A Novel Approach for Improving IoT data security Using Elliptic Curve Cryptography

[1]Dharmishtha Sinha, [2] Dr. D.A. Parikh

[1]PG student , [2]Associate Professor
[1] Department of Computer Engineering,
[1]L.D.College of Engineering, Ahmedabad, India

Abstract: **The rapid increase of connected services and the major advances in information and communication technologies have led to great emergence in the Internet of Things (IoT). IoT devices require software adaptation as they are in continuous transition. Most likely the most demanding of requirements for the widespread realization of many IoT visions is security. In this research we have proposed constructing a model for encryption and decryption using Elliptical curve cryptography and blockchain technology with the purpose to improve the security and safety of confidential information.**

Index Terms **– Security, Encryption, Decryption, Blockchain, ECC**

I. INTRODUCTION

In this era, Internet of Things is a popular term. IoT is a gigantic network connected by different devices which collect and shares data. IoT is used in different places like smart micro ovens, which cook food automatically for us in perfect time; self-driving cars, which detects objects in their path and avoid it; wearable fitness devices, which measure our heart rate and the number of steps we have taken, etc. Here, different devices are connected to an IoT platform, it collects data from different devices and analyses the data to share the most valuable information for computation and other use. These strong IoT platforms can separate data between which is exactly need and which has to be ignored. This data is used detect possible anomalies before they happen, to make recommendations and to detect patterns.

The information gathered using IoT devices help us to take right decisions about which product to stock, based on real-time information.

II. LITERATURE REVIEW

[1] proposed a light weight algorithm proposes a security scheme with a service scenario for an improvement of resource constrained IoT environment and open issues are discussed and a Hybrid light weight algorithm (HLA) is used.[2] The proposed algorithm enables the edge device to encrypt the data generated using Advanced Encryption Standard (AES) before transmitting to cloud. The key of the AES is encrypted by using RSA crypto system. The size of the key is taken as 128 bits.[11] mentions how block chain is used for data integrity.[5] proposes that in IOT, giving security to gadgets, Elliptic Curve Diffie Hellman(EC-DH) Algorithm has been implemented.

III. BLOCK CHAIN FOR DATA INTEGRITY

Bitcoin is based around an innovation known as the *blockchain*. Nodes in the Bitcoin network send and receive transactions to other nodes in the network, transactions are then checked for validity and placed together in a block of transactions. To calculate the current state of the network, the whole graph of blocks must be traversed. A new block is created approximately every 10 minutes, with all transactions that occurred since the last block creation stored in it. Figure 1 shows the chain of blocks. Each block contains the hash of its parent; a nonce that proves the validity of the block; and all the transactions in the block. Since any valid transaction is part of some block, and all valid blocks are chained together, the blockchain can be seen as a distributed ledger, and proof of the true state of the network. Once the block has been created, any subsequent changes to a block will invalidate the nonce, and thus invalidate the nonces of all child blocks.

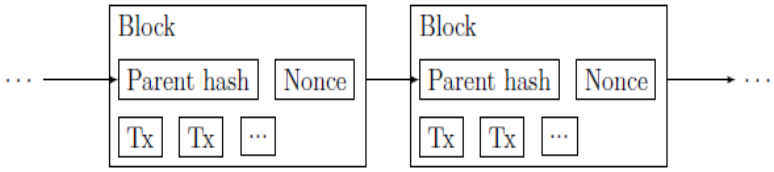

Figure 1: Block chain for data integrity

IV. ECC ALGORITHM FOR DATA SECURITY

ECC is pronounced as elliptic curve cryptography[13], developed by Neil Koblitz and Vector Miller in 1985. ECC provides better security with a smaller key size if we compare it with other asymmetric algorithms [9]. ECC 160-bit gives same level of security to data as RSA 1024-bit does. High level of security can be achieved using a small key size. ECC works on elliptic curve equation. Elliptic curve equation for binary field is written as-

$y^2+xy=x^3+ax+b$

where a and b are two constants, different elliptic curves will be shaped with different values of these two constants. Elliptic curve equation for prime field is given as-

$y^2=x^3+ax+b \bmod p$

here a and b are constants and p is a prime number. Grater the value of number p more will be the number of points generated on the elliptic curve. Large number of points on the curve gives high level of security. Elliptic curve is shown in figure 2 below-

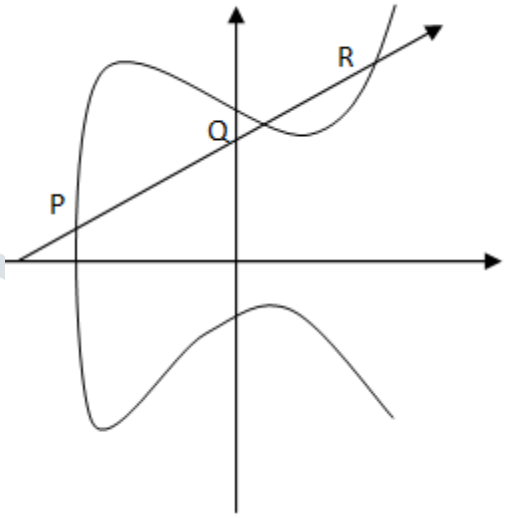

Figure 2: Elliptic curve[]

Motivation:

Various authors who have implemented text encryption and decryption using ECC have used agreed upon table which consist of characters and ECC coordinates mapping or used the ASCII value of the characters to produce affine elliptic curve coordinates by performing point multiplication operation with generator '*G*' and the corresponding ASCII value of the character. This algorithm proposes a novel idea where use of mapping on common look up table between the sender and receiver has been completely removed. The communicating parties agrees upon an Elliptic curve equation

$Y^2=x^3+ax+b \bmod p$ with the generator 'G' and makes the public keys 'Pa' and 'Pb' known to all and private keys 'nA' and 'nB' are kept secret. The size of each group is given by counting the total digits in the point p of above equation.

IV. PROPOSED SYSTEM ARCHITECTURE

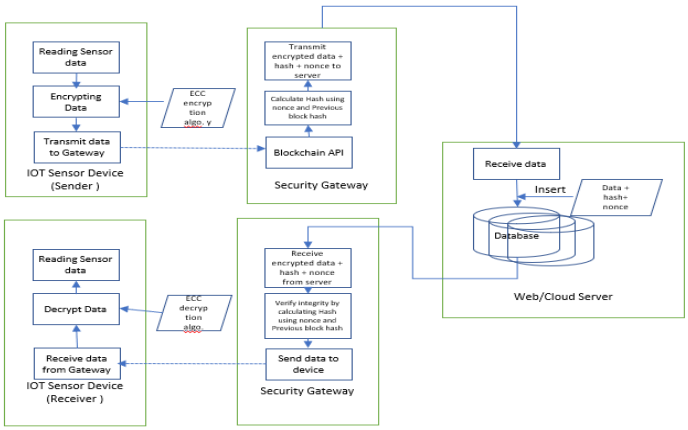

Figure 3: Proposed Architecture

The overall proposed system architecture is shown as above. The architecture is implemented in following sequence:

Data objects (sensor readings) are formatted as JSON and encrypted using the ECC algorithm before being transmitted to the gateway wirelessly.

Once data is received by the gateway it is processed into HTTPS and prepared for transmission to the server and during the same time the integrity of the data is made intact by using block chain API.

The encrypted data along with the hash value and nonce are stored into the server.

Receiver end:

In the receiver end the encrypted data is received by the gateway here the integrity of the data is checked using the block chain API if the data intact then the decryption process takes place by the receiving IOT device.

V. IMPLEMENTATION

Encryption

- Obtain the text to be send.
- Convert to its corresponding ASCII values.
- Partition the ASCII value as decided by counting digits of p.
- Each group obtained from the above step is converted into big integer values taking base as 256.
- Select random *k* value, *k* = Random value with range 1 to *n*−1. Compute *kG* and
- *kPb* using Point multiplication operation.
- Compute *Pm* + *kPb* using point addition or point doubling as required.
- Send *Pc* = {*kG*, *Pm* + *kPb*} as cipher text to the receiver side.

Decryption

- Get the cipher text *Pc*.
- Get the left part *kG* and right part *Pm* + *kPb* of the *Pc* separately.
- Multiply with *nB* to the left part and subtract it from the right part to get *Pm*.
- {Pm + kPb} − nBkG = Pm
- The above operation will yield the big integer value which is formed by combining
- group of ASCII values. Convert it back to list of ASCII values.
- Convert the list of ASCII values to its corresponding characters.

VI. EXPERIMENTAL PARAMETERS

The following parameters are considered for evaluation of both ECC algorithms for encryption and decryption schemes.

• Encryption time (Computation Time/ Response Time)

The encryption time is the time that an encryption algorithm takes to produce a ciphertext from a plaintext.

• Decryption time (Computation Time/ Response Time)

The decryption time is the time that a decryption algorithm takes to reproduce a plaintext from a ciphertext.

• Throughput

Throughput is equal to total plaintext in bytes encrypted divided by the encryption time. Higher the throughput, higher will be the performance.

• Plaintext Size Vs Ciphertext Size

In any cryptographic algorithm, it is essential to understand the size of the input and the size of output. Larger the size of the Ciphertext compared with the Plaintext, more secure is the Ciphertext against any Brute-Force attack.

Table 1: Table Encryption/Decryption time

	Encryption time(seconds)	Decryption time(seconds)
Base algorithm	0.2174	0.0294
Proposed algorithm	0.0861	0.0168

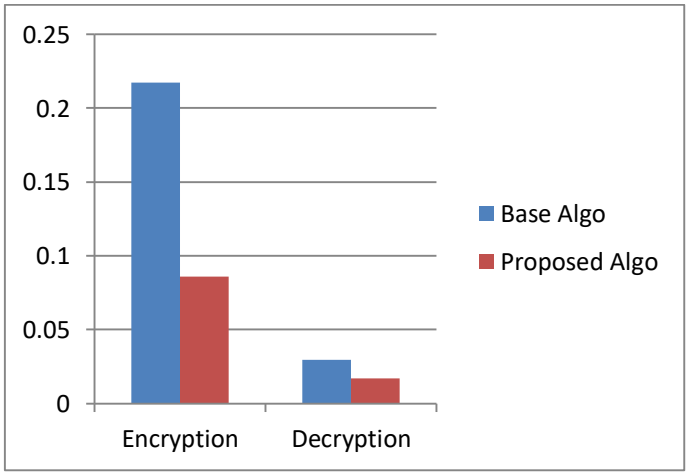

Figure 3: Chart showing Encryption/Decryption time

Table 2: Throughput in bytes/sec

	Throughput
Base algorithm	45.99816
Proposed algorithm	116.144

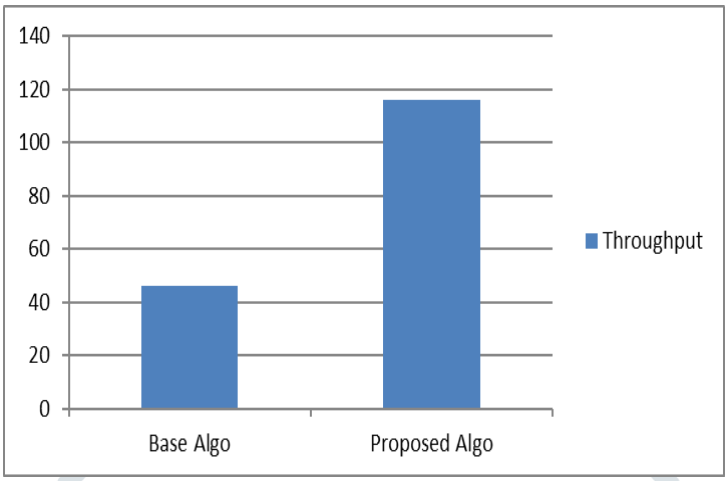

Figure 4: Chart showing comparison in throughput

VII. CONCLUSION

If the smart devices having low computational power and limited battery life are ensured and convinced enough regarding the safety factor of their data on the cloud, it will motivate them to shift to the cloud platform confidently. This research proposal tries to cover maximum possible aspects towards protecting the data of users by designing a new framework which will provide Security, Integrity, Confidentiality and Availability of data in the cloud environment.

REFERENCES

[1] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon,Jong Hyuk Park," Advance lightweight encryption algorithm for IoT devices", Springer-Verlag Berlin Heidelberg 2017
[2] Chandu Y,K. ,S. Rakesh Kumar, Ninad Vivek Prabhukhanolkar, Anish A N, Sushma Rawal," Design and Implementation of Hybrid Encryption for Security of IOT Data", 2017 International Conference On Smart Technology for Smart Nation
[3] Tanupriya Choudhury, Ayushi Gupta, Saurabh Pradhan, Praveen Kumar, Yogesh Singh Rathore," Privacy and Security of Cloud-Based Internet of Things (IoT)", 2017 International Conference on Computational Intelligence and Networks
[4] Manish Kumar, Sunil Kumar, M.K. Das and Sanjeev Singh," Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach", 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (Green Com) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (Smart Data)
[5] Elliptic Curve Cryptography based Security Framework for Internet of
Things and Cloud Computing DAISY PREMILA BAI T, ALBERT RABARA S, VIMAL JERALD M Department of Computer ScienceSt. Joseph's College, Bharathidasan University
Tiruchirappalli, Tamil Nadu INDIA
[6] Igor Zikratov, Alexander Kuzmin, Vladislav Akimenko, Viktor Niculichev, Lucas Yalansky "Ensuring Data Integrity Using Blockchain Technology",PROCEEDING OF THE 20TH CONFERENCE OF FRUCT ASSOCIATION, IEEE,2016
[7] Amirhossein Safi," Improving the Security of Internet of Things Using Encryption Algorithms", World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering Vol:11, No:5, 2017
[8] Wei Wang, Peng X and Laurence Tianruo Yang, "Secure Data Collection, Storage and Access in Cloud-Assisted IoT",IEEE
[9] X. C. Yin, Z. G. Liu and H. J. Lee, "An efficient and secured data storage scheme in cloud computing using ECC-based PKI," *16th International Conference on Advanced Communication Technology*, Pyeongchang, 2014, pp. 523-527.
[10] A. Alsirhani, P. Bodorik and S. Sampalli, "Improving Database Security in Cloud Computing by Fragmentation of Data," *2017 International Conference on Computer and Applications (ICCA)*, Doha, 2017, pp. 43-49.
[11] Ensuring Data Integrity Using Blockchain Technology, PROCEEDING OF THE 20TH CONFERENCE OF FRUCT ASSOCIATION,IEEE,2016

BOOKS

[11] Mather, T.; Kumaraswamy, S.; Latif, S. Cloud security and privacy: an enterprise perspective on risks and compliance. O'Reilly Media, Inc., 2009, pp 24-25.
[12] Whitman, M.E., and Mattord, H.J., Management of Information Security; 3rd Edition; Cengage Learning;2010, pp 6-7.

Dissertation

[13] Security for the Internet of Things KE'AHI COOPER DEGREE PROJECT, IN COMPUTER SCIENCE, SECOND LEVEL Stockholm, Sweden15
[14] Angseus J., Bachelor's Thesis, "Decentralized Cloud Computing Platforms" Chalmers University of Technology, 2015.
[15] Nordstrom E., Masrer's Thesis, "Personal Clouds: Concedo", Luleå University of Technology,2015

WEB REFERENCES

[16] Merkel Trees : https://en.wikipedia.org/wiki/Merkle_tree