International Journal of Engineering & Technology, 7 (2.6) (2018) 236-240

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A lightweight hybrid encryption technique to secure IoT data transmission

Tenzin Kunchok[1]*, Prof. Kirubanand V. B[2]

[1] Computer Science Department, CHRIST (Deemed to be University), Student, Bangalore, India
[2]Computer Science Department, CHRIST (Deemed to be University), Professor, Bangalore, India
**Corresponding author E-mail: kunchok55@gmail.com*

Abstract

Internet of Things(IOT) is the rising innovation without bounds is required to associate billions of devices. IoT is the future where many low power resources and constrained devices are connected by means of the internet for communication, compute process and take actions in the communication network. The increased number of communication is relied upon to produce heaps of information and the security of information can be a threat resulting a secure solution for communication is necessitates among heterogenous devices. Focus of the work is to provide confidentiality, authentication and integrity of data in transit between IoT edge devices and back-end systems. This paper proposes a lightweight hybrid encryption system using ECDH key exchange mechanism for generating keys and establishing connection, digital signature for authentication, thereafter AES algorithm for encryption and decryption of user data file. The proposed combination is referred to as “three way secured data encryption mechanism” which interpret all the 3 protection schemes of authentication, info security and verification with the characteristics of lower calculation cost and faster speed makes it robust for hackers to crack the security system, thereby protective data in transmission.

Keywords: *AES; Cryptography; Digital Signature; Elliptic Curve Diffie-Hellman(ECDH); Internet of Things(IoT);*

1. Introduction

Recently, the perception of the Internet as a set of interconnected computer networks has been interchanged to a set of connected environmental things of human’s living space providing a variety of information and communication facilities revolutionized the communication way of people. The increased number of sensors in the physical objects attain the ability to communicate, the new business framework is proposed to be created by the information networks, meliorate business processes, and scale down business costs and risks. The inter-networking of physical devices, mechanical and digital machines, building, vehicles embedded with sensors and network connectivity makes the object remotely access and exchange the information is referred to Internet of Things(IoT). IoT has been revolutionary accomplishment that provides the ability to compute and communicate within devices using wireless connection such as Radio Frequency Identification(RFID) technology, Bluetooth, WLAN, WMAN, ZigBee or WiFi etc. It is being estimated that every object in the real world will be virtually endless connected producing massive amount of data throughout the network and the increased number of interconnected devices tend to produce heaps of information demand high data security.

IoT architecture is generally divided into three layers, namely perception/physical layer, network layer and application layer from bottom to top. The bottom layer is the perception layer which is the combination of physical and MAC layer in internet architecture. This layer collects the data using sensors, RFID or GPRS and transform into digital readable signals. On the other hand, Network layer transmit these digital signals received from physical layer to corresponding platforms by dividing the messages to packets and routed these packets of signals from source to destination via a connected network. The application layer is the top most layer provides service directly to the other end system and the actual deployment of intelligence of IoT is comprehended at this layer. When the data is transmitted from one layer to other layer, it is vulnerable to various attacks such as DoS attacks, Man-in-middle attack or differential attacks. This result in enforcement of information security for data integrity, confidentiality and authentication.

Cryptography is the method to camouflage data in such a way that prevents third person/intruder to read and modify the data other than sender and message receiver. It plays a crucial role for information security within applications of public networks. Cryptography is a mathematical function applied for encryption and decryption process. This process is broadly classified into two categories i) Symmetric encryption algorithm also knowns as private key cryptography and ii) public key cryptography which is asymmetric encryption technique. Symmetric Algorithm is the single key encryption that uses same key for encryption and decryption process, such algorithm is DES, IDEA, Blowfish, RC4, RC5, RC 2, 3DES and AES. To encrypt and decrypt data in asymmetric encryption method, it uses two different keys for the process, such algorithm are RSA, ElGamal and Elliptic Curve Cryptography (ECC).

However, it is often considered that data in transit is less secure which means when the data is actively moving through the internet or private network, effective data protection scheme is must. The best option is lightweight encryption method that can handle resource constraints and eliminates the implementation of full encryption on IoT devices which requires uninterrupted power, large storage capacity, larger program code size which leads to longer execution times on the constraint devices. In the paper, a lightweight hybrid encryption algorithm is implemented which accomplish CIA triad (Confidentiality, Integrity and Authentication). It is three-way secure encryption mechanism wherein ECDH is a key agreement protocol that establish a shared secret and successful exchange of cryptography keys over public network, digital signature authenticates the digital message or documents and encryption algorithm encrypts the message contents sent over the insecure channel.

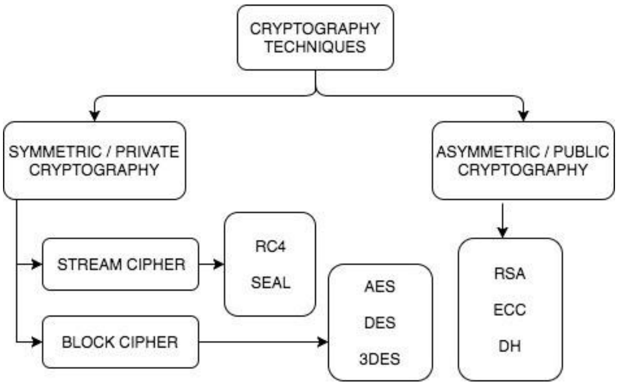

Figure 1. Cryptographic Techniques

2. Related work

Prakash Kuppuswamy and Saeed Q.Y.Al-Khalidi [1]: This paper presents the integration of two data encryption system which is known as hybrid encryption system using both public and private key algorithm. Such hybrid technique addresses the concerns of user's privacy, authentication and accuracy. Public key cryptography is based on linear block cipher and private key cryptography based on simple symmetric algorithm. The result of hybrid encryption algorithm that is the combination of linear block cipher and symmetric key takes minimum time resulting in faster execution compared with other pairs of algorithm by taking different length of messages in consideration.

B.Vinayaga Sundaram, Ramnath.M, Prasanth.M and Varsha Sundaram.J [2]: The objective of this paper is to enhance the security of smart home system includes air conditioners, water purifier, smoke detector, thermostats and lighting systems that are interconnected through IoT technologies. Encryption and hash algorithm are proposed in this paper through which IoT devices can securely exchange the data between them. In order to avoid the intruder to interpret the cipher text that is sent between devices, the encryption algorithm is used to ensure the confidentiality and hash algorithm is used to ensure the data integrity. Initial transformation, whitening key generation, sub-key generation, round function and final transformation are the main function in the proposed algorithm. The hash algorithm comprises of three major steps includes padding, compression and truncation.

Shaikh Ammarah P., Vikas Kaul, S K Narayankhedkar [3]: In this proposal, the idea is to enhance the security by combining AES and blowfish of symmetric algorithm. The strength of the algorithm(AES) is intensified by changing the S-boxes columns, and the upgraded blowfish and AES algorithm providing data confidentiality. ECDHA has been useful for key exchange, ECDSA for digital signature and MD5 is used for authentication. Performance of these algorithms are evaluated for document, image file, audio and video file on the basis of encryption and decryption process timing and throughput. Experiment results show AES is more secure than the Blowfish algorithm and the combination of these two algorithm proves to be strong and high secure against vulnerabilities.

Samiksha Sharma and Vinay Chopra [4]: The paper proposed a hybrid approach combining symmetric algorithm(AES) with ECDH algorithm that is asymmetric by nature and is an amalgamation of ECC and Diffie-Hellman i.e. anonymous key agreement protocol. ECDH helps to secure the communication for a session set up between client and server by generating key for AES which perform encryption and decryption to the digital content. Also Diffie-Hellman establishes a secret key shared between two groups that is used to exchange the cryptography keys of symmetric encryption algorithm like AES. Experimentation of proposed model is finished on the premises of various metrics like encryption and decryption time, storage, correlation and avalanche impact.

Kumar Gaurav, Pravin Goyal, Vartika Agrawal and Shwetha Lakshman Rao [5]: This paper introduced two ideas: one is to remove intermediary devices like mobiles and provide direct HTTPS connection between IoT devices and cloud for the transfer of data. The other is block chain characterised with two capabilities in IoT space i.e decentralisation and scalability. The block chain principle proved to be a good mechanism to preserve the data integrity in IoT devices and can be used to achieve decentralisation in IoT network. The idea of the proposed model is to remove dependency on intermediary devices by using direct HTTPS connection for IoT data transaction.

Neha and Mandeep Kaur [6]: In this paper, Encryption algorithm such as AES, Twofish and Blowfish algorithm are integrated to provide security to the data store in cloud. Since cloud computing is an emerging technology that provide multiple services such as unlimited storage, application development and deployment, networks, servers from anywhere and anytime. The author had proved that combination of AES and Twofish provide better output strength (less time in encryption/decryption process) when compared with the hybrid of AES and Blowfish by taking two different data files of 76kb and 103kb. Hence, the performance of Twofish algorithm is better and faster execution than Blowfish algorithm.

3. A brief preface to hybrid encryption algorithm

a) Elliptic Curve Cryptography(ECC)[7]
b) Elliptic Curve Diffie-Hellam(ECDH)[8]
c) Advance Encryption Standard(AES)[9]

a) Elliptic Curve Cryptography(ECC)[7]

ECC is an approach to a public key encryption algorithm based on the algebraic structure of elliptic curves o finite fields [7]. Through the properties of the elliptic curve equation, ECC generates keys instead of applying traditional key generation method as the result of two prime numbers. ECC algorithm proved to provide even strength of security with smaller key sizes when correlate to traditional cryptosystems such as RSA, resulting in faster computation and lower power utilization.

<u>ECC algorithm:</u>
Ec - Elliptic Curve
P - the degree of point on curve
n - prime number (max limit)

<u>Key Generation:</u>
It is a crucial part which generates two different private and public keys. The receiver's public key encrypts the message and at the same time it decrypts with private key.

X = d * P;
X = Public Key;
d = choose number 'd' with the range of (1 to n-1);

Encryption: m = message 'M' spot as 'm' on the curve 'Ec'
K = choose random integer

Ci1 and Ci2 = Two cipher text
Ci1= k * P
Ci2= m + k * X Decryption:
M= Ci2 -(d * Ci1)

b) Elliptic Curve Diffie-Hellman(ECDH) [8]

Elliptic Curve Diffie-Hellman is an alternative of the Diffie Hellman method for the elliptic curves. It is a key reconciliation protocol that establish a secret key between two communication parties using elliptic curves. It is commonly used in elliptic curve cryptosystem and ability to prevent the passive attack better. The precise steps involved to generate keys and establish a shared secret key:

1: Bob and Frank take public number P = 37, G =10

2: Bob selects a private key a = 8 and
Frank selects a private key b = 7

3: Bob and Frank calculate public values
Bob: y = (10^8 mod 37) = (100000000 mod 37)
= 26
Frank: z = (10^7 mod 37) = (10000000 mod 37)
= 10

4: Bob and Frank interchange public numbers

5: Bob gets public key y =10 and
Frank gets public key z = 26

6: Bob and Frank calculate symmetric keys
Bob: ka = y^a mod p = 100000000 mod 37 = 26
Frank: kb = z^b mod p = 8031810176 mod 31 = 26

7: Shared secret key is 26.

c) Advance Encryption Standard(AES) [9]

AES is a symmetric block cipher comprises 128 bits block length. The standard comprises 3 different key lengths: 128 bits, 192 bits and 256 bits. The encryption step uses a key that converts the data into an unreadable ciphertext, and then the decryption process uses the same key to convert the ciphertext back into the original data [10]. It uses a single key for both encryption and decryption rather than two different keys as asymmetric key. In AES algorithm, the number of round is determined by the length of the cipher key i.e. 10 rounds of repetition for 128-bit keys, 12 cycles for 192-bit keys and 14 cycles for 256-bit keys. The four rounds of transformation include one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The precise steps involved in encryption and decryption algorithm:

Sub Bytes: It implements the substitution of a non-linear function, using look-up table method to replace the corresponding byte per byte.

Shift Rows: In the matrix of each column to the left of each byte cyclic displacement, displacement is increasing with the number of rows.

Mix Columns: This step combines the four bytes of each column of matrix using invertible linear transformation.

Add Round Key—By using key schedule, cipher key generates each round key and it is combined with each byte of the matrix.

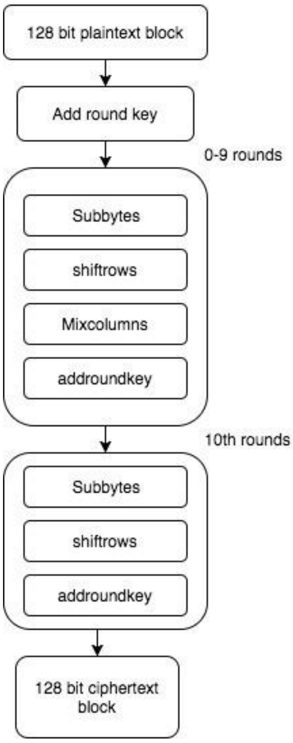

Figure 2. AES encryption

4. Proposed system

In the proposed architecture, three-way protection scheme is achieved by using hybrid encryption mechanism that provides the advantages of symmetric and asymmetric key performance. In symmetric encryption algorithms, the cryptography keys are the string of bits that helps in transforming the plaintext into unreadable(cipher) text for encryption and vice versa for decryption. Asymmetric/public key cryptography, is any cryptography system that uses pair of keys for encryption and decryption process. The keys are nonidentical and one key that is share with everyone is a public key. The proposed solution might not establish a secure communication path, but it helps improvise the strength of the cryptographic process and security. The aim is to use efficient technique to encrypt and decrypt plain text and keep information safe, secure from unwanted user interaction.

Initially ECDH is a key agreement protocol establish secret key between two communication parties that exchange data over public networks. Then the message is authenticated using digital signature. It is an approach that guarantees the contents of a message have not been modified in transit over insecure channel. Thereafter, AES algorithm is applied to encrypt and decrypt the user's data file. To provide effective data protection measures for in transit data and avoid data modification, all this is implemented to provide trusted computing environment. The proposed model work through two main stages which are key generation and exchange with ECDH, and message content signature and verification with Digital signature.

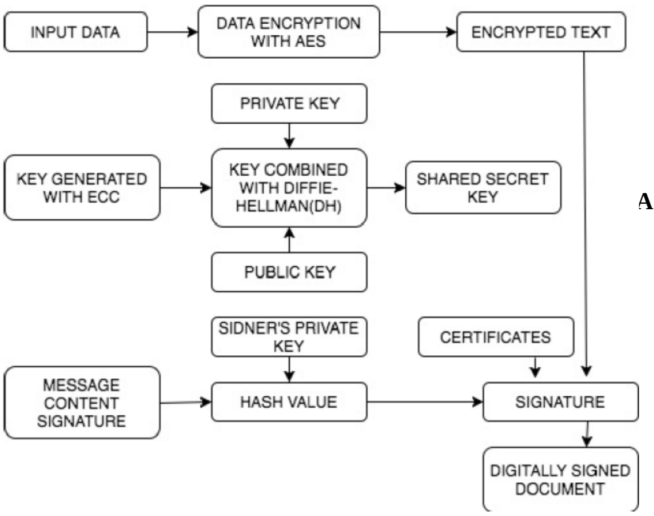

Figure 3. Proposed model

4.1 Stage 1: Key generation and exchange

Suppose two communicating parties Bob and Frank, wants to exchange information securely over public network so that interpreter can interrupt them but may not decode the data.

1. First, Bob and Frank generate their own public and private key.
   Bob's private key 'bPr' and public key 'bPu' = bPrG;
   Frank's private key 'fPr' and public key 'fPu' = fPrG; G is the base point that generates subgroup on the elliptic curve.

2. Bob and Frank exchange their public keys 'bPu' and 'fPu' over public networks.
   The intruder can interpret their public keys but cannot touch private keys 'bPr' and 'fPr' without solving the mathematical logarithm problem.

3. Bob and Frank find their shared secret key S by calculating with their own private key and other parties public key.
   Bob's Secret Key S= bPr fPu;
   Frank's Secret Key S= fPr bPu;
   Bob and Frank hold same secret key S = bPr fPu = bPr(fPrG) = fPr(bPrG) = fPr bPu;

   Below are the computation of Bob and Frank public/private keys, and their shared secret key over elliptic curve using
   secp256k1, a Koblitz curve from SECG

Curve: secp256k1
Bob's private key:
0xf8e0ca324ee2f8719a89dfab7c04e6d1bf54a38c35336197e5a
957f09031d2d4
Bob's public key:
(0x525b73fd949508b5f4f66612974069c4e06ebbf334e8d8004e68
471fcd4a5bb1,
0x9e8324e8d2f025bc627916a149f5ab055e6d20506d0e0ee736
a713c6fd58dabf)

Frank's private key:
0x75cbb6d48faa417342b6873a53d29227fddbf56d5a0858346
0480a3ae504e652
Frank's public key:
(0x3c8947fd1adde6fb79bc896cec1b38cc559116486dc8d082f
7b7d23c0347ed8b,
0xe3314117c999c0cf800b93bbb33befc7276600d0026f939dff
26c26ce5e13c7a)

Shared secret:
(0x2850da8d1c823bc3548dfbdbd13af55eabdf520edf5e508a0d
9198cf3d93c1e0,
0x2615448ee7bf3ad321bf7550377a9e8ebe88741c307708bb7c607
1539f36259f)

A. 4.2 Stage 2: Authentication using digital signature (ECDSA)

Suppose Bob has signed the message with his private key(bPr) and he wanted to certify the message signature using Frank's public key. Digital signature basically does not sign on message but rather it takes the hash of the message. It takes the hash value from the data by applying the mathematical function or hashing algorithm. That hash value with the certificate is a signature to the message.

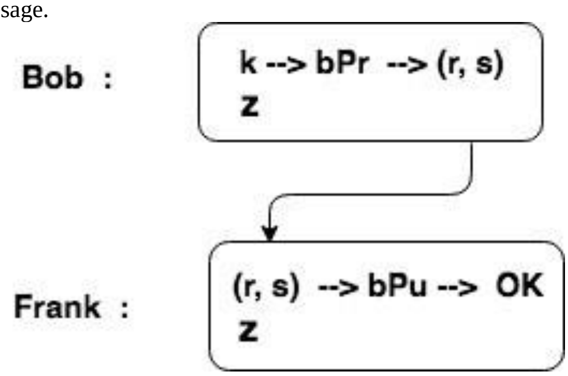

Figure 4. Signing and verification

Bob used his private key 'bPr' and random integer k to sign the hash value. By using Frank's public key 'fPu' Bob verified the message is signed correctly and allowed to send.

Curve: secp256k1
Private key:
0x6212a090a08d47e7e17354a57ba2e5c5b338819cebea51674
4978b3a217a7e76
Public key:
(0x1cfd0752316066ef46cfcb9a486964fa114c84afd8a9680aa0
bff0b067aed2bc,
0x461ec76a5163797fb93f5fe6ab6b5c647b61f1b2e8146bc198
cd82a537579872)

Message: 'halloween'
Signature:
(0x8ab4b50a81a5eacfbd345ce21ade99807647a10776f8fe0233
09305a6a54ad28,
0x41d70340e9736e2ed842d9520dd9d7ad2324b2f6cf064112d
35db7a5bca37da)
Verification: Signature matches

Message: 'Christmas'
Verification: Invalid signature

Message: 'halloween'
Public key:
(0x5992a4f9d86a7708ee6a33b456963fcc220c2151cd03f9311
8651d4e1aad7a10,
0xc423938b8df789df698f751ee696a4b22fdaf86a48ca241262
7174ab3b08c2b5)
Verification: Invalid signature

Initially the message (halloween) has been signed and verified the signature. Then, using same signature, it tries to verify the message (Christmas) and verification fails. Thereafter, using some random public key and verify the signature against the same correct message, the verification fails. This is how digital signature helps to authenticate the digital message, non-repudiation of sender and integrity of data.

5. Conclusion and future work

Internet of things is the emerging technology in the present era which allows the real-world object to compute and communicate with the virtual object. Since all the objects are interconnected, it produces a heap of data that lack behind with security and privacy of data. Cryptography is an approach that helps the data to be transmitted securely over the wireless medium and provide authentication, confidentiality, data integrity and non-repudiation. This paper proposed alternate lightweight cryptography solution combing the characteristic of symmetric and asymmetric encryption algorithm. The AES encryption algorithm is used for encryption and decryption of the data along with the use of ECDH which provide a secure channel for communication establishing secret key. This proposed model provides the flow of security for data in transit from IoT edge devices to back-end system. It accomplishes three major protection schemes of data security i.e. confidentiality, integrity and authentication. Future work will be to implement this hybrid approach in IoT real-time application and check the strength of proposed hybrid algorithm.

Acknowledgement

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

References

[1] Prakash Kuppuswamy and Saeed Q.Y.Al-Khalidi, Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm, 2014 Department of Management Information Systems, College of Commerce Vol. 19, No. 2, March (2014), pp. 1-13

[2] B.Vinayaga Sundaram,Ramnath.M, Prasanth.M and Varsha Sundaram.J, Encryption and Hash based security in Internet of Things, 3rd International Conference on Signal Processing, Communication and networking(ICSCN) 2015

[3] Shaikh Ammarah P., Vikas Kaul, S K Narayankhedkar, Security Enhancement Algorithm for Data Transmission using Elliptic Curve Diffie - Hellman Key Exchange, International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868, Foundation of Computer Science FCS, New York, USA

[4] Samiksha Sharma and Vinay Chopra, Data Encryption using Elliptic Curve Diffie-Hellman, International journal of Security and its Applications, Vol.11, No.3(2017), pp. 17-28

[5] Kumar Gaurav, Pravin Goyal, Vartika Agarwal and Shwetha Lakshmi Rao, IoT Transaction Security, 2015, 5th International Conference on the Internet of Things(IoT)

[6] Neha and Mandeep Kaur, “Enhanced Security using Hybrid Encryption Algorithm,” International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 7, July 2016

[7] Pedro Maat c. Massolina, Paulo S.L.M.Barreto, Wilson V.Ruggiero, Optimized and Scalable Co-Processor for McEliece with Binary Goppa Codes”, ACM Transactions on Embedded Computing Systems (TECS) - Special Issue on Embedded Platforms for Crypto and Regular Papers, Volume 14 Issue 3, May 2015

[8] Subashri Thangavelu1 and Vaidehi Vijaykumar2, Efficient Modified Elliptic Curve Diffie-Hellman Algorithm for VoIP Networks, The International Arab Journal of Information Technology, Vol. 13, No. 5, September 2016

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

[10] Fei Shao, Zinan Chang, Yi Zhang, AES Encryption Algorithm based on the High-Performance Computing of GPU, 2010 Second International Conference on Communication Software and Networks