International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 3732~3738
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp3732-3738

Enhanced encryption technique for secure iot data transmission

Rupesh Bhandari[1], Kirubanand V B[2]
[1] Department of Computer Science, CHRIST (Deemed to be University), India
[2] Faculty of Computer Science Department, CHRIST (Deemed to be University), India

Article Info

Article history:

Received Dec 7, 2018
Revised Apr 5, 2019
Accepted Apr 14, 2019

Keywords:

Cipher
Cryptography
Network Security
Public Key Server
Security Attack

ABSTRACT

Internet of things is the latest booming innovation in the current period, which lets the physical entity to process and intervene with the virtual entities. As all the entities relate to each other, it generates load of data, which lacks proper security and privacy standards. Cryptography is one of the domains of Network Security, which is one such mechanism that helps the data transmission process to be secure enough over the wireless or wired channel and along with that, it provides authenticity, confidentiality, integrity of data and prevents repudiation. In this paper, we have proposed an alternate enhanced cryptographic solution combing the characteristic of symmetric, asymmetric encryption algorithms and Public Key Server. Here, the key pairs of end points (User's Device and IoT device) are generated using Elliptic Curve Cryptography and the respective public keys are registered in Public Key Server along with their unique MAC address. Thereafter, both the ends will agree on one common private secret key, which will be the base for further cryptographic process using AES algorithm. This model can be called as multi-phase protection mechanism. It will make the process of data transmission secure enough that no intermediate can tamper the data.

Corresponding Author:

Rupesh Bhandari,
Department of Computer Science,
CHRIST (Deemed to be University),
Bengaluru 560029, India.
Email: rupesh.jackson@gmail.com, rupesh.bhandari@cs.christuniversity.in

1. INTRODUCTION

The Internet of Things (IoT) is an ecosystem of small-connected computational devices, which allows things to connect, collect and transact data, making it capable of directly communicating with computerized systems. IoT has changed the meaning of Internet, making it closer to people's livelihoods. Being capable of communicating over network, they are highly prone to security attacks and securing them is quite challenging. It is very much important to have a secure model for IoT device communication or the way IoT handles the data, so that the data remains secure.

As we can see from Figure 1, which is the architecture of IoT we have three layers: Physical Layer, Network Layer and Application Layer where Physical Layer being the bottom and Application being the top. The bottom part of IoT device is sensor that is able to connect to things and collect data from it. The data being collected by sensors needs to be parsed to make it understandable hence, we will use some secure network connectivity to transfer those collected data to some end point. Application layer is the layer in which we will persist our logic, UI design, etc. [1].

Protecting information and communication through the use of codes so that only those for whom the information is intended can read and process it is called Cryptography. This is one such mechanism through which we can maintain the security at any point of time. Figure 2 indicates, two Cryptography classification: a) Symmetric Algorithm, b) Asymmetric Algorithm.

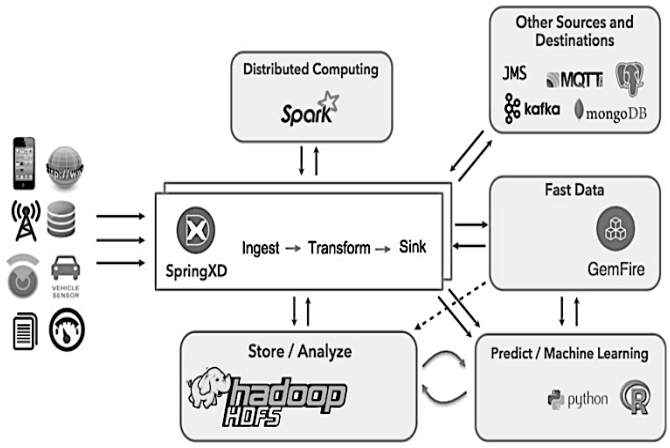

Figure 1. Simple IoT architecture

Symmetric technique utilizes one common key, which is known as Secret Key for both the encryption and deception process, while on the other side asymmetric technique use separate keys (key pairs) for encryption and deception process. The main loophole in any technique is sharing the keys. In our proposed model, we will be using features of both the techniques along with Public Key Server for key exchange mechanism.

In this paper, an enhanced encryption technique, which combines multiple encryption algorithms, Key Server mechanism is implemented for maintaining Confidentiality, Integrity and Authentication. So that the data being transmitted over internet between different nodes is safe and secure. We are dealing with IoT everyday in our life, which makes it very much important to make the communication of such devices secure enough so that no one can tamper the data.

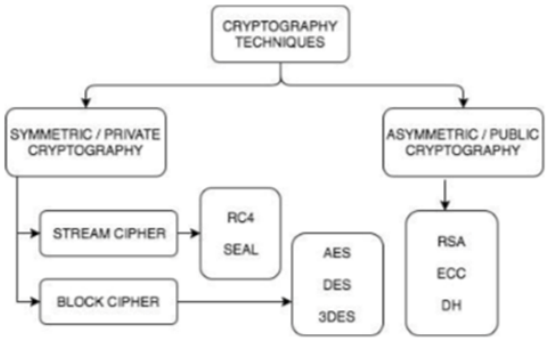

Figure 2. Different cryptography techniques

2. RELATED WORK

Usman et al. [2], this paper presents a lightweight encryption algorithm named as Secure IoT (SIT). They proposed a model in which a 64-bit block cipher requires 64-bit key to encrypt the data. The architecture of the algorithm is a mixture of festal and a uniform substitution-permutation network. This paper addresses the security of IoT along with computational power of any IoT device. Razzaq et al. [3] This paper presents the existence of different security attack and their respective countermeasures. Along with that, various security requirements or standards were stated to mitigate such attacks to some extent. Iqbal et al. [4] This paper aims to provides an overview about Internet of Things along with the major security challenges because of its exponential growth and different security primitives and solution approached are being taken to make communication secure and to protect the user's data.

Ahemd et al. [5] In this paper, the authors have evaluated the security challenge in all the layers of the IoT architecture and their respective solutions proposed. Not just that, different important security techniques like encryption are also analysed in the IoT context along with the countermeasures.

Kunchok et al. [6] Author of this paper has proposed three way secured data encryption mechanism, which compiles the features of different encryption algorithms, which makes the data being sent over network secure. Mayuri A. Bhabad, Sudhir T. Bagade [7] This paper has mainly focused on the concept of IoT, and its architecture and different possible security attacks along with suggested preventive methods and further areas of research needed.

3. BRIEF PREAMBLE TO "ENHANCED ENCRYPTION TECHNIQUE"

3.1. Public key server

Public Key Server is a server, which maintains the public keys of different entities; furthermore, it makes public keys of all the entities available in a common database where everybody can have access to it for encrypting messages to the respective entities. In our model, we have developed our own Public Key Server using Apache Web Server, which delivers the public key based on the parameter passed. Figure 3 illustrates the response from Public Key Server. Whenever the IoT boots up in the initial phase for the first time, it registers itself in the Public Key Server securely over HTTPS network by passing its Mac Address, Public Key as a parameter, so that it can communicate with network. Similarly, when User opens their app in the initial phase, a secure request is made over HTTPS to the Public Key Server for registering the User/User's Device by passing the same parameters (Mac Address of the Users device and its Public Key).


```
[
    {
        "id": "1",
        "identifier": "IOT_HOME_1",
        "mac": "b8:27:eb:d3:9f:b4",
        "keyy": "eRS9G8EE1fObRRW6mRf+bGSeluFEMiOi3UB"
    },
    {
        "id": "2",
        "identifier": "User_1",
        "mac": "00:50:56:c0:77:80",
        "keyy": "mQINBEtUTeQBEACejdGQhscmsDXM7xG2"
    }
]
```


Figure 3. Querying to a public key server

3.2. Elliptic curve cryptography (ECC)

The Public Key Server dealing with Public Keys were generated using ECC or Elliptic Curve Cryptography. ECC is an asymmetric cryptography algorithm, which is entirely computed on the algebraic complexity of elliptic curve over finite fields. Rather than implementing conventional key generation technique as the output of two primes, ECC generates Keys using the curve's degree of point. Even in blockchain implementations, ECC is used to generate Private and Public Key pairs [8].

3.3. Elliptic curve diffie hellman (ECDH)

Elliptic curve Diffie Hellman (ECDH) is a key agreement protocol that allows two entities to establish a shared key based on the public-private key pairs of both the entities generated using ECC [9].

a. Alice and Bob, both generates key Paris using ECC by taking a point on the curve using the format:
   $y^2 = x^3 + 7$
   with a prime number 'p' which is
   $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
   All the operations will be (mod p)
b. The private keys of both users are some random numbers
   d_A = Alice's Private/Secret Key
   d_B = Bob's Private/Secret Key
c. **'G'** is the greatest Point on the elliptic Curve
d. Alice's and Bob's Public key will be:
   Q_A (Alice's Public Key) = d_A x G
   Q_B (Bob's Public Key) = d_B x G

Then both Alice and Bob will exchange their public Keys with each other. And then, they both will use opponent's Public Key and their own Private Key to calculate the Shared Secret Key
SharedKey_Alice = d_A x d_B x G
SharedKey_Bob = d_B x d_A x G
Both the SharedKey will thus match. As shown in Figures 4 and 5.

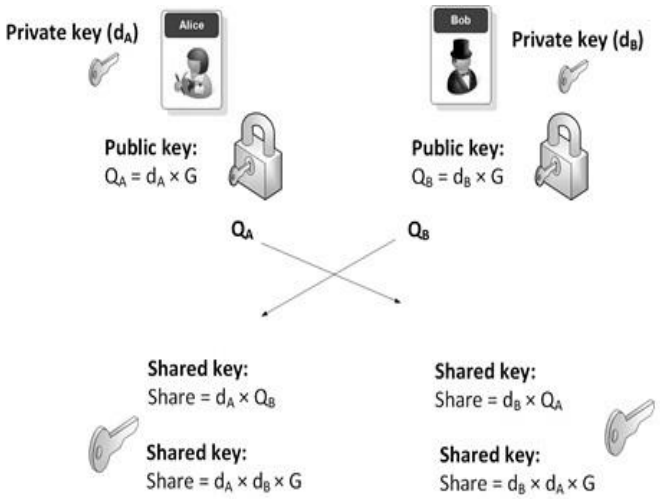

Figure 4. ECDH

```
G:      (55066263022277343669578718895168534326250603453777594175500187360389116729240L,
32670510020758816978083085130507043184471273380659243275938904335757337482424L)
P:      1157920892373161954235709850086879078532699846656405640394575840079088346716 63
-------------------------
Alice's secret key:
6359156757878328383395560871621362006330938246519612504549718472365479731016 9
Alice's public key:
(11042793526314155302899070048608746653894369623299830178364488918518012404155 0L,
69219167500104544524280470838570185624385311431120811522864460396787890152308L)
Bob's secret key:
2949976713486484224935649801295915574352180820644729944244076062301547705068 4
Bob's public key:
(62912178086549539484644020094111162335164485362423451532984730239670281197443L,
98649025411040223534878664046139560527886640300156086414596160280276828555877L)
-------------------------
Alice's shared key:
(57846323883723411284311063762993567190785463729779616806985957357768907177164L,
10532543312884879331629455085216251072617465664959240922672820874777683720578 8L)
Bob's shared key:
(57846323883723411284311063762993567190785463729779616806985957357768907177164L,
10532543312884879331629455085216251072617465664959240922672820874777683720578 8L)
-------------------------
The shared value is the x-value:
5784632388372341128431106376299356719078546372977961680698595735776890717716 4
```

Figure 5. Internal Computation of ECDH

3.4. Advanced encryption standard (AES)

The Advanced Encryption Standard is a block cipher algorithm based on symmetric key and it is a standard for best secure and classified cryptographic process. As we can see from Figure 6, AES comprises of three fixed size 128-bit block ciphers along with key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network [10].

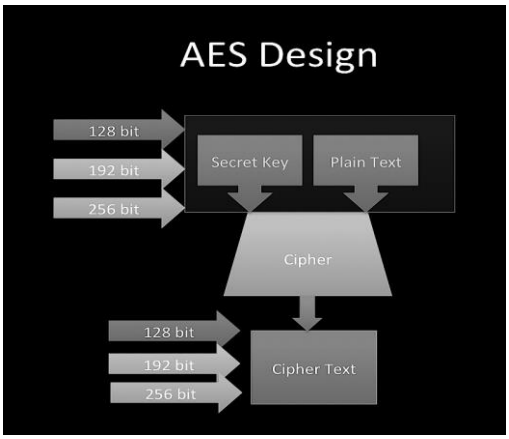

Figure 6. AES Design

4. RESULTS AND ANALYSIS

In our proposed model, we have four main key stages for secure data transmission. Our model comprises the properties of both symmetric and asymmetric algorithms along with Public Key Servers distribution technique. In symmetric cryptography, we have only one common key for both encryption process and decryption process. Having common key for both the process, Symmetric algorithm tends to be faster in the whole process as there is no key pair generation involved. On the other side, Asymmetric Cryptography have separate keys for encryption and decryption cryptographic process hence, also called Public Key Cryptography. This proposed model established a secure channel along with sub sequence cryptographic processes. Main goal is to transfer data/commands effectively and efficiently from one end (IoT) to another (User) securely while maintaining the Confidentiality, Integrity, Authentication.

Initially, entities (IoT devices, User/Users device) have to register itself in Public Key Server by passing its Public Keys, which is generated using Elliptic Curve Cryptography, Mac Address, which is unique to everyone as a parameter. If already registered then the registration process is skipped. After that, both the entities (IoT Device and User) will exchange their public keys securely with proper authentication so that no interception happens and no attacks like MITM takes place. Upon successfully exchanging the Public Keys, both entities will agree upon one common shared secret key which is computed using Elliptic curve Diffie Hellman. The Shared Secret Key will be an input to AES encryption algorithm, which will be responsible for encrypting and decrypting our commands/data being sent over network. See Figure 7.

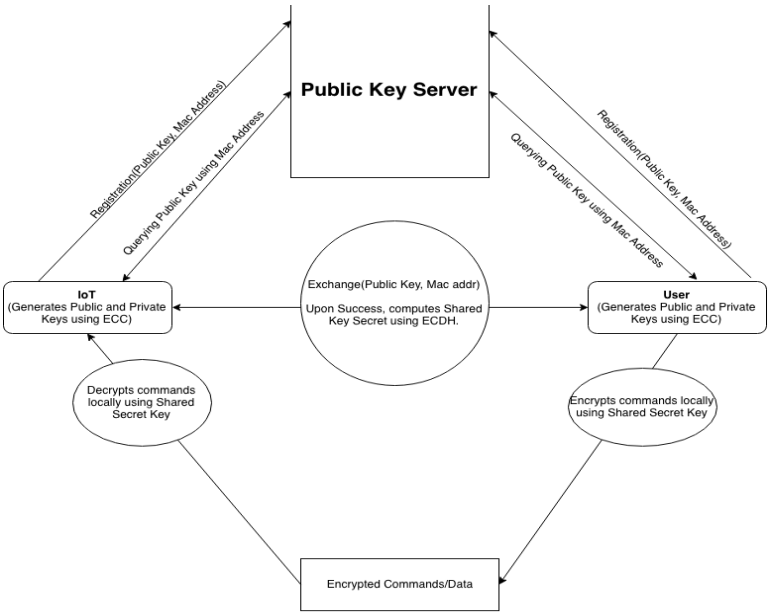

Figure 7. Proposed model

4.1. Stages to implement "enhanced encryption technique"

Every request made is over HTTPS network.

1. Alice being an IoT device and Bob being a user, will generate their key pairs using Elliptic Curve Cryptography.
2. Both the entities will then register itself in the Public Key Server securely over HTTPS network by passing their Public Keys and Mac Address as a parameter.
3. Alice and Bob will exchange their Public Keys securely over HTTPS network along with their Mac address with each other.
4. Upon receiving, Bob will query the Public Key Server Securely over HTTPS by passing Mac Address sent by Alice.
5. Public Key Server will respond with the Public Key of an entity from the public database, whose Mac Address is same as the requested one, which here will be of Alice's
6. Alice will do the same with Bob's Mac address and Public Key.
7. Now, Bob and Alice will verify if the Public Key received from opponent, party and Public Key Server are equal.
8. Upon success verification, Bob and Alice will agree on one common Shared Secret Key using each other's public Keys which they already have it now using Elliptic curve Diffie Hellman (ECDH).
9. After computation of secret key, Bob and Alice will use AES algorithm for encrypting and decrypting further communications.

5. CONCLUSION AND FUTURE WORK

Internet of Things has changed the usage of Internet by expanding the possibilities to sky limit. This proposed work concludes that the solutions provided by enhanced encryption technique, which comprise the features of symmetric, asymmetric cryptography along with Public Key Server technique for key exchange provides a better effective and efficient solution as compared with other existing models. In future, if the domain of IoT grows exponentially then this model can easily adapt the change with little modification.

ACKNOWLEDGEMENTS

This research was completed successfully under the guidance of Kirubanand V.B., Dr. Beaulah S, coordinator and Dr. Joy Paulose, H.O.D, CHRIST (Deemed to be University) as a part of Computer Science Department.

REFERENCES

[1] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswamia, "Internet of Things (IoT): Architectural Elements, and Future Directions, Future Gener," *Comput. Syst*., vol. 29, no. 7, pp. 1645-1660, Sep. 2013.

[2] Muhammad Usman, Irfan Ahmed, M. Imran Aslam, Shujaat Khan and Usman Ali Shah, SIT: "A Lightweight Encryption Algorithm for Secure Internet of Things*," International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 1, 2017.

[3] Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi and Saleem Ullah, *"*Security Issues in the Internet of Things (IoT): A Comprehensive Study*," International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 6, 2017.

[4] Muhammad A. Iqbal, Oladiran G. Olaleye & Magdy A. Bayoumi, "E Network, Web & Security," *Global Journal of Computer Science and Technology*, 2016.

[5] Wahab, Abdul & Ahmad, Omair & Muhammad, Mian & Shah, Munam, "A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT*," International Journal of Advanced Computer Science and Applications*, 8. 10.14569/IJACSA.2017.080768, 2017.

[6] Tenzin Kunchok, Prof. Kirubanand V. B, "A lightweight hybrid encryption technique to secure IoT data transmission", *International Journal of Engineering & Technology*, vol. 7, no. 2.6 , 2018

[7] Mayuri A. Bhabad, Sudhir T. Bagade, "Internet of Things: Architecture, Security Issues and Countermeasures," *International Journal of Computer Applications*, (0975 – 8887) Volume 125 – No.14, September 2015.

[8] Dragan Vidakovic and Dusko Parezanovic, *"Generating Keys in Elliptic Curve Crypto-systems," International Journal of Computer Science and Business Informatics*, Vol. 4, No. 1, August 2013.

[9] Subashri Thangavelu1 and Vaidehi Vijaykumar, "Efficient Modified Elliptic Curve Diffie-Hellman Algorithm for VoIP Net- works," *The International Arab Journal of Information Technology*, Vol. 13, No. 5, September 2016.

[10] Prasoon Raghav, Rahul Kumar, Rajat Parashar, "Securing Data in Cloud Using AES Algorithm," *IJESC*, Volume 6 Issue No. 4, ISSN 2321 3361 , 2016.

BIOGRAPHIES OF AUTHORS

Rupesh Bhandari,
Departement of Computer Science,
CHRIST (Deemed to be University),
Bengaluru 560029, India.
Email: rupesh.jackson@gmail.com, rupesh.bhandari@cs.christuniversity.in

Kirubanand V. B.,
Faculty of Computer Science Departement,
CHRIST (Deemed to be University),
Bengaluru 560029, India.
Email: kirubanand.vb@christuniversity.in