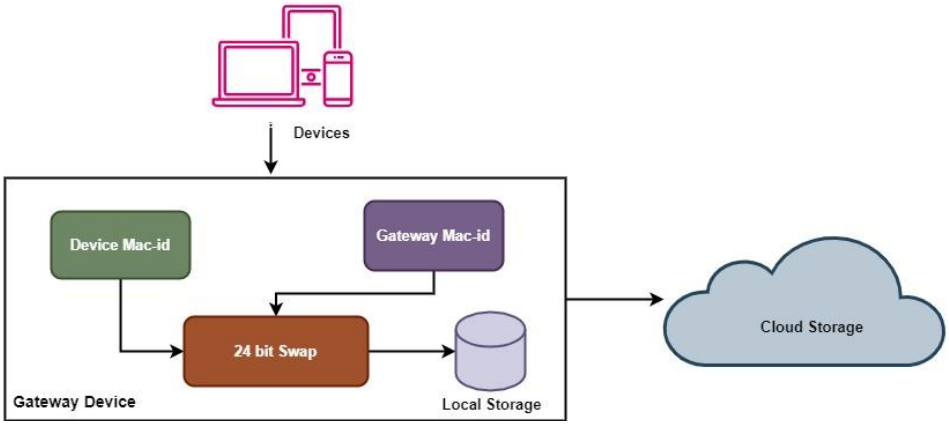

Fig. 3 : Hybrid MAC generation Process

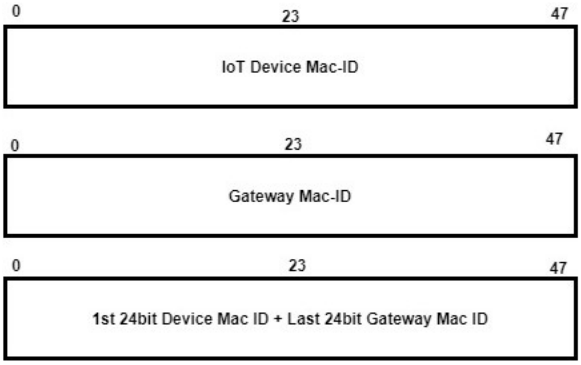

Fig. 4 : Hybrid MAC

Users are the people interested to interact with the IoT devices and to gain access to control, monitor the data, and use the data of IoT devices. To make use of the resources of these constraint devices proper authentication process has to happen. User at first has to register himself with the server. This process is termed as user registration. At the time of registration user will provide his basic information which is recorded in the server database. On successful Registration a physical token is generated by the server and questioned to user. Along with physical token a system generated random password is given as initial password credential which has to be changed on successful login for the first time. Figure 5. shows the user registration process.

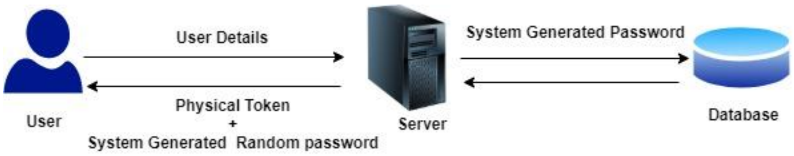

Fig. 5 : User Registration

Step 3 : Mutual Authentication Phase

The 12-digit hexadecimal numbers of MAC addresses are a length of 48 bits. MAC addresses are, by convention, Typically written in one of the two formats below:

MM: MM: MM: SS: SS: SS or MM-MM-MM-SS-SS-SS

The ID includes the first half of a MAC address The adapter manufacturer's number. These IDs are identities Regulated by a body regulating Internet standards. The serial address represents the second half of a MAC address. The number allocated by the manufacturer to the adapter.

After device registration and user registration the next phase is Mutual Authentication phase where IoT devices are authenticated with server. In this approach device will sends the MAC ID which is 48 bit length to the server to validate via gateway. The gateway plays the role of mixing the device and gateway mac by performing the 24 bit swapping. At the server end the Hybrid MAC is stored in the database which is validated against the gateway generated one. On successful validation IoT object is authenticated and an Acknowledgement is sent to device. If the device is not in the premises of the server then the NACK is sent to the gateway device stating that the device is not in the database. Figure 6 shows the mutual authentication process.

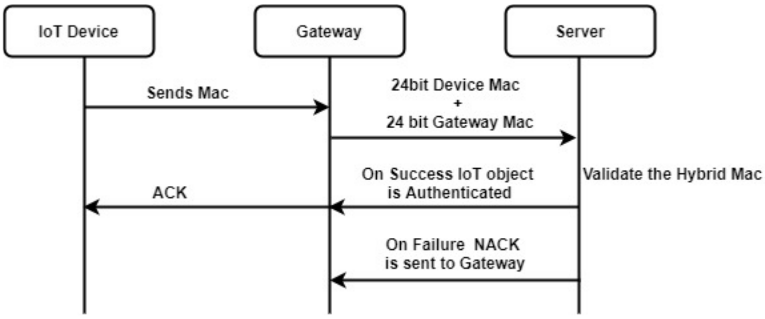

Fig. 6 : Mutual Authentication

Step 4 : Data Communication

The users register for the network once. Exchange of data will occur securely. As soon as a user wants to begin data transfer. In the method, a trigger is produced. This trigger causes the public-private key pair to be produced using the ECC process. Therefore; the device produces a random key pair for the user, which makes it more difficult for a hacker to predict key predictions. Encryption and decryption of information is performed using ECC using the key pair created by the device. Data on the sender is encrypted using the recipient's public key and the sender's private key. In order to provide mutual authentication, we use the "digital signature" concept. So, the sender applies a digital signature to the entire message while the data is being encrypted. On the receiver side, it is decrypted by merging the recipient's public key and the recipient's private key when the data is obtained. The receiver verifies for authentication with the public key of the sender r. Authentication is accomplished when both the decrypted texts match. Because no one else may decode messages, data protection is achieved and, thus, the sender is also authenticated to receive data only from the intended recipient. ECC is a public key cryptography technique focused on the algebraic structure over finite fields of elliptic curves. In contrast to non-EC cryptography, ECC enables smaller keys to provide equal protection. For key agreement, digital signatures, pseudo-random generators and other tasks, elliptic curves are applicable. The set of points that satisfy a particular mathematical equation is an elliptic curve. An elliptic curve equation looks something like this.

$$y_2 = x_3 + ax + b \tag{1}$$

where $4a^3 + 27b^2 \neq 0$

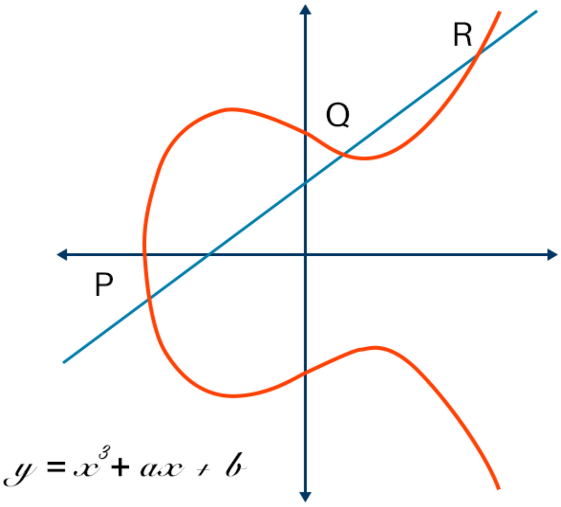

Fig. 7 : Elliptic curve

5. Results and Discussions

The proposed approach is implemented using Java Platform. ECC curve brainpoolp256r1 is used for point generation and then for generating the public and private key pair for sender and receiver. The key size reflects the maximum input length in asymmetric encryption techniques like RSA. So, for the encryption and decryption of three algorithms, AES, RSA and proposed, we have separately compared the different key sizes.

Key size in bits	AES	RSA	Proposed
6	1	0.8	0.5
25	0.85	0.5	0.30
48	1.1	0.72	0.35
102	2.5	1.2	0.68
128	0.25	0.12	0.09

Table 2 : Time taken to encrypt data in seconds

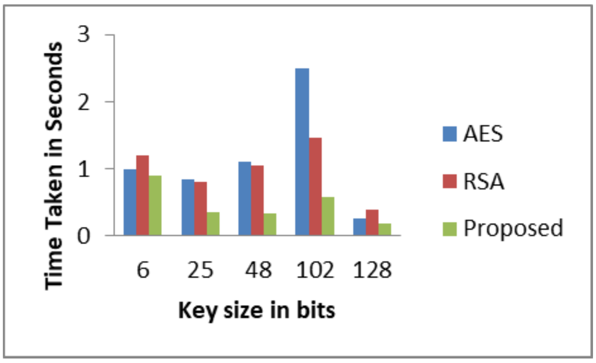

Fig. 8 : Graphical Representation of Time Taken for Encryption

Key size in bits	AES	RSA	Proposed
6	1	1.2	0.89
25	0.85	0.8	0.35
48	1.1	1.05	0.34
102	2.5	1.47	0.58
128	0.25	0.39	0.19

Table 3 : Time taken to decrypt data in seconds

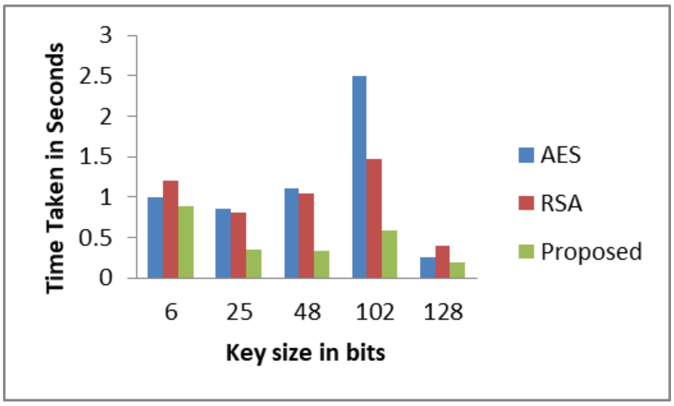

Fig. 9: Graphical Representation of Time Taken for Decryption

6. Conclusions

This paper explores an approach where Mutual authentication is accomplished to provide stronger authentication by using Hybrid MAC ID generated by IoT device and Gateway device. This approach does not allow the cryptanalyst to obtain the access to devices and to server who can alter some data in the database. Only legitimate and authenticated users are allowed to access the devices and can perform communication among them. ECC is used for authenticating and data communication between user and server whereas the Hybrid MAC is used for obtaining Mutual authentication between IoT devices and the server.

7. Acknowledgement

The authors like to thank the entire management of Dayananda Sagar College of Engg., Bangalore for all sorts of help rendered to the authors is successfully completing the manuscript.

References

1. R.S. Vairagade.; S.H. Brahmananda . (2020). Secured Multi-Tier Mutual Authentication Protocol for Secure IoT System. *2020 IEEE 9th International Conference on Communication Systems and Network Technologies* (CSNT). *Gwalior, India*. 195-200.

2. T. Afroz, M.N. Uddin Bhuiyan. M. N. Uddi. (2019). A Secure Mutual Authentication Protocol for IoT using ID Verifier Based on ECC. *2019 International Conference on Sustainable Technologies for Industry 4.0 (STI). Dhaka. Bangladesh*. 1-6.

3. M. Almulhim. N. Zaman. (2018). Proposing secure and lightweight authentication scheme for IoT based E-health applications. *2018 20th International Conference on Advanced Communication Technology* (*ICACT*). *Chuncheon*. *Korea* (*South*). 481-487.

4. J. Gowthami. N. Shanthi. (2018). Multi-factor Based User Authentication Scheme for Lightweight IoT Devices. *2018 International Conference on Intelligent Computing and Communication for Smart World* (*I2C2SW*). *Erode. India*. 89-99.

5. M. Hassan, K. Mansoor, S. Tahir, W. Iqbal. (2019). Enhanced Lightweight Cloud-assisted Mutual Authentication Scheme for Wearable Devices. *2019 International Conference on Applied and Engineering Mathematics* (*ICAEM*). *Taxila. Pakistan*. 62-67.

6. M.A. Kiran, S. Kumar Pasupuleti, R. Eswari, (2019). A Lightweight Two-factor Mutual Authentication Scheme for Cloud-based IoT. *4th International Conference and Workshops on Recent Advances and Innovations in Engineering* (*ICRAIE*). Kedah. Malaysia. 1-6.

7. C. Lin, D. He., N. Kumar, X. Huan, P. Vijayakumar, K.R. Choo. (2018). HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes. *IEEE Internet of Things Journal. 7*(2). 818-829.

8. H.N. Noura, R. Melki, A. Chehab. (2019). Secure and Lightweight Mutual Multi-Factor Authentication for IoT Communication Systems. *IEEE 90th Vehicular Technology Conference* (*VTC2019-Fall*). *Honolulu. HI. USA*. 1-7.

9. Phimphinith, X. Anping, Q. Zhu, Y. Jiang, Y. Shen. (2019). An Enhanced Mutual Authentication Scheme Based on ECDH for IoT Devices Using ESP8266. *IEEE 11th International Conference on Communication Software and Networks* (*ICCSN*). *Chongqing, China*. 490-496.

10. Sachan, D.N. Kumar, A. Adwiteeya. (2019). Light Weighted Mutual Authentication and Dynamic Key Encryption for IoT Devices Applications. *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). Ghaziabad, India*. 1-6.

11. Tewari., B.B. Gupta, A Mutual Authentication Protocol for IoT Devices Using Elliptic Curve Cryptography. (2018). *8th International Conference on Cloud Computing, Data Science & Engineering* (*Confluence*). *Noida. India*. 716-720.

12. Koblitz N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation.*

13. Miller V.S. (1999) Use of Elliptic Curves in Cryptography. *Lecture Notes in Computer Science.*