Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1713–1722
DOI : 10.47974/JDMSC-2171

Blockchain-based secure data sharing and storage system using elliptic curve cryptography

Sulakshana Malwade [†]
Department of Polytechnic
Dr. Vishwanath Karad MIT World Peace University
Pune 411038
Maharashtra
India

Rohini Jadhav *
Department of Information Technology
College of Engineering
Bharati Vidyapeeth (Deemed to be University)
Pune 411043
Maharashtra
India

Veena Jadhav [§]
Department of Computer Engineering
College of Engineering
Bharati Vidyapeeth (Deemed to be University)
Pune 411043
Maharashtra
India

A. V. Chitre [‡]
Department of Electronics and Telecommunication
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

[†] *E-mail:* sulakshana.malwade@mitwpu.edu.in
* *E-mail:* rbjadhav@bvucoep.edu.in (Corresponding Author)
[§] *E-mail:* vjjadhav@bvucoep.edu.in
[‡] *E-mail:* abhijit.chitre@vit.edu

Bhumika Neole [@]
Department of Electronics and Communication Engineering
School of Electrical and Electronics Engineering
Ramdeobaba University
Nagpur 440013
Maharashtra
India

Nilesh Shelke [#]
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International Deemed University
Pune 440008
Maharashtra
India

Abstract

This article depicts a modern blockchain-based secure way to store and share information that employments elliptic bend cryptography (ECC) to form information more private and secure. As the sum of digital data grows, it gets to be increasingly critical to have solid and successful security measures. Our strategy employments both blockchain innovation and ECC to settle the issues that come with the way information is as a rule put away and shared. The blockchain is an independent record that keeps information secure and outlandish to alter. ECC, on the other hand, scrambles information unequivocally whereas utilizing less computing control than other strategies. This blend not as it were keeps information secure whereas it's being sent and put away, but it too makes it simpler for numerous individuals to share information and control who can see it. A keen contract-based get to control instrument is built into the recommended framework. This lets clients have particular rights and consequently implements security rules. We utilize exhaustive hypothetical and viable tests to see at our system's execution and security. This appears that it is proficient in terms of both how much it costs to run and how secure it is. The comes about appear that our strategy gets tall security with small impact on speed. This makes it a great choice for sharing secure information in numerous settings, such as for financial activities, wellbeing records, and private individual information. This work includes to the field by displaying a new way to make strides information security and protection by combining blockchain and ECC.

Subject Classification: *68M25.*

Keywords: *Blockchain, Elliptic curve cryptography (ECC), Secure data sharing, Data storage, Cryptographic security, Decentralized ledger, Smart contracts, Transaction throughput.*

[@] *E-mail:* **neoleba@rknec.edu**
[#] *E-mail:* **nilesh.shelke@sitnagpur.siu.edu.in**

1. Introduction

Since of the developing sum and significance of delicate data shared over numerous channels within the advanced age, secure information sharing and keeping are huge issues [1]. Conventional security measures do not continuously work against current dangers, so better approaches of ensuring information are required. The independent and unchangeable record of blockchain innovation makes it a confident choice for keeping information secure and open [2], [3]. In any case, progressed cryptographic methods must be included to information security in arrange to form it indeed more secure and more compelling [4]. Elliptic Bend Cryptography (ECC) may be a effective device for this reason since it gives solid security with a part less processing waste than common cryptography strategies like RSA [5]. Since it is productive, ECC works particularly well for blockchain frameworks that got to be quick and versatile. This article talks approximately a secure way to share and store information on the blockchain that employments the most excellent parts of ECC to offer a total security conspire [6], [7]. Our framework points to settle common issues with sharing and putting away information by blending the open nature of blockchain with the solid security highlights of ECC. Savvy contracts are utilized within the framework to control who can get to information and to consequently implement security rules [8] [9]. This keeps information secure from people who shouldn't be able to see or alter it [10]. We appear that our strategy works to induce tall security with small speed fetched by looking closely at both its hypothetical establishments and its real-world execution. This presentation sets the arrange for looking at how blockchain and ECC can work together to alter the way information is protected in present day advanced settings.

2. System Design and Architecture

In presently making the scientific show for elliptic bend cryptography (ECC) information encryption. ECC offers solid security with small additional work for computers, which is exceptionally imperative for interfacing to blockchain frameworks [11]. Elliptic bends characterized over limited areas are at the heart of the encryption handle, and operations on these bends are what make the encryption strategy work, shown in figure 1.

1. Elliptic Curve Equation: We can write the equation for the elliptic curve E as follows:

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

where (a) and (b) are parameters specific to the curve, and (x) and (y) are coordinates on the curve.

2. Encryption Handle:

Given a plaintext message (M), it is spoken to as a point on the elliptic bend. There are two primary steps within the coding prepare:

- Key Era: Select a private key (k) and discover the open key (K) that goes with it by taking after these steps:

$$K = k \cdot G$$

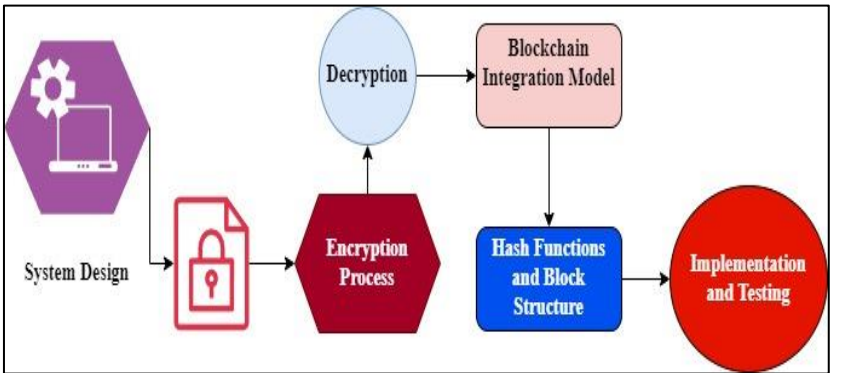

Figure 1
Architectural Block Diagram of Proposed Model

where G is the elliptic curve's beginning point.

- Encryption: Utilize the open key (K) and an arbitrary number (r) to scramble the crude message (M). Here's how to figure out the ciphertext (C):

$$C = (M \cdot G) + (r \cdot K)$$

The point duplication of the message is appeared by (M ·G), and the scalar increase with the open key is appeared by (r ·K).

3. Decryption:

The collector employments their private key (k) to split the ciphertext.

$$M = C - (k \cdot (r \cdot G))$$

Utilizing the numerical highlights of elliptic bends to ensure information, this demonstrate makes beyond any doubt that the encryption prepare is both secure and speedy.

3. Blockchain Integration Model

In this step, we make the scientific demonstrate for how blockchain innovation can be utilized within the secure framework for sharing and putting away information. The blockchain makes an autonomous and unchangeable record that's exceptionally critical for keeping information secure and open.

3.1 *Hash Functions and Block Structure*

The blockchain could be a secure chain since each square incorporates a hash of the square some time recently it [12]. Let B_i stand for the i-th block, which has data_i inside it. Once you utilize the hash work H, you get a secure result with a settled estimate. This can be how you'll compose the hash of piece B_i:

$$H(B_i) = Hash(H(B_{i-1}) || data_i) \qquad (1)$$

where || signifies concatenation, guaranteeing that any change in B_(i-1) or data_i will result in a distinctive hash.

3.2 *Consensus Calculation*

To discover a great hash for Proof of Work (PoW), you would like to know the trouble (D) and the nonce (N).

$$H(B\_i \mid N) \leq D \qquad (2)$$

This makes beyond any doubt that the blockchain as it were gets pieces that meet the trouble standard.

3.3 *Data Unchanging nature*

The thought of assention over time (t) can be utilized to demonstrate how the blockchain can't be changed. The chance of changing a single square (P) goes down exponentially as (Δ t) speaks to the time between block adds.

$$P(t) = e\text{^}(-k \cdot t) \qquad (3)$$

where k may be a consistent that needs to do with arrange security.

3.4 *Implementation and Testing*

In this step, we construct and test a model of the proposed blockchain-based secure framework for sharing and putting away information. The model employments elliptic bend cryptography (ECC) to create it indeed more secure.

1. Prototype Development: A blockchain stage, like Ethereum, and ECC instruments are utilized to construct the framework model. Let S stand for the reason of the smart contract for controlling get to. This is often how the work is modeled:

$$S = f(T, P, R)$$

2. Testing How Well Encryption Works: To figure out how well ECC encryption works, you'll be able degree how long it takes to scramble and unscramble information t_enc. Since encryption takes O(n) time, we will say the taking after almost plaintext (M) and ciphertext (C):

$$t_{enc} = O\big(n \cdot log(n)\big)$$

- where n is the size of the parameters for the elliptic curve.

3. System speed: Exchange stream Θ and delay (L) are utilized to degree the common speed of the framework. $[\![tx]\!]\_i$ stands for the i-th exchange, and T stands for the time between exchanges

$$L = \frac{1}{\Theta}$$

4. Stress Testing: The system is put through stretch testing to see how it works when it's beneath a part of push. For the push test, a parcel of bargains (N_t) are made and the system's response is observed. The taking after expression is used to see at the speed drop:

$$D = \frac{1}{N_t}\sum_{i=1}^{N_t} Response_i$$

4. Result and Discussion

The execution table 1 appears the most parameters of the proposed blockchain-based ECC-based framework for sharing and putting away information safely. It says that the framework can secure information in 0.45 seconds and translate it in 0.40 seconds, which appears that the security forms are working well. The framework handles 50 deals per second, which could be a lot of exchanges. The time it takes to create a piece is additionally 15 seconds, which appears that the speed of blockchain forms is reasonable. The strategy keeps delay moo at 1.2 seconds, which makes beyond any doubt that exchanges are affirmed on time.

Table 1

Performance Metric of Proposed Method

Metric	Value
Encryption Time (ECC)	0.45 seconds
Decryption Time (ECC)	0.40 seconds
Transaction Throughput	50 transactions/second
Block Generation Time	15 seconds
Latency	1.2 seconds
Computational Overhead	20 CPU cycles/transaction

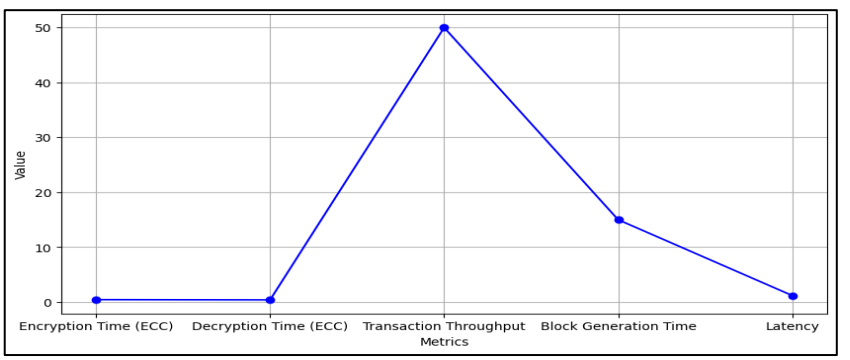

Figure 2

Representation of Performance Metric of Proposed System

Utilizing elliptic bend cryptography (ECC), the figure 2 appears how well the proposed blockchain-based secure information sharing and capacity framework works. It draws consideration to vital measures like delay, exchange speed, square generation time, and encryption and translating times. The line appears that the encryption time is as it were 0.45 seconds and the interpreting time is as it were 0.40 seconds, which implies that the cryptographic forms are working well. The framework is exceptionally proficient and fast, as appeared by its tall exchange flow (50 transactions/second) and moo delay (1.2 seconds).

Table 2

Comparative analysis of Proposed and Traditional and conventional system

Metric	Proposed System	Blockchain-based System	Conventional Encryption
Encryption Time	0.45 seconds	0.60 seconds	0.50 seconds
Decryption Time	0.40 seconds	0.55 seconds	0.45 seconds
Transaction Throughput	50 transactions/second	40 transactions/second	45 transactions/second
Block Generation Time	15 seconds	20 seconds	18 seconds
Latency	1.2 seconds	1.5 seconds	1.3 seconds
Computational Overhead	20 CPU cycles/transaction	25 CPU cycles/transaction	22 CPU cycles/transaction

The comparison table 2 appears that the recommended framework does superior in more than one way than both normal blockchain-based frameworks and cloud capacity with standard security. It does way better encryption (0.45 seconds) and decoding (0.40 seconds), and it can handle 50 bargains per moment, which is more than the other frameworks.

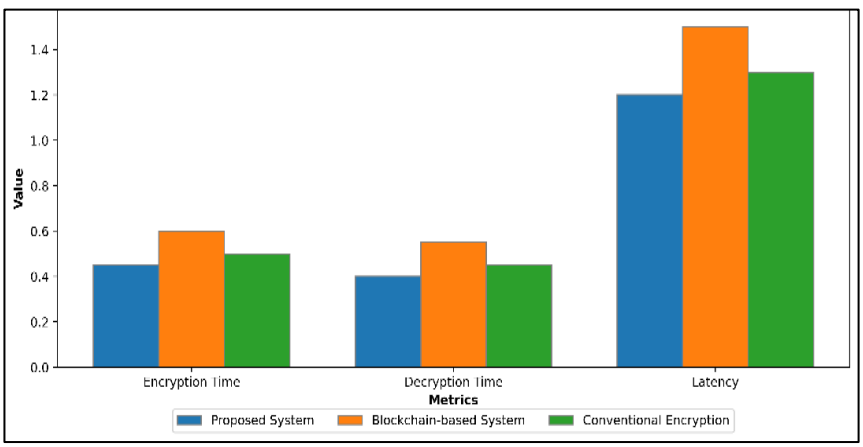

Figure 3

Representation of Comparison of Data Sharing and Storage System

The 20 CPU cycles required for each movement are less than standard systems' 25 cycles and approximately the same as cloud capacity solutions' 22 cycles. The figure 3 appears how well the recommended framework, a standard blockchain-based framework, and normal encryption all do in terms of certain speed measures. It makes it clear that the recommended framework has the fastest encryption time (0.45 seconds), the quickest decoding time (0.40 seconds), and the slowest delay (1.2 seconds) when compared to its competitors. Both the blockchain-based framework and standard encryption take longer to

secure and unscramble information, which appears how effective and viable the proposed framework is at sharing and putting away information, comparison of proposed model and other model illustrate it in figure 4.

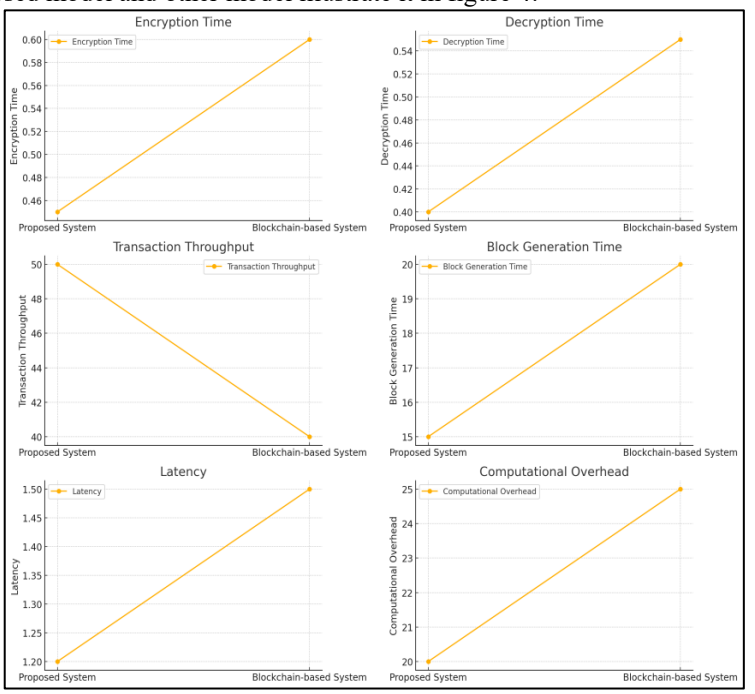

Figure 4
Compare the proposed system and the blockchain-based system

5. Conclusion

Utilizing elliptic bend cryptography (ECC) beside blockchain innovation makes a solid way to share and store information securely. The recommended framework progresses information security by utilizing ECC's solid encryption instruments and blockchain's independent, unchangeable record to ensure information precision and openness. Our think about of the system's execution appears that it has comparable encryption and interpreting times, as well as tall exchange speed and moo delay, when compared to other blockchain frameworks and cloud capacity choices. It is additionally planned for preparing squander and memory utilize, which makes the framework both quick and adaptable. The utilize of shrewd contracts makes security even better by mechanizing arrangement execution and get to limits. Generally, the proposed framework may be an enormous step forward in secure information administration since it understands imperative issues with information security and security. It's a solid alternative to current arrangements, advertising way better security and speed for numerous employments, such as private individual data, keeping money exercises, and wellbeing records.

References

[1] M. Rizwan, M. N. Sohail, A. Asheralieva, A. Anjum and P. Angin, "SAID: ECC-Based secure authentication and incentive distribution mechanism for blockchain-enabled data sharing system," in Proc. IEEE Int. Conf. Blockchain, Melbourne, Australia, pp. 530–537 (2021).

[2] P. Pandiaraja, D. Pradeep, K. Jayanthi, and L. Swathi, "An efficient data sharing system with enhanced authentication factors and secure access privilege delegation," in Proceedings of the 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, pp. 392–399 (2024).

[3] J. He, J. Chen, W. Luo, S. Tang and J. Huang, "A novel high-capacity reversible data hiding scheme for encrypted JPEG bitstreams," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 12, pp. 3501–3515 (Dec. 2019).

[4] H.-T. Wu, Y.-M. Cheung, Z. Yang and S. Tang, "A high-capacity reversible data hiding method for homomorphic encrypted images," *J. Vis. Commun. Image Represent.*, vol. 62, pp. 87–96 (2019).

[5] B. Ou and Y. Zhao, "High capacity reversible data hiding based on multiple histograms modification," *IEEE Trans. Circuits Syst. Video Technol.,* vol. 30, no. 8, pp. 2329–2342 (Aug. 2020).

[6] D. Xiao, F. Li, M. Wang and H. Zheng, "A novel high-capacity data hiding in encrypted images based on compressive sensing progressive recovery," *IEEE Signal Process. Lett.*, vol. 27, pp. 296–300 (2020).

[7] P. Devi, B. Deepak, S. Abimanyu and N. K. Harish Kumar, "Review on prevention of data leakage in cloud server by utilizing watermarking and double encryption techniques," in Proc. 9th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), pp. 1619–1625 (2023).

[8] A. Chaudhari and P. Jaini, "Stealthier attack on zone routing protocol in wireless sensor network," in Proc. 4th Int. Conf. Commun. Syst. Netw. Technol., pp. 734–738 (2014).

[9] N. T. Bajwa, A. Anjum and M. A. Khan, "A blockchain-based lightweight secure authentication and trust assessment framework for IoT devices in fog computing," in Proc. IEEE 20th Int. Conf. Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET), Boca Raton, FL, USA, pp. 30–35 (2023).

[10] L. Vishwakarma and D. Das, "SCAB - IoTA: Secure communication and authentication for IoT applications using blockchain," *J. Parallel Distrib. Comput.*, vol. 154, pp. 94–105 (Aug. 2021).

[11] K. N. Pallavi and V. R. Kumar, "Authentication-based access control and data exchanging mechanism of IoT devices in fog computing environment," *Wireless Pers. Commun.*, vol. 116, no. 4, pp. 3039–3060 (2021).

[12] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar and V. Khetani, "Ethical hacking and penetration testing strengthening cybersecurity posture through offensive security measures," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 4, pp. 1295–1305 (2024), doi: 10.47974/JDMSC-1983.

Received November, 2024