DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.4959

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ENHANCING THE SECURITY OF IOT DATA USING MULTILEVEL ENCRYPTION

A.Vithya Vijayalakshmi
Ph.D. Scholar, Department of Computer Science,
St. Joseph's College (Autonomous), Tiruchirappalli – 2.

Dr. L. Arockiam
Associate Professor, Department of Computer Science,
St. Joseph's College (Autonomous), Tiruchirappalli – 2.

Abstract: Internet of Things (IoT) plays a vital role in the field of Information Technology, Industries and Healthcare etc. As data in IoT applications will be related to the physical realm, ensuring data security is a primary constraint for many cases. Because in the IoT context not only users, but also authorized objects may access data.Security represents a critical component for enabling the widespread adoption of IoT technologies and applications. Therefore this paper proposes a multilevel encryption technique to enhance the security of the IoT data. In this approach the data sensed from the IoT devices are encrypted in the gateway using Merkle-Hellman encryption and Elliptic Curve Cryptography(ECC) to ensure the security of the data.

Keywords: Internet of Things, Data Security, ECC, Merkle-Hellman Cryptosystem

I. INTRODUCTION

Internet of Things (IoT) is a newer technology in this fastest world. Any physical objects like phone, laptop, refrigerator, printer, air cooler etc. are considered as smart things. "IoT can be defined as a network of uniquely identifiable, accessible, and manageable smart things that are capable of performing communication, computation and ultimate decision making"[1]. "It is aunified part of Future Internet and could be defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributed, use intelligent interfaces, and are seamlessly integrated into the information network" [2].

IoT requires components to enable communication between devices such as wireless connections like Sensors, RFID, Bluetooth, ZigBee,WSN, WLAN, WMAN or Wi-Fi.Sensor data is an essential part ofIoT system, and it sharesdata to third parties to avail usefulservices and applications like, locationbasedservices, smart home management and elderly monitoring etc.IoT data properties generate many data management issues such as scalability of data, interoperability, accessing data, data archiving etc. IoT data storage can be local, distributed and centralized. Here, data security is extremely challengingdue to the different data properties.

Providing data security to the streaming or sensed data is a major issue in IoT. In order to use device communication effectively, we need to improve the security. Cryptography is an effective way to protect the sensitive information. This paper proposes a multilevel encryption for IoT data using Merkle-Hellman Knapsack cryptosystem and ECC. ECC is well-suited for IoT applications that need long-term security requirements. Also, Elliptic curves offers high level of security andsmaller the key length [3]. Subset problem is created in Merkle Hellman knapsack cryptosystem to encrypt the data. Hence, the computation is very simple and efficient [4].

II. RELATED WORKS

Daisy Premila Bai et al. [9] proposed Elliptic Curve Cryptography based security framework for Internet of Things and Cloud Computing.This model adopted multifactor authentication which worked in seven phases. The proposed model gives data security againstsome of the major security issues such as integrity, confidentiality, privacy and authentication. The proposed framework were implemented and proved that it enhances security. Arghya Rai et al [4] proposed an encryption technique using Merkle-Hellman knapsack cryptosystem and discrete logarithms based on RSA concepts. The basic needs for cryptography were discussed in this paper. Two algorithms were used to encrypt amessage and strengthened the security of the data.Finally the proposed method was proved to be secure with mathematical model.

Mailov Arif et al. [10] discussed various cryptographic algorithms used for data encryption. Elliptic Curve Cryptography offers high security for IoT applications. The authors compared many Elliptical curvesand their key lengths and key generation timesfor securing e-ID.ECC algorithm was implemented in Azerbaijan E-ID Card and proved that ECC in e-ID production gave high performance and greater security than RSA algorithm.Laiphrakpam et al. [7] discussed Elliptic curve cryptography algorithm and proposed a new technique to enhance ECC by reducing its computational cost and time. They removed mapping of characters to affine points and replaced by using ASCII values. They proved by implementing the proposed work that gave better security when compared with other algorithms.

III. PROPOSED WORK

In this approach, a multilevel encryption technique (Merkle-Hellman Knapsack cryptosystem with Elliptic Curve Cryptography) is used. The purpose of the proposed technique is to secure the data sensed from the IoT devices.

Figure. 3 shows the system model of the proposed approach.Data from the IoT devices will be sent to the gateway using protocols such as CoAP and HTTP across the internet. Once data is received by the gateway, it is prepared for transmission to the server. Before the data being transmitted to the server, they are encrypted using multilevel encryption technique.

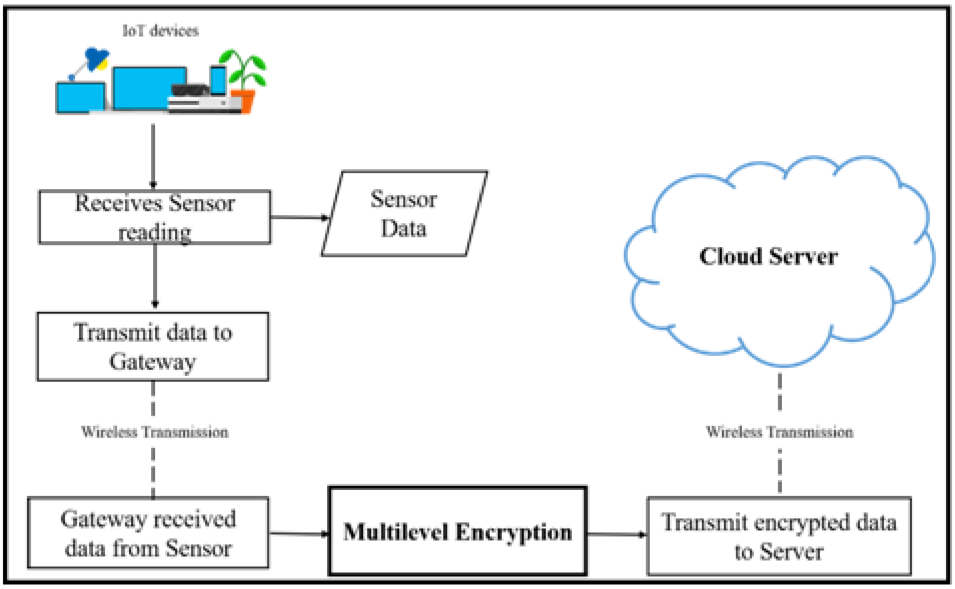

Figure.1. System Model of Proposed Approach

A. Elliptic Curve Cryptosystem Overview

Elliptic Curve Cryptography (ECC) is the public key cryptography approach used for data encryption. Neal Koblitz [5] and Victor Miller [6] proposed elliptic curves in 1985 to design public key cryptographic systems. This solves the major issue of public key cryptography by providing high level security with less key length.An Elliptic Curve is a plane curve defined by an equation

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

A standard form of elliptic curve E over finite field Fp (p is a large prime number) is computed by using the following equation

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

Then, the procedure involves choosing two non-negative integers a, b which are less than p such that, it satisfies the condition

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

1) Operations of ECC

1.1 Point Inverse

If S(x_1, y_1) is a point on an elliptic curve, then its inverse is given by -S(x_1, y_1). The following equation is used to calculate the inverse[7].

-S(x_1, y_1) = S(x_1, p-y_1) (4)

1.2 Point Addition

Point addition is one of the elliptic curve arithmetic operations [7]. When the two points of a curve P(x_1, y_1) and Q(x_2, y_2) are distinct (P≠ Q), t hen P+Q is given by the following calculation.

$x_3 = \lambda^2 - x_1 - x_2$ (5)

$y_3 = \lambda(x_1 - x_3) - y_1,$ (6)

Where

λ

1.3 Point Doubling

Point doubling is one of the basic elliptic curve arithmetic operations. When the two points of a curve P(x_1, y_1) and Q(x_1, y_1) overlap (P = Q), 2P is given by the following calculation [7].

$x_3 = \lambda^2 - 2x_1$ (7)

$y_3 = \lambda(x_1 - x_3)$ - y_1 (8)

Where

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

1.4 Scalar Multiplication

Let P be any point on the elliptic curve. Multiplication operation over P is defined by the repeated addition [7].

kP = P + P + P +…. + k times (9)

*Example:*Let us consider the elliptic curve over Fp where a=1, b =1 p =11 with the equation (1)

Now, y2 = x^3+ x + 1 (mod 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}, including the point infinity O.

Elliptic curve point addition shows as follows:

By given points, P = (1,1) and Q = (8,8)

λ = (8-1) / (8-1) mod 11 = 1

P + Q = (1,1) + (8,8)

$x^3 = 1^2 - 1 - 8 = -8 = 3$

$y^3 = 1(1-3) - 1 = -3 = 8$

P + Q = (1,1) + (8,8) = (3,8)

If the selected point P be (8,8), then the doubling operation is performed as follows.

$\lambda = (3 * 8^2 + 1) / (2 * 8) \bmod 11$

= (50/ 5) mod 11 = 10

$x^3 = 10^2 - 2 * 8 = 84 \bmod 11 = 7$

$y^3 = 10 (8 - 7) - 8 = 10 - 8 = 2$

2P = (8,8) + (8,8) = (7,2)

The result of point addition and point doubling is (3,8) and (7,2), because the elliptic curve points are in Abelian group.

General Procedure for ECC is as follows:
(i) Both sender and receiver agrees to send publicly-known data items. For this the following steps are followed
a) In elliptic curve equation, values of *a* and *b* and prime *p*
b) Points (elliptic group) computed from the elliptic curve equation
c) A base point *B*taken from the elliptic group
(ii) Each user generates public or private key pairs using the following steps
a) Private key (d): an integer x, selected from the interval [1, p-1]
b) Public key (Q): product of private key and base point Q = d*B

B. Merkle Hellman Knapsack Cryptosystem overview

Ralph Merkle and Martin Hellman invented the superincreasing subset problem in the year 1978. It attempts to disguise an easily solved instance of the subset problem called superincreasing subset sum problem, by modular multiplication and a permutation [8]. The nature of superincreasing order is hidden by vector $v_1$usingmodular multiplication and a permutation, and then the superincreasing vector is represented by v. The distorted vector forms the encrypted message. The original superincreasing vector forms the private key which is used to decipher the message.

<u>Key Generation</u>

Step 1: Both sender and receiver agree with the base point *P*

Step 2: Private key = d, public key Q = d * P

<u>Encryption</u>

Step 1: Select a elliptic curve $E_p(a, b)$. E has N points on it

Step 2: Plain text has to represent on the curve

Step 3: Randomly select ‘d’ from [1-(n-1)]

Step 4: Consider message ‘m’ has the point ‘M’ on the curve ‘E’

Step 5: Two cipher texts will be generated C_1 = d*P, C_2 = M + d*Q

(i) Superincreasing Order

A super increasing sequence is a sequence (a_1, a_2, a_3,….a_n) of positive integers with the property that $a_i > \sum_{j=1}^{i-1} b_j$ for each *i*, $2 \le i \le n$.

C. Multilevel Encryption Technique

The proposed multilevel encryption technique performs encryption in two steps.

(i) Firstly, the given plain text is parted by each characters and then convert it into its equivalent binary values. Binary values are then encrypted using Merkle-Hellman encryption scheme.Mainly, it is to generate a subset problem which can be solved fluently. Here,by using modular representation and permutation the super increasing nature can be hidden. The Merkle-Hellman encryption procedure is given below.

Step 1: Choose super increasing sequence of positive integers. where each numbers is greater than the sum of all preceding numbers *s* = (s_1, s_2, s_3,…s_n)

Step 2: Convert each character of the plain text into binary equivalent represented by *b.*

Step 3: Choose an integer (*a*) which is greater than the sum of all numbers in the sequence *s* and its co-prime (*r*)

Step 4: The sequence *s* and the numbers *a* and *r* form the private key of the cryptosystem.

Step 5: All the elements in the sequence *s*are multiplied with number *r*and the modulus of the multiple is taken by dividing with the number *a*.

Step 6:$p_i = s_i * r \, mod\, (a)$, where all the elements in the sequence *p*are multiplied with the corresponding elements of the binary sequence *b* and then adding the resulting sum.

Step 7: The encrypted Message is M = $\sum_{i=0}^{n} p_i * b_i$

(ii) Secondly, these encrypted characters are further encrypted by elliptic curve cryptography (ECC). ECC is utilized to generate the cipher text of the result provided by Merkle-Hellman encryption. The procedure for Elliptic Curve Cryptosystem is given below.

With these techniques, the data could be shared securely. Thefollowing section will give the mathematical model of the proposed work.In this proposed approach, the data is secured by applying two different encryption techniques such as Merkle-Hellman knapsack cryptosystem and Elliptic curve Cryptography. With these techniques, the data could be shared securely. The following section will give the mathematical model of the proposed work.

IV. MATHEMATICAL MODEL

Example – Encrypting the string “sir”

(A.) Firstly, the plain text is encrypted using Merkle Hellman knapsack cryptosystem

Step 1: choosing a superincreasing sequence.

In this case the sequence is *s* = 3, 5, 9, 18, 38, 75, 155, 312

Step 2: Convert the characters of a given string into their binary equivalent

Convert each character into their ASCII value and then find their binary equivalent

s = 1 1 1 0 0 1 1
i = 1 1 0 1 0 0 1
r = 1 1 1 0 0 1 0
The binary sequence b = (b_1, b_2, … b_n)

Step 3: Choose an integer *a* and its co-prime *r*

An integer *a* = 672 (greater than the sum of all values in the sequence *s*)

The co-prime *r* = 13

Step 4: Find sequence p = p_1, p_2, ….. p_n). where $p_i = s_i$* r*mod* (*a*)

p_1 = 3 * 13 mod 672 = 39
p_2 = 5 * 13 mod 672 = 65
p_3 = 9 * 13 mod 672 = 117
p_4 = 18 * 13 mod 672 = 234
p_5 = 38 * 13 mod 672 = 494
p_6 = 75 * 13 mod 672 = 303
p_7 = 155 * 13 mod 672 = 671
p_8 = 312 * 13 mod 672 = 24

Step 5: Encrypting the message M=‘sir’

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

(i) Character – ‘s’
p = (39, 65, 117, 234, 494, 303, 671, 24) and
b = (1 1 1 0 0 1 1)
Ms = 39 + 65 + 117 + 0 + 0 + 671 +24 = 916

(ii) Character – ‘i’
p = (39, 65, 117, 234, 494, 303, 671, 24) and
b = (1 1 0 1 0 0 1)
Mi = 39 + 65 +0 + 234 + 0 + 0 + 24 = 362

(iii) Character – ‘r’
p = (39, 65, 117, 234, 494, 303, 671, 24) and
b = (1 1 1 0 0 1 0)
Mr = 39 + 65 + 117 + 0 + 0+ 671 + 0 = 892

(B.) Secondly, the cipher text is again encoded using Elliptic Curve Cryptography

Consider message ‘m’ = “cipher text of Merkle-Hellman algorithm”

Step 1: Consider m = 916 (cipher text of ‘s’)

Step 2: Randomly select d = 10

Step 3: Public Key Q = d * P

Here, Base point P = 110 (sender and receiver agree to have common base point)and Public Key Q = 10 * 110 = 1100

Step 4: The message m has to represent point M on the Curve E. Here, we consider point M = 224

Step 5: Cipher text:

C1 = d* P = 10 * 110 = 1100
C2 = M + d*Q = 224 + 10*1100
C2 = 11224

V. CONCLUSION

The objective of the proposed work is to improve the security of the IoT data that are sensed by the IoT devices. This is achieved by the proposed multilevel encryption. The data are encrypted in the gateway before storing it in the cloud server.Encryption of data is performed in two stages. In the first stage, Merkle-hellman knapsack cryptosystem is used to encrypt the data. In the second stage, the encrypted text acts as an input for ECC. Finally, the obtained cipher text is sent to the cloud server.This approach ensures the security of the data andimproves computation time.

Acknowledgements

This research was supported by a grant from University Grants Commission (UGC) awarded to A. Vithya Vijayalakshmi under Junior Research Fellowship.

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. Arghya Roy and Santhoshi Bhat, “Enhancement of Merkle-Hellman Knapack Cryptosystem by use of Discrete Logarithmics”, International Journal of Scientific and Research Publications, 2013, ISSN:2250-3153, Vol.3, Iss.4, pp. 1-4.
5. Koblitz. N, “Elliptic Curve Cryptosystems”, Mathematics of Computation, 1987, Vol. 48, Iss. 177, pp. 203-209.
6. Miller. V, “Use of Elliptic Curves in Cryptography”, CRYPTO’85, Springer-Verlag, 1986, pp.417-426.
7. Laiphrakpam Dolendra Singh and Khumanthem Manglem Singh, “Implementation of Text Encryption using Elliptic Curve Cryptography”, Elsevier, Internation Multi-Conference on Information Processing, 2015, pp. 1 -10.
8. Alfred J.Menezes, Paul C.van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography”,Massachusetts Institute of Technology, 1996.
9. Daisy Premila Bai T, Albert Rabara S and Vimal Jerald M, “Elliptic Curve Cryptography based Security Framework for Internet of Things and Cloud Computing”, Recent Advances on Computer Engineering, 2015, pp. 1 -10.
10. Mailov Arif, Abbasov Habib, Isayev Rufat and Safaeov Azer, “Study and Implementation of Elliptic Curve Encryption Algorithm for Azerbaijan E-ID Card”, 2015, ISSN: 2320-9798, Vol.3, Iss. 5, pp. 3708-3713.

AUTHORS BIOGRAPHY

A. VITHYA VIJAYALAKSHMIis a full time research scholar in Department of Computer Science, St. Joseph's

College (Autonomous), Tiruchirappalli. She received her M.Phil degree from St. Joseph's College (Autonomous), Tiruchirappalli, MCA degree from Holy Cross College (Autonomous), Tiruchirappalli and UG degree from Lady Doak College (Autonomous), Madurai. She has presented papers in National and International Conferences and also attended many workshops, seminars and short courses. She has also acted as a resource person for the Seminar and State Level Workshop. Her area of research interests are Internet of Things and Cloud Computing.

Dr. L. AROCKIAM is working as an Associate Professor in the Department of Computer Science, St.Joseph’s College (Autonomous), Tiruchirappalli, Tamil Nadu. He has 29 years of experience in teaching and 20 years of experience in research. He has published 284 research articles in the International / National journals and conferences. He has also presented 3 research articles in the Software Measurement European Forum in Rome, Italy, a research article in the International Conference on Computational Intelligence and Cognitive Informatics in Bali, Indonesia and a research article in the International Conference on Intelligent Network and Computing at Curtin University, Sarawak, Malaysia. He has chaired 88 technical sessions and delivered invited talks in National and International Conferences. He has co-authored books on “Success through Soft Skills”, "Research in a Nutshell", "Object Oriented Programming with C#.NET" and "WEKA: A Practical Guide to Beginners". His area of research interests are: Internet of Things, Cloud Computing, Big Data, Data Mining, Software Measurement, Cognitive Aspects in Programming, Web Services and Mobile Networks.