STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **x**, Month 202x, pp 0–18.
Published online in International Academic Press (www.IAPress.org)

A Decentralized and Secure File-Sharing System for Education Using Ethereum Blockchain and IPFS

Omar Z. Akif [1], Alaa Raad Salman [2], Marwa Hussien Mohamed [2,3,*], Haitham Rizk Fadlallah [4], Mostafa Ali [5,6]

[1] *Computer Science Department, College of Education for Pure Science (Ibn al-Haitham), University of Baghdad, Iraq, omar.z.a@ihcoedu.uobaghdad.edu.iq*
[2] *Computer Technology Engineering Department ,Engineering Technologies College, Al-Esraa University,Baghdad, 10081 IRAQ,alaa.raad@esraa.edu.iq ; maraw@esraa.edu.iq; eng_maroo1@yahoo.com*
[3] *Department of Information Technology, College of Informatics, MidOcean University, Moroni RP 98123, Comoros.marwahassan@midocean.edu.km*
[4] *Network Department, Faculty of Information Systems and Computer Science, October 6 University Giza, Egypt.Haitham.rizk.csis@o6u.edu.eg*
[5] *Information System Department, Faculty of Computers and Artificial Intelligence, Fayoum University, Fayoum 63514, Egypt,mam16@fayoum.edu.eg*
[6] *College of Engineering and Information Technology, Buraydah Private Colleges, Buraydah 51418, Saudi Arabia*

Abstract The growing adoption of digital platforms in educational institutions poses a major challenge in ensuring secure file storage and sharing. Conventional cloud storage services are popular but the centralized infrastructure they use can cause issues with data privacy, security and availability. In this paper, we propose a blockchain based file sharing system for educational environments to overcome these difficulties. We propose a system that combines the Ethereum blockchain with the InterPlanetary File System (IPFS) to securely store academic documents and control who can access and share them. Files are encrypted with AES-256 before being uploaded to IPFS, Ethereum smart contract protocols are used to manage file registration, ownership and access permissions. MetaMask is used for wallet based authentication, which allows users to interact with the blockchain and approve transactions. The system allows owners to manage their documents, view requests for access and share documents with authorized users. The experimental results indicate that the system can upload and download files but the performance is different for different file sizes. The study also points out important security considerations such as: encryption key management, smart contract vulnerabilities and file availability. To summarize, the proposed solution provides a practical approach in managing educational files and reducing the dependency on central storage. Further testing is needed to evaluate its performance, scalability, and security under different operating conditions.

Keywords Blockchain, Security Meta Mask, AES encryption, DFS (Distributed File System)

DOI: 10.19139/soic-2310-5070-4632

1. Introduction

*B*lockchain and smart technology have recently gained huge attention from industries due to their distributed immutable ledger system, which enables frictionless transactions between parties [1]. The financial sectors are the primary users of blockchain-based technologies.
However, their application has increased in the pharmaceutical business, the Internet of Things (IoT), public services, reputation systems, and smart contracts. The Blockchain can be viewed as a public ledger, with each transaction recorded in a block or list of entries. In the wake of the new block's introduction, this chain of records

*Correspondence to: Marwa Hussien Mohamed (Email: ,maraw@esraa.edu.iq; eng_maroo1@yahoo.com). Computer Technology Engineering Department ,Engineering Technologies College, Al-Esraa University,Baghdad, 10081

ISSN 2310-5070 (online) ISSN 2311-004X (print)
Copyright © 202x International Academic Press

continues to expand [2].
The three major features of the blockchain system are anonymity, persistence, and decentralization. Additionally, it makes auditing easier and boosts productivity [3]. Cloud computing, artificial intelligence (AI), and big data [4, 5] have all been enhanced integrated technologies transformed by blockchain technology. This concept enables bilateral multiparty transactions and is a novel application of innovative computer technologies.
A few of the different shapes of blockchain security concerns incorporate double-pending security dangers, shrewd contract dangers, mining pool security dangers, wallet security dangers, and arrange security potential perils [6].
When a user makes a transaction using the same cryptocurrency more than once, double spending is dangerous. Security risks to mining pools arise when miners cooperate to launch a 51% attack on the Network. Blockchain network security concerns incorporate DDoS (Distributed Denial of Service) attacks, directing attacks, segment attacks, delay attacks, and Sybil attacks are all cases of DDoS attacks. The most common private key security risks, or wallet risks, include signature weakness and a lack of control over address generation [3]. At last, the Ethereum Virtual Machine (EVM) and the robustness of blockchains fuelled by smart contracts have imperfections.
This study employs using of the Ethereum blockchain to encrypt the file data. This work contributes significantly in the following ways:

- A key contribution of this work is the publication of a unique way of using the log to the website without the username and password.
- We use the wallet key data to log in to the website and see your files using different sites like MetaMask wallet.
- All files of the users are uploaded to the account based on the file size. We will deduct the fees from the wallet for uploading the file and encrypting the data using AES encryption.
- The file owner authorizes access to the shared file, and the recipient must obtain the corresponding AES decryption key to recover the original content. The AES key is a symmetric cryptographic key and is distinct from the user's Ethereum wallet private key, which is used to authorize blockchain transactions.
- The main novelty of this work is the use of the Ethereum blockchain and MetaMask wallet to share files and encrypt the uploaded data .
- The combination of Distributed File System (DFS) and blockchain technology allows for off-chain storage of files using IPFS, with the blockchain maintaining the file hashes or content identifiers and relevant metadata. This method avoids storing large files directly on the blockchain and allows for decentralized file sharing. The peer-to-peer network offers improvements in scalability, reliability, and data availability but these benefits are dependent on network participation and content replication.

The contribution of this work is the implementation and integration of already known technologies such as smart contracts from the Ethereum platform, IPFS, MetaMask, and AES-256 encryption into the decentralized file sharing platform tailored for educational purposes. The platform incorporates wallet authentication, encryption of the files, decentralized file storage, and the, use of the blockchain for storing the file-related information. The goal is to show how these technologies can be used for educational file sharing and to assess the performance of the implemented system in terms of uploading and downloading files. Hence, the contribution of the work is more practical than scientific in nature.
Educational file sharing creates requirements going further than simple transportation and saving of the files. Students, teachers, scientists, and educational institutions' administration may have the need of having various access permissions to lecture files, assignments, scientific works, and students' records. Moreover, files created in the scope of education may contain sensitive information that needs to be protected from the illegal usage and disclosure. Thus, good educational file sharing platforms need to ensure confidentiality, ownership, permission sharing, and possibility of file owners to give permission to certain people to access particular files.
Integrity and traceability of file-sharing activities are equally essential in cases where scholarly content is shared between multiple parties. While the aforementioned technologies of distributed storage and blockchain can be used for this purpose, they do not ensure privacy, compliance with regulations, and institutional permission. For this reason, the current research examines the application of Ethereum, IPFS, MetaMask, and AES-256 encryption as a framework for the safe sharing of educational materials.
Research Questions and Criteria for Evaluation:.

Research Questions and Criteria for Evaluation:
The research will test the ability to apply Ethereum, IPFS, MetaMask, and AES-256 for a secure sharing of educational files. The following three research questions are raised in this context:
RQ1: To what degree can the suggested system ensure file privacy and access control to shared files?
RQ2: In what way does the file size and operations performed influence the speed of file uploading and downloading?
RQ3: What security and availability restrictions emerge from the implementation of blockchain and decentralized storage?
The criteria for evaluation include the following: time needed to upload the file, time required to download the file, file size, access control behavior, and security restrictions. File uploading and downloading will be evaluated using files of various sizes, while security issues will be considered within threat analysis.

The remainder of the paper is organized as follows: Segment 2 will discuss blockchain protocol, segment 3 will detail all the benefits and advantages of Blockchain in education, segment 4 will discuss the characteristics of Blockchain, segment 5 Ethereum and Hyperledger, segment 6 will discuss the related work , segment 7 will propose a framework, segment 8 results, and framework discussion and eventually the conclusion.

2. BLOCKCHAIN PROTOCOL

A blockchain system is managed by a set of rules that explains the steps required to (i) produce and verify transactions, (ii) generate and verify new blocks, and (iii) broadcast the block and modify the Network's current state. This process is used whenever two users interact with the system, as shown in Figure 1.

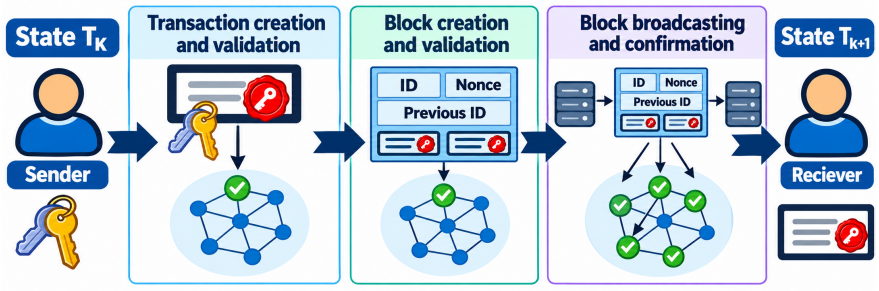


Figure 1. Blockchain protocol.

How to create and validate the transaction of Blockchain? Every user in the system over blockchains has a unique address connected to the wallet secured with cryptographic encrypted keys. Users in the Network use this key to log in to the wallet and verify that he is the wallet's owner and that transactions are distributed over the peer-to-peer Network so that these transactions are transparent. Every transaction is recorded on the system with a time stamp.
How to create and validate the block? Every block has a time for every transaction and is linked to the previous one based on the start time. The protocol uses cryptography to secure the data while creating the block using a hash function to add a block id. All information and transactions have many computations to verify that the users own this wallet and do this transaction.
How to broadcast the block and send it to the receiver? Every user on the Network has a copy of the blocks in the Blockchain with distributed data on the system. This system didn't fail and can update all errors automatically based on the data distribution and make a copy of data in different blocks. If one fails can get them from other blocks also, solve the data conflict. Finally, the interaction between users is very secure, and the system is decentralized, which is the main function of the Blockchain.

3. BLOCKCHAIN IN EDUCATION

Blockchain technology [5] was raised in 1991 for sharing digital documents and testing 'who,' 'what,' and 'when' to know and answer these questions. This technology was not used until 2009 with the launching of the first digital cryptocurrency Bitcoin. Satoshi Nakamoto uses this technology with Bitcoin, and its application now this cryptocurrency equals thousands of dollars in our real life. This data is secured digitally with Blockchain.
Why is it called cryptocurrency? Blockchains utilize cryptographic strategies to ensure the security of your cash [7]. Comparable techniques have been used in the keeping money sector for a long time to preserve the security of money-related exchanges. So, you might claim that cryptocurrency security is on standard with that of banks.
A blockchain block is made up of three parts [8]:

1. The data—its specifics and the participating nodes.
2. The hash of the block, which serves as an identification and is updated with each chain change.
3. The hash of the past block, which acts as a full log book.

Blockchain act like big data as the steps of creating data and how to divide the data into blocks, and how share and duplicate this data to save from missing also, it is not free of cost. This technology uses an 'Open Ledger' or 'Distributed Ledger' to encrypt the data with several nodes that must be defined first while creating the data sets.the datasets were connected via the same chain and Network and transparent to all Nodes using the hash keys.
Blockchain technology [9] can be used in education management as smart contracts to hire staff for a job in the school, follow performance and payments from day one in the work till the last day, and continue professional development.
Blockchain is used in education, like sending certificates [4, 10] understudies who complete all coursework. The University of Nicosia in Cyprus primarily sent the certification utilizing this innovation with genuineness confirmation using the Bitcoin blockchain.
Blockchain innovation can potentially move forward certification and accreditation administration and acknowledgment enormously. Blockchain innovation's permanence, straightforwardness, and integrity can significantly limit fraud.

Educational file-sharing platforms must support secure collaboration among students, teachers, and administrators while protecting confidential academic information. The proposed framework can be extended with a role-based access-control model in which permissions are assigned according to each user's institutional role.

1. Students can access their course materials, download learning resources, and upload assignments or project files for their teachers to review and evaluate.
2. Teachers can upload lecture notes, assignments, and research materials. They may accept or reject requests from other users to access their files.
3. Administrators manage user permissions and set access rules, controlling who can do what, and monitor things by reviewing system activity logs, all to make sure everything is running smoothly, and they don't need to look at the contents of individual files.

The system can be improved by logging file access activities such as access requests, approvals, rejections, timestamps, and file IDs. Such activities can be logged through blockchain smart contract events or transactions which make it easier to trace how files are shared and accessed.At the same time, sensitive user information and educational materials cannot be stored directly on the blockchain.
To safeguard user privacy, files should be encrypted prior to uploading them to IPFS. Also, the decryption keys must be well managed and shared only with users who are allowed access to files. The blockchain log should only include information necessary to manage access and review system activities. It is also important to ensure that the metadata associated with a transaction does not leak sensitive information, as information stored on the blockchain cannot be easily removed or changed.

Another important question is how the system behaves with revoked access. If you deny future access requests, users can still open files and use decryption keys they already possess. Additional measures such as rotation of

encryption keys or control of their distribution may be required to better manage access hence after revoking permissions. Addressing these issues would help improve the security, privacy, and overall reliability of the proposed system.

4. CHARACTERISTICS OF BLOCKCHAIN

We will list all characteristics of Blockchain and its importance in being used today [11]:

1. Decentralization: Each blockchain-to-peer block can track and hold each exchange. Without a third party's assistance, data is consequently traded and shared between nodes. In this decentralized framework, all members and nodes effectively participate in the activities and transactions. Decentralization could be a recognizing include of blockchain innovation that attracts more consideration than conventional systems' centralized authority.
2. Distrusting [2]: Due to the reality that blockchain innovation is utilized in a decentralized framework, clients don't ought to have a mutual belief to transfer data across organized nodes. The Blockchain uses decentralized or partial-center courses of action to establish trust between arranged nodes and disseminated framework structures. It is based on peer-to-peer organized convention essentials and simply scientific strategies. The Blockchain's pieces contain all the exchange information, making each exchange distrusting. A major issue that influences traders is belief within the business. The Blockchain addresses this issue with an agreement strategy and a hash work. Blockchain framework members are not capable of keeping up connections of shared trust.
3. Transparency [12]: All members share records and inquiry information on hubs in a decentralized framework through the Blockchain. Utilizing blockchain innovation, frameworks record and transmit information and data. Each part can inquire into the Blockchain records to form the information within the conveyed framework straightforward and reliable. Each transaction's report is detailed and reliable in a distributed framework. All nodes on the same platform have the same rights and commitments to get to approved data, and each node permits other nodes on the same arrangement to get to this data. If this technique is utilized, more individuals will lock in more exchanges.
4. Traceable and unforgeable [13]: The Blockchain moves forward the time measurement of information by distinguishing and recording each transaction with timestamps. This permits the node to keep exchange order and guarantees that the information can be followed. The timestamp approves the information whereas limiting the fetched of exchange following. Meanwhile, it supports changeless information or data changes. A business cannot be changed after being affirmed and included in the piece. Most framework nodes must begin with favor exchanges sometime recently; they can be logged. Indeed, if an attacker has solid computer capacity, it is challenging for that assailant to maintain a strategic distance from and adjust the framework. If the attacker has 51 percent or more of all nodes, this can happen. This work anticipates "twofold investing" issues and ensures the solidness and constancy of the blockchain framework.
5. Anonymity The blockchain employments deviated encryption strategies to scramble information. Blockchains utilize this deviated encryption for both computerized marks and information encryption. The use of information encryption by the Blockchain guarantees the security of exchange information and diminishes the potential of information misfortune or creation. Exchange information is sent over, arranged, and carefully marked to illustrate the character of the signatory and whether the exchange has been recognized. Supplying the participant's real hub recognizable proof within the blockchain framework isn't required. Even though this work is far from being true since it inadvertently bolsters a few illegal activities, such as cash washing, it shields the participants' security and protection.
6. Credibility Self-control is required for information trade on the Blockchain. It depends on each hub to supply a capable calculation to defend against outside dangers without human interaction. Members can perform the transaction in an untrustworthy setting and add to namelessness. It moves forward the transaction's security and legitimacy while securing all parties. Each blockchain node, too, keeps all the information. Indeed if programmers control as it were 51% of the Network's hubs, the framework remains secure and dependable.

Based on these characteristics, blockchain innovation is a coordinated, smart mechanism in which each convention or innovation collaborates to form a decentralized and scalable ecosystem.

5. ETHEREUM AND HYPERLEDGER

What precisely is Ethereum? Ethereum is an open-source conveyed open Blockchain organized. With the help of Smart Contract innovation, it empowers the advancement of decentralized apps on it [6].
Vitalik Buterin created Ethereum in expansion to the initial principal blockchain concept. He modified Bitcoin's protocols to accommodate uses other than the issuance of money. Its innovation is the simplicity with which Smart Contracts may be created and deployed. These are snippets of code that run across a network. Therefore, this platform could aid programmers in developing applications for creating decentralized organizations.
Anyone on Earth can join the Ethereum blockchain and keep the Network in its current state. As a result, the term "World Computer" is frequently used to describe Ethereum. Just what is meant by the term Hyperledger? It is an open-source development effort for the ecosystem of Hyperledger-enabled application customers and providers. It focuses on blockchain application scenarios that are applicable across diverse business organizations.
Every company and sector is unique in its manner. Thus apps meeting their needs must be tailored. Everything that operates on the Ethereum Blockchain network uses a generalized protocol. At the same time, Hyperledger can be viewed as software that allows users to create custom blockchains tailored to their needs. The Linux Foundation is the host of the open-source partnership known as Hyperledger. Like Ethereum, it is neither a platform nor a tool. It is a broad strategy with various platforms for creating business solutions. The purpose for which Hyperledger and Ethereum were created is their key difference.
The EVM is a state machine.State machines are computing units with multiple states that can flip. The EVM modifies Ethereum's state to suit the requirements of this contract call whenever a transaction causes a smart contract to execute [14].
Ethereum differs from more straightforward blockchains like Bitcoin in that the EVM's capacity to interpret and conduct smart contracts during transactions [15].
Applications utilized to be decentralized and arranged for wide utilization are run by Ethereum using the Smart Contracts on the EVM. Hyperledger, on the other hand, employments blockchain innovation for commercial purposes. It is made to support pluggable component usage that offers unmistakable levels of privacy, strength, and scalability. With its modular architecture, Hyperledger provides a lot of freedom in utilizing it. Future-looking enterprise blockchain solutions are offered by its expandable design.
Figure 2 below illustrates the process of this transaction:

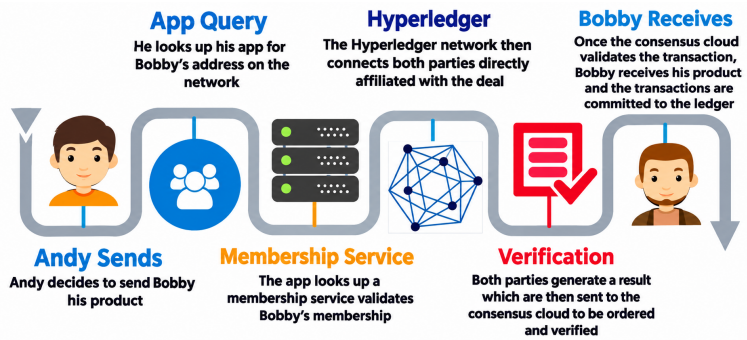


Figure 2. Sending data using Blockchain.

While using Hyperledger, Andy can offer pies to Bobby at a reduced cost without making this deal known to his other customers. However, in case Andy chose to carry out the same transaction using Ethereum, the whole thing would be impossible due to complete transparency of all the transactions carried out using Ethereum.

As a result, Hyperledger grants private exchanges. As a result, it offers organizations the protection and flexibility only to allow certain parties with the right encryption keys to see certain transactions.

6. RELATED WORK

Limitations of centralized cloud storage systems—particularly in educational environments—have stimulated further research in decentralized file-sharing networks. There are also studies that have moved toward blockchain file storage models to enhance data integrity, privacy, and accessibility.

Shetty et al. [16] proposed a secure file sharing system with the integration of Ethereum and IPFS.The focus was on immutability of file meta-data via intelligent contracts and distributed hash storage.

Likewise, Patil et al. [17] proposed a decentralized architecture using AES-256 encryption and SHA-256 authentication to provide file confidentiality and intelligent contracts for dynamic access control management.

von Tottleben et al. [18] made use of an academic-oriented IPFS cluster and observed that trustworthy file dissemination could be achieved at acceptable bandwidths . This presents the feasibility of peer-to-peer systems in the academic context .

Trautwein et al. [19] also performed measurements of IPFS file retrieval times from various geographic locations and showed that decentralized systems are able to efficiently manage typical academic workloads.

Doan et al. [20]proposed Course Sharing Technology based on IPFS and Ethereum to avoid large volume of course data and single point of failure issues with Xiamen University of Technology educational materials.

Shah et al. [21] proposed a general-purpose storage and retrieval system by combining the blockchain technology with IPFS.In their study, they investigated the use of this methodology in other fields and designed systems and performed experiments.

Likewise, in [21], Xu et al. [22]introduced InnerLight, a mental wellness content sharing platform. The platform uses IPFS, blockchain and a crypto-currency based reward system to incentivize users to contribute, curate and evaluate content. This shows that decentralized technologies can be useful outside of educational environments.The study demonstrates that IPFS and blockchain can be combined to build secure and decentralized file sharing systems. They also form a valuable basis for the development of our proposed platform for educational institutions.

Comparison of other decentralized storage and blockchain technologies:
Filecoin: Filecoin is a decentralized storage solution where users can store their data with storage contracts and verification systems. It's a useful option for storing plenty of data but you need to consider storage costs and retrieval times before using it in educational environments.
Storj:Storj is another decentralized cloud storage solution which secures files with client side encryption and erasure coding. It is a secure way to store data on multiple storage nodes. But, the pricing and file recovery performance should be assessed to see whether it is suitable for academic use.
Swarm: Swarm is a peer to peer storage network that lets you run decentralized applications. It can share files across the nodes and retrieve files without a central server . It's an alternative to IPFS for decentralized file sharing.
Hyperledger Fabric: is a permissioned blockchain platform that manages identity and access to data among organizations.This can be a great option for schools that require tighter control over user permissions, data privacy and access management..
EduASAC [23] (2023) presents an approach to access educational archives using smart contract technology. Other relevant works have combined Hyperledger Fabric with IPFS to share data securely among universities.There are also studies that have examined the use of blockchain to administer educational resources, and to verify academic credentials.

Ayare et al. (2025) [24] The authors reviewed some blockchain approaches based on IPFS for educational credential management . In their review they discuss how blockchain can improve the accuracy, transparency and verification of academic records, and reduce the reliance on centralized databases. This study also illustrates how Using distributed storage and tamper resistant records to protect information in education can be combined.

Chinnasamy et al. 2025 [25] proposed an electronic educational document management system using blockchain technology, role based access control and machine learning. The security of education documents during storage, authentication and verification is the basis of their system. It also seeks to improve access privilege management to ensure that only authorized persons can access sensitive academic files.

Chen et al. 2026 [26] The authors introduce a framework called Blockchain Indexed Searchable Encryption (BISE), which integrates blockchain technology with encrypted keyword search and decentralized storage. They tested the system for searching, refreshing data and overall performance.Though the framework was not made for education, but for data sharing in general, its features could be useful in educational contexts where many people need to securely store, search and share files.

Overall, these studies demonstrate how blockchain and decentralized storage can provide more secure and reliable management of educational information." They also give us useful knowledge to develop our proposed file sharing platform especially in terms of access control, document validation, privacy and efficient file retrieval.

7. PROPOSED SYSTEM

The primary goal of this suggested system is to create a decentralized storage system using Blockchain. We will use Blockchain to secure the data files uploaded via our website and encrypt the file's data using hashing algorithms and secure keys. Users will register to the site using many different crypto wallets like MetaMask They must have an account and wallet on the MetaMask application, or the website user will use his wallet to register. We must upload the file to the website via the user account using the file picker. Our system will check the size of the file uploaded and how much fees will deduct from the wallet based on the file size and the available allowed storage and ask for a key to decrypt the file data when downloading it again.

The meta mask data and Blockchain secure the user's data. We use IPFS technology on a website to distribute the file's data across the Network with 64 blocks like big data figure 3 shows the architecture of the proposed system.

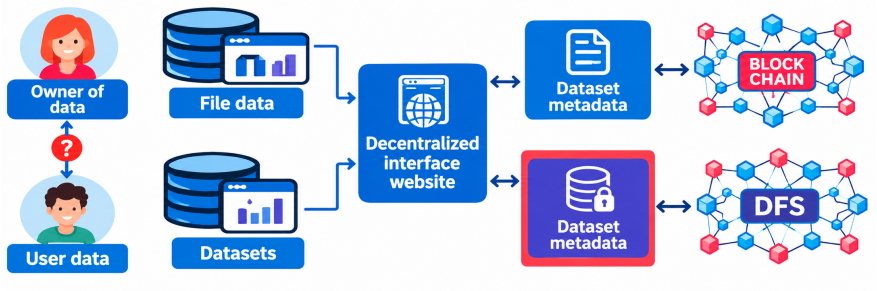


Figure 3. proposed system architecture.

The proposed framework integrates AES-256 encryption, decentralized IPFS storage, MetaMask-based authentication and file-owner authorization to provide a practical foundation for secure educational file sharing. The system has been used in practice in the educational environment of the university with the involvement of 100 students, who worked with the platform in the activities of educational document management and file sharing. This practical implementation illustrates the potential of integrating blockchain and decentralized storage technologies into university learning environments. Nevertheless, educational institutions may require additional access-control and governance mechanisms to address their specific requirements.

These include role-based access control for students, teachers, and administrators; consent tracking through auditable records of file-access requests and authorization decisions; and enhanced privacy protection by minimizing sensitive information stored on the blockchain and securely managing file-decryption keys. These mechanisms represent important directions for further development to improve the framework's suitability for institutional educational environments.

Although existing studies have demonstrated the use of IPFS and blockchain for decentralized storage, file integrity, and secure file sharing, the present work focuses on integrating wallet-based authentication, AES-256 encryption, owner-mediated access authorization, and IPFS-based file distribution into a single educational workflow.
Its intended educational use cases include sharing course materials, distributing assignments, and exchanging academic documents among authorized users. The proposed framework provides a basis for extending conventional decentralized file-sharing mechanisms with education-specific role-based permissions and auditable consent decisions. These features should be evaluated further to establish their effectiveness in institutional environments.
The proposed system uses private IPFS networks that return hash values using an AES 256-bit algorithm that produces the wallet address and the path for the file. The wallet address is also saved using the smart contract that hides the user's data and peer-to-peer users while sending and sharing data without using third-party agreements. They control the trade of resources or exchanges between nodes in particular occurrences. These lines of code are put away on a blockchain organized, and executed when certain conditions are met.
Once it has been shared among peers, the client with the hash values put away within the Blockchain can combine all of the small files into one huge one. The information client must enroll and log in to begin with. He can access the transferred record if the file's owner permits it. The client can look for the record and ask to see the information from the owner. The client can look at the record in case the owner grants consent. Cloud capacity has no data about the information proprietor, client, or block information; it is also impossible to follow the lead. If the owner wants to open and check the contents of the record, he need to provide the current hash value to the peer where the data is stored, otherwise the record will download with encrypted values.

1. **Smart Contracts:**
   It eliminates the third party to resolve the argument and allows the businesses to handle contracts freely [13]. The scripts are stored within the blockchain structure and are executed when certain conditions are met.If-then checks are made to ensure that exchanges are completed.
2. **Protocol IPFS:**
   The Interplanetary File System (IPFS) is a protocol and a peer-to-peer network where information is stored and traded in a distributed record framework. IPFS uniquely identifies each record using content-addressing, linking all computing devices to a global namespace. IPFS is not a centralized server but a distributed system of user operators. Each operator stores a portion of the total information. This provides a good strategy for sharing and storing records.Other peers in the organization use a distributed hash table (DHT) to search for and request content from any node that has it.
3. **Ethereum:**
   It is a public blockchain based open source distributed computing framework. Ethereum is a decentralized platform that enables the creation of intelligent contracts, programs that run exactly as programd without any possibility of manipulation, stoppage, fraud or third party interference. They operate on top of a world-wide very efficient system for representing assets and making payments.Developers are able to create markets, manage obligations, transfer assets and other smart contract use cases.
4. **MetaMask:**
   MetaMask cryptocurrency wallet [13] is required to communicate with Ethereum blockchain network. Users can connect their wallets and interact with the Ethereum blockchain through a browser extension or mobile app. The MetaMask browser extension will help our framework to connect to the Ethereum blockchain.Metamask is an identity vault and a user interface for you to talk to the blockchain.
5. **Data Encryption:**
   Files are protected using AES-256[23, 27] encryption.The data is encrypted with a secure cryptographic key before being stored, and then decrypted when the original file needs to be accessed by an authorized user.
6. **Proposed System Goals:**
   To enhance data security, files are encrypted and saved across several nodes within the network. AES encryption helps protect sensitive information and keep system performance optimal. In our proposed system, files are encrypted before being uploaded to IPFS, and are distributed among the different peers in the network. IPFS generates a unique content identifier (CID) for each file, which can then be written to the

blockchain to identify and retrieve the stored file.The Ethereum blockchain also offers a transparent and tamper-proof record of transactions, enabling secure tracking of file-sharing activities.

7.1. Smart Contract Design and Implementation

Smart Contract State Variables and Access Control: The smart contract can save essential information such as the file owner's wallet address, the IPFS Content Identifier (CID), information regarding file registration, and access request status. Access to their own files are controlled by their file owners. Other users can ask for access when they need it .These access rules are enforced by the smart contract so that only the owner of the file can approve or reject requests.
Events and Auditability: The smart contract can emit events when a file is registered, an access request is submitted, or a request is approved or rejected. These occurrences are a record of file-sharing on the blockchain and allow for tracking transactions and auditing actions in the past.The event names and parameters are defined based on the smart contract implementation and the requirements of the proposed system.

7.2. AES Key Management

The proposed system offers AES-256 encryption for educational documents prior to uploading them on IPFS. Each file is encrypted with an AES key which is also needed to decrypt the file when authorized user wants to access it.This key is separate from your Ethereum private key, which signs blockchain transactions via MetaMask.

Key Management: Encryption key management is an important part of maintaining system security. AES keys should be generated using a cryptographically secure random number generator to prevent them from being easily predicted. Never store these keys directly on the blockchain or in a publicly accessible location alongside the encrypted files.Before a user can share a file, the access request must be approved by the owner, who must then provide a secure means for the authorized user to obtain the decryption key.

Key Rotation, Revocation and Recovery: The system also needs clear procedures for updating encryption keys, revoking them, and recovering them. Key rotation is just a new AES key, re-encrypting the file with the new key, and changing how the new key is shared with authorized users. Revoking access will prevent a user from getting the key in the future, but it can not remove any keys or copies of the file they already possess. Key recovery should also be a secure process allowing authorized users to recover access to their files without exposing the encryption keys to unauthorized persons.

7.3. Threat Model and Trust Assumptions

Threat Model: The proposed solution aims at ensuring the security of educational documents from any possible unauthorized access, unauthorized sharing, modification of information stored in them and loss of confidentiality of their content. The system includes the use of users who authenticate themselves via MetaMask, Ethereum smart contracts that allow logging of supported sharing operations, AES-256 encryption for providing confidentiality of files and IPFS for file storing and retrieving. The following threats can be considered in the threat model: external attackers, malicious or unauthorized users, compromised user's devices, dishonest storage peers and smart contract/application vulnerabilities. The major security goals are the following:

1. Confidentiality:Educational documents should only be accessible to users who have permission to view them. Encryption helps keep these files private, as long as the encryption keys are stored securely and the encryption process is properly implemented.
2. Integrity: The system needs to be able to tell if a file has been modified without permission. IPFS content addressing and cryptographic hashing provide a way to verify the files are unchanged and match the original content.
3. Access Control: Users should only be able to access educational documents or obtain decryption keys if they have the required permissions.Permissions are controlled using the file-sharing rules defined in the system.

4. Account Authenticity: The blockchain can also prove which ethereum wallet address signed a transaction. However, the wallet address itself does not prove a user's real identity or their role in an educational institution.You might need to do additional verification to tie each wallet to the right user.
5. Auditability: The system should keep logs of important file-sharing activities such as access requests, approvals and denials.According to the information stored in the smart contract, the records can be checked via the blockchain.
6. Availability: Decentralized storage reduces reliance on a single server, thus boosting file accessibility. However, a file can only be retrieved if at least one reachable IPFS node still stores the required content.

The assumption is that the attacker can observe the transactions in the blockchain that are public and also access the metadata in the IPFS network. Additionally, the attacker can make requests for files without prior permission, try to misuse or play around with the file identifiers, and use any vulnerabilities in the software. An authorized attacker can also distribute a file even if it has been received legally.

Assumptions about Trust: The security of the suggested framework is based on the following assumptions concerning its main elements.

1. Ethereum blockchain: The framework operates on the basis of the consensus and cryptography systems of the Ethereum blockchain in order to ensure validation of transactions and integrity of the blockchain transactions. At the same time, the framework assumes that the smart contracts implemented in the system operate as required and implement necessary access rights and file sharing.
2. MetaMask wallet: MetaMask is trusted to enable users to control their wallet accounts and sign transactions on their behalf. The private keys and recovery keys for these are expected to be in possession of the rightful user. If either a private key is compromised or the user signs a harmful transaction, then the attacker can perform actions via this wallet account. Moreover, MetaMask verifies the control of a particular wallet address and does not verify the user as a student, teacher, or administrator separately in any way. Hence, institutional roles require a different trusted registration process.
3. IPFS distributed storage: IPFS is trusted to deliver content addressing and content retrieval using the peer-to-peer network. The assumption here is that the retrieved content will be verified based on the correct content identifier. IPFS itself does not offer any authorization for applications, confidentiality, guaranteed storage, or file availability. The files need to be encrypted before publishing, and the availability needs proper management of storage nodes.
4. Private IPFS network: It is assumed that the administrators of the private network correctly set up access control rules on nodes, safeguard administrator passwords, and ensure the integrity of participating nodes. Membership in the network protects from attacks by unauthorized peers, but does not exclude attacks from inside the organization, compromised nodes, traffic analysis, and misuse by legitimate users. The private network itself should thus be viewed as one more layer of security.
5. Encryption and key management: The AES-256 encryption is assumed to be performed in an appropriate secure manner, with correct key generation, secure storage, and where necessary authenticated integrity protection. Encryption keys should be transferred securely only to trusted parties. Compromise or loss of key will either result in exposure of a file or inability to recover it, respectively.
6. Application and users: It is assumed that the application user interface, authorization mechanism and key handling are working properly.While users are expected to keep their device and credentials secure, the design does take into account that authorized users may accidentally or maliciously expose information..

Security Constraints:Although the proposed system reduces the dependence on centralized storage and improves the security by means of encryption, transaction tracking and access control, there are some security risks still present. If encryption keys are leaked, intelligent contracts have vulnerabilities or users' devices are infected with malware, files could be exposed. There is also the risk of authorized users sharing decrypted files with others without permission. If access permissions and encryption keys are handled correctly, a user will not be able to access files through the system in the future after their access has been revoked.However, it can't delete files or already downloaded or gotten by the user decryption keys.

7.4. Comparison with Decentralized Authentication Schemes

The proposed system authenticates users with MetaMask by checking their cryptographic signatures, which indicates they control a certain Ethereum wallet address. However, unlike Decentralized Identifiers (DIDs) and Verifiable Credentials, wallet-based authentication alone cannot confirm a user's identity within an educational institution or verify their academic role. The system is also not fully decentralized because some parts still depend on application logic, encryption-key management, and the administration of the private IPFS network. For this reason, it is more accurate to describe the proposed system as a blockchain-based file-sharing platform rather than a completely decentralized solution.

8. RESULTS AND DISCUSSION

The first step is to start the server by running the required command on the local computer. Our proposed system combines blockchain technology, digital wallet authentication, and distributed file storage to provide a more secure way of managing and sharing educational files. Through the platform, file owners can manage their educational documents, control who can access them, and approve or reject file-sharing requests.

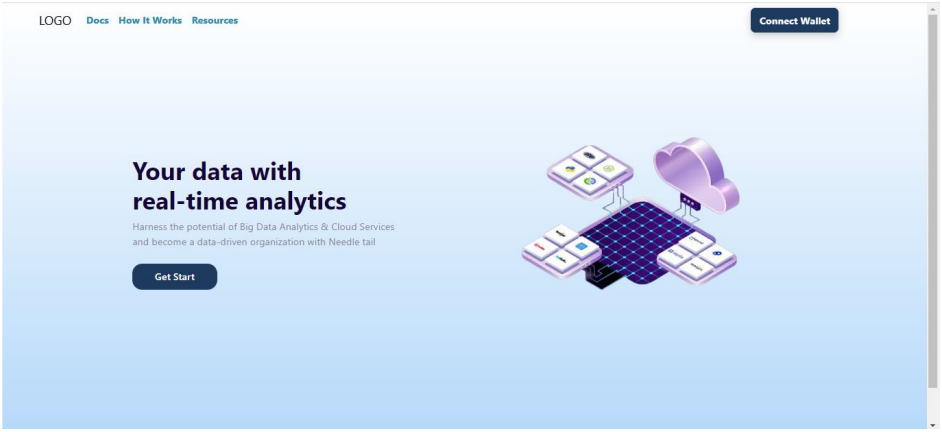


Figure 4. Homepage of cloud

To demonstrate how the application works, we first start the server on the host computer by running the required command. The homepage is displayed when the server is up and running as shown in Figure 4. This page is the main interface for users to access the features of the system.As shown in figure 5, to use the platform, the users have to connect their Metamask wallet or any other supported cryptocurrency wallet to authenticate themselves.

Connecting the wallet allows the application to interact with the user's blockchain account and enables users to approve the transactions required by the system. Once authentication is completed successfully, the file owner can access the record management interface, as shown in Figure 6. This interface gives users the ability to manage their files and control access permissions.

The main features of this interface allow users to upload educational records to distributed storage, view documents they have already shared, and check new requests from other users who want to access their files. File owners can also approve these requests and provide authorized users with the necessary decryption keys through the system's access control mechanism. These features give file owners more control over how their educational documents are managed and shared.

The use of blockchain technology and distributed storage can also allow the system to process transactions and store files independently, thus reducing the dependence on a centralized storage server. The main steps of the proposed system are shown in the figures 4, 5 and 6. Starting from the launching of the application and the

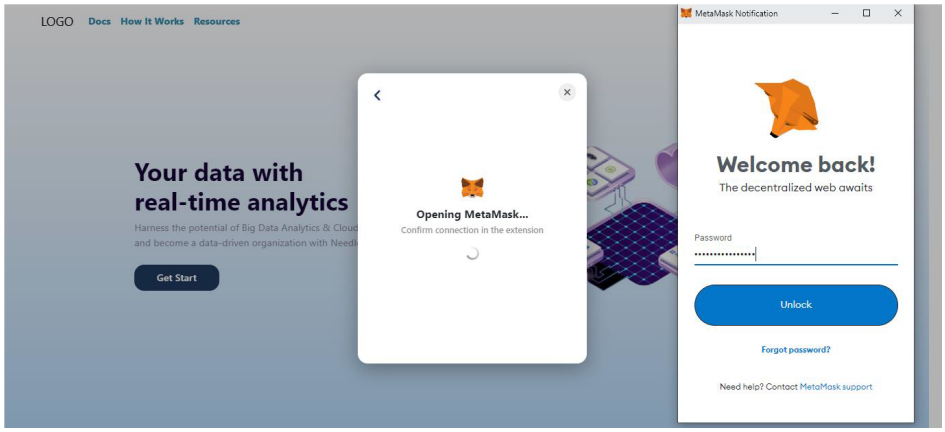


Figure 5. Login page with MetaMask

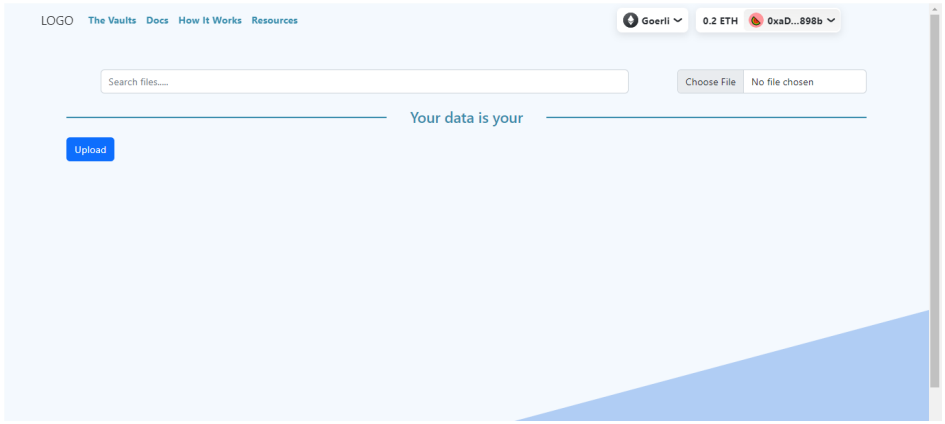


Figure 6. Upload file page

connection to a cryptocurrency wallet, and passing through the management of the educational records, the review of the access requests and the sharing of documents with the authorized users.

The proposed system allows users to search for the availability of educational records and send a standard inquiry to the file owners for access. The user can view or download the documents requested after the owner approves the request. This process is shown in Figures 7 and 8.

The authentication process ensures that only authorized users, who have been granted access by the file owner, can view educational documents. This lessens the risk of unauthorized access to sensitive academic information. The proposed system also separates the file storage and the access management. The storage layer stores the encrypted files, while the blockchain manages access permissions and keeps track of related transactions. This separation helps to protect the contents of the files and minimize the amount of sensitive information stored on the blockchain.

The application communicates with the storage module for uploading and downloading files. At the same time, the information management module provides several important features, including user registration, login, file uploading, document sharing, access request management, and encryption key management. Through these features, file owners can decide who is allowed to access their educational records and how those records are shared.

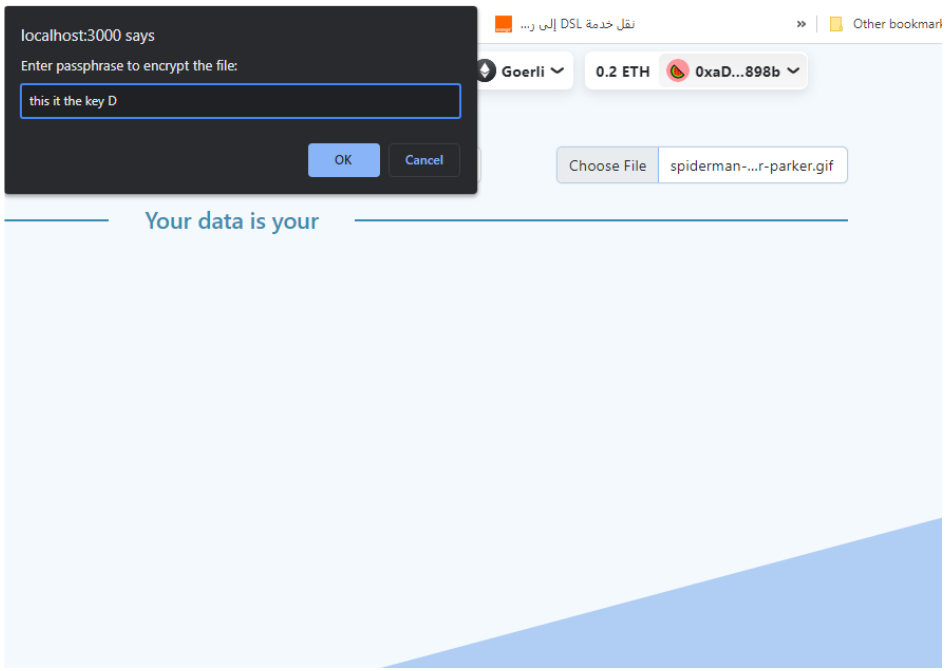


Figure 7. Key for data encryption.

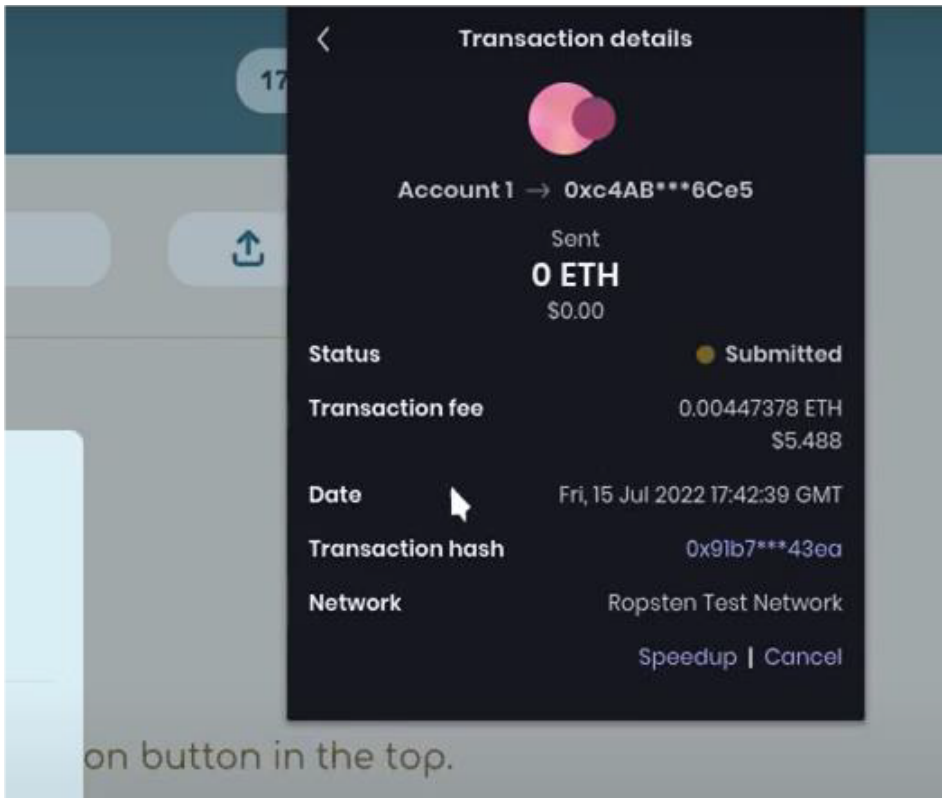


Figure 8. gets the file to upload the file based on the size of the wallet..

Figure 9 illustrates how educational records are encrypted before being uploaded to the storage network. The smart contract does not store the original document contents, it stores references to the necessary files and access information.

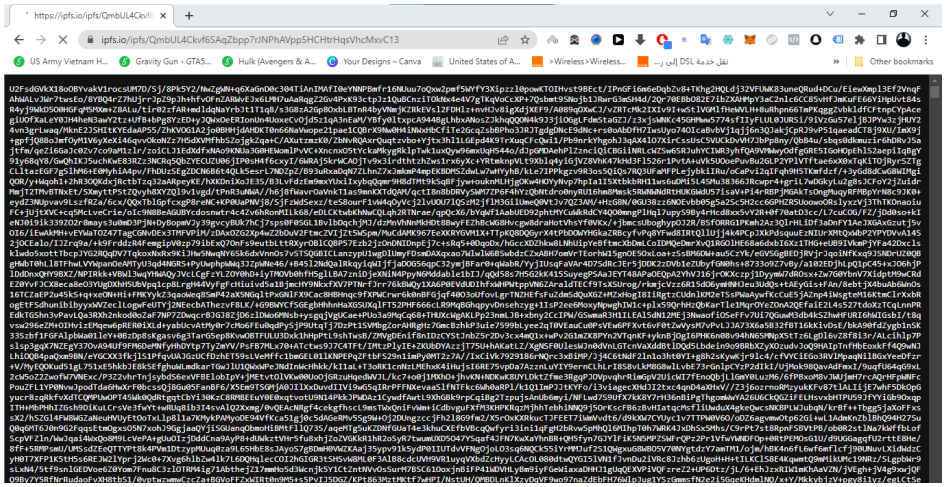

https://ipfs.io/ipfs/QmbUL4Ckvf
ipfs.io/ipfs/QmbUL4Ckvf6SAqZbop7rJNPhAVpp5HCHtrHqsVhcMxvC13
U2FsdGVkX18oOBYvaKV1rocsUM7D/Sj/8PkSV2/NwZgWN+q6XaGnD0c30aTiAnIMAfI0eYNNP8mfr16NUuu7oQxw2pmf5WYfY3Xipzzl0powKTOIHvst9BEct/IPnGFi6m6eDqbZv8+TKhg2HQLdj32VFUWK83uneQRud+DCu/EiewXmpl3Ef2VnqF
AhmALvJWr7twsEo/8YBQ4rZ7hUjrrJp29pJh+hfvOFnZARWVEJx6LUM7uaNaRqgZ2GvG4PxK93ctpJr1QuBCnziIOKhBx4e4V7gTKqVoCcXP+7Qsbmt9SNoJbi3RwrG3mSH4d/2Qr70EBbO82Ef1bZKAHMpY3aC2nlc6CC8SvHf3mKuFE66YiHpUvtB4s
B4yjHWd7OOHkGfM5Oae7ZALu/ei02zfAHewdldqNaYrbJt1Tiq8/s3G8za2GpNOKbXLBTnHABybyVWejK2RkEVslZFDWlzenvdtJvBigXdjXEF9/AN89qIOxC3/vZRTzE%2IXtv0IwuSt1VGWlfHeWVLHnBuRbpn66TmPKqggZvbKldfCFtmpCYpAce
giUOFXaLeV0JH4heN3awY2tz4Uf8+bPgBYzED+yJQWxOeERIonUm4UoxeCvOjd5z1qA3nEaV/VBfy0ltxpcA944BglbbxANosZJkhqQQOW4k9J3jiOGgLFdmStaGZJ/z3xjsWKc4SGHMww5774sfTIyFLUL0JURSl/9lVzGu57elBJPYw3zjHUY2
4vn3grLwaq/MknE2JSHItKYEdaAP55/ZhKVOG1A2joBBH9JdAHDKT0n66NaVwope21pae1CQBrX9NwOH4iNWxHbCfiTe2GcqZsbBPho3JRJTgdgDNcE9dNc+rs0oAbDfH7IwsUyo74OIcaBvbVj1qjj6n3QJakjCpRJ9vP51qaeadCT8j9XU/ImX9j
+gpfjQ88oJmfOyM1V6yXeXi46qvvGkoNZs7H5dXVHfNb5Zojgk2qeC/AXuttmzxO/ZbNvRQAxrQuqtzvboYjtx3hlliGEpd4K9IrXuqCfpQ+jtxJhlliGEpd4K9IrXuqCfpQ+jtxJhlliGEpd4K9IrXuqCfpQ+jtxJh

Table 1. Upload times are expressed in seconds.

File Size	Average Time (IPFS)
1 MB	Less than 1s
5 MB	Less than 1s
10 MB	Less than 1s
50 MB	1s
100 MB	2s
250 MB	9s
500 MB	9s

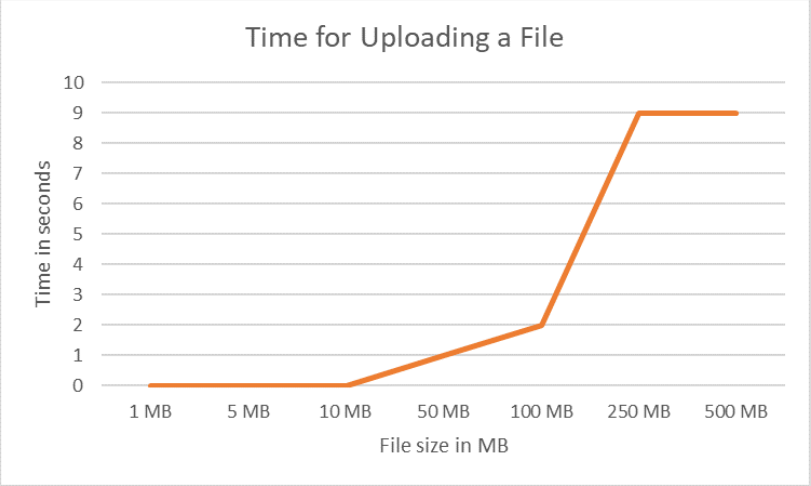


Figure 10. time for uploading files.

Table 2. Download times are expressed in seconds.

File Size	Average Time (IPFS)
1 MB	Less than 1s
5 MB	Less than 1s
10 MB	Less than 1s
50 MB	Less than 1s
100 MB	2s
250 MB	1s
500 MB	7s

each file size. Reporting the average download time and the variation between trials would provide a clearer and more reliable understanding of the system's performance.

8.1. Security Analysis Against Common Attacks

The system consists of AES-256 encryption, MetaMask authentication, Ethereum smart contracts, and IPFS storage; but still, there will be some security risks which will not be addressed by using these technologies alone. The table below shows potential attacks that may happen and how to protect against them.

1. Unauthorized Access: Unauthorized Access: AES-256 ensures the privacy of the files in case the keys are kept confidential. The files need to have their owners as well as access control enforced in smart contracts.

2. Replay Attacks: Attackers might try to reuse previous requests submitted to gain access or repeat an authorization without permission. To mitigate this risk, the system may contain request timeout times, and mechanisms for detection and rejection of duplicate requests. BuThese measures must be properly implemented and tested to ensure they work.
3. Vulnerabilities in Intelligent Contracts Flaws or weaknesses in the smart contract code may allow unauthorized users to do things they are not supposed to do. So, intelligent contracts need to be code reviewed and security tested before deployment. However, the current study does not give enough information to know whether such testing was done.
4. Sybil Attacks : An attacker may generate multiple wallet addresses and use them to pose as different users in the system. MetaMask can verify someone owns a specific wallet. It can not verify that person's real-world identity.This means that additional identity checks may be required to ensure that users are not creating multiple accounts to bypass the access rules.
5. DeDenial of Service (DoS): An attacker may send a large number of requests to the application or any of its supporting services, rendering it unavailable for legitimate users.This risk can be mitigated with techniques such as rate limiting, input validation and stress testing to see how much traffic the system can handle.
6. IPFS Node Failure: The files hosted on IPFS can become unavailable if the nodes that are hosting them go offline or stop serving the content. "I think things like pinning a file, replicating it on multiple nodes could help to keep files available. However, there needs to be further investigation in the proposed system about the implementation and effectiveness of these techniques in maintaining file availability.

To summarize, the proposed system is bolstered by AES-256 encryption, wallet-based authentication, smart contract technology and IPFS to improve its security. But together these technologies do not provide complete protection against security threats. We need to do more testing to see how well the system handles encryption keys, controls user access, protects smart contract systems from vulnerabilities, manages possible attacks, and keeps files available. These tests will assist in detecting potential vulnerabilities and improve the overall security and reliability of the platform.

9. CONCLUSION AND FUTURE RECOMMENDATION

This research has introduced a blockchain-based educational file sharing system that has implemented Ethereum smart contracts, IPFS, MetaMask authentication, and AES-256 encryption. In the experimental analysis, time taken to upload and download files for seven different sizes from 1 MB to 500 MB was measured. The recorded figures have offered an initial idea regarding the transfer of files in terms of various file sizes[28].
While the system contains several features for ensuring confidentiality of files, access control, and decentralization, none of these attributes have been proven by experiments because of lack of security testing, concurrency tests, and experiments on node failure. Moreover, there is no record of any gas fees in the experiment. In the future, there would be an emphasis on testing of the security aspect, improvements in the management of the AES keys, scalability test when working concurrently[29, 30], availability testing in case of node failure and comparison of the system with other blockchain systems. The usability tests using students and teachers would be used to check how suitable the system is for use in educational environment.

REFERENCES

1. H. Xu, Y. Cheng, Z. Li, and C. You, "Content Sharing Network based on IPFS and Blockchain," *IOP Conference Series: Materials Science and Engineering*, vol. 1043, no. 5, p. 052014, 2021.https://doi.org/10.1088/1757-899X/1043/5/052014
2. Shamsudheen, S., Paul, A. M., Appukuttan, A., Karickom, S. T., and Gobinathan, P., "Blockchain technology for enhanced security of academic certificates in education," *Journal of Information Systems Engineering and Management*, vol. 10, no. 20s, Article 3046, 2025. https://doi.org/10.52783/jisem.v10i20s.3046
3. Balobaid, A. S., Alagrash, Y. H., Fadel, A. H., & Hasoon, J. N. (2023). Modeling of blockchain with encryption-based secure education record management system. Egyptian Informatics Journal, 24, 100411. https://doi.org/10.1016/j.eij.2023.100411

4. Sayed, A.R., Khafagy, M.H., Ali, M., Mohamed, M.H., "Exploring the VAK model to predict student learning styles based on learning activity", Intelligent Systems with Applications, Volume 25,2025,200483, https://doi.org/10.1016/j.iswa.2025.200483 .
5. H. Dahshan, H. M. Eldeeb, and A. E.-D. R. Shehata, "An Efficient Cryptographic-based Access Control Mechanism for Cloud Storage," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 15, no. 3, pp. 144–155, Sep. 2024.
6. H. Gaikwad, N. D'Souza, R. Gupta and A. K. Tripathy, "A Blockchain-Based Verification System for Academic Certificates," 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), Puducherry, India, 2021, pp. 1-6, https://doi.org/10.1109/ICSCAN53069.2021.9526377 .
7. Park, J. (2021). Promises and challenges of blockchain in education. Smart Learning Environments, 8(1). https://doi.org/10.1186/s40561-021-00179-2
8. Fadlallah, H. R., Mohamed, M. H., Alayash, W., Stephan, J. J., Qasim, S. S., Alqabany, T., & Ali, M., 'SECURE IOT COMMUNICATIONS USING SCRP-DRIVEN DYNAMIC QUASIGROUP CRYPTOGRAPHY', Journal of Theoretical and Applied Information Technology, vol. 104, no. 1, Jan. 2026, https://doi.org/10.5281/zenodo.18259402.
9. Pazaitis, A. (2020). Breaking the chains of open innovation: Post-blockchain and the case of sensorica. Information, 11(2), 104.https://doi.org/10.3390/info11020104
10. Mohamed, M. H., Elkholy, M., and Marzouk, M.A. (2025). Innovative machine learning approaches for identifying pre-diabetes in patients. Journal of Information Hiding and Multimedia Signal Processing, 16(1), pp: 365–378. March.
11. Lu, Y. (2018). Blockchain: A survey on functions, applications and open issues. Journal of Industrial Integration and Management, 3(4), 1850015.https://doi.org/10.1142/s242486221850015x
12. Rahrouh, M., Ali Salim, R., Salman Qasim, S., Hussien Mohamed, M., & Mahmoud, N. (2026). A super-efficient and compact CNN for tomato leaf disease detection on resource-constrained devices. *Statistics, Optimization & Information Computing*, 16(2), 1045–1059. https://doi.org/10.19139/soic-2310-5070-3778
13. Maresca, M., Andreoli, L., & Baglietto, P. (2025). Leveraging geometric distribution with variable probability to pre-calculate block publication deadlines in a blockchain simulation. Blockchains, 3(2), 9. https://doi.org/10.3390/blockchains3020009
14. sang, Y. P., Wu, C. H., & Lee, C. K. M. (2022). BlockTrainHK: An online learning game for experiencing blockchain concepts. SoftwareX, 19, 101167.https://doi.org/10.1016/j.softx.2022.101167.
15. Friha, O., Ferrag, M. A., Benbouzid, M., Berghout, T., Kantarci, B., & Choo, K. K. R. (2023). 2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT. Computers & Security, 127, 103097. https://doi.org/10.1016/j.cose.2023.103097.
16. El-Aziem, Ayman H. Abd, Marwa Hussien Mohamed, and Ahmed Abdelhafeez. High-Security Image Encryption Using Baker Map Confusion and Extended PWAM Chaotic Diffusion. *Computers*, 15(2):106, 2026. https://doi.org/10.3390/computers15020106
17. Patil, N. P., Mane, Y. D., Vasoya, A., Agrawal, A., & Raut, S. (2025). "Secure file sharing using blockchain and IPFS with smart contract-based access control". Journal of Information Systems Engineering and Management, 10(16s), 184–194. https://doi.org/10.52783/jisem.v10i16s.2588.
18. Amine, S., Fatima Koulouh, Mohammed Es-sabry, & Nabil El Akkad. (2026). Fast and Secure Color Image Cryptosystem Based on 2D Henon Chaotic Map and Josephus-ZigZag Permutation. *Statistics, Optimization & Information Computing*, 15(6), 5284–5312. https://doi.org/10.19139/soic-2310-5070-3210
19. D.Trautwein, A.Raman, G.Tyson, I.Castro, W.Scott, M.Schubotz, B.Gipp, and Y.Psaras, "Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web," in Proceedings of the ACM SIGCOMM 2022 Conference, Amsterdam, Netherlands, Aug.2022, pp.739–752, https://doi.org/10.1145/3544216.3544232.
20. Dhia Jaafar , H. ., Jabbar Hassan, T. ., Hussien Mohamed , marwa, Abdullateff Abad , B. ., & Salman Qasim, S. . (2026). Artificial Intelligence and Ensemble Learning for Coronary Artery Disease Prediction. *Statistics, Optimization & Information Computing*, 15(5), 4255–4276. https://doi.org/10.19139/soic-2310-5070-3354
21. Saif, M. B., Migliorini, S., & Spoto, F. (2024). Efficient and secure distributed data storage and retrieval using Interplanetary File System and blockchain. Future Internet, 16(3), 98. https://doi.org/10.3390/fi16030098.
22. H. Xu, Y. Cheng, Z. Li, and C. You, "Content Sharing Network based on IPFS and Blockchain," IOP Conference Series: Materials Science and Engineering, vol.1043, no.5, p.052014, 2021, https://doi.org/10.1088/1757-899X/1043/5/052014
23. Hu, R., et al. (2023). EduASAC: A Blockchain-Based Education Archive Sharing and Access Control System. Computers, Materials & Continua, 77(3), 3387–3422,https://doi.org/10.32604/cmc.2023.042000
24. Ayare, A. A., Jadhav, V. A., Banatwala, M. K., et al. (2025). A systematic review on blockchain-based framework for storing educational records using InterPlanetary File System. Cureus Journal of Computer Science. https://doi.org/10.7759/s44389-024-00745-y
25. Chinnasamy, P., et al. (2025). Blockchain based electronic educational document management with role-based access control using machine learning model. Scientific Reports, 15, 18828. https://doi.org/10.1038/s41598-025-99683-5
26. Chen, M., Hao, P., Meng, W., Aizezi, Y., & Sun, G. (2026). BISE: Enhance data sharing security through consortium blockchain and IPFS. Journal of Information Security and Applications, 97, 104320.https://doi.org/10.1016/j.jisa.2025.104320
27. Nibras Abo Alzahab, Giulia Rafaiani, Massimo Battaglioni, Ana Cavalli, Franco Chiaraluce, Marco Baldi, "BiometricIdentity dApp: Decentralized biometric authentication based on fuzzy commitment and blockchain", SoftwareX, Volume 28, 2024, 101932,https://doi.org/10.1016/j.softx.2024.101932
28. Yessenbayeva, A., Mazakov, T., Mailybayeva, A., Jomartova, S., & Mazakova, A. (2026). Mathematical Modeling of Investments in the Development of an Information Security System: An Optimal Control Approach. Statistics, Optimization & Information Computing, 16(2), 1493–1508. https://doi.org/10.19139/soic-2310-5070-3221
29. Hilal Sultan Duranoglu Tunc, Abebu Ademe Bayleyegn , Joachim Notcker, Riccardo Bassoli and Frank H.P. Fitzek. 2025. " Resilience analysis of quantum network against targeted attacks: Recovery via rerouting and purification " Optical Switching and Networking 57: 100810. https://doi.org/10.1016/j.osn.2025.100810

30. Alayash, W., Rahrouh , M. ., Abbas Ibrahim , A. ., Hussien Mohamed , M. ., Theab Ahmed , S. ., Hamed Albarri , M., & Hasan Ahmed , M. . (2026). Assessing LSTM and GRU for Multi-Dataset Intrusion Detection in IoT Environments.*Statistics, Optimization & Information Computing*, 15(4), 3155–3173.https://doi.org/10.19139/soic-2310-5070-3226.