An Optimal Multilevel Encryption Technique for Securing the Data Transmission in IoT

Ananya Roy, Prodipto Das, Rajib Das

Abstract*: *Internet of Things(IoT) is playing a pivotal role in our daily life as well as in various fields like Health, agriculture, industries etc. In the go, the data in the various IoT applications will be easily available to the physical dominion and thus the process of ensuringthe security of the data will be a major concern. For the extensive implementation of the numerous applications of IoT , the data security is a critical component. In our work, we have developed an encryption technique to secure the data of IoT. With the help of Merkle-Hellman encryption the data collected from the various IoT devices are first of all encrypted and then the secret message is generated with the help of Elliptic Curve Cryptography.

Keywords* : *Elliptic curve cryptography, Merkle-Hellman encryption.

I. INTRODUCTION

In today's world, IoT is a fast growing technology. Various objects like printer, cooler, phone etc are all considered as smart objects as IoT has enabled them to communicate with one another. According to [1], IoT is a network where various smart objects have the capacity of communicating among themselves, thereby also performing various computation. In the dynamic network of IoT, the physical objects are integrated into the network system. This global network is self-configuring which follow the standard protocols [2]. The data from the sensors or RFID etc are very important for the IoT. This data is being shared with other wireless components which are part of the network as in an health care system the data from the various hospitals are shared in the global network. In case of a location monitoring system, the location details collected with the help of sensors are shared globally. And at this point the crucial thing is the security of the data. How to protect this data? Also this task is very challenging. For effective and secured communication, the security needs to be improved. To safeguard the profound information cryptography is an effective approach. In this paper, we have used the Merkle-Hellman Knapsack cryptosystem and ECC. For better level of security and smaller key length, elliptic curve is used[3]. In the Merkle Hellman Knapsack system, subset problem is created which makes the calculation modest and effectual [4].

Revised Manuscript Received on February 04, 2020.
***** Correspondence Author
Ananya Roy*, Department of Computer Science, Assam University, Silchar Assam, India. Email: ananyaroykxj@gmail.com
Prodipto Das, Department of Computer Science, Assam University, Silchar Assam, India. Email: prodiptodas@gmail.com
Rajib Das, Department of Computer Science and Application, Karimganj College, Karimganj Assam, India. Email: rajibdas76@gmail.com

II. CORRELATED WORKS

An encryption method based concept of RSA and using erkle-Hellman knapsack cryptosystem was suggested by Ashish Agarwal [4]. With the help of a mathematical model, the proposed work was proved to be a secure one. In this approach two algorithms were used to encode the message.

The Elliptic Curve Cryptography based safety structure for Internet of Things and Cloud Computing was proposed by T.Daisy Premila Bai.[5]. This paper focuses on card level security which is considered to be the major element in securing the entirety of the IoT. In this paper, we find the security construction based on ECC for various IoT Applications using smart card which proved to be a secured application.

The encryption of text by Elliptic Curve Integrated Encryption Scheme was proposed by D R Susantio et al. [6]. For the various IoT applications, Elliptic Curve Cryptography provides better security. The text we decide to encrypt is divided into chunks and then begin the process execution.

The Elliptic curve cryptography algorithm was discussed by Keerthi K et al. [7] and then they proposed a new way to augment ECC by dipping its calculating time and cost. They used ASCII values instead of plotting characters to points. Their work proved to give better performance after implementing when made to compare with other works.

III. PROPOSED METHODOLOGY

In this approach, a multilevel encryption system (Merkle-Hellman Knapsack cryptosystem with Elliptic Curve Cryptography) is used. The resolution of the proposed system is too safe the information collected from the various sensors.

Fig.1 shows the proposed approach. Protocols such as CoAP and HTTP are used to send the data collected from the various sensors or IoT devices to the gateway. After the collection of data by the gateway, the next task is to transmit it to the server, but before that the data is encrypted using the multilevel encryption technique.

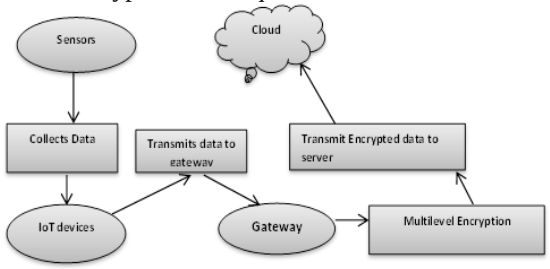

Fig 1: Block Diagram of Proposed Model

Retrieval Number: C5355029320 /2020©BEIESP
DOI: 10.35940/ijeat.C5355.029320

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

A. **ECC (Elliptic Curve Cryptosystem)**

Elliptic curve equation is

$$y^2=x^3+ ax + b \ldots\ldots\ldots\ldots \quad (1)$$

Elliptic curves were proposed by Neal Koblitz[8] and Victor Miller[9] with a strategy to propose public key cryptographic systems. It helps to elucidate the main concern of public key cryptography. The public key cryptography method used for data encryption is Elliptic Curve Cryptography (ECC)
By using the following equation,

$$E: y^2 = x^3 + ax + b \pmod p \ldots. \quad (2)$$

Over Fp (where p is a prime no) the E is calculated.
After this, we choose two non-negative integers a, b(less than p) to fulfill the condition

$$4a^3 + 27b^2 \pmod p \neq 0 \ldots\ldots \quad (3)$$

Tasks of ECC

a) Point Inverse

On the elliptic curve if C (a_1, b_1) is a point, then the inverse of the point is calculated as –C(x_1, y_1). The equation used to calculate the inverse 7] is

$$-C(x_1, y_1) = C(x_1,p-y_1) \ldots\ldots \quad (4)$$

b) Point Addition

Let R(x_1, y_1) and S(x_2,y_2) be two points and are dissimilar (R≠S), then R+S is given by

$$R(x_1, y_{1)} + S(x_2, y_2) = T(x_{3,} y_3)\ldots.. \quad (I)$$

$$x_3= (\lambda^2- x_1- x_{2)} \bmod p\ldots\ldots\ldots \quad (5)$$

$$y_3= (\lambda (x_1- x_3) - y_1) \bmod p\ldots\ldots \quad (6)$$

Where

$$\lambda=\frac{(y_2-y_1)}{(x_2-x_1)} \bmod p$$

c) Point Doubling

This is also an arithmetic operation. When the points P(x_1, y_1) and Q(x_1, y_1) intersect, then 2P is given by the following formula [7].

$$x_3= (\lambda_2- 2x_1) \bmod p\ldots\ldots\ldots... \quad (7)$$

$$y_3 = (\lambda (x_1-x_3) - y_1) \bmod p\ldots \quad (8)$$

Where

$$\lambda = \frac{(3x_1^2+a)}{2y_1} \quad \bmod p$$

d) Scalar Multiplication

Let us consider P to be any point on the elliptic curve. The multiply action on P is defined by continuous addition

$$sP= P+P+P+\ldots..s \text{ times}\ldots\ldots\ldots \quad (9)$$

Let us take an example:
Let the values of a and b be 1 & also let p be 11 for the curve F_p
Putting this values in equation 1, we get

$$y^2= x^3 +x +1 \pmod{11}$$

The set of solutions are E= {(1,10), (1,1), (3,5), (3,6), (4,2), (4,9), (6,4), (6,7), (8,3), (8,8), O}

The point addition is calculated as

For the points, P = (2, 2) & Q= (6,6)

$$\lambda= (6-2)/ (6-2) \bmod 11=1$$

$$P+Q= (2, 2) + (8, 8)$$

$$x_3=(1^2 -2- 6) \bmod 11=4$$

$$y_3= (1(2-4)-2) \bmod 11=7$$

Thus,

$$P + Q = (2, 2) + (8,8) = (4,7)$$

Let point P be (6, 6), then the doubling operation is.

$$\lambda = (3 * 6^2 +1)/ (2 * 6) \bmod 11$$
$$= (108/12) \bmod 11$$
$$= 9$$

$$x_3=(9^2 – 2 * 6) \bmod 11=69 \bmod 11=3$$

$$y_3= (9(6-3)-6) \bmod 11=10$$

$$2P= (6,6) + (6,6)=(3,10)$$

The result of point addition and point doubling is (4, 7) and (3,10), because the elliptic curve points are in Abelian group. The steps for *Elliptic* Curve Cryptosystem are as below: Here the sender and the receiver agree to a point to refer openly or public data.

For this following three steps are needed

i. The values of a, b and p(prime no) is considered
ii. From the equation of elliptic curve the points are intended.
iii. From the computed points, a point B (base point) is taken.

Public and private key pairs are generated by each user following the steps as given:

i. For private key generation (d), from the values[1, p-1] an integer is chosen
ii. For public key generation (Q): it is Q= d(private key) * B(Base point)

B. Proposed Algorithm

Process for generation of key

Step 1: First of all the sender and the receiver settle with the base point B
Step 2: Then the public key is computed as public key Q = d (private key) * B

For the encryption part

Step 1: We select a elliptic curve Ep (a, b) having N points
Step 2: Then the plain text is represented on the curve
Step 3: We arbitrarily select ‘d’ from [1-(n-1)]
Step 4: The message ‘m’ has the point ‘M’ on the curve ‘E’
Step 5: Lastly two cipher texts are produced C1 = d*P, C2 = M + d*Q

C. Merkle Hellman Knapsack Cryptosystem outline

With the help of flexible multiplication and a permutation, it easily solves the super increasing subset sum problem [10]. The super increasing vector is represented by v and using multiplication and permutation super increasing order is hidden by vector v_1. The message is decrypted by the super increasing vector which develops the private key.

i. Order of Super increasing: It is a sequence (a1, a2, a3,….an) of positive integers
Such that $a_i > \sum_{j=1}^{i-1} b_j$ for each i, $2 \le i \le n$.

D. Multilevel Encryption Technique

The encryption is performed in two steps in the proposed technique.

Step 1: First of all, the text to be encrypted is split by individual characters and then it is converted to their corresponding binary values. With the help of Merkle-Hellman encryption, the binary values are encrypted. The main purpose is to generate a subset problem. The Merkle-Hellman process is as below:

Phase 1: A sequence like s= (s1,s2,s3,…..sn) is considered. Each no is added to its preceding no. And we chose the next no to be greater than the sum of the previous nos..

Phase 2: Than the binary value (bn) of the plain texts characters are found.
Phase 3: An integer a is chosen which is greater than than s (sequence) and its co-prime (r).

Phase 4: The private key is formed by a, the co-prime r and the sequence s.

Phase 5: Then all the numbers in s is multiplied with r. With the result modulus is taken by dividing with a.

$$p_i = s_i \; r \bmod(a)$$

Phase 6: In the final stage, we multiply each number in sequence p with bn(binary value) and then add them.

$$\sum_{i=0}^{n} p_i * bn_i$$

Step 2: In the second step , the characters which were encrypted in the previous step are again encrypted using ECC. It is done for generating the cipher text of the outcome given by Merkle-Hellman . The process of ECC is as follows:

Following this process the data can be shared between various recipients securely. The mathematical technique of the projected work is given below. In our projected work, both ECC and Merkle-Hellman knapsack cryptosystem is used.

IV. PROPOSED MATHEMATICAL TECHNIQUE

For example – Encrypting the string “air”

a) First of all, by using the Merkle Hellman knapsack cryptosystem the string is encrypted .

Step 1: We choose a super cumulative sequence.
Here, the sequence is s = 2, 4, 8, 16, 32, 64, 128

Step 2: The binary equivalent of the characters of the given string is calculated.
Each character is converted into their ASCII value and then their equivalent binary value is found.
a = 1 1 0 0 0 0 1
i = 1 1 0 1 0 0 1
r = 1 1 1 0 0 1 0

bn = (bn1, bn2 , … bn(n) - the binary order
Step 3: We assume the value of a and its co-prime r
Let a = 670 (higher than the sum of all values in the order s)
Co-prime r = 11
Step 4: We find the sequence p = (p1, p2, ….. pn). where pi = si* r mod (a)
$p_1 = 2 * 11 \bmod 670 = 22$
$p_2 = 4 * 11 \bmod 670 = 44$
$p_3 = 8 * 11 \bmod 670 = 88$
$p_4 = 16 * 11 \bmod 670 = 176$
$p_5 = 32 * 11 \bmod 670 = 352$
$p_6 = 64 * 11 \bmod 670 = 34$
$p_7 = 128 * 11 \bmod 670 = 68$
Step 5: We encrypt the message M=‘air’

$$\sum_{i=0}^{n} p_i * bn_i$$

(i) Character – ‘a’
p = (22, 44, 88, 176, 352, 34, 68) and
bn = (1 1 0 0 0 0 1)
Ma= 22+44+0+0+0+0+68 = 134

(ii) Character – ‘i’
p = (22, 44, 88, 176, 352, 34, 68) and
bn = (1 1 0 1 0 0 1)
Mi = 22 +44+0+176+0+0+68 = 310

(iii) Character – ‘r’
p = (22, 44, 88, 176, 352, 34, 68) and
bn = (1 1 1 0 0 1 0)
Mr = 22+44+88+0+0+34+0 = 188

b) Secondly, using Elliptic Curve Cryptography the cipher text is encoded again

Let us take message ‘m’ = “cipher text of Merkle-Hellman algorithm”
Step 1: Let us take m = 134 (cipher text of ‘a’)
Step 2: Let d = 11
Step 3: Public Key Q = d * P
Here, Base point B = 112 (sender and receiver agree to have common base point)and Public Key Q = 11 * 112 = 1232

Step 4: The point M has to be represented on the curve E. Here, let us consider M=226.
Step 5: Cipher text:

C1 = d* P = 11 * 112 = 1232
C2= M + d*Q=226 +11*1232=13778

V. RESULT ANALYSIS

We have done the implementation using C.
Table 1 below shows comparison of elliptic curves encryption with other algorithms.

Table 1: Comparison Table

Methods	Words count	Encryption Time	Decryption time
Proposed Method	409 words	0.075 seconds	0.11 seconds
RSA	512 words	1.35 seconds	1.86 seconds
NIST curves	512 words	2.3 seconds	2.15 seconds
Reference[7]	409 words	0.20 seconds	0.30 seconds
Reference [11]	1 word	1.95 seconds	0.83 seconds

VI. CONCLUSION

The main objective of our approach is to increase the safety of the data that are collected from the IoT devices. For this, the multilevel encryption is used. Before the data are stored in the cloud server, the data is encrypted. In two phases, the data is encrypted. In the first phase, the data is encrypted using Merkle-Hellman knapsack cryptosystem and in the second phase, this encoded data is used as an input for ECC. After comparing our results with the previous work done, we can conclude that our proposed algorithm takes less time for performing the encryption and then the decryption. So, this approach can be used in generation of cipher texts in all future works.

REFERENCES

1. Isha and Ashish Kr. Luhach, "Analysis of Lightweight Cryptographic Solutions for Internet of Things", Indian Journal of Science and Technology, 2016, ISSN: 0974-6846, Vol. 9. Iss.28, pp. 1-7.
2. P. Nandhini and Dr.V.Vanitha, "A Study of Lightweight Cryptographic Algorithms for IoT", International Journal of Innovations and Advancement in Computer Science, 2017, ISSN: 2347-8616, Vol.6, Iss.1, pp. 26-35.
3. S.D.Pingle, "A Survey of Latest Trends in Cryptography and Elliptic Curve Cryptography", International Journal of Scientific Research and Education, 2016, ISSN: 2321-7574, Vol.4, Iss.5, pp. 5294-5301.
4. Ashish Agarwal, "Encrypting Messages using the Merkle-Hellman Knapsack Cryptosystem", International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011.
5. T.Daisy Premila Bai , "ECC based Security Architecture for IoT Cloud Integrated Smart Applications", International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 13,Number 24(2018), pp. 16812 -16818.
6. D R Susantio, I Muchtadi-Alamsyah, " Implementation of Elliptic Curve Cryptography in Binary Field ", Journal of Physics: Conference Series **710** (2016) 012022.
7. Keerthi K and Dr.B.Surendiran, "Elliptic Curve Cryptography for Secured Text Encryption", 2017 International Conference on circuits Power and Computing Technologies [ICCPCT], 978.- 1- 5090-4967-7/17/$31.00 © 2017 IEEE.
8. Koblitz. N, "Elliptic Curve Cryptosystems", Mathematics of Computation, 1987, Vol. 48, Iss. 177, pp. 203-209.
9. Miller. V, "Use of Elliptic Curves in Cryptography", CRYPTO'85, Springer-Verlag, 1986, pp.417-426.
10. Alfred J.Menezes, Paul C.van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography",Massachusetts Institute of Technology, 1996.
11. S.Maria Celestin Vigila and K. Muneeswaran, Implementation of Text based Cryptosystem using Elliptic Curve Cryptography, *International Conference on Advanced Computing, IEEE*, pp. 82–85, December (2009)

AUTHORS PROFILE

Ananya Roy, is presently working as an Assistant Professor in the Department of Computer Science And Application, Karimganj College, Karimganj, Assam, India. She is also a research scholar in the Department of computer Science, Assam University, Silchar. She has received her MCA degree from IGNOU, New Delhi. Her area of interest is Internet of Things.

Prodipto Das, is presently working as an Assistant Professor in the Department of Computer Science, Assam University. He has completed his M.Sc and Ph.D from Assam University. He has published numerous papers in various National and International Journals.

Rajib Das, is presently working as an HOD in the Department Of Computer Science And Application in Karimganj College, Karimganj, Assam. He has done his MCA from IGNOU, New Delhi. He has completed his Ph.D in Mobile Ad-Hoc Network from Assam University, Silchar. He has published numerous papers in various National and International Journals.