Semiconductor Optoelectronics
ISSN:
1001-5868

A SIMULATION STUDY OF ECC ALGORITHM TO PROVE SUPERIORITY IN KEY LENGTH AND SECURITY USING NS3 IN FOG COMPUTING

Mr. Dhavalkumar Sunilbhai Patel
Ph.D Research Scholar, Department of Computer Science and Engineering, Madhav University, Pindwara, Sirohi, Rajasthan, Email- erdhavalpatelce@gmail.com

Prof. (Dr.) Sanjay Chaudhary
Professor,Dept. of Computer Science, Faculty of Engineering & Technology, Madhav University, Pindwara, Sirohi, Rajasthan, Email- schaudhary00@gmail.com

Keywords: Elliptic Curve Cryptography, Encryption, Decryption, Key Exchange, NS3, Fog, Cloud, IoT

1. Introduction:

For accessing, sharing and processing of data over any network from anywhere, the Cloud, Fog and Edge like distribution systems are very useful[1]. The evolution of these distribution systems has been exponential due to seamless interconnectedness of various subdomains in the computer science arena[2]. A device can connect to cloud or fog layer from anywhere across the globe using Internet-Of-Things [IOT] devices and yield humungous amount of data that can be transferred over a different processing center[3]. But this transfer of data through cloud or fog architecture asks for robust security measures over the nodes on which the data is processed. An important aspect in security arena is key exchange mechanism which is immune to attack on a cloud or fog layer[4].

2. Network Model and Problem Statement:

The network model presented in Figure1 shows that cloud servers are at the top tier and can communicate with each other[5]. In the network model, there is a middle layer of fog nodes, in this layer, there is a central fog whose main task is to manage other fog nodes. The middle layer can be connected to the top layer and the low layer[6]. The purpose of developing has layer was to reduce latency for bottom layer processing, they send their data to the to the fog layer for processing. In the fog layer, the central node needs to be aware of the identity of the nodes so they can exchange data with each other[7]. Furthermore, because the central node is being processed and managed, a secure, lightweight key exchange scheme is needed that can withstand known attacks.

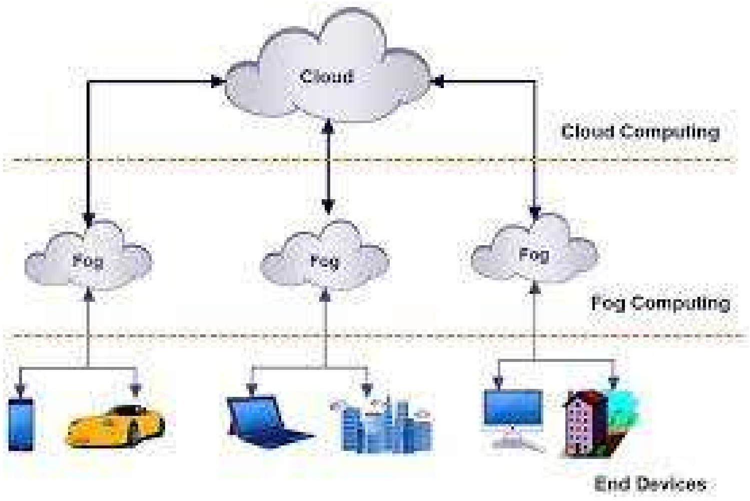

Figure 1: Network Model of Fog Computing

3. ECC Methodology:

In the mid-80's [Koblitz, 1987; Miller, 1986] proposed an encryption method based on elliptic curves Elliptic Curve Cryptography [ECC][8,9]. ECC is an Asymmetric and public key cryptography two keys are used, namely public key and private key where public key is known to all and the private key is kept as secret[10]. In private key cryptography the one same key is used for encryption as well as decryption. The implementation of an ECC process involves key generation that includes both public and private key. The message [plaint text] is encrypted by the sender using the public key and the message [cipher text] is decrypted by the received using the private key. Lightweight cryptographic algorithm is used to ensure the security of low-cost systems such as RFID, smart cards, sensors etc. as they are resource constrained devices[11]. Currently, ECC is treated as the most efficient public key cryptosystems because it utilizes shorter keys[12].

According to ECC's creators, an elliptic curve is a plain curve defined by the following equation[13].

$y^2 = x^3 + ax^2 + b$------------------- [1]

Where a and b are integers,

If the characteristics of the finite field F is 2, then the binary field GF[2^m] points will be generated by using an irreducible polynomial equation.

$y^2 + xy = x^3 + ax^2 + b$------------------- [2]

Where a and b are not equal to zero.

The efficiency of this algorithm is based on finding a discrete logarithm of a random element, which belongs to an elliptic curve. The Binary field Elliptic curve defined by the pairs [x,y] satisfying the irreducible polynomial equation is shown in figure 1. Where'P', 'Q', and 'R' are points on the curve[14].

4. Methodology:

Consider Sender and Receiver as two communicating parties. They agree upon a common Elliptic curve equation and a generator 'GP'. Let Sender and Receiver private keys be 'SK' and 'RK' respectively.

Where, SK < N and RK< N
Sender and Receiver public keys are given by
PS = SK * P-------------------[3]
and
PR = RK * P------------------- [4]
Respectively.

If Sender wants to send a message PT to Receiver, Sender use Receiver's public key to encrypt the message. The cipher text is given by
CT = RIK * GRK * PT + RIK * PR------------------- [5]
Where,
A cipher text=CT
A Key [Random integer] =RIK
A plain text= PT
A Global Random Key =GRK
A public key= PR

Receiver decrypts the message by subtracting the coordinate of GRK multiplied by RK from PT + RIK * PR. As the multiplier RK is the secret key of Receiver, only receiver can decrypt the message send by Sender.
PT = CT + RIK * RP – RK * RIK* GRK------------------- [6]
Where,
P_m is a plain text=PT
C_m is a cipher text=CT
K is a Key[Random Integer] = RIK
A public key=PR
A private key =RK
The random 'RIK' make sure that even for a same message the cipher text generated is different each time.
The following equation is used to generate the public key.
PK = RIK * GP------------------- [7]
Where,
K is the private key which is a random number are in the range of 1 to 'n'
A public key =PK
A global parameter =GP

5. Simulation of Text Encryption and Decryption using ECC:
In order to make it possible to create a simulation of mobility using Network Simulator version 3 [NS3] with system configuration of i7 processor @2.70 GHz and 8 GB RAM, the parameter of the simulation deployed are as follows;
The inputs and output for the ECC encryption algorithm are as follows.
Inputs: SK, RK, GP, RIK, PT
Outputs: PS, PR, CT Where,
PT is a plain text.

CT is a cipher text.
RIK is a key
PS, PR are public keys.
SK, RK are private keys.
GP is a Global Parameter.

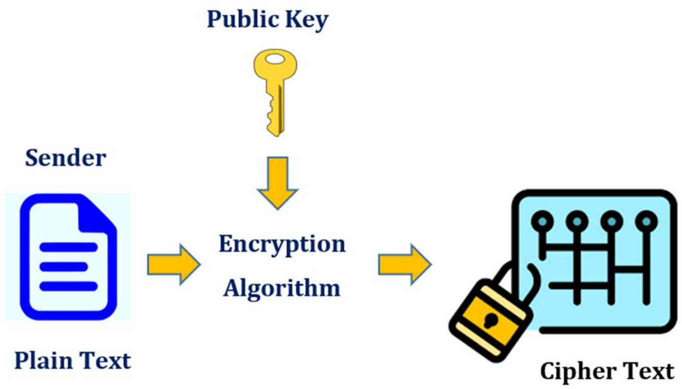

Figure 2: ECC Encryption

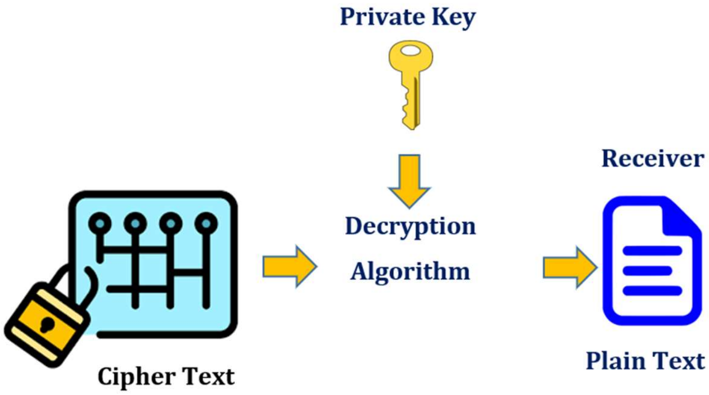

Figure 3: ECC Decryption

The given plain text is 00010101, the corresponding cipher text is 00010000 using the following equation.

CT + RIK * GP * PT + RIK * PR ------------------- [6]

The obtained cipher text is 00010000, then the decrypted plain text is 00010101 using the following equation.

PT = PT + RIK * PR – RK * RIK * GP ------------------- [7]

6. Results:

Here, with Random Curve
The Curve form is= 0
a6 :   1c 5e629417 3dbdf669 b9fca0fe cd2165b0
With Base Point
x :   c 358df1ea 9ebc2e42 2fbec069 dde73d2c

y : 9 eb318786 772fce50 72bbc1f8 22ed38bb

For creating private keys of each side
Side 1 secret: :c d2a3e242 4ce7401a 58e0e961 b20afcdf
Side 2 secret: :39 99d659e8 3428a5da 9b130925 aed734d8

Let generate each side public key Side 1 public key
x : 34 69023735 749bc2f7 27123ddd 13c421e8
y : 2a 82945bef 8826b76a 59602c5 1caaf73a
x : 26 8856d11 8ce1eed7 2390aeae7b3bf293
y : 1f 1f18ec52 652f16ee 9fa9b2c3 36c8422f

To create a message data
Plain Text [with sent data] : 16 f93ff6c8 e42f891b d8aeabdf cd419f2f

The data on curve is hidden and is send from side 1 to 2 in hidden from
x : 31 b71d6293 bb851393 2a92dbb5 fc19958c
y : 3d d2ff2282 87d2accb 970f677a c5c82180

So now the Random points are-
x : 12 2abaa729 775cb900 bf443998 548c3e9c
y : 1e 24719fb0 5c4e03db e67be1f0 b46cac9f

And, the recovered transmitted message is
Plain Text [at the received data]: 16 f93ff6c8 e42f891b d8aeabdf cd419f2f

7. Conclusion:

A major bottleneck in the Fog computing arena is secure exchange of keys[15]. The present research resulted in providing a secure and less resource intensive method for key exchange using Fog computing. The work was simulated using NS3 tools. Both encryption and decryption was performed swiftly while employing a large number word size in the input, and it also yielded smaller cipher text size when comparison was made with other established methods thereby saving energy costs and lessening bandwidth use[16]. The ECC basically exploited the difficulty in solving discrete logarithmic properties of Elliptical curves. The advantage of using ECC in various cryptographic methods with similar extent of security lies in its ability to use smaller keys. This property makes ECC highly sought after algorithm of choice in wireless sensors, mobile devices, and other networks that have inherent issues of storage, energy utilization and processing powers. It also provides highest level of security per bit with low cost for computing when comparing to other public key systems[17]. The deployed of ECC in computer cryptography has gained traction in recent times mostly due to the properties mentioned above. ECC has found a coveted place among standards set by ANSI X9.63, IEEE P1363, ANSI X9.62 etc. and is continuously getting explored in others arenas too[18].

References:

1. Kalyani Y, Collier R. A Systematic Survey on the Role of Cloud, Fog, and Edge Computing Combination in Smart Agriculture. Sensors [Basel]. 2021 Sep 3;21[17]:5922. doi: 10.3390/s21175922.

2. Dezfouli, B.; Liu, Y. Editorial: Special Issue “Edge and Fog Computing for Internet of Things Systems”. Sensors 2022, 22, 4387. https://doi.org/10.3390/s22124387

3. Alwakeel, A.M. An Overview of Fog Computing and Edge Computing Security and Privacy Issues. Sensors 2021, 21, 8226. https://doi.org/10.3390/s21248226

4. Jiang Y, Wu S, Mo Q, Liu W, Wei X. A Cloud-Computing-Based Portable Networked Ground Station System for Microsatellites. Sensors [Basel]. 2022 May 7;22[9]:3569. doi: 10.3390/s22093569.

5. Caminero, A.C.; Muñoz-Mansilla, R. Quality of Service Provision in Fog Computing: Network-Aware Scheduling of Containers. Sensors 2021, 21, 3978.

6. Varshney, P.; Simmhan, Y. Characterizing application scheduling on edge, fog, and cloud computing resources. Softw. Pract. Exp. 2021, in press.

7. Haghi Kashani, M, Rahmani, AM, Jafari Navimipour, N. Quality of service-aware approaches in fog computing. Int J Commun Syst. 2020; 33:e4340. https://doi.org/10.1002/dac.4340.

8. Koblitz, N. Elliptic curve cryptosystems. Math. Comput. 1987, 48, 203–209.

9. Miller, V.S. Use of elliptic curves in cryptography. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Linz, Austria, 9–11 April 1985; pp. 417–426.

10. C. A. Lara-Nino, A. Diaz-Perez and M. Morales-Sandoval, "Elliptic Curve Lightweight Cryptography: A Survey," in IEEE Access, vol. 6, pp. 72514-72550, 2018, doi: 10.1109/ACCESS.2018.2881444.

11. Verri Lucca, A.; Mariano Sborz, G.A.; Leithardt, V.R.Q.; Beko, M.; Albenes Zeferino, C.; Parreira, W.D. A Review of Techniques for Implementing Elliptic Curve Point Multiplication on Hardware. J. Sens. Actuator Netw. 2021, 10, 3. https://doi.org/10.3390/jsan10010003.

12. K. E and B. V. [2022]. Blockchain Based Electronic Voting Protocol. British Journal of Computer, Networking and Information Technology. 10.52589/BJCNIT-7LST204K. 5:1. [56-115].

13. Diro, Abebe & Chilamkurti, Naveen & Kumar, Neeraj. [2017]. Lightweight Cybersecurity

Schemes Using Elliptic Curve Cryptography in Publish-Subscribe fog Computing. Mobile Networks and Applications. 22. 10.1007/s11036-017-0851-8.

14. Zhou Y, Liu H, Xiang Q, Yin C. High-Performance and Flexible Design Scheme with ECC Protection in the Cache. Micromachines[Basel]. 2022 Nov 9;13[11]:1931. doi: 10.3390/mi13111931. PMID: 36363952; PMCID: PMC9697281.

15. Nassif, N.; Munch, A.O.; Molnar, C.L.; Pasdast, G.; Lyer, S.V.; Yang, Z.; Mendoza, O.; Huddart, M.; Venkataraman, S.; Kandula, S.; et al. Sapphire Rapids: The Next-Generation Intel Xeon Scalable Processor. In Proceedings of the 2022 IEEE International Solid-State Circuits Conference [ISSCC], San Francisco, CA, USA, 20–26 February 2022; pp. 44–46

16. Chen Y, Chen J. A biometrics-based mutual authentication and key agreement protocol for TMIS using elliptic curve cryptography. Multimed Tools Appl. 2022 Oct 12:1-24. doi: 10.1007/s11042-022-14007-3. Epub ahead of print. PMID: 36250183; PMCID: PMC9553637.

17. Qi Xie, Bin Hu, Xiao Tan, Mengjie Bao, and Xiuyuan Yu. 2014. Robust Anonymous Two-Factor Authentication Scheme for Roaming Service in Global Mobility Network. Wirel. Pers. Commun. 74, 2 [January 2014], 601–614. https://doi.org/10.1007/s11277-013-1309-3.

18. Radhakrishnan N, Muniyandi AP. Dependable and Provable Secure Two-Factor Mutual Authentication Scheme Using ECC for IoT-Based Telecare Medical Information System. J Healthc Eng. 2022 Feb 14; 2022:9273662. doi: 10.1155/2022/9273662.