Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Privileged-Based Secure Sharing of Student's Credentials using Blockchain Technology and Secret Image Sharing Scheme

Puja Sarkar

p.sarkar@astu.ac.in

Assam Science and Technology University

Parag Jyoti Kalita

Central Institute of Technology Kokrajhar

Research Article

Keywords: Blockchain, Secret Sharing, IPFS, Smart Contracts, Ethereum

Posted Date: March 27th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-8345952/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Privileged-Based Secure Sharing of Student's Credentials using Blockchain Technology and Secret Image Sharing Scheme

Puja Sarkar[a], Parag Jyoti Kalita[b]

[a]Department of Computer Science and Engineering, Assam Science and Technology University, Guwahati, 781013, Assam, India
[b]Department of Computer Science and Engineering, Central Institute of Technology, Kokrajhar, 783370, Assam, India

ARTICLE INFO

Keywords:
Blockchain
Secret Sharing
IPFS
Smart Contracts
Ethereum

ABSTRACT

Any educational ecosystem that comprises a wide range of stakeholders, including students, teachers, various institute committees, administrations, government agencies, and many more, must have a framework in place for the sharing of students' credentials. All of these stakeholders take extensive steps to ensure the authenticity and confidentiality of shared student testimony. Despite these concerns, the distribution of students' credentials is a vulnerable, potentially complex, and sometimes insecure process. The aim is to use blockchain technology and secret-sharing scheme to mitigate existing security concerns when sharing the students' credentials. Due to the immutable nature of blockchain technology, the problem of safely exchanging student credentials can be resolved using blockchain technology. This paper proposes a privileged system for storing student credentials that ensures security and privacy while sharing sensitive credentials with other parties. This can be achieved by combining blockchain technology with the SIS (secret Image Secret Sharing) scheme and IPFS (Interplanetary File System), giving students the privilege of sharing their information. Moreover, to ensure limited access and enhanced privacy, the system also includes student privilege management. As a result, the proposed scheme provides tamper-proof, immutable, authentic, non-repudiation, privacy-preserving exchange of student credentials among stakeholders.

1. Introduction

Nowadays, online document sharing is preferred due to its many advantages such as speed (near-instantaneous), simplicity, global access, availability of always-on connectivity in a variety of applications used for storing and sharing of student credentials, forensic and medical imaging, military imagery, and satellites [1]. However, sharing confidential information online does not always guarantee the privacy, accuracy, integrity, security, or accessibility of shared files. It is challenging to ensure these features even when a dedicated facility exists, such as a password-based Encryption or steganographic schemes, which are also vulnerable to attack. Encryption and steganography are the two conventional approaches used to provide security while distributing and storing the security of digital confidential images. Encryption transforms sensitive information into incomprehensible and meaningless forms using a secret key. Steganography can conceal the existence of secrets, usually by enclosing them in a cover to prevent unwanted snooping. However, None of the above methods will reveal the secret, even if some of the data will be lost or destroyed, it often becomes inaccessible. Also, in the above methods, confidentiality and availability cannot be achieved simultaneously or in parallel. However, lossless restoration of the original secret images is often crucial for the above applications. As a result, we combined SIS with the IPFS distributed file storage system to provide a privileged-based storage and distribution system for sensitive images. In doing so shared images generated from sensitive credentials are stored in a distributed manner using IPFS, increasing availability in the event of deletion or loss in a single location. In 1979, Shamir proposed a novel secret-sharing scheme, where a trusted Dealer generates and distributes shares in such a way that no individual gets any information regarding the secret [2]. In 2002, Thein and Lin further extended it to confidential image data [3]. Furthermore, the properties of the secret sharing scheme guaranteed that no individual share reveals any confidential information related to the secret. Additionally, the proposed scheme has a permission-based feature, which ensures that without the privilege of the authorized party, no one can access confidential information. As the IPFS is open access, blockchain technology is used for further verification of the shares, enhancing privacy even more. The features like tamper-proof, immutable, authentic, non-repudiation, privacy-preserving, and share-friendly nature of the blockchain are used for enhancing the security and privacy of the hybrid architecture for securely exchanging student credentials [4].

ORCID(s):

This paper proposes a blockchain-based system for securely distributing student records in a safe and secure manner. It also includes student privilege management using secret image sharing which gives students the ability to regulate access to and privacy of their credentials, ensuring that their information is shared only when necessary and securely.

1.1. Motivation of the work

Any organization that manages student certificates, including businesses and educational institutions, faces so many complications. A typical example is the job application process: after a student submits an application for employment, it is the staff member's responsibility to thoroughly authenticate the certificate received. It is also possible that the company may need to get in touch with the particular institute to inquire about the certification's validity. Despite taking so long, the system is insecure, which makes it difficult to deal with fraud and tampering.[5]. Additionally, private information is contained in students' credentials, making privacy crucial when releasing this information. New privacy laws, including the General Data Protection Regulation (GDPR), make it legally necessary to protect the privacy of personal information.[6]. The necessity for a safe and effective method to exchange student credentials within and outside of educational institutions is what inspired this paper. A more robust and trustworthy method of distributing and validating students' credentials is required given the growing use of digital credentials and the expansion of online learning and career opportunities.

Blockchain technology, which is well-known for being decentralized and unchangeable, provides a transparent and tamper-proof platform for storing and validating shared credentials. With the help of blockchain, the system may keep an everlasting and verifiable record of the credential-sharing process, fostering confidence and enabling speedy verification by educational institutions, employers, or other authorized authorities. Additionally, in order to address the privacy concerns created by credential sharing, student privilege is crucial. The right to privacy is protected and the risk of misuse or unauthorized disclosure is decreased when students have the capacity to control who has access to and how their credentials are distributed. This helps to preserve students' right to privacy.

Therefore, the motivation of the proposed paperwork is to create and build a complete system that combines blockchain technology with the student privilege system. The proposed approach aims to improve the security, privacy, and effectiveness of the credential sharing process, thereby supporting students, educational institutions, employers, and other parties involved in the sharing and verification process.

1.2. Objectives

The main objectives of our paper are:

a. **Create a reliable and secure system:** The main goal is to plan and set up a system for the secure transmission of student credentials. SISS is used for splitting credentials into shares and use of IPFS network for decentralized storage and for further verification and transparency blockchain technology is used.
b. **Controlled access to credentials:**The system attempts to ensure that access to student credentials is controlled. This means that only authorized parties can request and decrypt credentials. The goal is to establish a secure, consent-based exchange method that is accomplished through collaboration between students and authorized parties. The system attempts to ensure that access to student credentials is controlled. This means that only authorized parties can request and decrypt credentials. The goal is to establish a secure, consent-based exchange method that is accomplished through collaboration between students and authorized parties.
c. **Providing student privilege:** Students would feel more empowered during the sharing process if they were given control over their own credentials. In order to safeguard their privacy and keep ownership of their academic achievements, students will have the choice of accepting or rejecting access to their share.
d. **Use blockchain for immutability and transparency:** The objective is to provide a transparent and immutable record of credential-sharing operations using blockchain technology. The blockchain's decentralized structure boosts trust and enables stakeholders to verify the legitimacy and integrity of the shared credentials.
e. **Examine scalability and efficiency:** The purpose of this paper is to address scalability and efficiency issues associated with exchanging large numbers of student transcripts. The goal is to implement IPFS on distributed storage and improve system speed so that the system can manage a large number of requests and provide an effective release mechanism.

1.3. Our contributions

Addressing the fundamental issues with student credential security is the main goal of our study. In order to increase the security, control, and efficiency of the credential-sharing process, the paper offers a student privilege management

system that integrates secret image sharing scheme, blockchain technology, and IPFS. The concept of this paper is how to share and manage student credentials using blockchain technology and SISS in conjunction with an off-chain storage system.

a. We proposed a blockchain-based architecture to securely share student credentials.
b. To protect the confidentiality of student credentials, we proposed a student privilege management that uses secret sharing for data protection.
c. We have adopted an off-chain storage mechanism using IPFS to improve system scalability.
d. Using Ethereum, we have created a decentralized application (DApp) that serves as a prototype of the proposed architecture.
e. Our system uses smart contracts and costs are calculated based on the execution time of key processes.

2. Related Work

Among the many benefits of using blockchain in educational systems are the immutability and provenance of uploaded credentials, peer-to-peer secure exchanges between parties, transparency, trust, and a distributed digital ledger and so on. These benefits have led to extensive research, some of which are briefly described in this section.

Arenas and Fernandez [7] proposed a mobile application for storing and validating student credentials using the Hyperledger blockchain (permissive). However, it does not demonstrate proper checking of mobile apps for computational complexity and execution time. Also, certificates are stored on-chain, making further expansion difficult. Andreev and Daskarov [8] proposed a blockchain framework that allows the exchange of student registration data from schools to learners to businesses (or vice versa). However, the proposed model is partially decentralized as it uses a central database to store data. This paper also does not provide any implementation or experimental evaluation. A similar problem arises in the work of Young and Berhulst [9]. The work is a case study on a blockchain platform for storing student degrees implemented by the Massachusetts Institute of Technology (MIT). Each credential has a unique URL that you can share with others. The recipient of the URL can verify that the URL is genuine by visiting the official website and checking the authenticity of the URL.

Han et al. [10] introduced a blockchain-based architecture for storing educational documents on the blockchain. However, this work does not include implementation or test-based results. The student certificate management architecture proposed by Gräther et al.[11] uses a distributed file system to store certificate authority profile information. However, the actual certificate (in plaintext) appears to be stored in a central system. Another problem is that every time a student wants to share his or her credentials, the request must be approved by the agency that manages the central system.

The author Joan Hope [12] reported that a Central New Mexico Community College is using blockchain to store student ID cards, allowing students to own their educational credentials. Students can download their credentials to any device using their wallet address. However, it does not contain an implementation. Their work uses on-chain storage, which is expensive and therefore not scalable. A study published by Kanan et al.[13] used a blockchain-based prototype consisting of two types of users: one for administrators and another for students. Administrators can add certificates to student accounts and students can view certificates. However, their work does not include the cost of various smart contracts.

Ocheja et al.[14] proposes that each institution, via a smart contract, store student files, and grant access to data storage used to protect student privacy. This architecture raises many security and privacy issues because the data stored is plain text and the database is centralized. Additionally, even after an institution grants access to a student, the institution may continue to allow other students access to its learning logs. Therefore, students do not have full control over their personal data. Furthermore, this work does not address how the entry of new users will be possible. For the effective preservation and upkeep of electronic health records, Jayneel Vora et al. [15] developed a Blockchain-based infrastructure. They also described a method for patients, healthcare professionals, and other parties to access medical data securely and effectively while maintaining patient privacy.

The authors Kalani and Aditya [16] proposed storing student credentials on the Ethereum blockchain and analyzed the complexity of smart contracts in terms of cost calculation and time required to mine the transactions. Certificates appear to be stored directly on the blockchain, which creates scalability issues. Duong et al. [17] introduced IU-SmartCert, a blockchain-based system and process for issuing, validating and exchanging educational certificates with selective disclosure capabilities. However, the actual certificate seems to be stored on-chain, making it difficult to scale further.

Another important issue faced by many stakeholders is trust and enables stakeholders to verify the legitimacy and integrity of the shared credentials. The potential for fraud on the part of the certifying authority or dealer and/or other stakeholders or participants was one issue with the traditional secret image sharing methods. The concept of detecting fraud by dishonest dealer and participants was initially developed by Chor et al. [18]. The primary problems with most verifiable secret image sharing schemes (VSISS) are that they either need too much computer power or don't meet all of the requirements of VSISS. This inspired Chattopadhyay et al [19] to create a secret image sharing system that is computationally cheap and can verify shared images before the actual reconstruction process takes place. The XOR-based scheme, ensures low computational complexity. Each secret image is XORed with a random image matrix generated by a pseudorandom number generator to produce a noise-like image. Then shares are generated from the original images just by using XOR operation. Cascading secret image hashes to allow proper verification of recovered secrets (in case the trader is dishonest and intentionally submits false shares) with a single comparison to public data added by the method. Additionally, each member can independently verify their share using a publicly available hash code to spot fraudsters. Shares submitted to a combiner may also be reviewed by the combiner. A specially used hash function reduces the computation time of the verification process.

This paper addresses the issues mentioned in the related work section by fully decentralizing the system to ensure confidentiality, integrity, and trust, and by storing certificates on distributed off-chain servers to make the system scalable using a hybrid architecture based on SISS, Blockchain as well as IPFS network.

3. Preliminaries

This paper presents a secure and tamper-proof structure for sharing student credentials with other stakeholders. The purpose of the proposed structure is to ensure both protection and privacy. The proposed architecture consists of two phases, first securely sharing and storage of student credentials by the certifying authority and second retrieving the verified student credentials as and when required by the other stakeholders with the permission of the student. A safe, reliable, and scalable architecture is described in the first phase using SISS and IPFS network, which makes use of off-chain storage to enhance scalability. The architecture is improved further by including student privilege with the help of secret sharing to control the access and sharing of student credentials. This guarantees that their private information is kept private and shared only with necessary parties, protecting their right to privacy and reducing the chance of abuse or unlawful disclosure. And in the second phase, blockchain technology is used for verifying the integrity of the students' credentials.

a. **Secret image sharing scheme**: In a scenario where more than $k \leq n$ participants can form a clique (a selfish group) and deceive the rest, the (n,n) secret-sharing scheme has a better performance than the (k,n) threshold. could also be better. A secret-sharing scheme in the sense of exploiting sensitive secrets without others knowing. However, the (n,n) secret release scheme guarantees that the secret will be released if all participants are present (since all n shares must be sent). Here we propose a (n, n) secret image publishing scheme using his bitwise XOR operation. Using Boolean operations ensures high performance in building shares and reconstructing secrets. In the proposed scheme, the time complexity of the secret reversible reconstruction method is O(n). where n is the number of shares. Additionally, this scheme produces scalable shares that can be easily stored and transmitted within the network [20], [21].
b. **IPFS**: IPFS is a version-controlled, content-addressed file system in the sense that any data that is posted to an IPFS network produces a hash, which is used to retrieve the data. On the IPFS network, anyone can provide storage, and everyone gets rewarded with crypto tokens. The network allows for the distribution and replication of data, which results in data permanence. It seeks the closest copy of the requested data while making the request, which causes significant latency and gets around any bottleneck points. Since the data is entirely dispersed, there is no scope for data centralization. When a file is submitted to IPFS, the hashed Content Identifier (CID) is generated and shared with peers. Anyone who has the hash value can access or view the file using the hash address. The owner of the file will no longer have access once it has been uploaded to IPFS [22].
c. **Blockchain**: A blockchain is, as its name implies, a network of interconnected blocks. The structure is used for storing important information in each block, which has a distinct hash value and contains a specific quantity of transaction data. By incorporating a unique hash value for the previous block, these blocks are linked chronologically, assuring the security of the entire blockchain network. A decentralized blockchain network ensures the security of cryptocurrency networks since there is no central authority. The following three primary features make blockchain technology suited for addressing security issues:

- **Decentralization:** Distributed blockchain technology can prevent a single point of failure and significantly lower the cost of system maintenance for a large system as compared to traditional centralized management approaches.
- **Immutability:** Blockchain technology can exist in an immutable form in which no network participant can ever be able to change, cancel, or remove the transaction
- **Transparency:** The term "blockchain transparency" refers to the unique property of the blockchain that guarantees all transactions and data on the network are accessible to anybody with system access [23].

4. Proposed work

This paper considers an academic environment that is composed of three different parties, or stakeholders. These stakeholders play one-of-a-kind roles, which are stated below:

a. **Educational Institutions**: Educational institutions of any kind, like schools, colleges, universities, etc., are represented by the stakeholder "Educational Institutions." Their role is both that of an issuer and a viewer. The reason for this is that institutions will issue certificates to enrolled students when they meet the requirements and also refer to other students' certificates issued by other institutions. Registered institutions are responsible for publishing and verifying credentials, as well as revoking certificates if the certificate was issued incorrectly or the student is engaged in dishonest behavior.
b. **Students**: Credentials must be displayed and securely stored in the academic portfolio for future use. Students are required to show credentials upon admission to a particular university or during a recruitment process. Thus, the roles of the student are both a viewer and to provide access to the certificate.
c. **Companies and Other Stakeholders**: At the time of hiring, the company will most likely need to view the credentials of the applicant. Also, when a student completes their training or internship with the organization or a particular company, it is the responsibility of the respective company to issue a corresponding certificate. Similar to institutions, companies can also be publishers and viewers.

4.0.1. Proposed Scheme

We used an XOR-based method for secret sharing of student credentials in our suggested system. The plan entails dividing the credentials into two parts, giving the student one share and storing the other half on a blockchain that only authorized parties may access. The shares must be acquired, and an XOR operation must be carried out in order to decrypt the credentials. The suggested framework and the associated algorithms are described in detail below:

4.1. System Architecture

The corresponding architecture of our proposed model for secured sharing of student credentials is shown in Fig. 1. This architecture includes different parties or stakeholders, the process, and also distributed file storage with an off-chain mechanism (i.e., IPFS). To record the interactions taking place between the various stakeholders, blockchain is used in the form of immutable transactions. The accomplishment of such transactions is achieved by deploying smart contracts on the blockchain to manage all the necessary interactions between the stakeholders and provide various functionalities. To achieve student privilege, we proposed an XOR-based, verified, secret image sharing technique. In our suggested system, n participants will each get n share photos that are encoded with n secrets. The one-way hash function, a particular pseudo-random image-matrix generation algorithm, and XOR operations are used to create the shared images.

The methodology for the proposed system is as follows:

a. **Registration of Institutes:** Registration of institutes is done by the Central Authority. The Central Authority enables institutes to register themselves on the network with a lifelong permanent account on the blockchain. The registration includes the institute's permanent network address, institute name, institute acronym, institute's official website, and the courses it provides.
b. **Log In:** After successful registration, institutes can log in with the same network address they used while registering. Institutions go through a one-time registration process, which would simplify subsequent logins.
c. **Student Enrollment:** This is utilized by the academic organization at the time of admission. For enrolling the student, the institution appears to confirm the existence of the student's account using the blockchain's public key. After verification, the Institute enlists the student by using the public key. Additionally, this is displayed on the student's account.

d. **Creating and Uploading of Credentials:** If students meet the course or program requirements, the institute will issue credentials to enrolled students. These credentials (degrees, certificates, transcripts, etc.) are sizeable pieces of data, so storing them on the blockchain becomes an expensive proposition. In this view, the proposed architecture uses distributed file storage (off-chain storage) to store credentials. The overview of the process is as follows:
   i. **Certificate Conversion:** The institution first converts the certificate into matrix form. Then it generates a random matrix of the same size. This random matrix is named Share 1 and is provided to the respective student. The XOR operation is performed between the two matrices, and the resulting matrix is named Share 2. Share 1 is provided to the student, while Share 2 is retained by the institute.
   ii. **Share Distribution:** The student is granted a share that gives them authority over their own certificate and the people who can access it. The part that the institute owns is kept in a secure location for backup and possible future recovery.
   iii. **IPFS Storage:** The institution uploads its share (Share 2) to the distributed file system known as IPFS, which was created for the purpose of storing and distributing files on a decentralized network. The share is saved in IPFS and given a distinct hash that represents its content.
   iv. **Blockchain Storage:** The institute stores the IPFS content's location or hash on the blockchain. This establishes a reference or proof of existence on the blockchain and paves the way for later retrieval and verification.
   v. **Scalability Advantages:** The blockchain's scalability is increased by merely holding the certificate's hash rather than the whole certificate itself. The certificate is stored in a condensed form on the blockchain, allowing for quick queries and verifications without the need for a lot of data storage.

e. **Certificate Retrieval and Verification:** This allows the student and other stakeholders to retrieve (and view) credentials uploaded by the participant. To retrieve and view the uploaded credentials, both shares (Share 1 and Share 2) are required to decrypt the certificate. Share 2 must be taken from the blockchain by an authorized entity that wishes to access and decrypt the student's certificate, and the student's share must be requested. The overview of the process is as follows:
   i. **Retrieval of share:** The required data is extracted from the blockchain by an authorized entity that wishes to access the student's credentials. From the IPFS network, the authorized party retrieves the IPFS material indicated by the location or hash. By gaining access to the relevant hash linked to the certificate, the authorized person can get the share kept on the IPFS.
   ii. **Request for Share:** The authorized person sends an access request to the student asking for their share to be decrypted after taking the other share from the blockchain. The notification prompt in the student dashboard contains all the pertinent details on the request and the reason for gaining access to the certificate.
   iii. **Response by student:** The student examines the information in the request after receiving it and then chooses whether to approve or reject the decryption request. If the student agrees to the request, they send their portion to the designated person through a secure and reliable communication channel.
   iv. **Decryption and Share Combination:** After receiving the student's share, the authorized party combines it with the share that was retrieved from the blockchain. The original certificate is unlocked and made available by performing the XOR procedure on the two shares. The overview of the encryption and decryption process of the certificate is shown in Fig. 2
   v. **Usage of Credentials:** When the certificate has been successfully decrypted, the authorized party can use it for its specified function.

This strategy combines the advantages of decentralized and immutable blockchain technology with distributed file storage utilizing IPFS. By dividing the certificate into shares, the institute can guarantee the certificate's availability and backup while the student keeps ownership of their credentials. This strategy guarantees that the student maintains control over their share and has the ability to decide whether to allow access to their certificate in an informed manner. The student can confirm the validity of the decryption request before delivering their part thanks to the access request's notice and authorization mechanisms. Scalability is improved by merely maintaining the certificate's hash on the blockchain, as this relieves the blockchain of having to store a lot of certificate data. The actual certificate may be kept effectively and decentralized via IPFS, and authorized parties can access it using the appropriate hash saved on the blockchain.

5. Implementation

The implementation of our prototype is explained in this segment. The prototype of our proposed system is a Decentralized Application (DApp) for the secure sharing of students' credentials.

5.1. Backend technologies

Given that blockchain application development is still immature, DApps can be made in a variety of ways. The approach we take in our work makes use of the subsequent technologies:

a. Metamask: A browser extension that gives us the ability to interact with Ethereum. MetaMask version used in our paper is 10.23.2.
b. Ether.js: Through the JSON-RPC (Remote Procedure Call) protocol, Web3.js connects MetaMask to the client application. A JavaScript framework called Ether.js offers a handy and extensive collection of functions for interacting with the Ethereum blockchain. These features include account administration, transaction handling, the deployment and use of smart contracts, event monitoring, and more. The ether.js version used in this paper is 6.2.3.
c. React is a front-end JavaScript library that is open-source and free to use when developing user interfaces based on UI components. React version used in this paper is 18.2.0.
d. Crypto: A built-in module for Node.js which offers cryptographic features like message verification, hash generation, encryption, and decryption. Crypto version used in this paper is 4.1.1.
e. IPFS: A distributed file system for peer-to-peer data sharing. It functions according to the concept of content-based addressing. Data is returned as a hash when it is uploaded, and this hash can be used to later access the data. The version used in this paper is 0.16.0.
f. XOR-based secret image sharing scheme: Cryptographic approach called XOR-based secret image sharing uses XOR operations to split a secret into several shares, distribute them among participants, and secure their anonymity. This method also makes it possible to reconstruct the secret by combining enough shares using XOR.

5.2. Application Stack

Our prototype DApp's application stack consists of a front-end running on a back-end distributed server.

a. Front end: Users communicate with the DApp using the MetaMask browser extension, which links the application to the blockchain. Next.js is the foundation of the user interface. The DApp sends various kinds of queries to the distributed servers on the backend by utilizing the capability offered by Web3.js and MetaMask. The frontend also uses crypto to generate a SHA256 hash.
b. Decentralized server: The smart contracts set up on Ethereum handle requests produced by users. The IPFS responds to some requests.

5.3. Various smart contracts:

Interaction between the different smart contracts is shown in Fig. 3
Various variables and functions associated with the smart contracts are as follows:

a. **"InstituteRegistry" Contract:** This contract serves as a registration for educational institutions. Information retrieval and registration for institutions-related features are available. This is covered under the contract:
    i. Struct and Variables: To represent an educational institution, the contract specifies a structure named "Institute." Name, email, ins address (the institute's address), link, and acronym are just a few of the data it includes. The contract keeps track of a mapping named "institutes" to record the information about each institute along with its corresponding locations. In order to keep track of the addresses of the registered institutes, it also maintains an array named "instituteAddresses."
    ii. registerInstitute: With this function, an institute can register itself by supplying the required information, including its name, email address, physical address, URL, and acronym. It confirms that the institute hasn't previously registered before adding its information to the mapping for "institutes." The "instituteAddresses" array is expanded to include the institute's address.
    iii. getInstitute: This function returns information about an institute based on the institute's address. When given an address, it produces the name, email address, ins address, hyperlink, and acronym of the associated institute.
    iv. getInstituteCount: By passing the "instituteAddresses" array's length, this method calculates the total number of institutions that have registered.
    v. isRegisteredInstitute: This function determines whether the supplied address belongs to an institute that is registered. If the address is located when iterating over the "instituteAddresses" array, it returns true, indicating that the institute is registered. It returns false if the address cannot be located.

b. **"CertificateGenerator" Contract:**The creation, revocation, and retrieval of certificates are handled by the "CertificateGenerator" contract. It has the following features and capabilities:

i. Struct and Variables: The contract has a "Certificate" struct, which stands for a certificate. The fields include instituteAddress, instituteName, studentName, studentAddress, recordName, description, isRevoked, and ipfs. It also has other fields like recordName and description. Moreover, the contract keeps track of a mapping named "certificates" that pairs each certificate with its corresponding ID. The "certificateCount" variable is also used to keep track of the overall number of certificates.

ii. generateCertificate: With the help of this function, a registered institute can create a certificate specifically for a certain student. It checks to see whether the institute is legitimate and makes sure the certificate isn't already in existence or hasn't been cancelled. A new certificate is generated and added to the "certificates" mapping if the requirements are satisfied.

iii. revokeCertificate:With the help of the function revokeCertificate, the issuing organisation can revoke a specific certificate. It demands that the institute be the one who issues the certificate and verifies that it has not yet been cancelled. The certificate's "isRevoked" flag is set to true if the requirements are satisfied.

iv. getCertificatesByStudent: With the help of this function, you can find all the certificates linked to a certain student's address. A list of certificates that match the student's address is returned after iterating through the certificates.

v. getCertificate: The function retrieves a specific certificate based on the institute name, student name, and record name. It searches for a matching certificate and returns it if found; otherwise, it reverts with an error message.

Together, these contracts offer a thorough system for producing, archiving, and retrieving certificates while upholding the registration and certification of educational institutions. The InstituteRegistry contract acts as a register for institutions, simplifying their registration and information retrieval. And the CertificateGenerator contract manages the functionality connected to certificates,

6. Experimental results

The overall performance of the prototype DApp is calculated by forming distinctive checks. To carry out the evaluation, a local host test network is used. Ganache provides us with this environment host installation. it is a private Ethereum blockchain environment that permits us to emulate the Ethereum blockchain in order that allows one to interact with smart contracts privately for testing and development purposes. It uses Proof-of-Authority (PoA) consensus set of rules.

6.1. Cost computation and execution time of the smart contracts

The decentralized peer-to-peer network can be safely managed and to achieve that the blockchain needs to give certain incentives to the miners. The miners get rewarded for validating the transactions and also for mining the new nodes or blocks on the blockchain network. The computational capability of the system that is required to validate the transactions generally decides the reward on Ethereum. The rewards are paid to the prevailing miner in the form of gas by the sender. Therefore, to ensure profitability, it is necessary to execute the smart contract and the cost calculation of the important functions.

Deploying smart contracts on the blockchain requires two types of costs: transaction costs and execution costs. The smart contract and the data which is required for verification are sent together and the transaction cost is basically just the gas used. Transaction charges are based totally on the cost of sending data to the blockchain. Execution costs are based totally on the cost of the computational operations that are completed due to the transaction. Remix is used to calculate values for each charge.

The expenses of smart contracts are indicated in Table 1 and cost transactions required by the essential functions are indicated in Table 2.

The execution time for the application comprises mining the blocks, time for transmission, and the time associated with the execution of smart contracts. Processing of a large number of requests is handled by the Dapp, so utmost importance needs to be given to the overall time required for the execution of user requests. The transmission requests of any particular user can be of two types. The two types are reading and writing data. Reading data is done almost instantly. However, the transactions need to be validated first before the block gets mined so writing to the blockchain requires some time. The time to process a transaction on a local host is almost immediate. But the average time to

Contract	Execution Cost (Gas)	Transaction Cost (Gas)
Students	1014967	1387679
Institute	1680954	2269244
Share Files	556381	791677
Request	919455	1272875
Company	894242	1242750

Table 1
Cost of smart contracts.

Transaction	Cost in Gwei	Cost in Ether	Cost in USD
Registering an Institute	72230	0.00007214	0.015
Uploading a credential*	158413	0.000158413	0.034
Certificate Retrieval*	158288	0.000156499	0.032

*depends on the title and description length

Table 2
Transaction cost of important functions

process a transaction on other networks will vary.

6.2. Analysis of Reconstructed Certificate

6.2.1. Correlation coefficient analysis:

For a meaningful image, the correlation coefficient between neighboring pixels in the vertical, horizontal, and diagonal axes is fairly high and close to 1. (carrying a lot of information). On the other hand, given a random image, this number is very near to zero. So, when compared to the correlation coefficient of the sharing photos, the correlation coefficient for the relevant secret images (which varies from -1 to 1) is excessively high[24]. In the equation, r_{xy} stands for the calculations needed to determine the correlation coefficient between two sets of adjacent pixels, x_i and y_i.

The correlation coefficient (r_{xy}) between two sets of adjacent pixels, x_i and y_i, can be calculated using the following formula 1:

$$r_{xy} = \frac{\sum((x_i - \bar{x})(y_i - \bar{y}))}{\sqrt{\sum(x_i - \bar{x})^2}\sqrt{\sum(y_i - \bar{y})^2}} \tag{1}$$

where:

- x_i and y_i are the values of the adjacent pixels in the two sets.
- $\bar{x}$ and $\bar{y}$ are the means of the values in the respective sets.

The range of the correlation coefficient (r_{xy}) is -1 to 1, with values near to 1 indicating a high positive correlation, close to -1 indicating a strong negative correlation, and close to 0 indicating little to no correlation between the two sets of pixels.

The value of (r_{xy}) for the meaningful original image is almost equal to 1, while it is almost equal to 0 for the shared images, as can be seen in table 5.

Original Image	Horizontal	Vertical	Diagonal	Shared Images	Horizontal	Vertical	Diagonal
I_1	0.9738	0.9907	0.9834	$Share_1$	0.0150	0.0282	0.0323
				$Share_2$	0.0099	0.0176	0.0122

Table 3
Structural similarity index measure (SSIM) between the shares.

Original Image	I_1
Reconstructed Image	I_1'
SSIM	1.000

Table 4
SSIM values between the original image and reconstructed image.

6.2.2. Structural similarity index matrix (SSIM) analysis

The structural similarity index measure (SSIM) is used in the secret sharing scheme to assess how closely the secret image and the shared image resemble one another[25]. To calculate similarity, SSIM takes into account the structure together with luminance and contrast. The SSIM value ranges from 0 to 1. The two photos are not similar if the SSIM value is zero, but they are similar if the SSIM value is one. The SSIM value between two images, IA and IB, can be determined using Equation 2. To compare the reconstruction of our secret to the original image, we employed SSIM. It is also used to assess how distinct the generated share image is from the source image. Our experimental results reveal that the original certificate image I_1 and the reconstructed certificate image I_1' are similar, as given in the table 4, where I range from 1 to k. It follows that only the combination of the two shares has the ability to divulge details regarding the original image or certificate. Authorized entities can download Share 1 from the public IPFS network, but without the proper collaboration of the student, no information about the original certificate is disclosed.

$$\mathrm{SSIM}(IA, IB) = \frac{(2\mu_{IA}\mu_{IB} + C_1) \cdot (2\sigma_{IA,IB} + C_2)}{(\mu_{IA}^2 + \mu_{IB}^2 + C_1) \cdot (\sigma_{IA}^2 + \sigma_{IB}^2 + C_2)} \tag{2}$$

Figure 4 illustrates the progression from the original certificate image to its transformation into two noisy shares. These shares are then merged using XOR operation to reconstruct the certificate image, resembling the original certificate image.

6.3. Comparison with related works

Table 5 distinguishes our work from existing related studies. Data size is paramount to securely issuing, viewing, and sharing all types of educational credentials. Using on-chain data storage incurs prohibitive costs that may not be affordable for stakeholders, especially students. Therefore, our proposed architecture uses off-chain distributed file storage. This reduces costs and improves scalability. Unlike related works, the security elements offered by our paper includes confidentiality, authenticity, integrity, and availability. A student acquires complete ownership of a credential after it has been granted. Our work also reveals the implementation information of the DApp and conducts experiments to affirm its feasibility.

6.4. Working of proposed DApp

The major use cases that our implemented DApp provides are a central authority portal for allowing the registration of institutes, issuing of certificates after successful registration of institutes, revoking of certificates by the registered institutes, and allowing the students to access and share their required certificates.

a. **Homepage:** Home page of the proposed DApp. Institutes can register themselves and start issuing certificates for their students. Other stakeholders can access students' certificates, provided they have the authority and get access from the respective students. The student dashboard provides an efficient way for them to access, view, and give access to their certificates. Fig. 5 shows the homepage of the proposed DApp.

Table 5
Comparative study of our proposed scheme with various existing secret image sharing schemes

Schemes	Confidentiality	Authenticity	Integrity	Privacy	Off-chain	Cost compute	Execution time	Scalability
Arenas and Fernandez [7]	*No*	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*	*No*
Andreev and Daskalov [8]	*No*	*Yes*	*Yes*	*No*	*No*	*No*	*No*	*No*
Young and Verhulst [9]	*No*	*Yes*	*Yes*	*No*	*No*	*No*	*No*	*No*
Han et al. [10]	*No*	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*	*No*
Grather et al. [11]	*No*	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*	*No*
Joan Hope [12]	*No*	*Yes*	*Yes*	*No*	*No*	*No*	*No*	*No*
Kanan et al.[13]	*No*	*Yes*	*Yes*	*No*	*No*	*No*	*No*	*No*
Ocheja et al.[14]	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*No*	*Yes*
Kalani and Aditya [16]	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*No*
Duong et al.[17]	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*No*
Our work	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

b. **Interface to register institutes:** The interface allows the institutes to register themselves in the central authority portal, and only the registered institutes can issue certificates. Fig. 6 shows the Central Authority Portal for the registration of institutions. After filling out the necessary details, institutions have to enter the verification code that they will get at their provided email for successfully completing the registration process

c. **Issuing of certificates:** After the registration of institutes, the institute portal becomes accessible, and the institute can issue the requested certificates for the students. The interface for the registered institutes to issue certificates to their students is shown in Fig. 7.

d. **Revoking of certificates:** If the institute wants to revoke any particular certificate of a student, it can do so which will attach a revoked message to that particular certificate. The DApp offers a way to revoke a credential in the event of fraudulent or unauthorized use by allowing the issuing institution to revoke a certificate. This guarantees that only legitimate and current credentials are recognized by authorized parties, maintaining the system's credibility. The interface to revoke a certificate is shown in Fig. 8

e. **Viewing Certificates:** The proposed DApp has a "View Certificate" portal that enables users to access and examine the relevant student credentials, as well as those of other organizations, businesses, or other permitted parties. They must get their portion of the certificate from the issuing organization in order to accomplish this. The 'View Certificate Portal' is shown in Fig. 9 To view the actual certificate the stakeholder has to ask the student for permission to access their share by submitting a request. The decision to accept or reject the request rests with the student. The stakeholder is given access to the student's share and is permitted to examine the certificate if the student allows the request. Nevertheless, the stakeholder's access is restricted if the student refuses the request. Fig. 10 shows the stakeholder getting access from the student. Fig. 11 shows the stakeholder getting denied access from the student.

f. **Student Dashboard:** The student dashboard is made to give an in-depth look at all of the student's certifications, both active and revoked. The dashboard interface shows the list of certificates the student has earned together with pertinent information such as the name of the certificate, the institution that issued it, the record name, the record description, and any other data. All revoked certificates, if any, are denoted with a cross symbol to indicate their status. By making it simple for the student to recognize and distinguish between active and revoked certificates, this feature promotes transparency and guarantees that only legitimate credentials are offered for verification. The interface of the student dashboard is shown in Fig. 12
Moreover, the student dashboard has a function that alerts the student if someone seeks access to their certificate. A notice is generated on the student dashboard whenever a stakeholder or other entity asks to examine a certain certificate, informing the student of the request. Following a review of the request, the student can decide whether to allow or refuse access to their certificate in accordance with all the relevant information. Fig. 13 shows the student getting a request for access to a certificate.

6.5. Screenshots of the proposed DApp

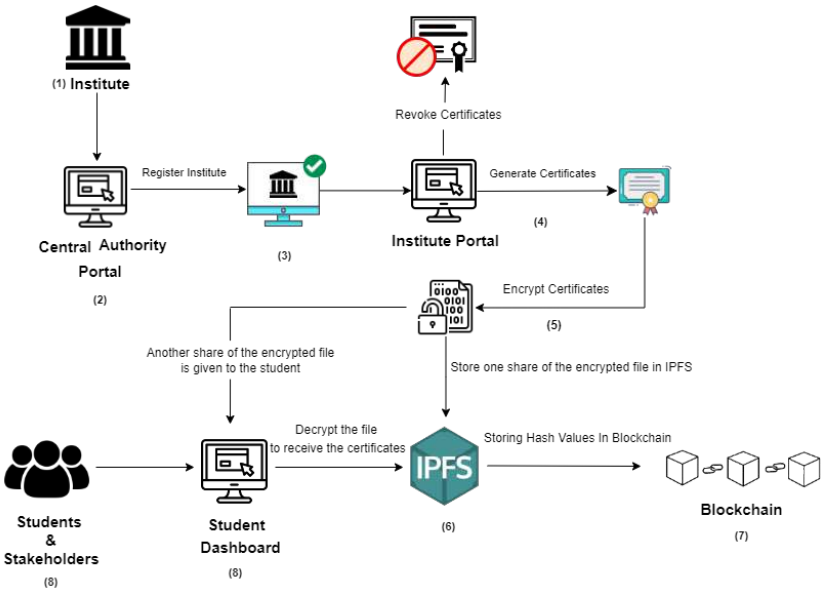


Figure 1: System Architecture

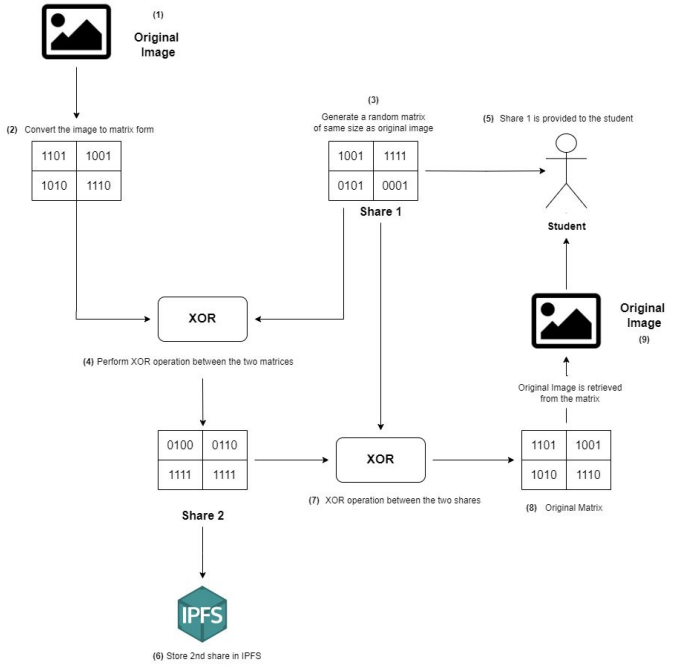


Figure 2: Certificate encryption and decryption process

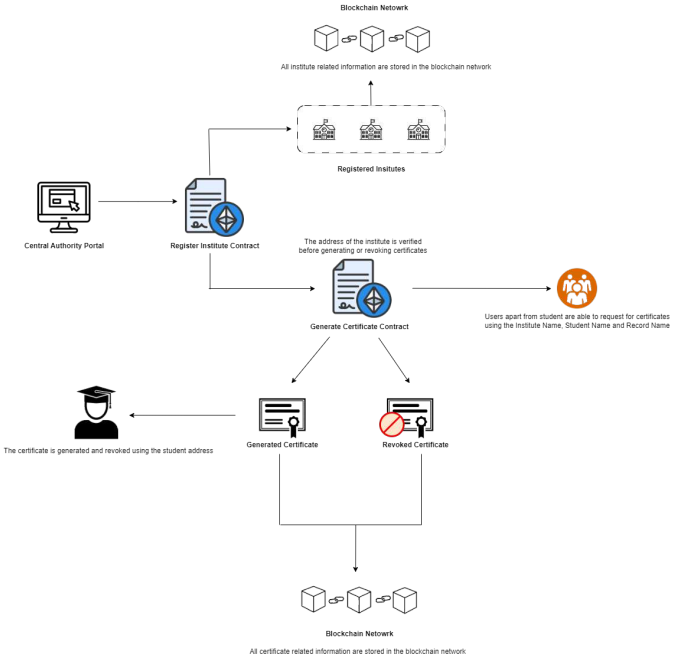


Figure 3: Interaction between different smart contracts.

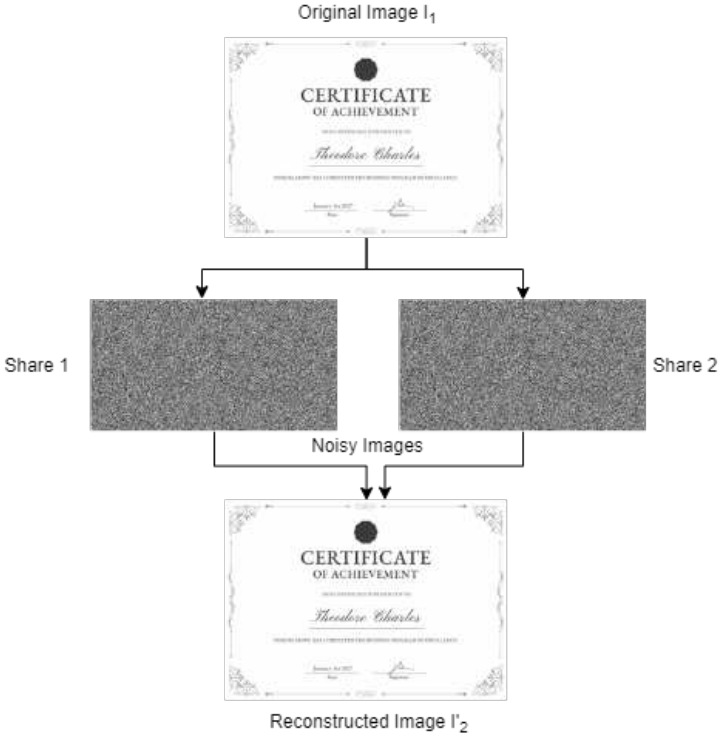


Figure 4: Reconstruction of Image

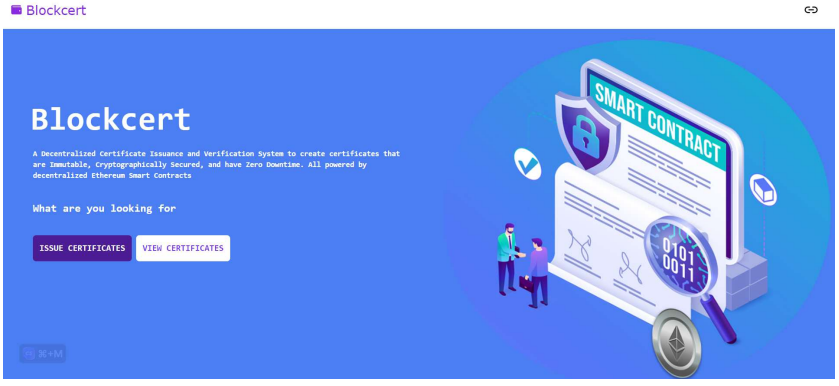


Figure 5: Homepage of the DApp

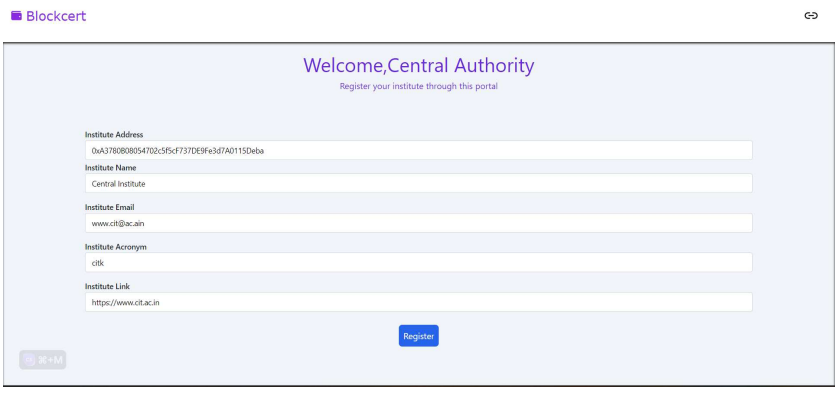


Figure 6: Institute Register Portal

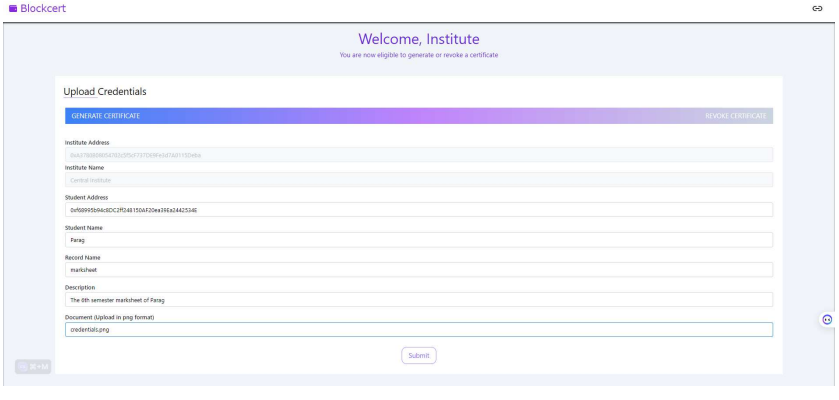


Figure 7: Issuing Certificates

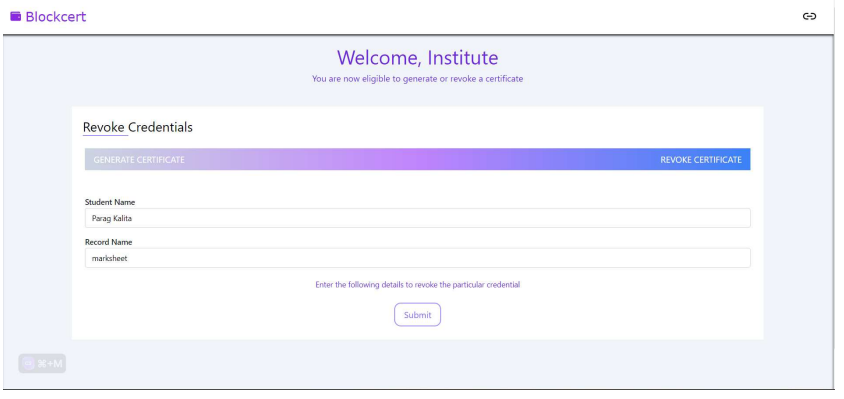


Figure 8: Revoking Certificates

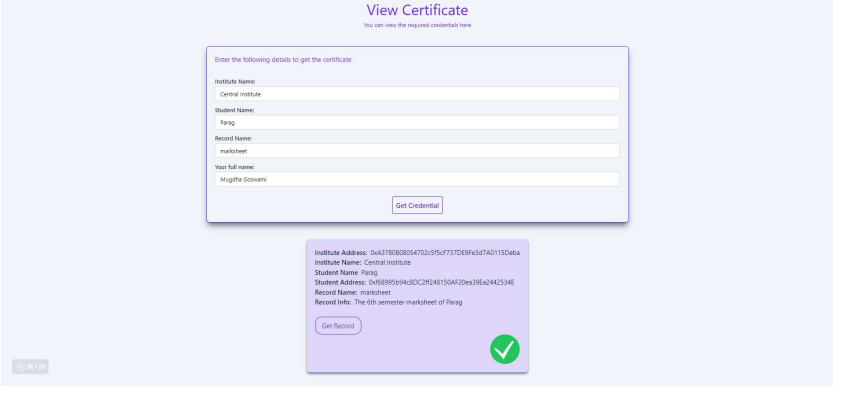


Figure 9: View Certificate Portal

7. Conclusion

In conclusion, this study proposes a thorough framework for multi-secret sharing and blockchain technology-based safe student credential exchange. The suggested method takes care of the requirement to safeguard confidential data while permitting authorized individuals to access and decode the credentials. The purpose, approach, and potential future use of the system were all covered in this paper.

The significance of student privilege in managing access to their credentials was emphasized, underlining the requirement of a secure and user-centric strategy. The study was motivated by the growing demand for safe sharing methods in educational institutions, where student credentials must be protected from illegal access and modification. The methodology provided a step-by-step procedure for transforming the certificate into two shares, distributing them to the student, and storing one share on IPFS with the associated hash on the blockchain for scalability. The decryption method requires retrieving the other share from the blockchain and requesting the student's share. The certificate was then decrypted using the XOR operation. Topics for additional study and development, including real-world deployment and assessment, were identified in the future work section. The system's functionality, security, and usability are intended to be improved in order to keep up with changing demands and technological improvements.

However, it is crucial to take into account the actual implementation difficulties and potential complexity linked to combining IPFS, blockchain, and multi-secret sharing technologies. To maintain the effective operation and security of these systems, more resources, knowledge, and maintenance work may be necessary.

The suggested system, which combines the benefits of blockchain for immutability and tamper-resistance, IPFS for decentralized and scalable file storage, and multi-secret sharing for data secrecy, offers a solid solution for the secure sharing of student credentials. The system can offer a dependable and effective mechanism for safeguarding student credentials, upholding privacy, and guaranteeing restricted access in educational settings and beyond by putting the suggested approach into practice and taking future research fields into account.

8. Future work

Our future plan is to concentrate on further enhancing the system's usability and user experience to boost adoption and acceptability. In order to make it better, and evaluate its usability, performance, security, and efficiency in real-world situations, our plan is to perform real-world system deployments and assessments at educational institutions or other pertinent contexts.

References

[1] Ashish Singh and Kakali Chatterjee. Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79:88–115, 2017.

[2] Adi Shamir. How to share a secret. Communications of the ACM, 22(11):612–613, 1979.

[3] Chih-Ching Thien and Ja-Chen Lin. Secret image sharing. Computers & Graphics, 26(5):765–770, 2002.

[4] Mohammed Shuaib, Noor Hafizah Hassan, Sahnius Usman, Shadab Alam, Surbhi Bhatia, Arwa Mashat, Adarsh Kumar, and Manoj Kumar. Self-sovereign identity solution for blockchain-based land registry system: a comparison. Mobile Information Systems, 2022, 2022.

[5] Linda J Børresen, Einar Meier, and Stig Arne Skjerven. Detecting fake university degrees in a digital world. In Corruption in Higher Education, pages 102–107. Brill, 2020.

[6] Paul Voigt and Axel von dem Bussche. Enforcement and fines under the gdpr. In The EU General Data Protection Regulation (GDPR), pages 201–217. Springer, 2017.

[7] Rodelio Arenas and Proceso Fernandez. Credenceledger: a permissioned blockchain for verifiable academic credentials. In 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), pages 1–6. IEEE, 2018.

[8] Ognyan Andreev and Hristian Daskalov. A framework for managing student data through blockchain. In Proceedings of X international scientific conference e-governance and e-communications, 2018.

[9] Andrew Young and Stefaan Verhulst. Creating immutable, stackable credentials through blockchain at mit, 2018.

[10] Meng Han, Zhigang Li, Jing He, Dalei Wu, Ying Xie, and Asif Baba. A novel blockchain-based education records verification solution. In Proceedings of the 19th annual SIG conference on information technology education, pages 178–183, 2018.

[11] Wolfgang Gräther, Sabine Kolvenbach, Rudolf Ruland, Julian Schütte, Christof Torres, and Florian Wendland. Blockchain for education: lifelong learning passport. In Proceedings of 1st ERCIM Blockchain workshop 2018. European Society for Socially Embedded Technologies (EUSSET), 2018.

[12] Joan Hope. Give students ownership of credentials with blockchain technology. Enrollment Management Report, 23(2):6–7, 2019.

[13] Tarek Kanan, Ahamd Turki Obaidat, and Majduleen Al-Lahham. Smartcert blockchain imperative for educational certificates. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pages 629–633. IEEE, 2019.

[14] Patrick Ocheja, Brendan Flanagan, Hiroshi Ueda, and Hiroaki Ogata. Managing lifelong learning records through blockchain. Research and Practice in Technology Enhanced Learning, 14(1):1–19, 2019.

[15] Jayneel Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, Mohammad S Obaidat, and Joel JPC Rodrigues. Bheem: A blockchain-based framework for securing electronic health records. In 2018 IEEE Globecom Workshops (GC Wkshps), pages 1–6. IEEE, 2018.

[16] Aditya Kalani. Student Credential Sharing System Using Blockchain DApp. PhD thesis, California State University San Marcos, 2021.

[17] Thanh-Tung Tran and Hai-Duong Le. Iu-smartcert: A blockchain-based system for academic credentials with selective disclosure. In International Conference on Future Data and Security Engineering, pages 293–309. Springer, 2021.

[18] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In 26th Annual Symposium on Foundations of Computer Science (sfcs 1985), pages 383–395. IEEE, 1985.

[19] Arup Kumar Chattopadhyay, Amitava Nag, Jyoti Prakash Singh, and Amit Kumar Singh. A verifiable multi-secret image sharing scheme using xor operation and hash function. Multimedia Tools and Applications, 80:35051–35080, 2021.

[20] Arup Kumar Chattopadhyay, Amitava Nag, and Jyoti Prakash Singh. An efficient verifiable (t, n)-threshold secret image sharing scheme with ultralight shares. Multimedia Tools and Applications, 81(24):34969–34999, 2022.

[21] Xuehu Yan, Junhao Li, Zulie Pan, Xiaofeng Zhong, and Guozheng Yang. Multiparty verification in image secret sharing. Information Sciences, 562:475–490, 2021.

[22] Randhir Kumar, Rakesh Tripathi, Ningrinla Marchang, Gautam Srivastava, Thippa Reddy Gadekallu, and Neal N Xiong. A secured distributed detection system based on ipfs and blockchain for industrial image and video data security. Journal of Parallel and Distributed Computing, 152:128–143, 2021.

[23] Zibin Zheng and Shaoan Xie. Hongning. Dai, Xiangping Chen and Huaimin Wang, 2017.

[24] Umme Sara, Morium Akter, and Mohammad Shorif Uddin. Image quality assessment through fsim, ssim, mse and psnr—a comparative study. Journal of Computer and Communications, 7(3):8–18, 2019.

[25] Zhou Wang, Alan C Bovik, Hamid R Sheikh, and Eero P Simoncelli. Image quality assessment: from error visibility to structural similarity. IEEE transactions on image processing, 13(4):600–612, 2004.

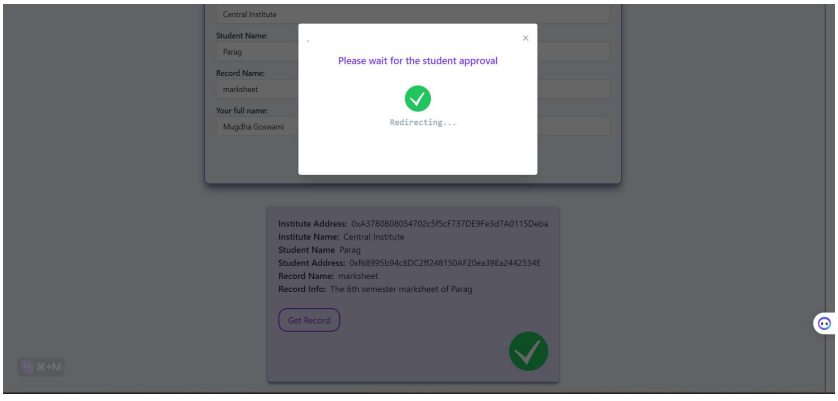


Figure 10: Stakeholder is given access by the student

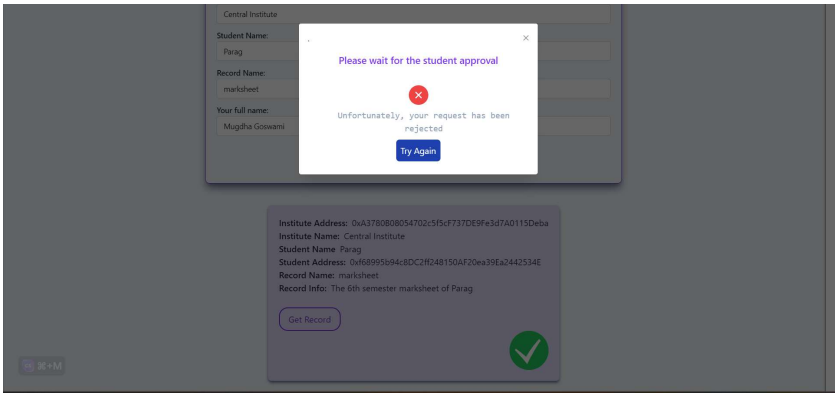


Figure 11: Stakeholder is restricted by the student

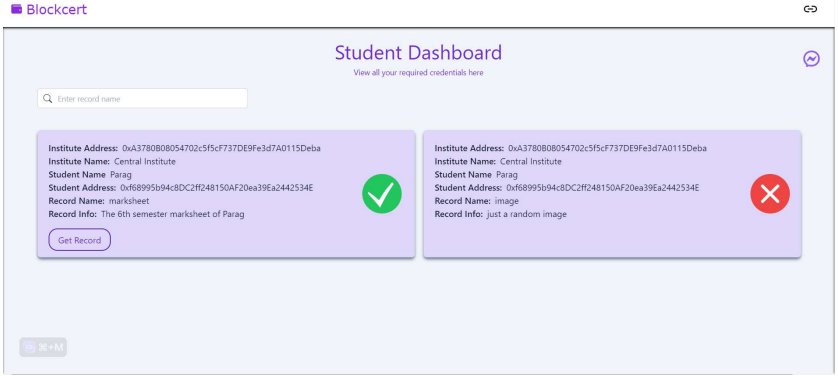


Figure 12: Student Dashboard

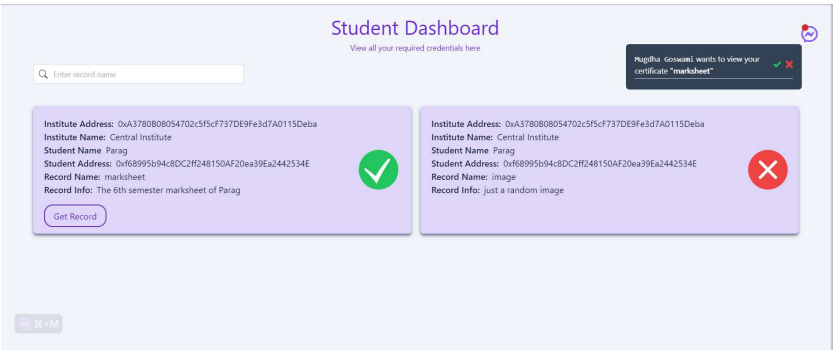


Figure 13: Request for access

9. Declaration

We hereby declare that the Submitted manuscript is our original work and no part of it has been published anywhere else in the past. I(author) along with my co-author take full responsibility, that if in future, the paper is found invalid according to basic rules, the last decision will be of the Authorities concerned. Any form of plagiarism will lead to disqualification of the paper.
Date: 22/12/2025

Title	Privileged-Based Secure Sharing of Student's Credentials using Blockchain Technology and Secret Image Sharing Scheme
Journal	EURASIP Journal on Information Security
Corresponding Author	Puja Sarkar
Google Scholar ID	Puja Sarkar - Google Scholar

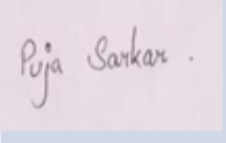
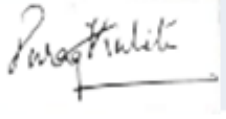
Author(s) name	Highest Degree	Signature	Contributions
Puja Sarkar	PhD		Structure preparation, Data collection and analysis, first draft preparation and comment.
Parag Jyoti Kalita	B.Tech		Material preparation, Data collection and analysis, Figure formation.

Figure 14: Author's Declaration