



# 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 4, April 2025**

# **IPFS Based File Storage Access Control and Authentication Model for Secure Data Transfer using Block chain Technique**

**D.Uhesh, K. Upender, Y.Vishnu Priya, N.Venkata Sravya**

Department of CSE, Malla Reddy University, Hyderabad, India

**ABSTRACT:** In the digital age, ensuring the authenticity and security of academic certificates is a critical challenge faced by educational institutions, employers, and individuals alike. Traditional methods for verifying academic credentials are often cumbersome, time-consuming, and susceptible to fraud. However, the emergence of blockchain technology offers a promising solution to address these issues. The proposed system utilizes a blockchain network, where each academic certificate is stored as a digital asset on the blockchain. These digital certificates are cryptographically secured, time stamped, and associated with unique identifiers, such as hashes or public keys, ensuring their integrity and immutability. Anyone with access to the blockchain network can verify a certificate's authenticity, using the Meta Mask extension and Ethereum network, eliminating the need for intermediaries and reducing the risk of fraudulent credentials. The main strength of the paper is that the data that are stored in the blockchain are unique identifiers of the encrypted data, which is encrypted by using an encryption technique that provides more security to the academic certificates. Furthermore, IPFS is also used to store large amounts of encrypted data. We introduced the CHACHA20 encryption algorithm as an extension to the existing Chebyshev algorithm for enhanced security and faster encryption. Our evaluation reveals CHACHA20's superiority in computation time, being 70% faster. Additionally, we addressed network security concerns by incorporating intrusion detection systems, leveraging machine learning models. Traditional methods relying on human-defined traffic features are less effective in the era of big data. Our approach aims to improve accuracy by adapting to dynamic network behaviors without explicit feature engineering. This research contributes to securing data transfer and enhancing network security through innovative access control, encryption techniques, and anomaly detection mechanisms.

**KEYWORDS:** academic certificates, encryption, blockchain, Meta Mask, Ethereum, IPFS.

## **I. INTRODUCTION**

In the ever-expanding digital landscape, the need for secure and decentralized file storage and data transfer mechanisms has become paramount. Traditional centralized solutions pose inherent risks, such as a single point of failure and potential privacy breaches. This is where the integration of Inter Planetary File System (IPFS), blockchain, an sophisticated access control/authentication model comes into play.

### **Blockchain for Immutability:**

Integrating blockchain technology adds an extra layer of security through immutability. Each file transfer and access request can be recorded on the blockchain, creating an unalterable and transparent ledger. This not only ensures data integrity but also establishes a trustless environment where users can verify the authenticity of files and transactions.

### **Access Control and Authentication:**

A robust access control and authentication model is crucial for maintaining data confidentiality and preventing unauthorized access. Smart contracts on the blockchain can enforce access policies based on predefined rules. Public and private key pairs can be used for user authentication, adding an extra layer of security. Permission levels can be defined, allowing users to access only the files they are authorized to view or modify. Unlike conventional systems that rely on centralized servers for access management, this model leverages blockchain smart contracts to define and enforce file access policies. Users can upload files as either public or private, where public files are freely downloadable, and private files require the owner's approval before access. The authentication mechanism relies on blockchain's immutability and cryptographic security, making unauthorized access or data tampering nearly impossible. Additionally, all access

transactions are recorded on the blockchain ledger, ensuring transparency, auditability, and protection against malicious activities. By integrating decentralized authentication, fine-grained permissions, and blockchain-based access management, this system eliminates single points of failure, enhances data security, and ensures controlled and secure file-sharing in a distributed environment. To enhance security, **granular access control** allows file owners to grant specific permissions, such as "read-only" or "download access," depending on the requester's role.

**Secure Data Transfer:**

File transfers can be executed securely using cryptographic techniques. Encryption algorithms can be employed to secure the data during transit, ensuring that only authorized parties can decipher and access the content. The decentralized nature of IPFS ensures that the data is distributed across multiple nodes, reducing the risk of interception and unauthorized access during transfer.

**II. LITERATURE SURVEY****[1] A Blockchain-Based Framework for Data Sharing With Fine- Grained Access Control in Decentralized Storage Systems**

This review explores the synergies between IPFS and blockchain for decentralized file storage, emphasizing the evolving landscape of access control and authentication models. It provides insights into the advancements made in ensuring secure data transfer within this integrated framework.

**[2] A blockchain based incentive provisioning scheme for traffic event validation and information storage in VANETs**

Examining potential vulnerabilities, this paper investigates security challenges encountered during the integration of IPFS and blockchain for file storage. It offers a critical analysis of existing access control and authentication models, identifying areas for improvement and proposing novel solutions. Due to the resource constraints of vehicles, the blockchain is implemented on the RSUs. The RSUs get the aggregated packets sent by the vehicles. The packets contain the events' information that occur in the vehicles' surroundings. After verifying a packet, RSUs store the information related to the event in IPFS and reputation value of the sender vehicle in the blockchain. The reputation value of a vehicle is calculated based upon the correctness of an event .

**[3] Dynamic Access Control in IPFS: A Blockchain-Powered Approach**

Focusing on dynamic access control mechanisms, this work introduces a novel model that harnesses blockchain technology to adaptively manage access privileges within an IPFS-based file storage system. The paper discusses the implications of such dynamic controls on enhancing overall data security which determines how much data to store on each node, with the objective of minimizing the total amount of data stored in the network. By combining the memory-allocation algorithm with the data-interleaving algorithm, an optimal solution to realize the file storage scheme in tree networks is established.

**[4] SSS: A Personal File Storage System Considering Fairness among Users Based on Pure P2P Model**

Addressing scalability concerns, this study evaluates the performance of IPFS and blockchain integration in large-scale file storage systems. It assesses the impact on access control mechanisms and authentication processes, providing valuable insights into optimizing system efficiency. Replica control and fairness are realized by simple protocols without a trusted third party. SSS was implemented in Java. The measurement results showed that SSS recovers from a condition in which 80% of replicas has been lost within only 1 minute with keeping fairness.

**[5] Blockchain-Based Decentralized Storage Design for Data Confidence Over Cloud-Native Edge Infrastructure**

Focusing on the role of smart contracts in access control within IPFS, this survey delves into the intersection of blockchain- based smart contracts and decentralized file storage. It reviews existing models, identifies challenges, and proposes improvements for secure data transfer. When operating on a containerized edge infrastructure, this storage system provides higher data-transfer speeds than the interplanetary file system. This research thus blends the advantages of cloud-native frameworks with the security mechanisms of blockchain, crafting a storage system that addresses the present-day challenges of data management in decentralized settings.

### III. PROPOSED SYSTEM

The overview of our proposed system is shown in the below figure.

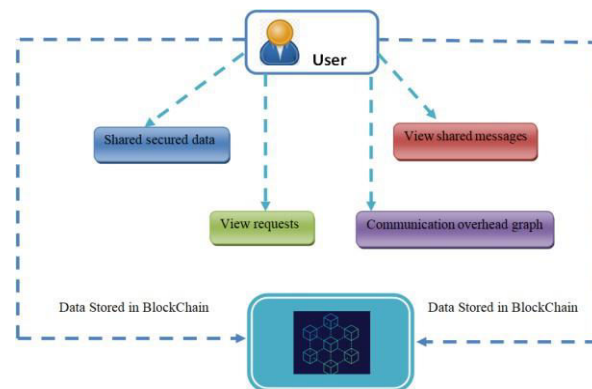


Fig. 1: System Overview

#### Implementation Modules

##### Data owner

- In this module, owner is registered and login with valid user name and password. After successful login, owner share the msg and upload the file to users. Before he uploads the file, the browser encrypts the data and stored into the cloud server.

##### User

- In this module, user is registered and login with valid user name and password. After successful, login, user view the shared msg details, and check the communication graph.

#### Chacha20 work

ChaCha20 generates a keystream that is XORed with the plaintext to produce ciphertext.

Step 1: State Initialization

ChaCha20 starts with a 16-word (512-bit) state matrix, consisting of:

$$S = \begin{bmatrix} C0 & C1 & C2 & C3 \\ K0 & K1 & K2 & K3 \\ K4 & K5 & K6 & K7 \\ C & N0 & N1 & N2 \end{bmatrix}$$

where:

$C0, C1, C2, C3$  = "expand 32-byte k" (constant)

$K0, K1, \dots, K7$  = 256-bit key

$C$  = Block counter

$N0, N1, N2$  = 96-bit nonce.

ChaCha20's core operation is a quarter-round, which mixes four state words using simple operations: for four words (a,b,c,d)

Addition:  $a = a + b$ ,

XOR:  $d = d \oplus a$ ,

Left Rotate:  $d = d \lll 16$  (circular shift left). ChaCha20 uses **20 rounds** to mix the state using quarter-rounds. After 20 rounds, the transformed state is added to the original state (mod  $2^{32}$ ) to generate a 512-bit keystream block.

$$S' = S + \text{Original } S$$

This keystream is then XORed with the plaintext:

$$C_i = P_i \oplus S'_i$$

$C_i$  = Ciphertext byte

$P_i$  = Plaintext byte

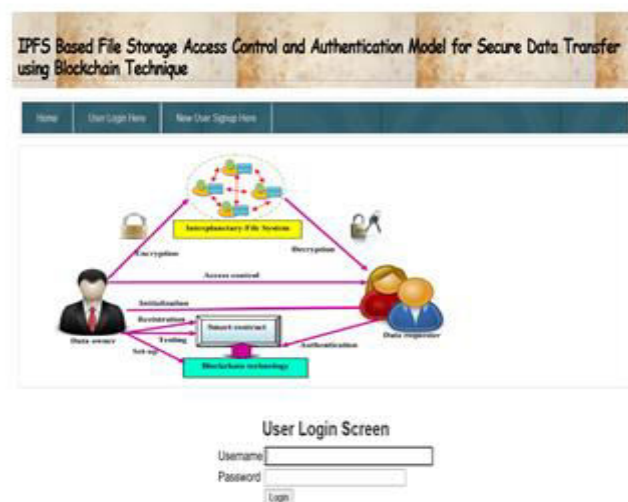
$S'_i$  = Keystream byte

## IV. RESULTS



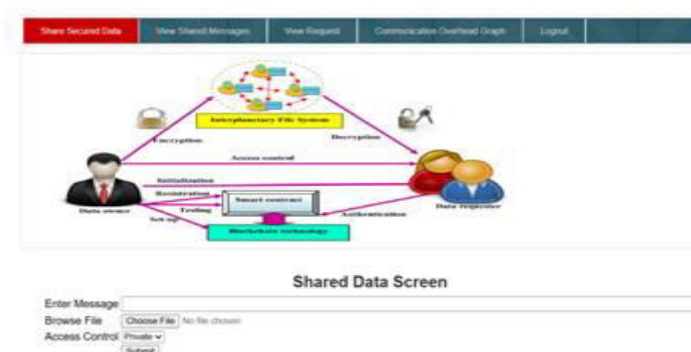
The screenshot shows the 'User Signup Screen' of the IPFS-based file storage system. At the top, there is a navigation bar with 'Home', 'User Login Here', and 'New User Signup Here'. Below the navigation bar is a diagram illustrating the system architecture, showing a user interacting with a blockchain network and a data repository. The main form contains the following fields: Username, Password, Contact No., Gender, Email ID, and Address. A 'Submit' button is located at the bottom right of the form.

Fig. 2: New Registration



The screenshot shows the 'User Login Screen' of the IPFS-based file storage system. At the top, there is a navigation bar with 'Home', 'User Login Here', and 'New User Signup Here'. Below the navigation bar is a diagram illustrating the system architecture, showing a user interacting with a blockchain network and a data repository. The main form contains the following fields: Username and Password. A 'Login' button is located at the bottom right of the form.

Fig. 3: Login Page



The screenshot shows the 'Shared Data Screen' of the IPFS-based file storage system. At the top, there is a navigation bar with 'Share Selected Data', 'View Shared Messages', 'View Request', 'Communication Overhead Graph', and 'Logout'. Below the navigation bar is a diagram illustrating the system architecture, showing a user interacting with a blockchain network and a data repository. The main form contains the following fields: Enter Message, Browse File, Access Control, and a 'Submit' button.

Fig. 4: Share File

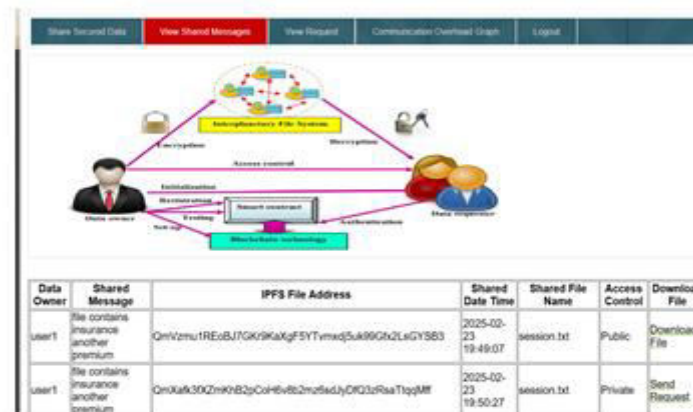


Fig. 5: View Shared File

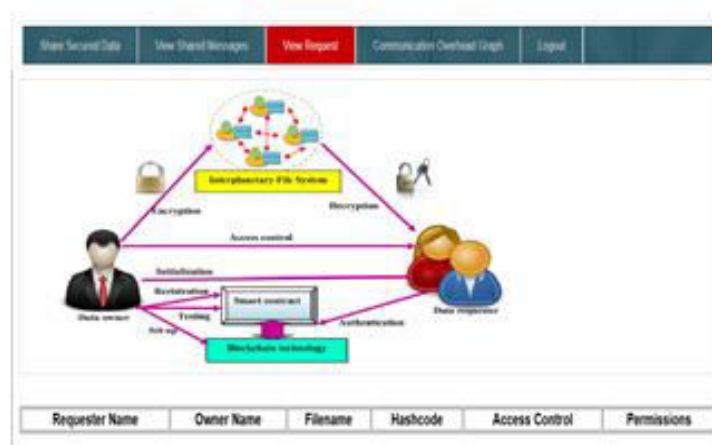


Fig. 6: Download File

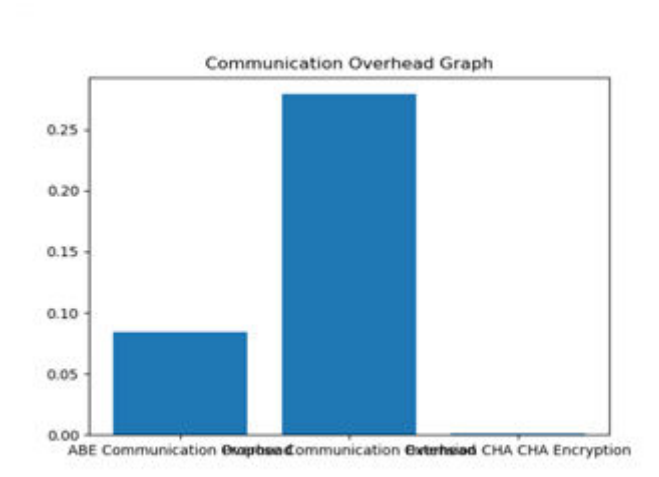


Fig 7: Communication Graph

## **V. CONCLUSION**

The IPFS-based file storage access control and authentication model using blockchain technology provides a comprehensive solution for secure and efficient data transfer. Its decentralized nature, coupled with robust security mechanisms, offers a promising framework for addressing contemporary data storage and transfer challenges. Future enhancements and broader application of this model could pave the way for more secure and reliable data management solutions across various industries. By allowing users to upload files with public or private access and managing permissions through blockchain, our system ensures data confidentiality and integrity. The extension of CHACHA20 encryption enhances security and efficiency in file encryption processes. Furthermore, the incorporation of intrusion detection systems addresses evolving threats in network security by adapting to dynamic traffic patterns without explicit feature engineering. Through these innovations, our proposed system not only provides a robust framework for secure file storage and transfer but also contributes to the advancement of network security practices.

## **REFERENCES**

- [1] Muneeb, M., et al. "A secure storage and data sharing model in IPFS based on blockchain." 2020 6th International Conference on Computer and Technology Applications (ICCTA). IEEE, 2020. This paper presents a model for secure storage and data sharing using IPFS and blockchain to enhance security and access control.
- [2] Singh, A., & Chatterjee, K. "Securing IoT devices through blockchain technology and IPFS." 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2017. The authors discuss using blockchain technology and IPFS for securing IoT devices, providing a solid
- [3] Liang, K., & Shen, H. "Secure and efficient data storage and sharing using blockchain and IPFS." *Future Generation Computer Systems* 107 (2020): 841-849. This study explores a method for secure data storage and sharing using blockchain and IPFS, addressing issues of data integrity and access control.
- [4] Ahmed, N., et al. "IPFS-Blockchain based secured data sharing platform for healthcare." 2019 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2019. A practical application of IPFS and blockchain for secure data sharing in healthcare, highlighting the benefits of the technology for access control and data transfer.
- [5] Cai, W., et al. "Decentralized applications: The blockchain-empowered software system." *IEEE Access* 6 (2018): 53019-53033. The paper provides an overview of decentralized applications, including the use of blockchain and IPFS for secure data storage and transfer.



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details