CR3ED: A Blockchain-based, Decentralized File Management Solution for Secure Collaboration in Web3 Ecosystems

Akshaj Vidyarthy
220953468
Department of I&CT
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal- 576104, Karnataka, India
Email:
akshaj1.mitmpl2022@learner.manipal.edu

S Sitaraman
200953080
Department of I&CT
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal- 576104, Karnataka, India
Email:
sitaraman.s@learner.manipal.edu

Nikillan Rajesh
220953620
Department of I&CT
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal- 576104, Karnataka, India
Email:
nikillan.mitmpl2022@learner.manipal.edu

***Abstract* - This paper presents CR3ED, an innovative solution designed to address the data security and collaborative requirements of decentralized autonomous organizations (DAOs) and Web3-based teams. CR3ED offers a scalable, permission-based file sharing system that ensures team-based access control through a hybrid AES-RSA encryption model. Files are stored on the Inter Planetary File System (IPFS), while blockchain technology enables immutable access permissions. CR3ED dynamically re-encrypts data to accommodate new team members, preserving historical file access while maintaining security. The system integrates Biconomy for gasless transactions and Push Protocol for real-time updates, providing seamless usability in decentralized environments.**

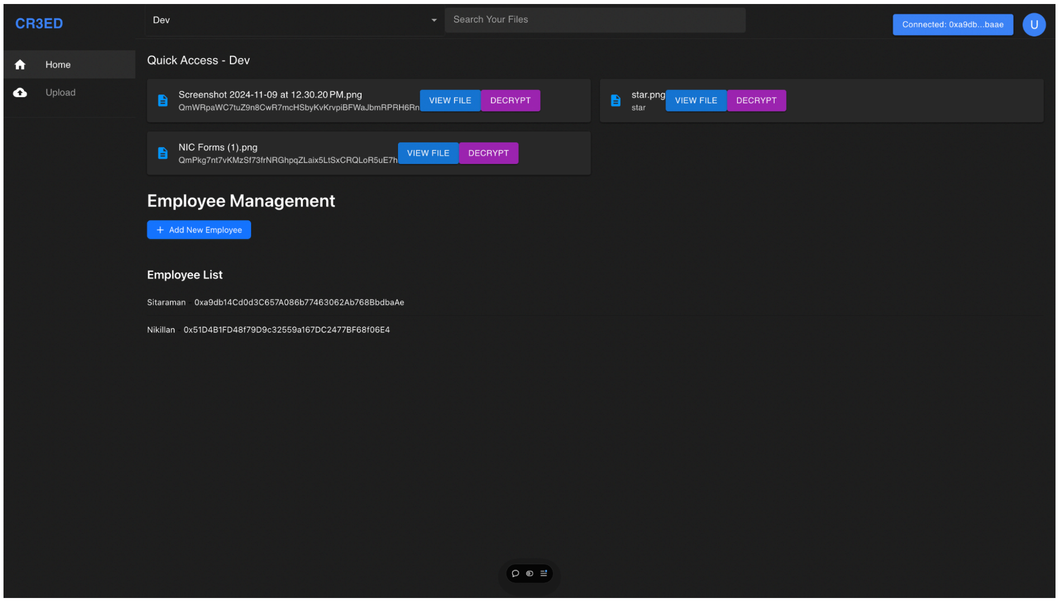
Index Terms—Decentralized File Management, Blockchain Access Control, Hybrid Encryption (AES-RSA), Permissioned File Sharing, Decentralized Autonomous Organizations (DAOs), Web3 Security, InterPlanetary File System (IPFS), Role-Based Access Control (RBAC), Gasless Transactions, On-Chain Data Integrity, Dynamic Key Management, Push Protocol Notifications, Biconomy Integration, Scalable Decentralized Systems, Data Privacy in Web3.

I. INTRODUCTION

Background: As blockchain and decentralized technologies gain traction, there is an increasing demand for secure, scalable, and reliable data-sharing systems tailored for decentralized teams, particularly DAOs. Traditional Web3 tools often lack robust encryption and dynamic access controls necessary for organizational use, making secure collaboration challenging.

Problem Statement: Existing decentralized storage solutions, like IPFS, provide an immutable file storage structure but lack strong, team-based security protocols. This limitation exposes sensitive information, as current systems often rely on personal rather than organizational-level security, lacking real-time updates for evolving team structures.

Objective: CR3ED aims to fill these security gaps by combining on-chain, permissioned access control with advanced encryption. The system dynamically adjusts access to sensitive files based on team membership, ensuring security and scalability. It provides DAOs and Web3 teams with secure data sharing, robust encryption protocols, and a decentralized architecture that evolves with team needs.



Screenshot 2024-11-09 at 12.30.20 PM.png
QmWRpaWC7tuZ9n8CwR7mcHSbyKvKrvpiBFWaJbmRPRH6Rn

star.png
star

NIC Forms (1).png
QmPkg7nt7vKMzSf73frNRGhpqZLaix5LtSxCRQLoR5uE7h

Sitaraman 0xa9db14Cd0d3C657A086b77463062Ab768BbdbaAe

Nikillan 0x51D4B1FD48f79D9c32559a167DC2477BF68f06E4

Fig 1. CR3ED Dashboard

II. RELATED WORKS

A. **IPFS and Decentralized Storage:** Recent studies explore IPFS's potential for decentralized file storage, particularly its capacity for data immutability and distributed access. While IPFS provides a decentralized means to store files, it lacks built-in encryption, posing risks in contexts requiring high security.

B. **Hybrid Encryption in Web3:** Hybrid encryption systems, like AES combined with RSA, have shown to be effective in balancing security with performance. Studies demonstrate that this approach allows for robust, scalable encryption while minimizing resource overhead, a key consideration for Web3 applications where efficient key management is essential.

C. **Blockchain-based Access Control:** Research has highlighted blockchain's ability to provide transparent, immutable records of access permissions. By storing access rules on-chain, blockchain-based access control enhances security but may incur high costs due to gas fees, a factor that CR3ED addresses through gasless transaction protocols.

D. **Role-Based Access in Decentralized Systems:** Role-based access control (RBAC) mechanisms have proven valuable for team-based access management in traditional IT systems. Adaptations for Web3 demonstrate that RBAC is highly compatible with smart contract-based solutions, enabling flexible and granular permissions within DAOs

F. **Gasless Transactions and Blockchain Efficiency:** Integration of protocols like Biconomy reduces transaction costs in decentralized applications. This approach has been increasingly adopted, as gasless transactions lower the barrier for broader usage of blockchain systems by DAOs and Web3 teams, making CR3ED's system more accessible

III. SYSTEM DESIGN & ARCHITECTURE

A. Overview

CR3ED's architecture combines decentralized storage, blockchain access control, and hybrid encryption. The system leverages **IPFS** for file storage, utilizing its immutable nature to maintain the integrity of stored files. Simultaneously, **Ethereum smart contracts** facilitate permission management on-chain, ensuring that access permissions are recorded and enforced immutably.

B. Hybrid Encryption Model

To secure files, CR3ED employs a **hybrid AES-RSA encryption model**:

- **AES (Advanced Encryption Standard)** is used for file encryption due to its efficiency in handling large datasets.
- **RSA (Rivest-Shamir-Adleman)** encryption provides secure key management, with encrypted AES keys stored in smart contracts.

  Upon file upload, the system generates a unique AES key for file encryption. This key is then encrypted using RSA for each authorized team member, stored securely in smart contracts linked to their public keys. This setup allows the system to re-encrypt data dynamically, adapting to changes in team structure without exposing past records.

C. Access Control Mechanism

CR3ED introduces a **Role-Based Access Control (RBAC)** model, which allows team leaders to manage permissions according to organizational roles. Access permissions are defined in smart contracts that can only be modified by authorized administrators, creating a permission hierarchy tailored to the organization's structure. When a team member's role changes or when new members are added, CR3ED dynamically re-encrypts the file keys for the new structure, enabling smooth and secure transitions.

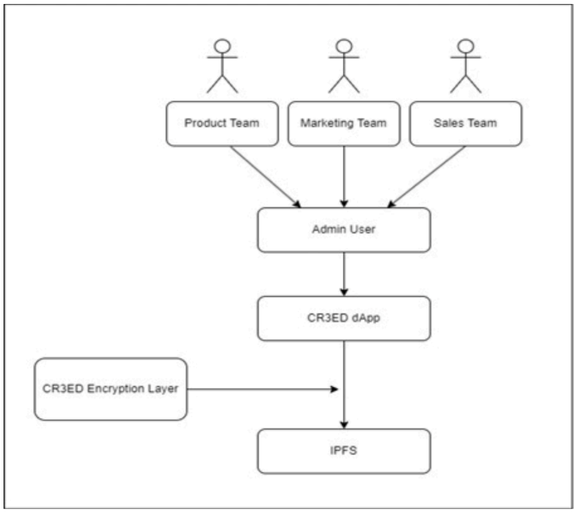


Fig 2. RBAC

D. Biconomy and Push Protocol Integration

- **Gasless transactions with Biconomy:** Describe the setup for gasless transactions and how it lowers barriers to entry, enabling cost-effective access control.
- **Push Protocol notifications:** Explore possible notification types (e.g., file access granted, permission changes) and how these keep users informed without central servers. Additionally, discuss potential extensions, such as integrating more notification options or adding automated reminders.

IV. IMPLEMENTATION

A. File Upload and Encryption

When a file is uploaded:

1. **AES encryption** is applied to secure the file.
2. The AES key is encrypted using each authorized member's **RSA public key**.
3. The encrypted file is uploaded to **IPFS**, and the corresponding AES key is stored in smart contracts with access permissions set according to team roles.

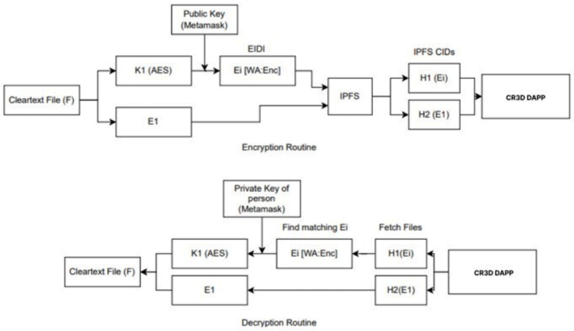


Fig 3. CR3ED Routines

B. Key Management and Dynamic Re-encryption

CR3ED addresses the need for **dynamic key management**. For instance, when a new team member joins, the AES key is re-encrypted using their public key, ensuring seamless access without affecting previous permissions. This is crucial for DAOs, where membership changes frequently, allowing real-time access updates without compromising historical data access.

C. Role-Based Access Control

Smart contracts enable administrators to assign roles with predefined access levels, ensuring that only authorized individuals can modify file access. These contracts serve as a decentralized access control list (ACL), providing auditability and transparency.

V. SECURITY AND PRIVACY ANALYSIS

A. Data Security

The CR3ED platform's data security framework relies on a hybrid AES-RSA encryption model to balance robust encryption with efficient performance. AES (Advanced Encryption Standard) encrypts file data due to its speed and ability to handle large data volumes effectively, making it an industry-standard choice for secure data handling. RSA encryption, applied to the AES key, leverages the strength of public-key cryptography to manage access, ensuring that only authorized users can retrieve and decrypt the AES key stored in smart contracts. This dual-layer encryption provides a high level of protection against unauthorized access, especially critical in decentralized environments where sensitive data is shared among multiple stakeholders.

CR3ED's dynamic key management is another essential security feature. By re-encrypting AES keys for new team members, CR3ED ensures that access permissions are adjusted without exposing historical access records. This adaptability is particularly valuable in the DAO context, where team membership can be fluid. Each re-encryption is verified on-chain, guaranteeing a traceable and transparent key exchange while protecting data from exposure during transitions.

B. Access Integrity

Access integrity within CR3ED is ensured through blockchain-based access control. Each permission change is recorded immutably on the blockchain, establishing a verifiable audit trail that provides a clear record of all modifications. This on-chain approach eliminates traditional vulnerabilities such as tampering or unauthorized access, as smart contract permissions cannot be altered without validation through secure blockchain transactions.

The use of Role-Based Access Control (RBAC) further enhances integrity by defining permission hierarchies that align with organizational roles. Only authorized administrators can modify these roles or add new members, ensuring a secure and streamlined approach to access control. Additionally, smart contracts function as decentralized Access Control Lists (ACLs), which provides transparency and allows team members to review access history and permissions, reinforcing trust within decentralized teams.

C. Privacy Preservation

To safeguard user privacy, CR3ED employs decentralized identifiers (DIDs) instead of traditional identifiers like email or phone numbers. DIDs facilitate anonymous, verifiable interactions within the system, which is crucial in Web3 environments where users prioritize privacy and often prefer pseudonymous identities. By avoiding centralized user identifiers, CR3ED minimizes exposure to data breaches and unauthorized identity tracking.

Furthermore, CR3ED's approach to privacy includes selective data sharing via the encrypted file structure and limited visibility based on team roles. Only essential access permissions and role metadata are stored on-chain, while private data remains secured off-chain on IPFS. This layered approach ensures that only necessary data is shared, thus preventing data leakage and promoting a privacy-by-design approach, aligning with emerging data protection standards within decentralized and Web3 ecosystems.

D. Future Enhancements for Security and Privacy

To strengthen CR3ED's security model, future enhancements could include integrating zero-knowledge proofs (ZKPs) for verifying user permissions without exposing sensitive data. ZKPs would allow users to prove access rights to specific files without revealing the contents or structure of those files, adding a layer of privacy-preserving authentication. Additionally, implementing more granular access controls within the RBAC structure would enable specific permissions at a finer level, such as read-only or edit-only access, providing DAOs with greater flexibility and security when sharing sensitive information.

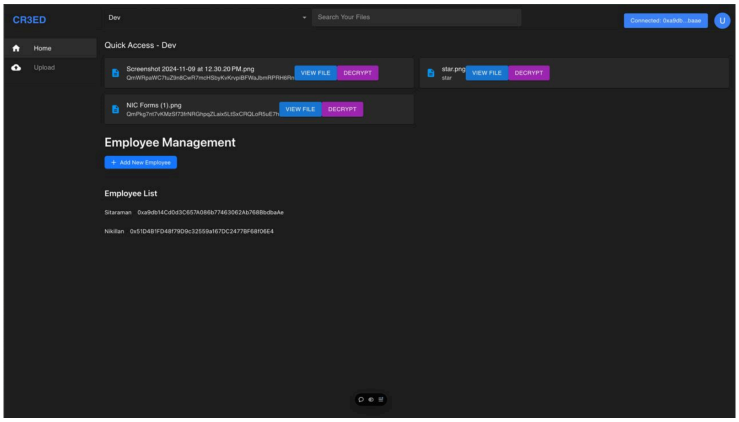
CR3ED could also explore decentralized insurance or staking models to provide economic incentives for maintaining security and privacy standards. This could further reinforce trust in the system by encouraging best practices in secure file management and incentivizing responsible data handling among team members.

VI. Application Flow and User Interface

The CR3ED platform provides a streamlined interface for decentralized file management, designed to ensure secure and efficient collaboration. The user experience is divided into two main sections: the **Home** page for quick access and the **Upload** page for securely adding new files to the system.

A. Home Page – Quick Access to Files

The **Home** page serves as the primary dashboard, where users can view and manage recently accessed files. This section displays the file names along with options for **View** and **Decrypt**. Files are listed with their IPFS hash, ensuring users can track and validate the integrity of each file stored on the decentralized network. Additionally, users can manage team access via the **Employee Management** section, where new members can be added to specific groups, with each user identified by their unique wallet address.



Quick Access - Dev

Screenshot 2024-11-09 at 12.30.20 PM.png
QmWRpaWC7tuZ9n8CwR7mcHSbyKvKrvpiBFWaJbmRPRH6Rn

star.png
star

NIC Forms (1).png
QmPkg7nt7vKMzSf73frNRGhpqZLaix5LtSxCRQLoR5uE7h

Employee Management

Employee List

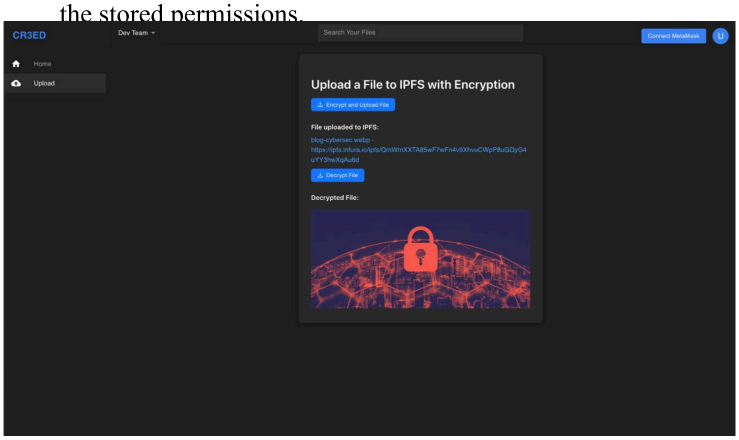
Sitaraman 0xa9db14Cd0d3C657A086b77463062Ab768BbdbaAe

Nikillan 0x51D4B1FD48f79D9c32559a167DC2477BF68f06E4

Fig 4. Home Page

B. Upload Page – Secure File Upload and Encryption

The **Upload** page is designed for securely adding new files to the IPFS network with encryption. Users begin by selecting the group (e.g., "Dev") to categorize their file. They then specify the team members authorized to access the file, using wallet addresses as identifiers. After setting their public key, users can proceed to **Encrypt and Upload File**, ensuring the file is encrypted with AES and the key is protected with RSA. This setup allows only authorized users to decrypt the file based on the stored permissions.



Upload a File to IPFS with Encryption

File uploaded to IPFS:

blog-cybersec.webp - https://ipfs.infura.io/ipfs/QmWmXXTA85wF7wFn4v9XhvuCWpP8uGQyG4uYY3hwXqAu6d

Decrypted File:

Fig 5. Upload Page

IV. CONCLUSION

CR3ED offers a secure, decentralized file management solution tailored for Web3 teams and DAOs. By integrating IPFS for storage, blockchain for role-based access control, and a hybrid AES-RSA encryption model, CR3ED ensures data security and adaptability. Its dynamic key management allows seamless team updates without compromising past permissions, meeting the collaborative needs of decentralized organizations.

The platform's use of gasless transactions via Biconomy and real-time notifications through Push Protocol enhances usability, making secure file sharing accessible and efficient. Looking forward, CR3ED has the potential to incorporate features like zero-knowledge proofs and expanded access controls, broadening its impact within the decentralized ecosystem.

In summary, CR3ED combines blockchain, decentralized storage, and advanced encryption to address the unique challenges of secure, permissioned data sharing in Web3, setting a foundation for future decentralized collaboration.

V. REFERENCES

1. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," 2014. [Online]. Available: https://ipfs.io
2. G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," *Ethereum Whitepaper*, 2014.
3. S. Devadas, et al., "Security Mechanisms for Blockchain Applications," in *Proceedings of the IEEE Blockchain Symposium*, 2017.
4. M. Al-Bassam, "DAOs and Decentralized Governance Models: A Survey," *Web3 Foundation*, 2020.

IS Project.pdf

ORIGINALITY REPORT

4%	3%	3%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	wap.dgxieli.com Internet Source	2%
2	www.atlantis-press.com Internet Source	<1%
3	Abubakar-Sadiq, Muhammad Shehu. "Establishing Secure and Privacy Preserving Digital Identity with Self-sovereign Identity", Universidade do Porto (Portugal), 2024 Publication	<1%
4	asmedigitalcollection.asme.org Internet Source	<1%
5	www.mhprofessional.com Internet Source	<1%
6	H L Gururaj, M R Pooja, Francesco Flammini. "Recent Trends in Computational Sciences", CRC Press, 2023 Publication	<1%