Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

Elliptical Curve Cryptography with Cuckoo Search algorithm for Internet of Things (IoT) Environments

T. Padmavathy [1], M. Mamatha Laxmi [2]
Assistant Professor [1], Assistant Professor [2]
[1,2] Department of Computer Science & Engineering at Vignan's Institute of Engineering for Women, JNTK

Abstract:- **Internet of Things (IoT) plays a vital role in the field of Information Technology, Industries and Healthcare etc. It consists of a large number of connected objects that are communicating with each other. 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 an Elliptic Curve Cryptography technique to enhance the security of the IoT data. Elliptic Curve Cryptography (ECC) uses two keys private key and public key. Private key is used in encryption by the user and public key is used to identify user in the case of authentication. Similarly, the sender encrypts with the private key and the public key is used to decrypt the message in case of confidentiality. Choosing the private key is always an issue in all public key. If tiny values are chosen in random the security of the complete algorithm becomes an issue. Since the values. This paper proposes Cuckoo Search Algorithm for randomly choosing the values.**

Keywords: Internet of Things, Elliptic Curve Cryptography, Cuckoo, Security

INTRODUCTION

The Internet of Things (IoT) is the network of physical objects or "things" Embedded with electronics, Internet connectivity, and other forms of hardware (such as sensors), these devices can communicate and interact with others over the Internet, and they can be remotely monitored and controlled[1][2][3] .The 'Thing' in IoT can be any device with any kind of built-in-sensors with the ability to collect and transfer data over a network without manual intervention. The embedded technology in the object helps them to interact with internal states and the external environment, which in turn helps in decisions making process.

IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. Moreover, IoT applications support different daily activities such as route planning, navigation, transportation decisions, traffic and healthcare monitoring, elderly and children supervision, and many more [4]. As is the future of the Internet, the provision of security services, such as authentication, is an essential factor to encourage people to use new technologies and securely access various IoT resources. Users would not be convenient to share and exchange their data and personal information unless protection schemes are used to prevent any malicious behavior. Therefore, efficient security and authentication techniques are necessary for comprehensive and fast deployment of IoT.

ECC

Elliptic curve cryptography is a public key cryptosystem developed by Neil Kobiltz and Victor Miller in 19th century [5] [6].

The primary advantage of Elliptical curve cryptography is reduced key size. Elliptical curve-based algorithms use smaller key sizes than the non-elliptic curve equivalents.

The difference in equivalent key sizes increases dramatically as the key sizes increase. ECC is a public key cryptography which has public and private keys for authentication. It is based on elliptical curves over finite fields. To generate cryptographic algorithms the ECC cryptographic schemes uses the properties of elliptical curves.

In ECC, the private key is chosen randomly. However, if the parameters that are chosen randomly are not selected properly, this leads in wrong calculations and the cipher text generated will not be decoded to plain text correctly. Hence there is a need to use optimization algorithms like Cuckoo Search that is elaborated in ''Private Key Selection using Cuckoo search algorithm.

An ECC over a prime field is defined by following general equation in two variables with coefficients

$y^2=x^3+ax+b$, where x, y, a and b are elements of some Field.

KEY GENERATION

Key Generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Selecting a random number d by using CS algorithm, within the range of n. Using the following equation, we can generate the public key Q=d*P, where d=the random number selected by the Cuckoo Search algorithm. P is the point on the curve.

Q is the public key and d is the private key.

E=Elliptical Curve

P=Point on the Curve

n=Maximum Limit (This should be prime)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

GENERATOR POINT

Cryptographic schemes based on ECC reply on scalar multiplication of elliptical curve points. Scalar multiplication of elliptical curve points can be computed efficiently.
Initially G (0,2) and (x1, y1) = (0,2) are selected, based on that initial point set of elliptical points can be created.

Calculations
(x2, y2) = (0,2) (0,2)
$\lambda = (3x1^2+a)/2y1 \bmod p$
$x3=\lambda^2 - x1-x2 \bmod p$
$y3=\lambda(x1-x2)-y1 \bmod p$
calculate up to 28 points, by assigning the values of x3 and y3 to x1 and y1.

GENERATED POINTS

X	Y	Point	Ascii Value
0	2	1	97
13	12	2	98
11	9	3	99
1	12	4	100
7	20	5	101
9	11	6	102
15	6	7	103
14	5	8	104
4	7	9	105
22	5	10	106
10	5	11	107
17	9	12	108
8	15	13	109
18	9	14	110
18	14	15	111
8	8	16	112
17	14	17	113
10	18	18	114
22	18	19	115
4	16	20	116
14	18	21	117
15	17	22	118
9	12	23	119
7	3	24	120
1	11	25	121
11	14	26	122
13	11	27	123
0	21	28	124

Table 1: Scalar point multiplicative values of P

Generated Elliptical points on the curve

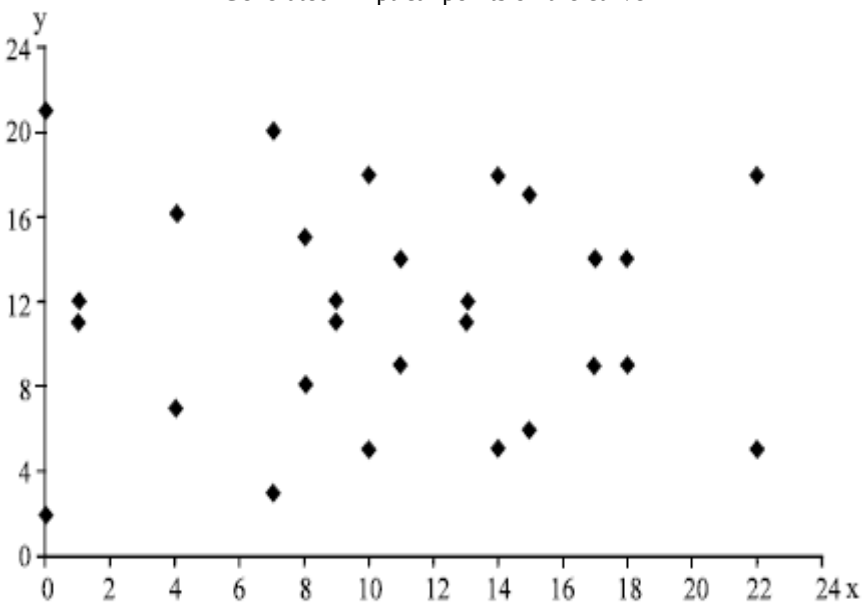

Fig 1: Scatterplot of elliptic group

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

In this method, the main idea is that convert each character of the plain text into ASCII values. Based on the ASCII value, the corresponding point can be selected. Selected points can be encrypted into cipher points. At the receiver side, cipher points can be converted into plain points.

ENCRYPTION

Let m be the message that we are sending. We have to represent this message on the curve. Consider m has the point M on the curve E. Randomly select K by using Cuckoo Search algorithm from [1-(n-1)]. Two cipher texts will be generated let it be C1 and C2
C1=K*P
C2=M+K*Q
C1 and C2 will be send
Decryption
We have to get back the message 'm' that was send to us,
M=C2 – d * C1
M is the original message that we have to send.

PROOF

To get back the message,
M=C2 – d * C1
M can be represented as
C2 – d * C1
C2 – d * C1=(M + K * Q) – d * (K * P)
(C2 = M + K * Q and C1= K * P)
=M + K * d * P – d * K * P
(Cancelling out K * d * P)
=M

EXAMPLE

Let M=abc is the plain text to be transmitted. Let d=5 and k=23
Convert the plain text into ASCII values. The ASCII value of 'a' is 97. Based on the ASCII value select the point from the table1. C1=23P and C2=116P. 116P is not present in the table. Perform 116%28=4 because 28 points are generated. The x and y coordinates for 4P are (1,12). It is the cipher point and it can be transmitted to the receiver. Perform the conversion for all characters in the plain text.
At the receiver side, apply the formula
M=C2 – d * C1
=4P – 5 * 23P
=4P-115P(115%28=3)
=4P-3P
=1P
From the table 1, the value of 1P is 97. And the character is 'a' for the ASCII value 97

PRIVATE KEY SELECTION USING CS

Here Cuckoo Search algorithm is used to optimize the value of private key used in ECC. Cuckoo Search is a new met heuristic algorithm to as a solution to optimization problem. Xin- She Yang and Susah Deb proposed this algorithm. This is dependent on the concept where a cuckoo bird chooses nest of other birds to lay its egg as
Cuckoos are ill-famed cheats where they don't build the nest by self. They just use the nests of others birds for further process of hatching eggs to chicks. Cuckoo Search is characterized by 3 laws [10]:
1. Cuckoo lays a single egg at an instance and places the egg in a randomly picked host nest.
2. Best nest with a tremendous quality of eggs can carry over to successive generation.
3. A number of host nest tend to be secure and the chance of egg discovered by the host bird is Pa e [0, 1] which is either 1 or 0 to represent success or failure.

CUCKOO SEARCH ALGORITHM

```
Generate initial population of
n host nests xi (i = 1, 2, ..., n)
while (t<MaxGeneration) or (stop criterion)
Get a cuckoo randomly by Levy flights
evaluate its quality/fitness Fi
if (Fi > Fj),
replace j by the new solution;
end
A fraction (pa) of worse nests
are abandoned and new ones are built;
Keep the best solutions
(or nests with quality solutions);
Rank the solutions and find the current best
end while
Postprocess results and visualization
end
```

Table 2: Cuckoo Search Algorithm

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

CONCLUSION

In this paper, a new authentication scheme Elliptical Curve Cryptography with Cuckoo Search in the context of Internet of things (IoT). ECC provides a better security with lesser key size. ECC takes less time for decryption than RSA in the higher security level. ECC performs in less total time for Encryption and decryption of details among User, Gateway, and Sensor nodes. In ECC, private key can be selected by using Cuckoo Search algorithm

REFERENCES

[1] Brown, Eric (13 September 2016). "Who Needs the Internet of Things?". Linux.com. Retrieved 23 October 2016.
[2] Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". Linux.com. Retrieved 23 October 2016.
[3] "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.
[4] Chen, Tien-Ho, Hsiu-lien Yeh, and Wei-Kuan Shih. "An advanced ECC dynamic id-based remote mutual authentication scheme for cloud computing." Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on. IEEE, 2011.
[5] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, Vol.49, pp. 203-209, 1987. V.S. Miller, Use of Elliptic Curves in Cryptography, Advances in Cryptology
[6] Moncef Amara and Amar Siad, Elliptic Curve Cryptography and its Applications, 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), IEEE, 2011, pp. 47-250.
[7] Thuan Thanh Nguyen, Anh Viet Truong, Tuan Anh Phung, A novel method based on adaptive cuckoo search for optimal network reconfiguration and distributed generation allocation in distribution network, International Journal of Electrical Power & Energy Systems, Volume 78, June 2016, Pages 801-815
[8] X.-S. Yang, S. Deb, in Cuckoo Search via Levy Flights. Proceedings of World Congress on Nature & Biologically Inspired Computing (NaBIC 2009), India. IEEE Publications, USA, Dec 2009
[9] L.D. Singh, K.M. Singh, in Implementation of Text Encryption using Elliptic Curve Cryptography. Eleventh International MultiConference on Information Processing-2015 (IMCIP-2015), Elsevier
[10] S. Maria Celestin Vigila, K. Muneeswaran, in Implementation of Text based Cryptosystem using Elliptic Curve Cryptography. International Conference on Advanced Computing IEEE (2009), pp. 82–85