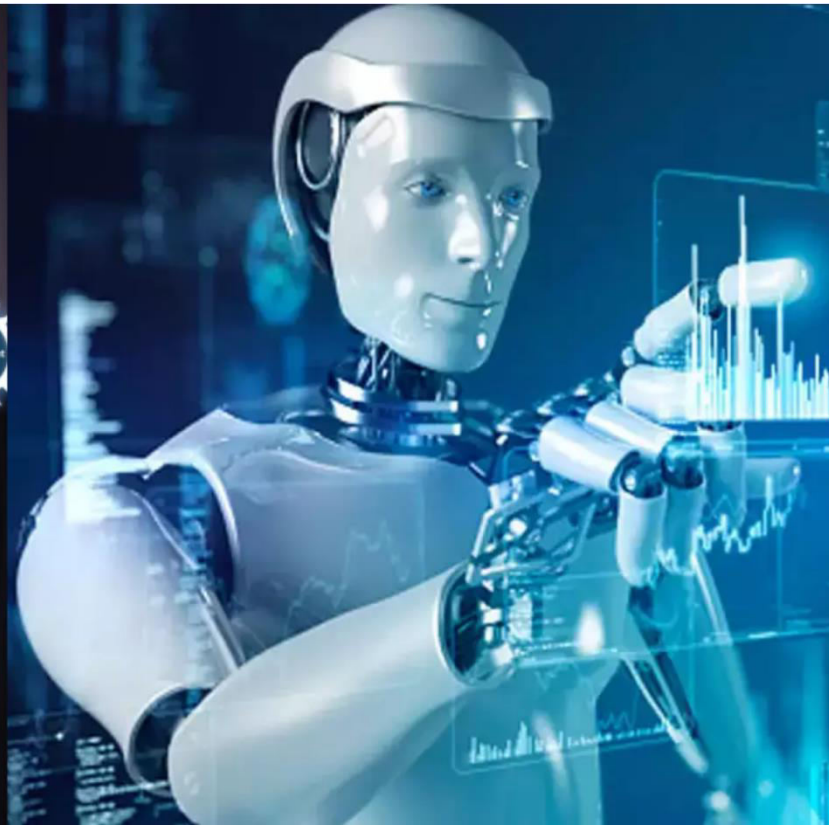
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 8, August 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

A Blockchain-Based Framework for Secure Image Storage and Sharing using Elliptic Curve Cryptography

Naveen Kumar Reddy Basireddy, Mahesh Sreenag Bukkapatnam, Chandrakanth Kosana, Sai Srikar Dabbukottu

U.G. Student, Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bengaluru India

U.G. Student, Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bengaluru India

U.G. Student, Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bengaluru India

U.G. Student, Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bengaluru India

ABSTRACT: As technology continues to rapidly advance, various data sharing technologies have increasingly permeated across different fields. As a result, the importance of ensuring both data sharing and security has become paramount in unlocking the true value of data. However, the traditional model of data sharing lacks the ability to effectively monitor electronic data usage, which presents a significant challenge. Additionally, the reluctance of data providers to share their data further compounds this issue. In order to address the issues of traditional centralized data sharing and management in terms of security and control, this research proposes a blockchain-based image storage and sharing system that utilizes elliptic curve cryptography (ECC) for secure image encryption. The system allows authorized users to upload images and send requests for access, which are then stored securely on the blockchain. The system's smart contract enables access control mechanisms that ensure only authorized users can access the images. The proposed system provides high security and privacy, ensuring that only authorized users with the correct decryption key can view the encrypted images. This research demonstrates the proposed system's feasibility, security, and efficiency, making it a highly secure and transparent platform for storing and sharing images. Incorporating ECC encryption provides an additional layer of security to the image storage system, making it a robust and reliable solution for industries thatrequire secure image storage and sharing, such as healthcare, finance, and government.

KEYWORDS: Blockchain, Cryptography, ECC, Image security.

I. INTRODUCTION

Blockchain-based secure image encryption using ECC (Elliptic Curve Cryptography) is a method of securing visual data by combining blockchain technology's security with ECC's advanced encryption capabilities. This approach is designed to provide high security for sensitive visual data, making it difficult for unauthorized parties to access or tamper with the data.

ECC is a type of public-key cryptography that is based on the mathematics of elliptic curves. It is widely used in secure communication protocols, including HTTPS, SSL, and TLS. The use of ECC in combination with blockchain technology provides an extra layer of security for visual data, making it more difficult for hackers or unauthorized users to access or tamper with the data. Blockchain technology provides a decentralized ledger for storing and sharing visual data. By using a distributed network of computers to validate and record transactions, blockchain technology ensures that the data is tamper-proof and transparent. Combining this technology with ECC allows the visual data to be securely

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

encrypted, and authorized parties can only control the decryption process.

Overall, blockchain-based secure image encryption using ECC is a powerful tool for securing sensitive visual data, and has the potential to revolutionize how image data is shared andprotected in various industries

A. Overview

In this paper, a novel scheme for securing images on the blockchain using ECC has been proposed. It involves encrypting the image using the ECC technique before storing it on the IPFS (Inter Planetary File System). The IPFS then generates a hash value for the encrypted image, which is used to retrieve the image from the blockchain. The Ethereum blockchain has been chosen due to its flexibility and security features, as it offers a robust smart contract framework and is well-suited for managing digital assets. The proposed scheme offers several benefits, including enhanced security and privacy for sensitive image data. By leveraging the advanced encryption capabilities of ECC and the tamper-proof nature of the blockchain, the proposed scheme provides a high level of protection against unauthorized access and tampering of the images. Additionally, the use of IPFS for storage ensures that the images are easily accessible and retrievable, while also reducing the risk of data loss.

B. Objectives

The objectives of a blockchain-based secure image encryption project are to provide enhanced security, privacy, and accessibility for digital images. The key objectives of such a project include:

1. Secure Image Encryption: The primary objective of this project is to develop a secure method of encrypting images using elliptic curve cryptography (ECC). ECC is a highly secure form of public key cryptography, and it is well-suited to the encryption of large data sets like images.
2. Integration with blockchain: The project aims to integrate the ECC-based image encryption method with a blockchain-based system. The blockchain technology will ensure the security and transparency of the image encryptionprocess, making it more difficult for unauthorized parties to access the encrypted images.
3. Decentralized storage: The project aims to store the encrypted images on a decentralized storage system, such as the Inter Planetary File System (IPFS). Decentralized storage will ensure that the images are highly available and resistantto censorship or data loss.
4. Authentication and verification: The project also aims to develop a method of authenticating and verifying the encrypted images using blockchain-based smart contracts. This will enable users to ensure the authenticity and integrityof the images they receive.
5. Improved security: By encrypting the digital images and storing them on a decentralized blockchain platform, the risk of data breaches and unauthorized access is reduced, providing enhanced security for the images.

C. Motivation

Blockchain technology has grown by leaps and bounds in recent years, revolutionizing how we store and access data. With the significant rise in the usage of dApps (Decentralized Applications) and smart contracts, blockchain technology is being applied everywhere, from storing simple documents topowering complex metaverse ecosystems.

However, when storing and sharing images on the web, the current data storage farm systems have several vulnerabilities. The images stored in such systems can be easily accessed by unauthorized users, putting the privacy and security of the images at risk.

To address this issue, the proposed method of encrypting images using ECC and storing them on a blockchain-based system offers a much more secure alternative. By encrypting the image using ECC and sending it along with the decryption key to the intended user, the image can be viewed only by those whom the author of the image has granted access.

This method also provides the author with complete control over who can view the image, as they can easily grant or revoke access at any time. As the image is stored on the blockchain and uses the digital signature of the user, there is an immutable record of who has accessed the image, providing a strong level of accountability and transparency. Overall, this proposed method of using blockchain technology to secure image encryption offers a robust solution for storing and sharing images online, providingusers with greater control and privacy over their data.

D. Problem Statement:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

Existing techniques for image encryption often rely on a centralized authority and a trusted third party, which can result in security issues and potential vulnerabilities. This is because centralized systems have a single point of failure, and any security breaches or attacks on the central authority can compromise the entire system.

The challenge in developing secure image encryption solutions is to provide a safe and secure system without relying on a centralized authority or requiring human intervention. Blockchain-based systems can help address this challenge by providing a decentralized and distributed infrastructure that ensures the integrity and security of storedand shared data. The challenge of developing secure image encryption solutions requires the development of decentralized and distributed systems that can ensure the security and privacy of data without relying on a centralized authority. Blockchain-based systems that use cryptographic techniques can help address this challenge and provide a more secure and reliable solution.

II. LITERATURE SURVEY

In recent years, the topic of security and privacy in cloud storage has garnered significant attention from researchers. It has become increasingly evident that centralized cloud storage systems are susceptible to vulnerabilities that can compromise the confidentiality of sensitive data. In light of this, researchers have proposed numerous techniques to tackle these challenges and safeguard the privacy and security of datastored in the cloud.

Throughout this literature survey, we have extensively examined research articles that concentrate on the preservation of privacy in the cloud, as well as identifying and mitigating security vulnerabilities. Our analysis has delved into the utilization of blockchain technology and image encryption algorithms as potential solutions to these challenges.

As per the literature [1] proposes a Blockchain-based XOR Elliptic Curve Cryptography (XORECC) method to enhance the security of IoT-based patient health monitoring systems. By addressing vulnerabilities and potential attacks on medical data, the proposed method aims to improve data confidentiality and integrity. Evaluations against traditional encryption methods like AES and RSA show that XORECC provides superior security for data transmission

Encryption has been implemented using multiple methods each offering distinct mechanisms. Studies in [2][3] demonstrates AES and logistic mapping technique and fractal matrix method for enhancing security. [4] explores image encryption utilizing a chaotic system which is significantly more challenging for an attacker to intercept and decipher the key. [5] highlights a visual cryptography for encrypting images. In their study, Huang et al. proposed a color image encryption framework that incorporates a permutation- diffusion operation [6]. This particular method is characterized by a low computational complexity and a high processing speed. The integration of blockchain technology with Internet of Things (IoT) security, highlighting blockchain's potential to address IoT challenges was proposed [7]. Blockchain enhances secure information exchange and authenticated transactions, contributing to decentralization, improved efficiency, and transparency

The proposed blockchain-aided searchable attribute-based encryption (BC-SABE) system [8][9] enhances data confidentiality and access control for IoT devices while addressing security and privacy issues. By replacing centralized servers with decentralized blockchain systems for key management and user revocation, the system eliminates the need for ciphertext re-encryption and key updates. The cloud server stores encrypted data, performs searches, and pre-decryption, significantly reducing the computational burden on users

Furthermore, the survey identified the challenges related to DoS attacks, which can significantly degrade the performance of a database server, rendering it unavailable to all users [10]. While a DoS attack may not reveal the contents of a database, it can cause substantial financial losses and time wastage for the victims. To address these challenges, some researchers have explored using a blockchain for securing images. Another research paper [11][12] investigates the use of blockchain technology to enhance cloud computing security against DDoS, MITM, and SQL injection attacks. It proposes incorporating blockchain features at each layer of the OSI. model to strengthen cloud defences. The integration of blockchain technology in cloud security holds significant potential for improving the security of cloud environments.

The use of blockchain and image encryption algorithms presents potential benefits in achieving these goals by

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

providing a secure and decentralized method for storing and sharing data in the cloud.

WORKING PRINCIPLE

A. Block Diagram

Input Image: The input image is the image that needs to be encrypted and protected from unauthorized access.

Encryption using ECC: The input image is encrypted using the Elliptic Curve Cryptography (ECC) algorithm, which is a public-key cryptography method used for securing data. ECC is used to generate a key pair that includes a public key and a private key. The public key is used to encrypt the data, and the private key is used to decrypt the data.

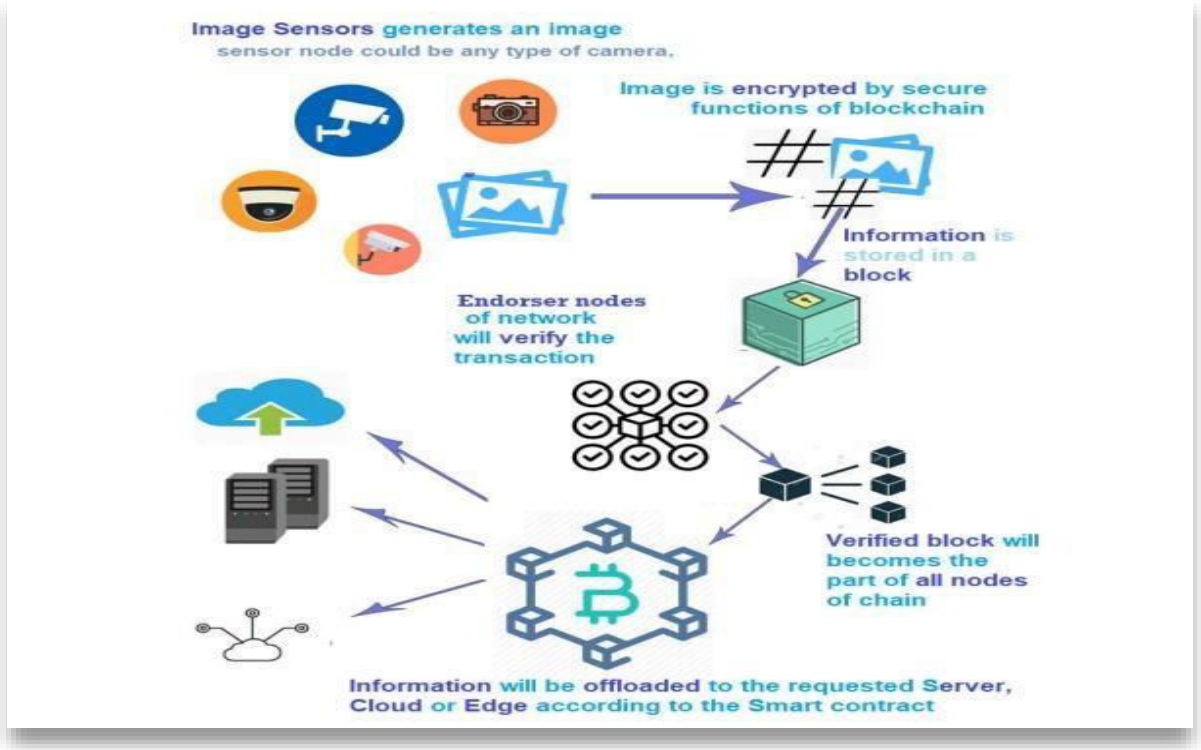


Fig. 1 Block Diagram

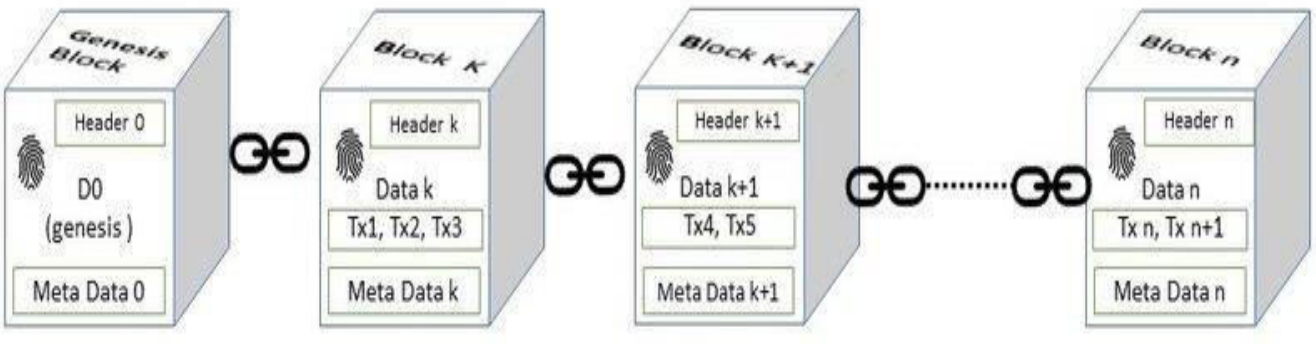


Fig. 2 Basic illustration of a block chain

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

Blockchain: The encrypted image is stored in the blockchain, which is a distributed and decentralized ledger that records all transactions on a secure network. The blockchain provides a high level of security by storing each block in the chain with a unique cryptographic hash that is linked to the previous block, making it almost impossible to alter any previous blocks without being detected.

Decryption using ECC: When the user wants to access the encrypted image, they use the private key to decrypt the image. Since the private key is only accessible to the authorized user, it ensures that the data is protected from unauthorized access.

Output Image: The decrypted image is the final output of the system, which can be accessed and viewed by the authorized user.
Overall, the system as in Figure 1 provides a secure and decentralized way to store and access images without the need for a centralizedauthority or trusted party.

B. Blockchain
Originally developed for monetary purposes, the blockchain has now evolved beyond cryptocurrency and is poised to have a significant impact on numerous industries. Its primary goal was to eliminate intermediaries from financial transactions by creating a trustworthy digital currency. A blockchain can be thought of as a digital ledger that maintains a comprehensive history of all transactions performed on the network. It is essentially a collection of interlinked blocks that are connected through hash values that have been generated over time. All information stored on the blockchain is permanent and immutable. Figure 2 provides a basic illustration of a blockchain, where the first block in the chain is known as the genesis block. Each node in the chain comprises all the relevant information and is connected to the previous node through a hashed address.

The salient features of Blockchain Technology (BCT) include:
1.Minting: Before adding a new block into the chain, the blockchain ensures the minting process. This involves creating a new block on the blockchain network that contains the details of the new cryptocurrency or token. This block is then validated by the network nodes and added to the existing blockchain, making the new cryptocurrency or token available for use.

2.Immutability: It is a fundamental attribute of a blockchain technology (BCT) that serves to safeguard the integrity of the network. The permanence of data stored on the blockchain ensures that it cannot be tampered with or corrupted, thereby establishing a high degree of trust and transparency. The hashing and encryption functions used by the blockchain are highly sophisticated, making it extremely difficult, if not impossible, to modify or reverse the data stored on it. If an attacker intends to alter the transaction data, they would have to modify the data across all nodes in the network, which is an extremely challenging feat to accomplish.

3.Reliability: It ensures the accuracy and consistency of the data stored on the blockchain. In a blockchain system, reliability refers to the ability of the system to maintain the integrity and security of the data, even in the face of potential threats or attacks.

3.Anonymity: It refers to the ability of users to perform transactions on the blockchain network without revealing their identities. Blockchain networks provide a certain level of anonymity by design, which has important implications for privacy and security. Users are identified by their public key, which is a randomly generated string of characters that acts as a pseudonym. Transactions on the network are linked to public keys rather than real-world identities, which provides a certain level of anonymity.

4. Decentralization: Decentralization is one of the core principles of blockchain technology, and it refers to the distribution of data and processing across a network of nodes rather than a single centralized authority. This approach provides several benefits, including increased security, resilience, and transparency.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

III. PROPOSED METHODOLOGY AND FLOW DIAGRAM

A. Methodology

The methodology for building a blockchain-based secure image encryption project shown in Figure 3 uses NodeJS, Angular, and Solidity and involves the following steps:

- Requirements gathering: Understanding the requirements and constraints of the project, such as the desired level of security, privacy, and accessibility, is critical to determining the most appropriate blockchain platform and encryption algorithms to use.
- Image encryption: Digital images are encrypted using secure encryption algorithms, such as ECC, before being sent to the blockchain platform.
- Blockchain platform selection: The Ethereum blockchain platform is selected, as it provides a robust and secure decentralized platform for the storage and management of encrypted image data.
- Smart contract development: Smart contracts are developed in Solidity, the programming language used for Ethereum, to manage the distribution and usage rights of the images, ensuring that they are only accessible to authorized users.
- Front-end development: A user-friendly front-end interface is developed using Angular, a JavaScript- based web framework, to allow users to interact with the blockchain solution.
- Back-end development: The back-end of the application is built using NodeJS, a JavaScript-based server-side framework, to handle image encryption and storage, as well as the interaction with the blockchain platform.
- Deployment: The smart contracts are deployed on the Ethereum blockchain, and the front-end and back-end of the application are deployed on a web server.
- Testing and validation: The application is thoroughly tested to ensure that it is functioning as expected, and that the encrypted image data is secure and accessibleonly to authorized users.

Uploading Image to Ethereum Network:

Firstly, the image must be encrypted using ECC before it is uploaded to the Ethereum network. This ensures that the image is secured and cannot be accessed by unauthorized parties. ECC is a powerful cryptographic algorithm that is commonly used in blockchain systems like Ethereum because it is secure and efficient, making it ideal for encrypting data that is to be stored on the blockchain.

Once the image has been encrypted using ECC, it can be uploaded to the Ethereum network using a dApp. The dApp will interact with the Ethereum network using smart contracts, which are self-executing contracts that are stored on the blockchain. The smart contract will define the rules and conditions for the image to be uploaded, including the fee that must be paid and the conditions for accessing the image.

When the image is uploaded to the Ethereum network, it will be stored on the blockchain as a transaction, just like any other data that is stored on the blockchain. The transaction will be broadcast to the network and validated by the nodes on the network. Once the transaction is validated, the image will be stored on the blockchain and can be accessed by anyone with the necessary permissions. Uploading an image to the Ethereum network after encrypting it using ECC requires the use of a dApp and smart contracts. This ensures that the image is secured and stored on the blockchain in a way that is transparent, decentralized, and tamper-proof. The use of ECC ensures that the image is encrypted and secure, which is crucial for maintaining the privacy and security of the data on the blockchain.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

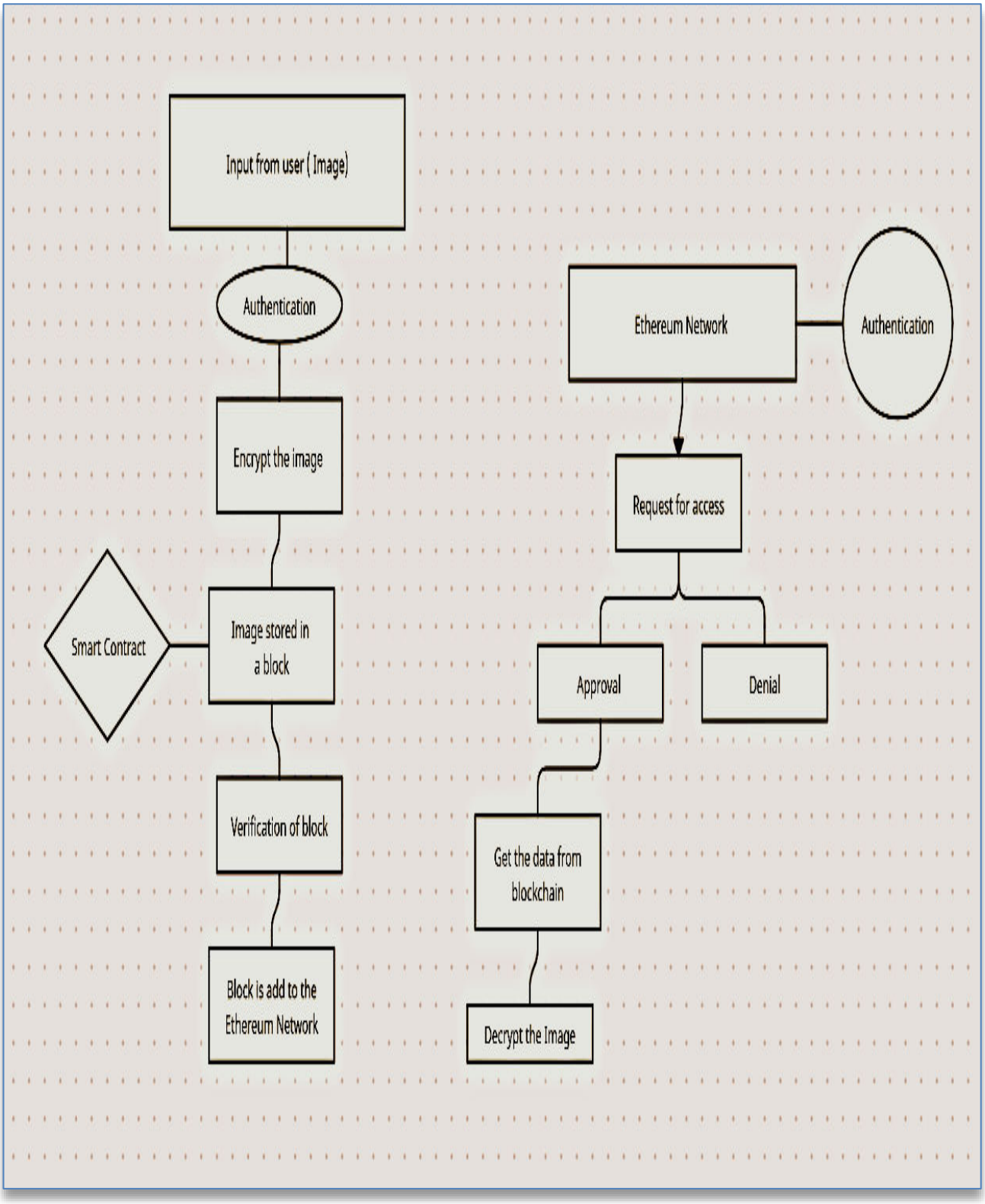


Fig. 3 Implementation Process

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

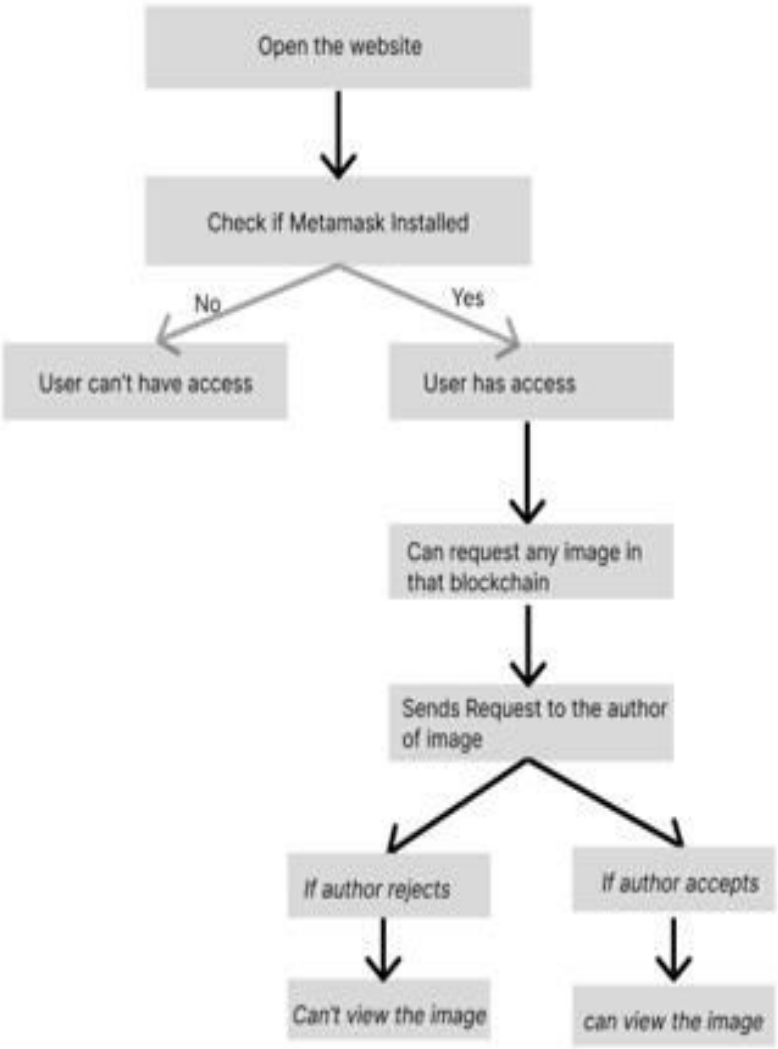


Fig. 4 Request Image Process

Sending Request:
When it comes to accessing an image that has been stored on the Ethereum network, it is necessary to send a request to the author of the image to grant or revoke access to view the image . This can be accomplished through a smart contract that is designed to manage access to the image.

To send a request to access an image that is available on the Ethereum network, the requester must first interact with the smart contract that is associated with the image. The smart contract is a self-executing contract that defines the rules and conditions for accessing the image, including the fee that must be paid and the conditions for granting or revoking access to the image.

The requester must submit a transaction to the Ethereum network that includes a request to access the image, along with any additional information that is required by the smart contract. The smart contract can be designed to include a notification system that alerts the author of the image that a request for access has been made.

Once the author of the image receives the notification, they can decide whether to grant or revoke access to the image.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

This decision can be communicated back to the smart contract, which will then update the access permissions for the image accordingly. If access is granted, the requester will be able to view the image and use it as needed. If access is revoked, the requester will no longer be able to access the image.

It is important to note that the use of a smart contract to manage access to an image on the Ethereum network is transparent and decentralized, which means that all transactions and data on the network are publicly visible. This includes the transactions that are used to request access to the image, as well as the transactions that are used to grant or revoke access to the image. Therefore, it is important to ensure that the smart contract is designed to protect the privacy and security of the data on the network. The Request image process is shown in Figure 4.

IV. RESULTS AND DISCUSSIONS

Implementation of a user interface (UI) and smart contract for uploading images and sending requests to access them is an important step towards the development of a secure and transparent image storage system using blockchain technology. The process is shown in Figure 5,6,7. However, there are still several critical functionalities that need to be implemented in order further to enhance the security and functionality of the system.

One key functionality that is implemented is the ability to send authorization for viewing images. This will involve creating a mechanism that enables the authorized users to access the images they have requested. This can be achieved by modifying the smart contract to include additional access control mechanisms, such as digital signatures or multi-factor authentication, that ensure only authorized parties can access the images. This will provide an additional layer of security to the system and prevent unauthorized access.

Another important functionality that is implemented is the use of elliptic curve cryptography (ECC) to encrypt the images before they are sent to the blockchain. This will involve incorporating ECC encryption into the smart contract and the user interface. By adding ECC encryption, the images will be securely encrypted as in Figure 8, and only authorized parties with the correct decryption key will be able to view them. This will provide a high level of security and privacy to the image storage system.

We have designed a basic webpage where user can login using their metamask wallet and upload image and written a smart contract to interact with Ethereum blockchain.

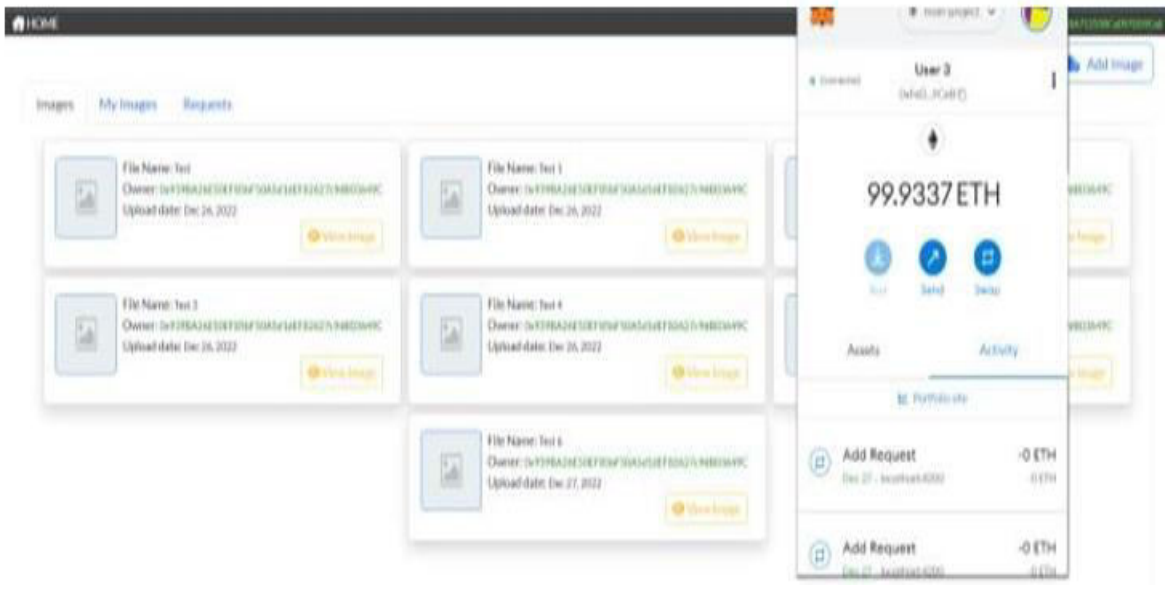


Fig. 5 Images available in the blockchain

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

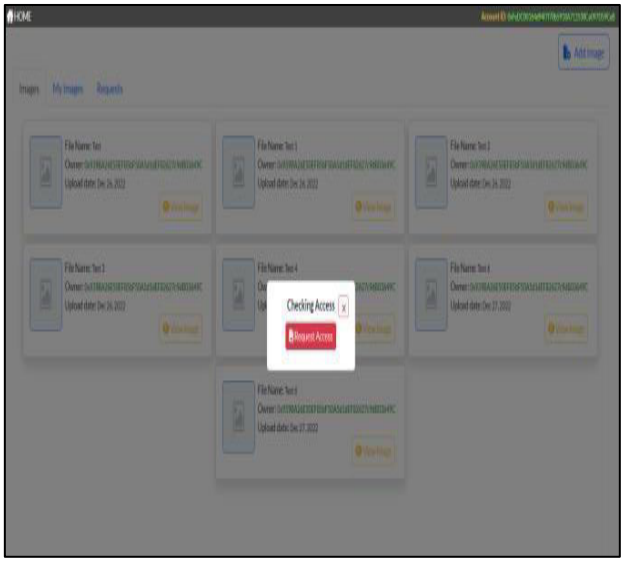


Fig. 6 Image Access Request

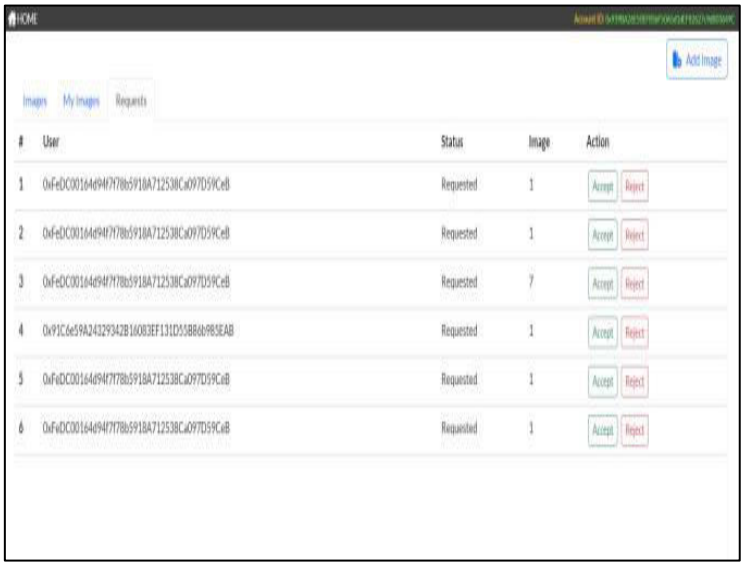


Fig. 7 Request Dashboard

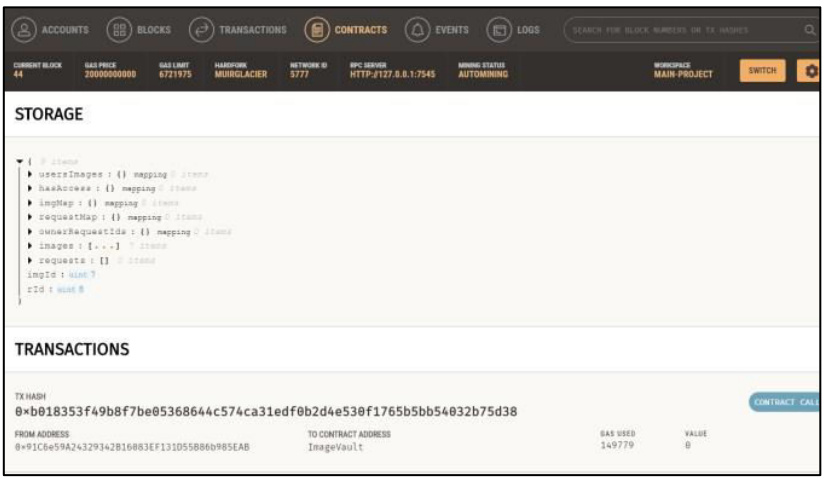


Fig. 8 Ganache snapshot of an encrypted image

V. CONCLUSION

In conclusion, blockchain-based secure image encryption is a promising solution that can offer several benefits, including improved security, increased privacy, faster and more efficient image sharing, reduced costs, and better traceability. By leveraging the decentralized and immutable nature of the blockchain, it's possible to create a tamper-proof system that provides enhanced security and privacy, while also facilitating more efficient and faster sharing of images. While the technology is still relatively new, its potential for use in a variety of industries, such as healthcare, finance, and e- commerce, is promising. As with any new technology, there are also potential challenges that need to be addressed, including scalability, adoption, and regulatory issues. Blockchain-based secure image encryption has the potential to transform the way we share and protect sensitive visual data. With continued development and refinement of blockchain-based encryption techniques, we can expect to see more widespread adoption of this technology in the future.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 8, August 2025

|DOI: 10.15680/IJIRSET.2025.1408091|

REFERENCES

1. Shalet Benvin; Arvind R; Sugunadevi C; S. Gomathi Meena; Sujo Oommen; Ramya Maranan, “Block Chain based Secured Wireless Patient Health Monitoring System”, 2023 7th, International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) , 10.1109/I-SMAC58438.2023.10290245
2. Meghana N, Sapna P J, “Multimedia Encryption for Enhancing Data Security Using AES and Logistic Mapping”, International Journal of Creative Research Thoughts (IJCRT), Volume 10, Issue 2 February 2022 | ISSN: 2320-2882
3. Pradhumn Porwal, Adarsh Kumar Panda, Himanshu Sarad, Hritambh Hritvij, Dr. Sapna PJ, “Security System Based on Image Encryption Using Fractal Matrix Method”, International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), Volume:04/Issue:07/July-2022 e-ISSN: 2582-5208
4. Wang, X.; Teng, L.; Qin, X. A novel colour image encryption algorithm based on chaos. Signal Process. 2012, 92, 1101–1108.
5. Shreyanka Chougule, Sapna P.J “Randomized Visual Cryptography to Enhance Security” 3rd IEEE International Conference on recent trends in Electronics, Information and Communication Technology, RTEICT-18th 19th May,2018
6. Huang, L.; Cai, S.; Xiong, X.; Xiao, M. On symmetric color image encryption system with permutation-diffusion simultaneous operation. Opt. Lasers Eng. 2019, 115, 7–20.
7. Hind Abu-tarboush; Jin Hie Lee; Maha Al-shrouf; Nowf O. Maaitah; Nidal A. Al-Dmour, “Blockchain and its Integration with IoT Security ‘ 2024 2nd International Conference on Cyber Resilience (ICCR), 26-28 February 2024, 10.1109/ICCR61006/2024.10533104
8. Suhui Liu, jiguo Yu, Yinhao Xiao, Zhiguo Wan, Shengling Wang, Biwei Yan “BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT, “, IEEE Internet of Things Journal(Volume: 7, Issue: 9, September 2020) , 10.1109/JIOT.2020.2993231
9. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications ,2011
10. Li, Y., Zhang, P., & Ma, L. (2019). Denial of service attack and defense method on load frequency control system. Journal of the Franklin Institute, 356(15), 8625 8645.
11. Sapna P J, S.S. Rajanandan Rao, Abhishek A.B, Prajwal B P, Karan Deshmukh, “Visual Cryptography using Quadri Directional Search Algorithm with Remote Accessibility” International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 9 Issue 07, July-2020
12. Nagendra Singh; Harsh Pratap Singh; Anuprita Mishra; Anula Khare; Mamta Swarnkar; Shekh Kulsum Almas, Blockchain Cloud Computing: Comparative study on DDoS, MITM and SQL Injection Attack, 2024 IEEE International Conference on Big Data & Machine Learning (ICBDML), 10.1109/ICBDML60909. 2024. 10577412

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details