International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Elliptic Curve Cryptography: A New Method for Increasing IoT Data Security

Subhashini R,Assistant Professor,Dept. of CSE,Cambridge Institute of Technology,Bangalore and Research scholar,Dept. of CSE,Bangalore Institute of Technology,Bangalore. e-mail id: subhashini050@gmail.com

Dr D G Jyothi, HoD, Department of AI & ML, Bangalore Institute of Technology,Bangalore
e-mail id: jyothi.bitcse@gmail.com

Abstract : The Internet of Things has greatly emerged as a result of the significant advancements in information and communication technology and the quick expansion of linked services (IoT). IoT devices need software adaptability since they are always changing. Security is arguably the most difficult criterion to meet for the general implementation of many IoT concepts. In this study, we made a suggestion. building a paradigm for encryption and decryption utilising blockchain technology and elliptical curve cryptography with the aim of enhancing the security and safety of sensitive data.

Keywords: Index Terms – Security, Encryption, Decryption, Blockchain, ECC

INTRODUCTION

Internet of Things is a buzzword in this day and age. IoT is a vast network of linked devices that gather and share data. Smart micro-ovens that prepare meals for us automatically and in the ideal amount of time; self-driving automobiles, which recognises obstacles in its route and steers clear of them; wearable fitness equipment that counts our walks and measures our heart rate, etc. Here, many devices are linked to an IoT platform, which gathers data from various sources and analyses it to provide the most important information for computation and other uses. These robust IoT solutions can distinguish between data that is actually needed and that must be discarded. This information is utilised to identify patterns, make suggestions, and anticipate potential abnormalities.

The examination of the literature reveals several strategies and methods put forth by researchers to deal with the security issues in IoT contexts. These methods incorporate AES and RSA encryption, lightweight algorithms, blockchain technology for data integrity, and key exchange techniques like ECDH. These initiatives strive to strengthen the security of IoT devices and shield them from potential security risks in contexts with limited resources. To ensure the secure and dependable operation of IoT devices in a variety of applications, further research and development is required in this field.

The requirement for safeguarding these devices and their data has grown essential in recent years due to the rising deployment of Internet of Things (IoT) devices in a variety of fields. Several strategies and techniques have been put forth by various academics to handle the security issues in IoT contexts with limited resources. The authors of [1] suggested a simple method that tries to increase security in IoT contexts while using the fewest resources possible. They examined unresolved IoT security challenges and offered a security plan with a service scenario. They suggested a Hybrid Lightweight Algorithm to accomplish lightweight encryption (HLA).

With the help of the suggested technique in [1], edge devices can encrypt data produced using the Advanced Encryption Standard (AES) before sending it to the cloud. The RSA cryptosystem is used to encode the key used in AES encryption. A better level of security is ensured by selecting a key size of 128 bits. With this strategy, communication between edge devices and the cloud is intended to be quick and safe while preserving data privacy.

[11] highlights the usage of blockchain for data integrity in IoT in addition to encryption techniques. A distributed and decentralised ledger system called blockchain can offer safe and open data storage and verification. Data integrity in IoT contexts may be maintained by utilising blockchain, avoiding unwanted data manipulation or change.

The Elliptic Curve Diffie-Hellman (ECDH) technique is also suggested by [5] for use in protecting IoT devices. A popular key exchange technique that offers safe communication between entities over an unsecure channel is the ECDH algorithm. [5] seeks to improve the security of IoT devices and shield them from different assaults by leveraging the ECDH algorithm.

Blockchain For Data Integrity

The examination of the literature demonstrates that many strategies and methods have been put forth by researchers to address the security issues related to IoT settings. One such strategy is the creation of simple algorithms that are intended to function effectively in IoT situations with limited resources. These simple methods are designed to offer appropriate security while reducing computational load and energy consumption on IoT devices, which frequently have constrained memory, processor, and energy resources.

The use of encryption methods, such as the Advanced Encryption Standard (AES) and the RSA cryptosystem, to guarantee the secrecy and integrity of data exchanged between IoT devices and the cloud is another popular strategy. In contrast to RSA, a commonly used asymmetric encryption algorithm for safe key exchange and data encryption, AES offers a high level of security and is used to encrypt data. Researchers want to make sure that IoT data is safe while being sent and stored by using encryption techniques to prevent unwanted access..

The literature study also emphasises the applicability of blockchain in IoT contexts for maintaining data integrity. Blockchain, a distributed and decentralised ledger technology, is suited for verifying the integrity and authenticity of IoT data since it can offer an immutable and visible record of data transfers. Blockchain can stop unlawful data change or tampering, preserving the integrity and dependability of the data.

In order to create secure communication between entities in IoT contexts, key exchange strategies like the Elliptic Curve Diffie-Hellman (ECDH) algorithm are further offered. With the help of the popular key exchange algorithm ECDH, safe key negotiation may be achieved without sending the actual key across the communication channel. Researchers want to build secure communication between IoT devices using key exchange algorithms to avoid listening in or unwanted access to private data.

In particular in resource-constrained contexts where the limits of IoT devices might make it difficult to apply comprehensive security measures, these research activities strive to enhance the security of IoT devices and defend them from possible security threats. To continue improving the security of IoT devices and guaranteeing their secure and dependable functioning in a variety of applications, more research and development are necessary. Addressing security issues will be a crucial area of effort as the IoT environment develops in order to maintain the privacy, integrity, and security of IoT data and devices..

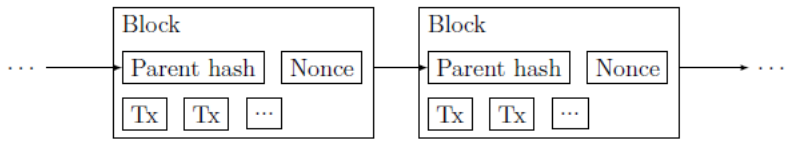

Figure 1. Block chain for data integrity

ECC For Data Security

The 1985 invention of Neil Koblitz and Vector Miller, Elliptic Curve Cryptography (ECC), is pronounced "elliptic curve cryptography" [13]. ECC offers greater security with fewer key sizes than other asymmetric algorithms [9]. In actuality, a 1024-bit RSA key and a 160-bit ECC key both provide the same amount of security. ECC uses elliptic curve equations to provide high security levels with small key sizes.

The equation for an elliptic curve in a binary field is written as:

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

where "a" and "b" are constants that shape different elliptic curves based on their values.

On the other hand, the equation for an elliptic curve in a prime field is given by:

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

where "a" and "b" are constants, and "p" is a prime number. The value of "p" determines the number of points generated on the elliptic curve. A larger "p" results in a higher number of points on the curve, which in turn offers a higher level of security. Refer to Figure 2 below for a graphical representation of an elliptic curve.

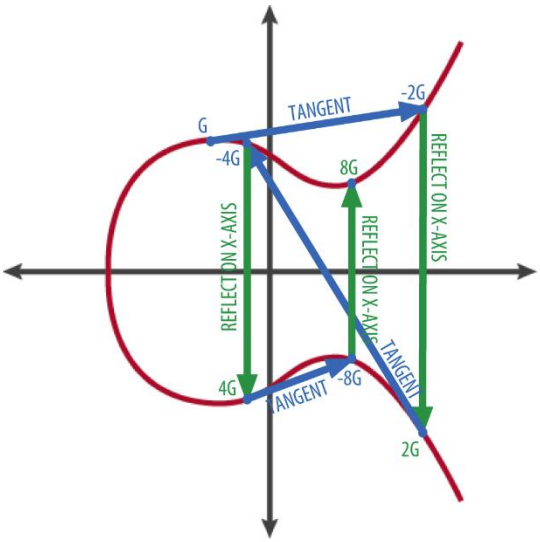

Fig 2. Elliptic curve

Proposed Algorithm

Here is a diagram of the proposed system's general design. The following order in which the architecture is implemented: Before being wirelessly communicated to the gateway, data objects (sensor readings) are encoded as JSON and encrypted using the ECC method.

As soon as data is received by the gateway, it is converted to HTTPS and made ready for transmission to the server while also being protected from tampering by utilising block chain API. The server stores the encrypted data together with the hash value and nonce. recipient end: The gateway at the receiver end receives the encrypted data, and if the data is intact, uses the block chain API to validate its integrity before the receiving IOT device begins the decryption process.

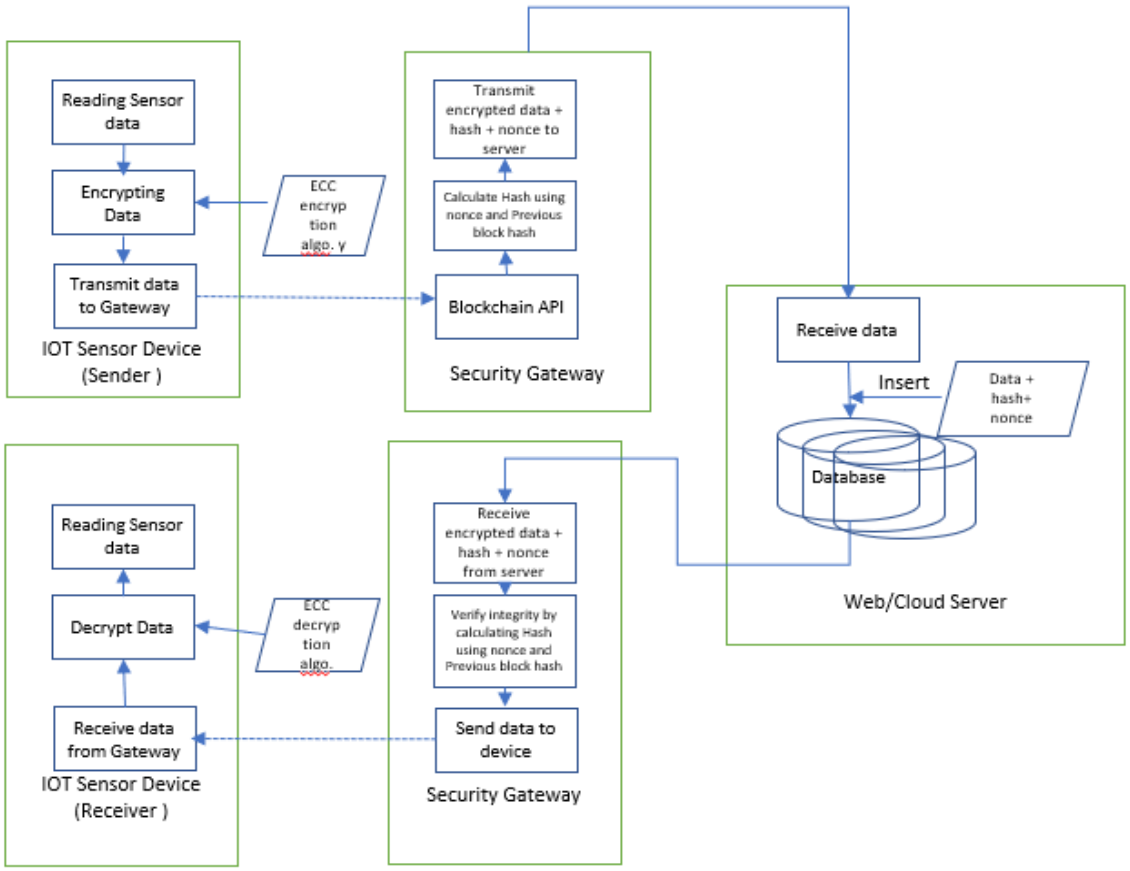

Fig 3. Flowchart of Proposed System

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.

Implementation

The following considerations are made while evaluating ECC algorithms for encryption and decryption systems.

• The encryption-related calculation and response times
The encryption time is the amount of time it takes an encryption technique to transform plaintext into ciphertext.
• Decryption time (processing time/response time)
The decryption time measures how long it takes a decryption algorithm to reconstruct plaintext from ciphertext.
• Efficiency
By dividing the total number of encrypted bytes of plaintext by the encryption time, throughput is computed.
The larger the throughput, the better the performance.
• Plaintext vs. Ciphertext Size
Any cryptographic process must take the input and output sizes into account. The greater the Ciphertext is relative to the Plaintext, the more secure it is against any Brute-Force attack.

According to experimental findings, the basic method achieves a throughput of 45.99 with encryption times of 0.21 seconds and 0.0294 seconds, and throughput times of 0.086 seconds and 0.0168 seconds, respectively, for the proposed system.

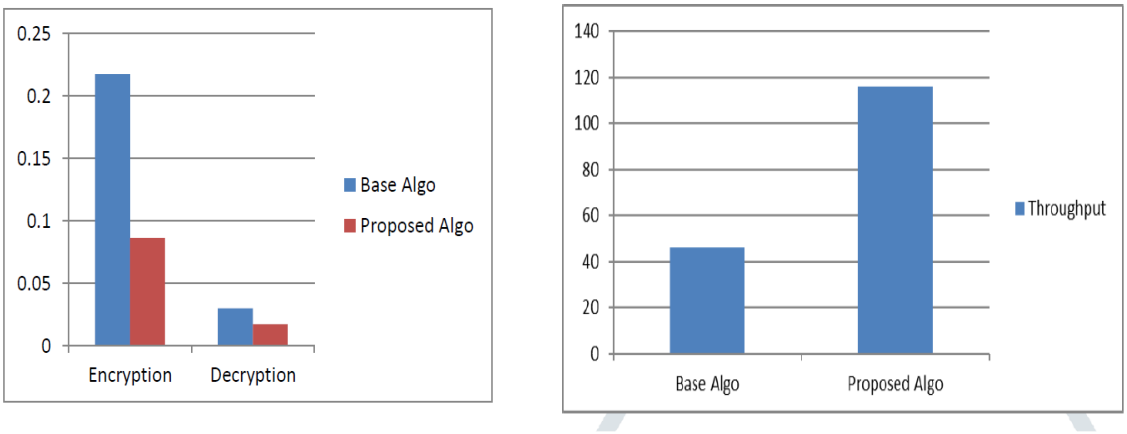

Fig 4. Comparison of Base and Proposed Method for encryption time, decryption time and throughput.

Conclusion

If smart devices with limited processing power and battery life are adequately confident and convinced of the security of their data there, they will be encouraged to move to the cloud platform with confidence. The objective of this research project is to create a new framework that will guarantee the security, integrity, confidentiality, and availability of data in a cloud environment, providing users with as much data protection as is practical.

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