E-Certificate Generation and Verification using Blockchain

Achyuth Anand 205001003
Laxman D 205001058

BE CSE

Semester 8

Dr. S. Kavitha
Supervisor

Project Review: 1

February 10, 2024

Batch ID: G4_5

Department of Computer Science and Engineering

SSN College of Engineering

Contents

1. Abstract

In the contemporary context, the production and validation of electronic certificates encounter significant obstacles. Traditional methods of certificate distribution involve physical copies, making verification a time-consuming and resource-intensive task. As a consequence, counterfeit certificates have become increasingly prevalent, making it difficult to distinguish between genuine and fake credentials. Existing solutions, often relying on centralized databases, can be vulnerable to hacking and manipulation. Recent news reports have highlighted the alarming frequency of certificate frauds, shedding light on the pervasive and elusive nature of such incidents. These fraudulent activities are not only challenging to detect but also have far-reaching consequences, affecting numerous lives and undermining the trustworthiness of educational and professional qualifications. In response to these challenges, we propose a secure decentralized certificate generation and verification ecosystem using blockchain technology. Our proposed system ensures the integrity of student records and offers robust verification, enhancing security and protecting sensitive student information.

2. Introduction

In this section, we delve into the foundational aspects of our project, exploring its background, purpose, and scope. The problem statement underscores the necessity for our intervention, while the outlined objectives guide our endeavors. Anticipating tangible outcomes, this section serves as a compass, charting the course for a robust and innovative solution within the defined project scope.

2.1 Background

In recent years, blockchain has emerged as a technology on the move. It entered the market as an infrastructure for cryptocurrency. Today, with the help of smart contracts, blockchain can be used to store and share data throughout the blockchain network. The data written to the blockchain is immutable. New blocks are created for each update if previous data logs are still available. This ensures that data on the blockchain cannot be tampered with. Because blockchain is a distributed network, it avoids a single failure. Today, every business is trying to convert their business

processes to blockchain. The increase in the number of users of cryptocurrencies is an indicator of the development of blockchain technology, as Figure 1 shows.

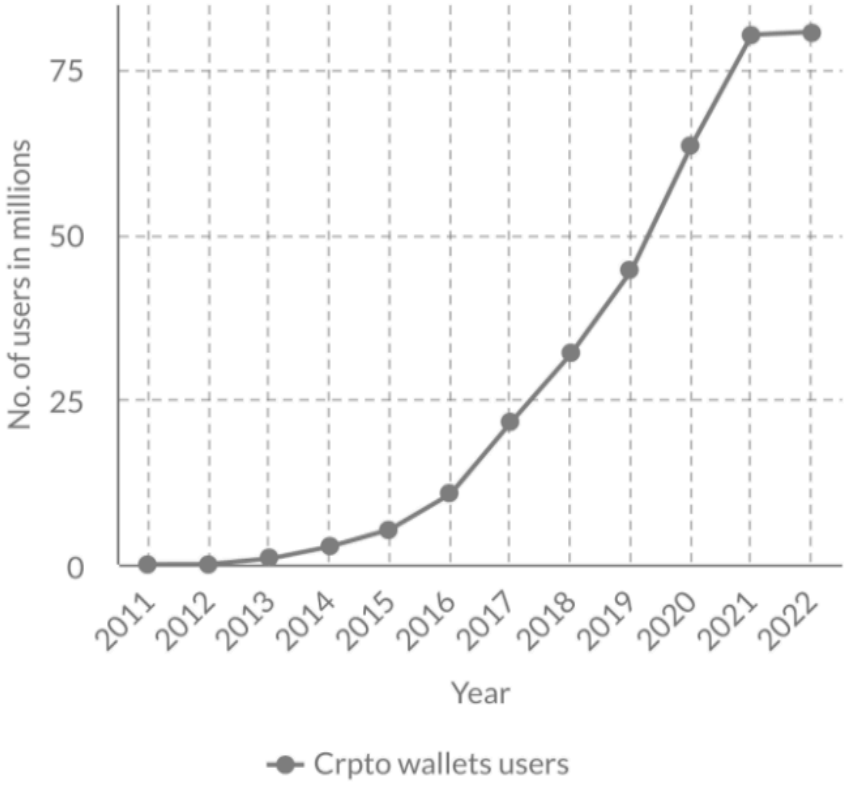


Figure 1. Number of crypto wallet users

Choosing digital certification using blockchain technology offers numerous advantages. It ensures the immutability and security of certification records, making them tamper-proof and transparent. This not only safeguards the integrity of certificates but also fosters trust among various stakeholders, such as educational institutions, students, and recruiters. With decentralized storage, certificates are easily accessible and resistant to single points of failure. The integration of blockchain technology adds an additional layer of trust, streamlining the verification process while enhancing data privacy. Recruiters can efficiently and reliably verify certificates, reducing the risk of fraud. [8] Overall, the combination of blockchain and decentralized storage technologies offers a robust and transparent approach to digital certification, benefiting education and employment ecosystems.

2.2 Purpose

The purpose behind our project proposal on e-certificate generation and validation using blockchain is rooted in the essential need to embrace innovative technology and address critical societal challenges. In a world experiencing rapid advancements in technology and data processing capabilities, the effective management of certificates is increasingly crucial for both institutions and individuals.

Through the utilization of blockchain's secure and transparent features, our aim is to present a solution that not only serves the interests of educational institutions but also aligns with the broader social objective of minimizing certificate fraud and ensuring the credibility of academic and professional qualifications.

This innovative approach not only fosters accessibility and cost savings but also contributes to environmental sustainability by reducing paper waste. Moreover, the prospect of exploring and implementing cutting-edge technology in the domain of decentralized storage and blockchain technology is not only exciting but is also anticipated to pave the way for numerous significant opportunities in the future for us.

2.3 Scope of the project

In the current educational and professional environment, the demand for a streamlined and secure certificate management system is unmistakable. Our project endeavors to deliver a pragmatic solution that optimizes the certificate generation process for institutions and introduces a verification approach centered around the user.

Through the utilization of decentralized storage and blockchain technology, we aim to establish a system that facilitates uncomplicated certificate issuance, granting certificate holders increased authority over the entities permitted to verify their credentials. Embracing the chance to employ state-of-the-art technologies to tackle these challenges, our project sets the stage for a more efficient and user-centric paradigm in certificate management.

2.4 Problem Statement

The current certificate generation and verification processes face issues like forgery risks, insecure hash exposure, and complex data storage. Existing solutions lack clarity, rely on centralized databases, and involve impractical verification methods.

To address these gaps, we aim to develop a user-friendly, decentralized system using IPFS and blockchain technology, ensuring secure hash generation, transparent storage, and a reliable verification process with unique identifiers, mitigating risks and enhancing the overall certificate management experience.

2.5 Objectives

In response to the identified gaps in existing certificate generation and verification processes, the primary objectives of our project are outlined below:

1. To provide institutes a friendly interface for customized certificate generation:

Develop a user-friendly interface to empower institutes with a streamlined and efficient process for the customized generation of certificates. This interface will facilitate the seamless creation of personalized certificates tailored to the specific needs of each institution.

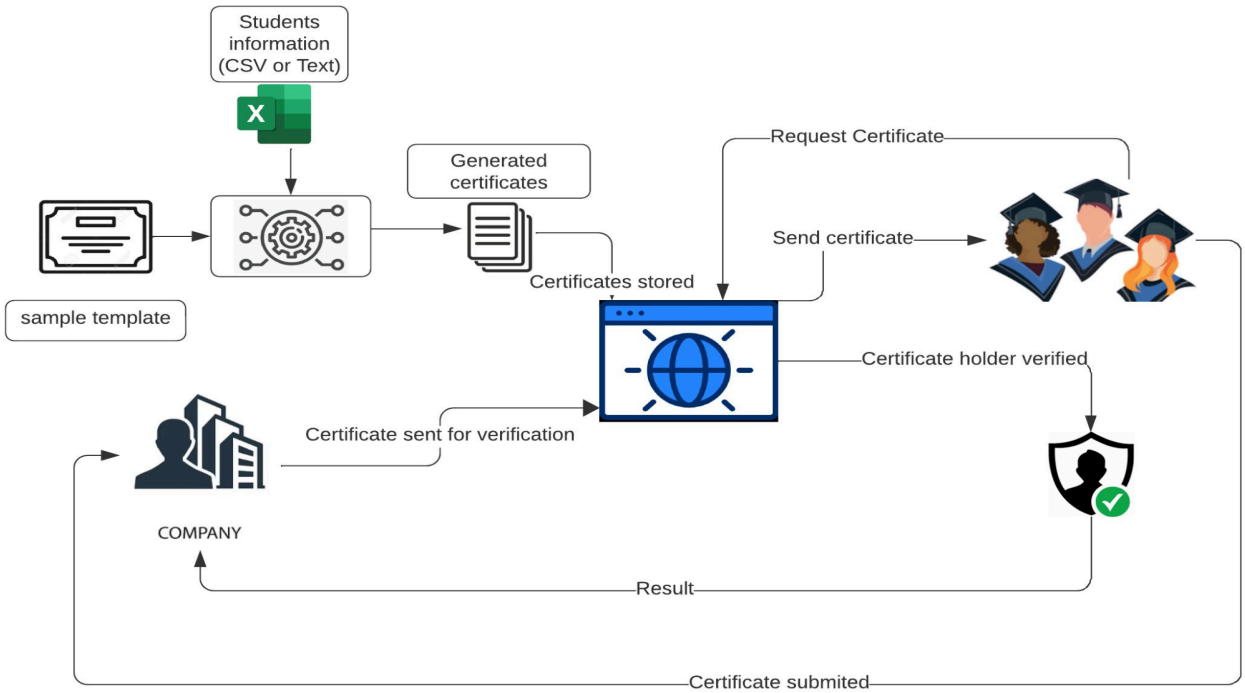
2. To provide students a secure portal to access and download their certificates:

Establish a secure portal for students, ensuring a robust and protected environment for accessing and downloading their certificates. This platform will prioritize the privacy and security of student data, allowing convenient and secure access to their academic and professional qualifications.

3. To offer recruiters and higher institutes a streamlined and secure means of verifying certificate validity with the certificate holder's permission:

Implement an easy and robust verification system that enables recruiters and higher education institutes to verify the validity of certificates with explicit permission from the certificate holder. This process will enhance the overall reliability and trustworthiness of academic and professional qualifications, contributing to a more transparent and secure verification ecosystem.

2.6 Project Overview



Our proposed system leverages Ethereum-based blockchain technology with smart contracts, encompassing three key stages:

1. Customized certificate generation:

   Enables institutions to create personalized certificates while simultaneously delivering them to students via email.

2. Storage-Retrieval using Interplanetary File System (IPFS) and Blockchain:

   The generated certificates undergo encryption and are stored in a decentralized manner using the IPFS protocol. References to these stored certificates are recorded in the blockchain.

3. Certificate Verification:

   The validation process includes a two-factor authentication for students to initiate verification and a comparison between the certificate stored in IPFS and the one submitted to the verifying party.

2.7 Expected Outcomes

The anticipated outcome of our final year project is a cutting-edge solution that revolutionizes the certificate management process for educational institutions. Upon successful implementation, we expect the following end result:

1. Efficient and Customized Certificate Generation:
   Institutions will benefit from a streamlined process for creating personalized certificates, enabling seamless and simultaneous delivery to students via email. This integrated approach enhances efficiency and reduces the administrative burden associated with the certificate generation process.

2. Secure and Decentralized Storage-Retrieval Mechanism:
   Certificates will undergo encryption and decentralized storage through the Interplanetary File System (IPFS) protocol. Simultaneously, references to these stored certificates in the blockchain will establish a secure and tamper-resistant storage-retrieval mechanism, effectively minimizing the risk of unauthorized access or manipulation.

3. Enhanced Certificate Verification with Two-Factor Authentication:
   The validation process will feature a robust two-factor authentication to ensure the authenticity of the certificate requester, complemented by a comparison between the certificate stored in IPFS and the one submitted to the verifying party. This dual-layered approach enhances the overall security and reliability of the verification process.

4. Minimization of Certificate Fraud:
   The decentralized nature of the system, coupled with blockchain's immutability, is anticipated to substantially diminish the occurrence of counterfeit certificates, while the augmented security features will concurrently bolster the trustworthiness and resilience of the certificate ecosystem against fraud.

5. Empowered Students with Greater Control:
   Certificate holders will gain increased control over the verification of their credentials, fostering a sense of ownership and trust in the system. This user-centric approach will empower students to securely and conveniently manage their certificates throughout their academic and professional journeys, ensuring a seamless and user-friendly experience.

2.8 Structure of the Report

To begin, we will thoroughly justify our problem statement, elucidating the significance and relevance of the issue within the broader context. Afterward, we will conduct a comprehensive literature review to assess the existing research landscape, identifying both accomplishments and remaining gaps in addressing the stated problem. Subsequently, we will undertake a critical evaluation of previous studies, pinpointing their shortcomings and proposing avenues for improvement or refinement in methodologies and approaches. Following this assessment, we will highlight areas that warrant further investigation, thus guiding the direction of our research and outlining potential contributions to the field. Finally, we will delve into the intricacies of the system architecture, providing a detailed overview of its design and implementation strategies to ensure alignment with our research objectives and address the identified gaps in the literature.

3. Justification

In the evolving field of data management and security, the combination of decentralized storage and blockchain technology emerges as a transformative force, promising enhanced efficiency and innovation. This integration begins by addressing cost-efficiency concerns, optimizing resources through the elimination of expansive centralized data storage. Beyond cost reduction, it fortifies against cyber threats by decentralizing storage, distributing data across multiple nodes, ensuring resilience, and mitigating vulnerabilities.

1. Blockchain Security:

   Blockchain reinforces system security with cryptographic techniques and tamper-resistant certificates, ensuring trust in transactions and efficiently preventing certificate fraud during verification processes.

2. Efficient Fraud Prevention:

   Blockchain excels in detecting and preventing certificate fraud, streamlining verification for recruiters and institutions, offering a secure approach to ensuring the authenticity of academic and professional qualifications.

3. Environmental Sustainability:

   Decentralized storage and blockchain reduce reliance on data centers and paper certificates, actively curbing environmental impact and minimizing the carbon footprint associated with traditional data management.

4. Eco-Friendly Practices:

   Prioritizing security and sustainability, the integration minimizes the need for data centers and embraces digital alternatives, positioning the system as an advocate for eco-friendly practices and positive change towards a greener future.

5. Future Opportunities and Innovation:

   The integration of cutting-edge technology in decentralized storage and blockchain anticipates future advancements, where technological evolution converges with sustainability initiatives, redefining the landscape of data management and security.

4. Literature Survey

Certain recent studies have delved into the development of credential verification systems, using a blend of blockchain technology and document analysis. These systems seek to simplify and secure the verification process for digital certificates, promising advantages for educational institutions, students, and recruiters.

4.1 Research Papers

[1] Generating and Validating Certificates Using Blockchain

Authors: T.S.Raja Rajeswari & Sk Khaja Shareef
Conference: ICCES-2021

Proposal and Process:

- Propose a system to generate unique hash values by incorporating the candidate's Roll no, Year, and Stream, and embedding this hash directly onto the certificate.
- Utilize the SHA-256 algorithm on the Generation page to create hash codes, ensuring a robust and unique identifier for each certificate.
- Implement a process where the generated hash serves as a direct identifier on the certificate itself.
- On the Verification page, use the unique hash as a parameter to validate the authenticity of the certificate.

Limitations:

- Certificates are not actively involved in the hash generation process, potentially leaving room for forgery and compromising the security of the certificate generation system.
- Historical certificates are not stored, raising concerns about data retrieval or verification of past certificates.
- The direct exposure of the hash value lacks additional layers of security, potentially making it susceptible to unauthorized access or tampering. This may compromise the overall integrity and security of the certificates stored using this system.

[2] VAULT: A Scalable Blockchain-based Protocol for Secure Data Access and Collaboration

Authors: Justin S. Gazsi & Sajia Zafreen
Conference: IEEE-2021

Proposal and Process:

- Implement a comprehensive blockchain-based protocol dedicated to ensuring secure data storage and retrieval.
- Employ the Interplanetary File System (IPFS) for decentralized and distributed file storage, enhancing data accessibility.
- Mitigate scalability issues and reduce overhead by avoiding direct data storage on the blockchain.
- Leverage IPFS to store files, with the blockchain recording Content Identifiers (CIDs) to facilitate retrieval.
- Enhance security by storing data in blocks with hash links on the blockchain, providing a transparent mechanism to detect tampering.
- The VAULT protocol adeptly combines blockchain and IPFS technologies to establish a secure, scalable framework for data access and collaboration.

Limitation:

- The paper does not explicitly delve into the application of the proposed IPFS and Blockchain combination in the context of certificate generation and verification. While the presented technique is robust for secure data storage and retrieval, its specific applicability and advantages in the realm of certificate management are not explicitly explored. However, the innovative use of IPFS and Blockchain suggests potential benefits for certificate-related processes.

[3] Performance Analysis of E-Certificate Generation and Verification using Blockchain and IPFS

Authors: Manjula K Pawar & Prakashgoud Patil
Conference: ICICT-2022

Proposal and Process:

- Discuss the advantages of utilizing IPFS for efficient data storage.
- Propose a system leveraging IPFS for enhanced performance in e-certificate generation and verification.
- Conduct a graph comparison analysis, comparing the time to generate a hash with IPFS versus without IPFS.
- Analyze the transaction time for inserting full data into the blockchain versus inserting IPFS hash.
- Highlight the variable transaction time without IPFS concerning data length, with IPFS providing a fixed 46-byte length.
- Address the cost-effectiveness by comparing the expense of storing the entire file in the blockchain versus storing only the IPFS hash.

- Conclude that IPFS-based electronic certificates result in reduced administration time, space savings, lower costs, and improved security and efficiency.

Limitations:

- The paper introduces a complex data storage system utilizing IPFS and blockchain technology, yet lacks clarity in practical implementation, particularly in the context of certificate generation and verification.
- Certificates are not stored; instead, student details reside in IPFS, and the corresponding Content Identifier (CID) is stored in the blockchain.
- Transaction hash id on certificates may potentially expose them to tampering.
- The absence of a unique identifier for each certificate may lead to multiple certificates sharing the same hash values, raising concerns about data integrity and uniqueness.

[4] Certificate Generation System

Authors: Bharti Chikankar & Sidhant Jaiswal
Journal: IJRESM-2020

Proposal and Process:

- Develop a user-friendly web certificate generation system with a primary focus on the user interface.
- Enable users to upload participant details manually or through the system.
- Provide a variety of elegant certificate templates for customization.
- Facilitate the creation of certificate templates through a clear and intuitive frontend interface.
- Implement additional features, including login and signup systems, import/export participant details, and dynamic certificate generation.
- Aim to save paper, reduce management costs, prevent forgery, and deliver accurate digital certificates.
- Simplify the entire certificate generation and distribution process, ensuring a seamless experience for users.

Limitations:

- The system relies on a centralized database (DB), which may pose challenges in terms of scalability and potential single points of failure.
- The paper predominantly focuses on certificate generation from a frontend perspective, potentially overlooking comprehensive considerations related to backend processes, security measures, and data storage.

[5] Providing Authentication and Privacy for University Certificates Using Smart Contracts in Blockchain Technology

Authors: Gururaj Harinahalli Lokesh & Vignesh Vijay Kumar
Conference: INDECS-2022

Proposal and Process:

- Propose a 3-module system for certificate management in university settings.
- Module 1: Allow students to enter personal details, academic coursework, and university code to request certificates.
- Module 2: Reserved for university administrators, involves verifying and approving/rejecting certificate requests based on established policies.
- Module 3: Implement third-party verification using the supplied certificate and certificate ID. The process includes hash comparison and blockchain data for tamper-proof verification.
- Detail the verification process involving calculating Hash (hsc) of sc and comparing it with the hash present on the blockchain, obtained by mapping the certificate ID input. A match signifies a valid certificate, while a mismatch indicates an invalid one.

Limitations:

- The certificates are not stored, raising potential concerns regarding long-term accessibility and data retention.
- The system's reliance on students to request certificate generation and the subsequent involvement of the institute in validation may be impractical, leading to issues such as spam requests, human errors in validation, and continuous participation of institute officials, which may not always be feasible or affordable.

[6] Generating E-Certificate and Validation using Blockchain

Authors: Rohan Hargude & Ghule Ashutosh
Journal: IJCRT-2021

Proposal and Process:

- Introduce a blockchain-based e-certificate system with the primary objective of preventing forgery.
- Provide an overview of the system's architecture, incorporating tools such as Visual Studio Code, React JS, and Ethereum.
- Explain the module integrity within the system, ensuring the security and reliability of the certificate generation process.
- Describe the frontend interface functionalities and user experience (UX) design, including options for custom template creation and template uploading.

Limitations:

- The paper lacks adequate implementation details, potentially leaving gaps in understanding the practical application of the proposed blockchain-based e-certificate system.
- Highlight the requirement for the verifier to upload both the certificate/serial number and a QR code, which may introduce additional steps and complexities in the validation process.

4.2 Review Paper

2023 IEEEAccess Review Paper A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification:

- The systematic literature review conducted by A. Rustemi, Fisnik Dalipi, and Vladimir Atanasovski focus on exploration of blockchain-based systems for academic certificate verification in higher education. The review highlights the benefits of using blockchain technology to enhance the verification process of academic certificates, including increased speed, reliability, and independence from a central authority. The report addresses two key questions and provides solutions for each. Firstly, in relation to "Blockchain's Role in Preventing Diploma Falsification" the review emphasizes that blockchain technology ensures the security of academic credentials, effectively preventing document forgery. By providing a secure and unchangeable platform for storing and verifying credentials, unauthorized alterations are prevented. Secondly, in the context of "Platforms and Solutions for Diploma Falsification Prevention" the review identifies Ethereum and Bitcoin as commonly used platforms for implementing blockchain networks. Smart contracts, a crucial component of blockchain technology, play a vital role in executing services related to diploma generation and verification. However, none of them provided a full fledged flow of system interaction and also no proper in detail implementation of the system. .

- The research reveals gaps in the current landscape of blockchain-based academic certificate verification systems. One notable issue is the inadequate security mechanisms. To enhance security during diploma generation, the review suggests incorporating additional measures such as digital signatures and biometric identifiers into the architecture of the blockchain system. Additionally, there is a demand for maintenance of blockchain systems, which often requires external service providers. The decision to engage external

maintenance services should consider cost considerations. Lastly, achieving automatic diploma generation without intermediaries is a significant challenge. The recommended solution involves implementing automatic generation and verification processes to eliminate concerns about potential abuses.

- In conclusion, We aim to develop a user-friendly, decentralized system using IPFS and blockchain technology, ensuring secure hash generation, transparent storage, and a reliable verification process with unique identifiers, mitigating risks and enhancing the overall certificate management experience.

4.3 Research Gaps

From the literature survey conducted, it is evident that while several studies propose blockchain-based solutions for certificate generation and verification, there exists a significant gap in the practical implementation and comprehensive consideration of security measures. Specifically, the current landscape lacks robust mechanisms to ensure the integrity and long-term accessibility of certificates.

One notable gap is in securely storing certificates while ensuring their authenticity and uniqueness. Current proposals often overlook key aspects, like involving certificates in the hash generation process, risking vulnerabilities. Unclear practical implementation, particularly with blockchain and IPFS integration, hampers widespread adoption and effectiveness.

Moreover, there is a pressing need for additional security measures beyond basic hash generation, such as digital signatures or biometric identifiers, to fortify the certificate management process against potential tampering or forgery. Additionally, the reliance on external maintenance services for blockchain systems raises concerns about sustainability and cost-effectiveness, necessitating further exploration into self-sustaining models.

Overall, addressing these gaps requires a holistic approach that considers both technical intricacies and user-centric design principles to develop a robust, decentralized system for certificate management. Such a system should prioritize security, transparency, and ease of use to ensure the integrity and reliability of academic certificates in the digital age.

5. Proposed System Architecture

Our proposed system establishes a comprehensive platform for certificate issuance and verification. Educational institutions will generate and distribute certificates, utilizing the IPFS protocol for decentralized storage and associating content identifiers (CIDs) with student email addresses and Certificate Numbers (CSN) on a blockchain. Students can share certificates with recruiters, triggering a verification process that involves uploading the certificate, automatic extraction of the CSN, blockchain cross-referencing, student approval, retrieval of the original certificate from IPFS using the stored CID, and a final legitimacy check through SHA256 hash comparison, providing recruiters with the results of the authentication.

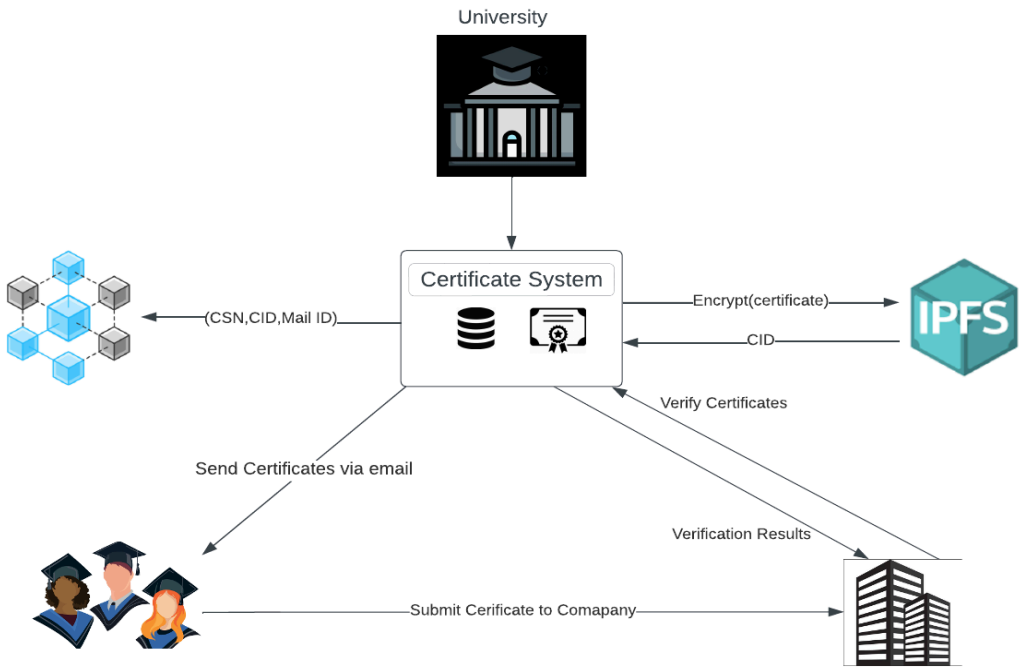
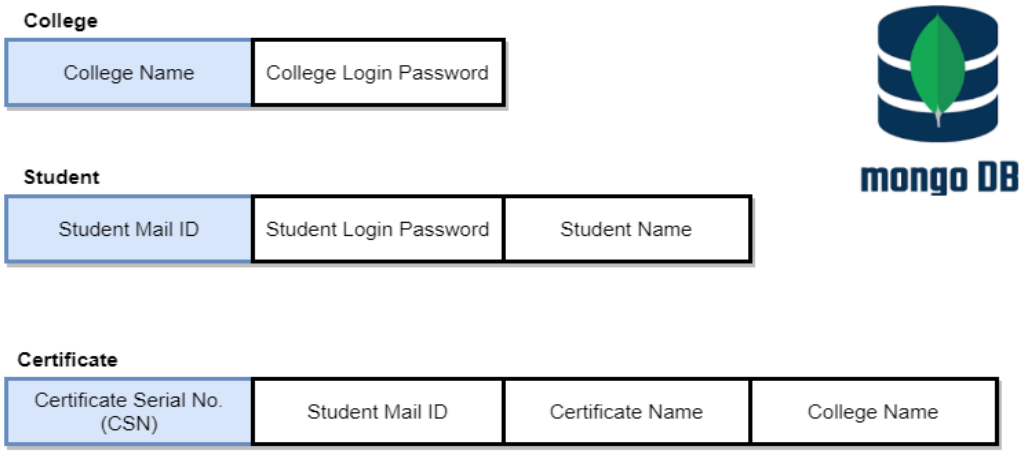


Figure 3: Workflow of the Proposed System

The higher level workflow of the proposed system is depicted in Figure 3. The entire project is split up into three modules:

1. E-certificate Generation
2. Certificate retrieval for students
3. Verification of certificates.

5.1 Data Model



The proposed data model for the backend of our project adopts a structured approach reminiscent of SQL databases, despite utilizing MongoDB, a NoSQL database. The SQL-esque approach offers familiarity and ease of understanding while leveraging the advantages of MongoDB's NoSQL capabilities. The model comprises three tables, each representing a crucial entity within the system:

1. College Table:

The College table serves as a repository for institutional information, with the College Name acting as the primary key, ensuring the uniqueness and integrity of each college entry. The College Login Password attribute enhances security by providing access control to authorized users and it is encrypted before storage for protection.

2. Student Table:

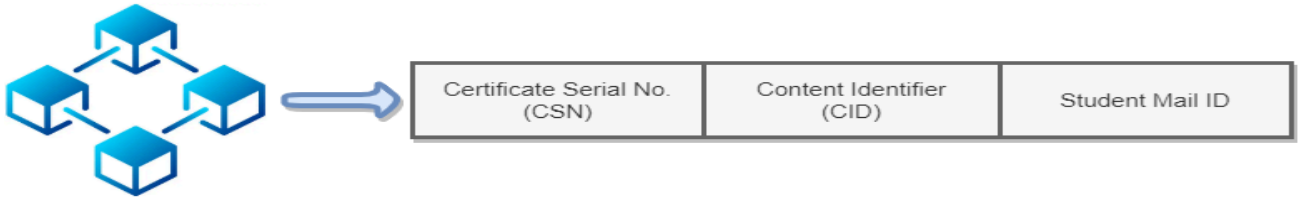
The Student table stores essential details about individual students, utilizing the Student Mail ID as the primary key, ensuring its uniqueness and non-null status. This design choice facilitates efficient and unambiguous identification of each student in the system. Student Login Password is encrypted before storage and is crucial for a student to login to his account. Additionally, the Student Name attribute caters to personalization aspects.

3. Certificate Table:

The Certificate table encapsulates certificate-specific information, employing the Certificate Serial Number as the primary key for uniqueness and non-null

constraints. This design ensures a distinct identification for each certificate within the system. The inclusion of Student Mail ID and College Name attributes establishes crucial associations, linking certificates to specific students and their respective colleges.

5.2 Blockchain Configuration



Blockchain Tuple Structure

Incorporating the public Ethereum blockchain into our project serves as a pivotal component for ensuring transparency, security, and immutability. The integration involves meticulous consideration of data structures to minimize storage costs while ensuring robust security. To optimize storage efficiency, the tuple structure includes three key attributes:

1. Certificate Serial Number (CSN):

Uniquely identifying each certificate, the CSN acts as the primary lookup key, streamlining certificate access while minimizing storage overhead.

2. Content Identifier (CID) returned from IPFS:

To address cost implications, actual certificates are not stored directly. Instead, the CID returned from IPFS, obtained upon storing the encrypted certificate, is utilized, reducing storage expenses while preserving data integrity.

3. Student Mail ID:

The inclusion of the student's mail ID serves a dual purpose. It acts as an additional verification layer during certificate validation, enhancing security and mitigating fraud risks. Additionally, the student's mail ID ensures ownership confirmation, providing a reliable means to verify the rightful owner of the associated certificate.

The tuple structure is meticulously designed for the immutability of Ethereum blockchain-stored data. The CSN, CID, and student mail ID remain unchanged, reinforcing the permanence of certificate information and enhancing security. This commitment to immutability boosts the trustworthiness of the certificate verification process, detecting tampering promptly. [9] Implementing this tuple on the public Ethereum blockchain aims to establish a balanced foundation for decentralized certificate management, aligning storage efficiency, security, and immutability.

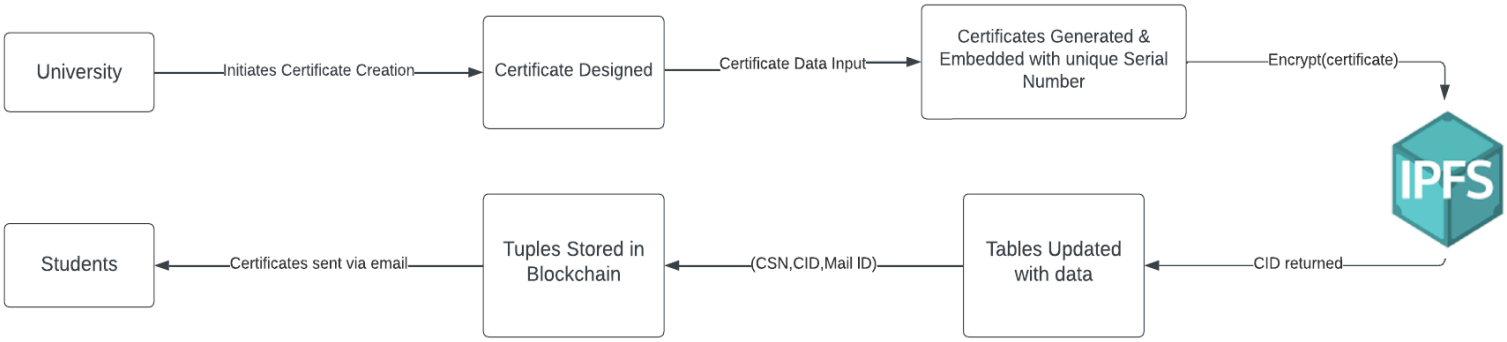
6. Proposed Design

In the implementation phase, our project will leverage a powerful combination of technologies to construct a robust and secure decentralized certificate management system. The technological arsenal includes:

1. NodeJS Backend Server + APIs
2. EthereumTest nets Blockchain
3. MongoDB
4. Remix Solidity Environment – Smart Contracts
5. ReactJS as the Frontend Framework
6. Ganache to track transactions

This diverse set of tools will facilitate the development of a dynamic and efficient platform. Now, we will delve into the workflow of each module, providing a comprehensive understanding of their roles and interactions in building a cutting-edge decentralized certificate generation and verification ecosystem.

6.1 E-certificate Generation and Automation



The process begins with colleges and universities, who, in the real world, initiate the account creation by directly contacting the administrator to validate their credentials for creating an account in the decentralized certificate management system. Upon successful validation, colleges will be provided a log in using their designated name and password, gaining access to a personalized dashboard.

Within their dashboard, colleges are empowered to design custom certificate templates tailored to their specific requirements or choose one of the pre-designed templates. These templates, whether newly created or chosen from predesigned options, are seamlessly saved and associated with the respective college. Importantly, college staff are prompted to assign a name to each certificate template, serving as a key identifier for storage in the certificate database under the category of "certificate type."

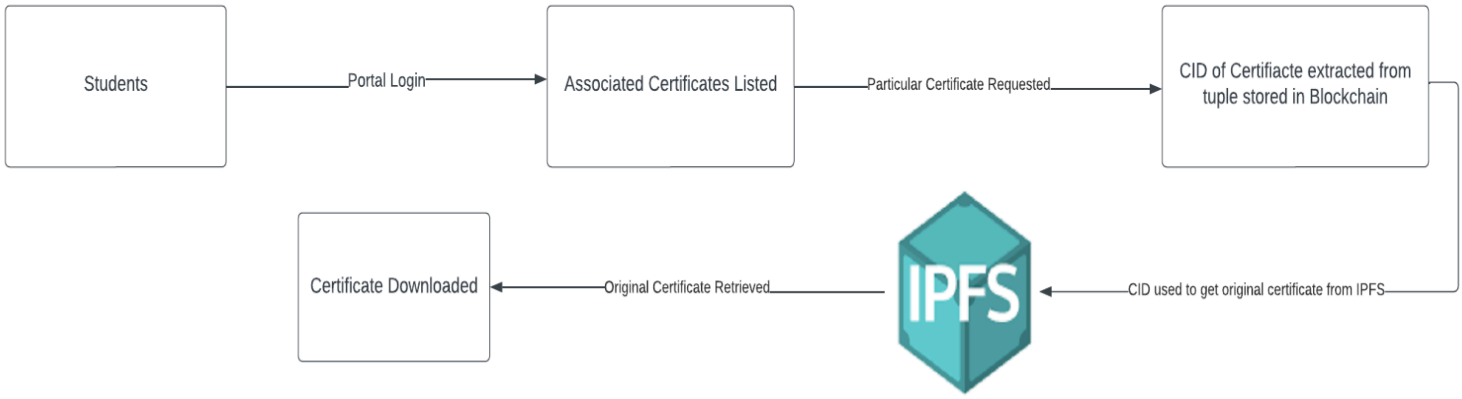
The next step involves placing placeholders on the selected or designed template. These placeholders, facilitating dynamic information incorporation, are draggable and droppable anywhere on the certificate. It is imperative that each placeholder shares the same label name as the attribute it represents, ensuring accurate mapping during data entry.

When creating new certificates, college staff are prompted to enter the student's mail ID and name, along with other placeholder information. A check is conducted to verify if the associated student's mail ID already exists in the student database. If not, a randomly generated password is assigned, and a new entry is made

in the student database. Subsequently, these credentials are mailed to the student for logging-in. If the student's mail ID already exists, the system bypasses the account generation step, expediting the process.

Certificate generation is then initiated by mapping the data provided, either through an uploaded Excel file or manual entry, onto the designated placeholders. Each certificate receives a randomly generated, unique Certificate Serial Number (CSN). To ensure security and traceability, the CSN is embedded into each certificate using steganography techniques. Finally, the certificate files are encrypted before storage in IPFS, and the finalized certificates are emailed to the corresponding students, completing the comprehensive certificate issuance process.

6.2 Certificate Retrieval



For students, the journey begins with a simple login process, where they input their registered mail ID and password. Upon successful authentication, students gain access to their personalized dashboard. Here, an organized list of certificate names and the issuing colleges is prominently displayed. This information is dynamically retrieved by querying the certificate table using the student's mail ID, providing an overview of the certificates associated with the student.

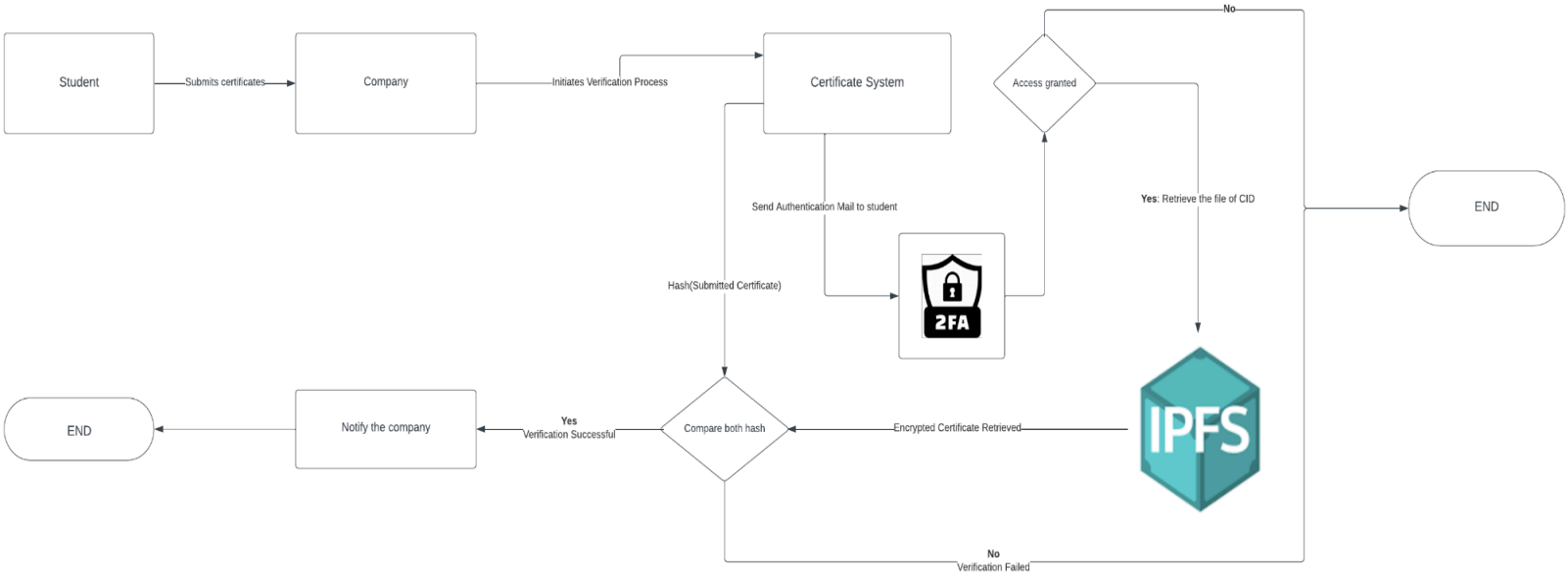
On the dashboard, each certificate entry serves as a clickable link. Upon selecting a specific certificate, a new page opens, and the Certificate Serial Number

(CSN) associated with the chosen certificate is used to perform a lookup in the blockchain tuple structure.

This lookup yields the Content Identifier (CID) linked to the certificate. Utilizing this CID, the original certificate is retrieved from IPFS, where it is securely stored.

Subsequently, the certificate is decrypted and presented to the student for viewing. Additionally, a convenient download option is made available, enabling students to obtain a digital copy of their certificates for their records. This streamlined process ensures efficient access and verification of certificates, enhancing the overall user experience for students within the system.

6.3 Verification of certificates



In the verification module, companies or recruiters initiating the certificate validation process will navigate to the verification website. Here, they are prompted to enter the student's mail ID and upload the certificate for verification. The system first checks whether there is an existing student entry corresponding to the provided mail ID. If no entry is found, the system notifies the company or recruiter that there are no certificates associated with the given mail ID.

If a student entry is identified, the Certificate Serial Number (CSN) embedded in

the uploaded certificate is extracted. Two scenarios arise at this point: if the CSN in the uploaded certificate differs from the one stored in the database, it suggests potential tampering, and this information is communicated to the verifying party.

In cases where the CSN matches, the system proceeds to the next step. A lookup in the blockchain is performed using the CSN, verifying that the email ID stored in the tuple matches the one entered by the recruiter or company for ownership confirmation. If the email IDs align, the Content Identifier (CID) stored in the blockchain is retrieved.

A pivotal 2-factor authentication step ensues, where the student receives a verification request email. Upon approval, the system proceeds with verification. Using the CID, the encrypted certificate file stored in IPFS is retrieved.To ensure data integrity, the submitted certificate is encrypted using the same algorithm employed by IPFS, typically SHA256. The system then compares the retrieved file with the submitted one. If they match, the system indicates that the certificate is valid. Conversely, if a discrepancy is detected, it is communicated that there may have been tampering with the certificate, providing a comprehensive and secure verification process for companies and recruiters.

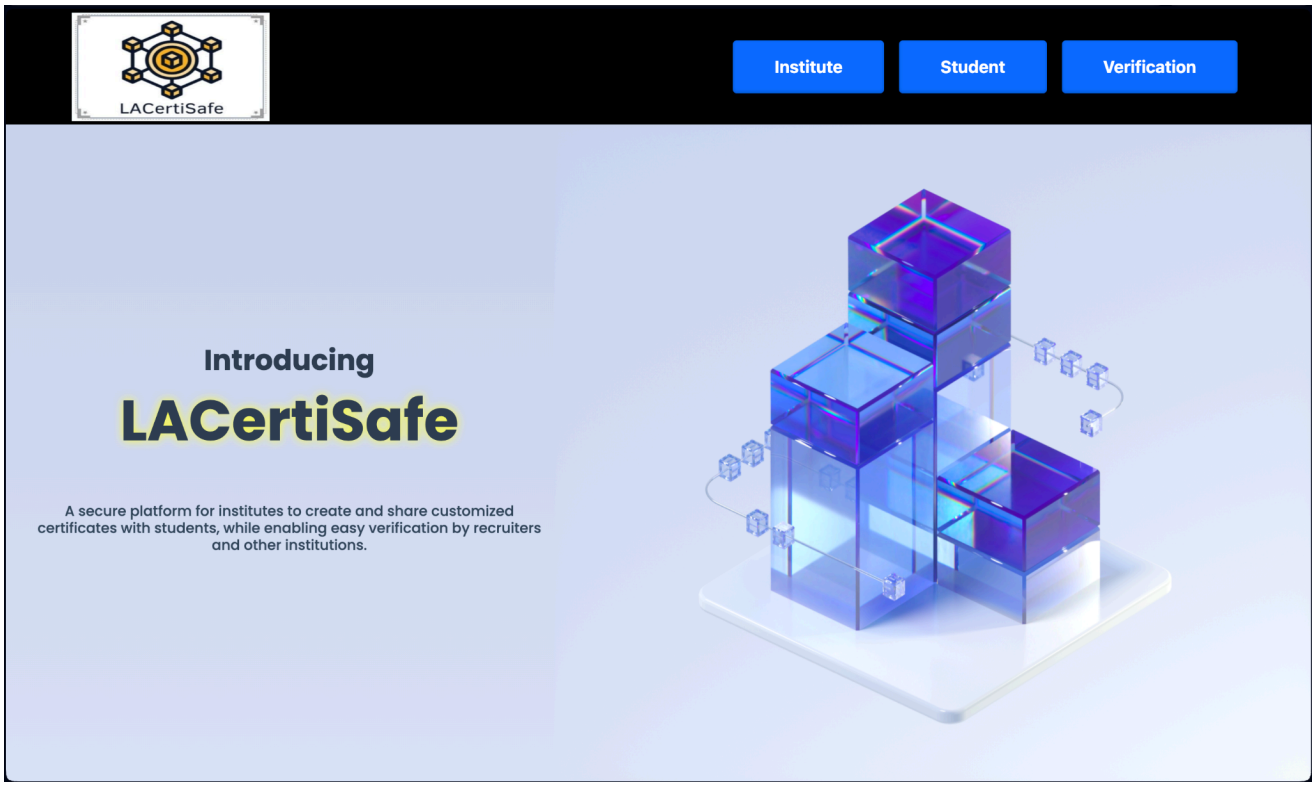
7. Timeline of the Project development

Review	Module	January	February	March	April
Review 1	System Design Refinement				
	Modules Ideations and Sample Implementations				
Review 2	Frontend Design Interface				
	Storage and Retrieval in IPFS and Blockchain				
Review 3	Verification				
	Overall Integration				

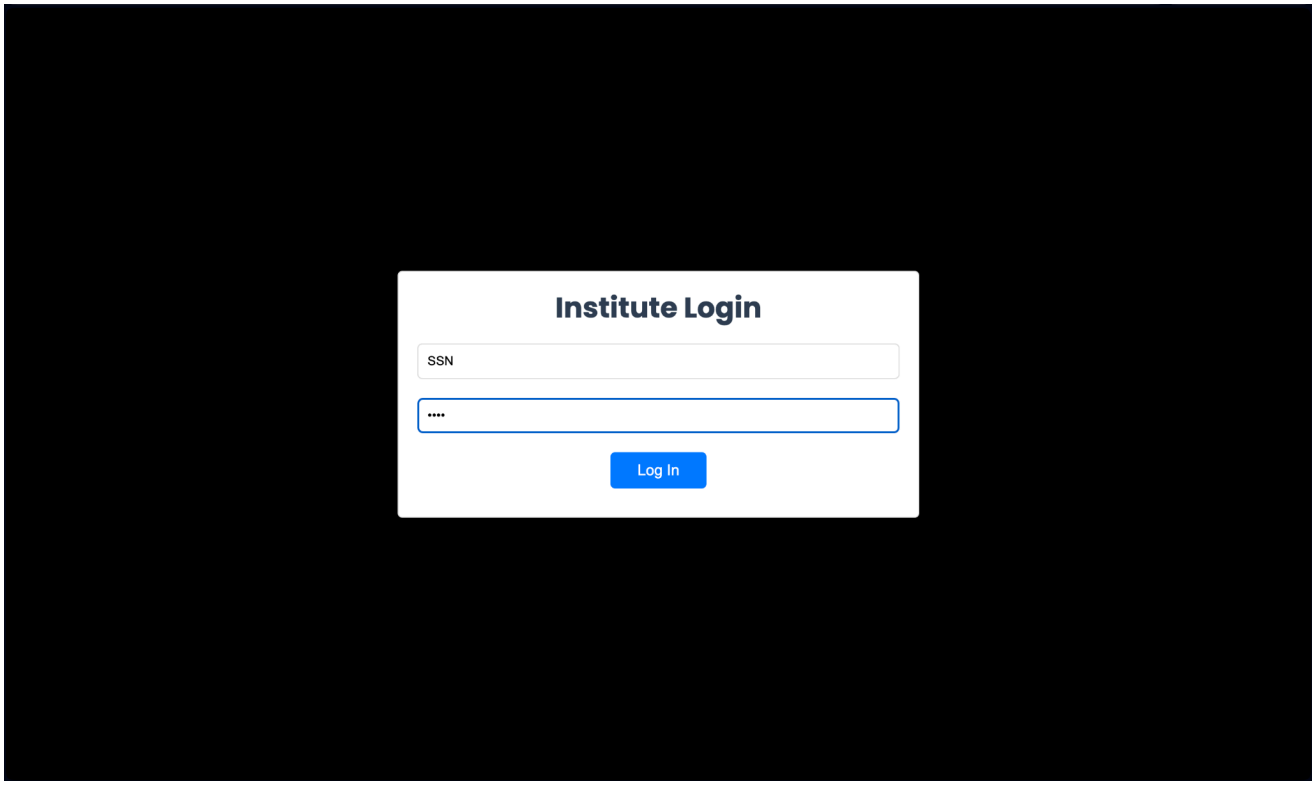
8. Implementation

8.1 Completed

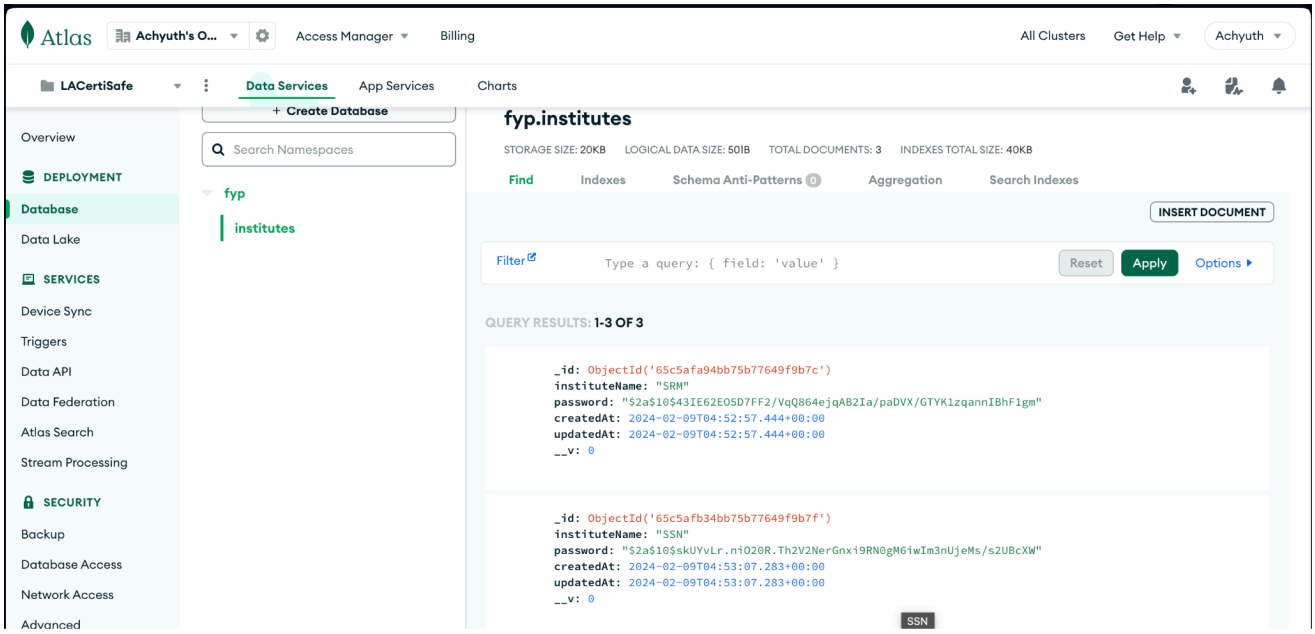
Frontend landing page



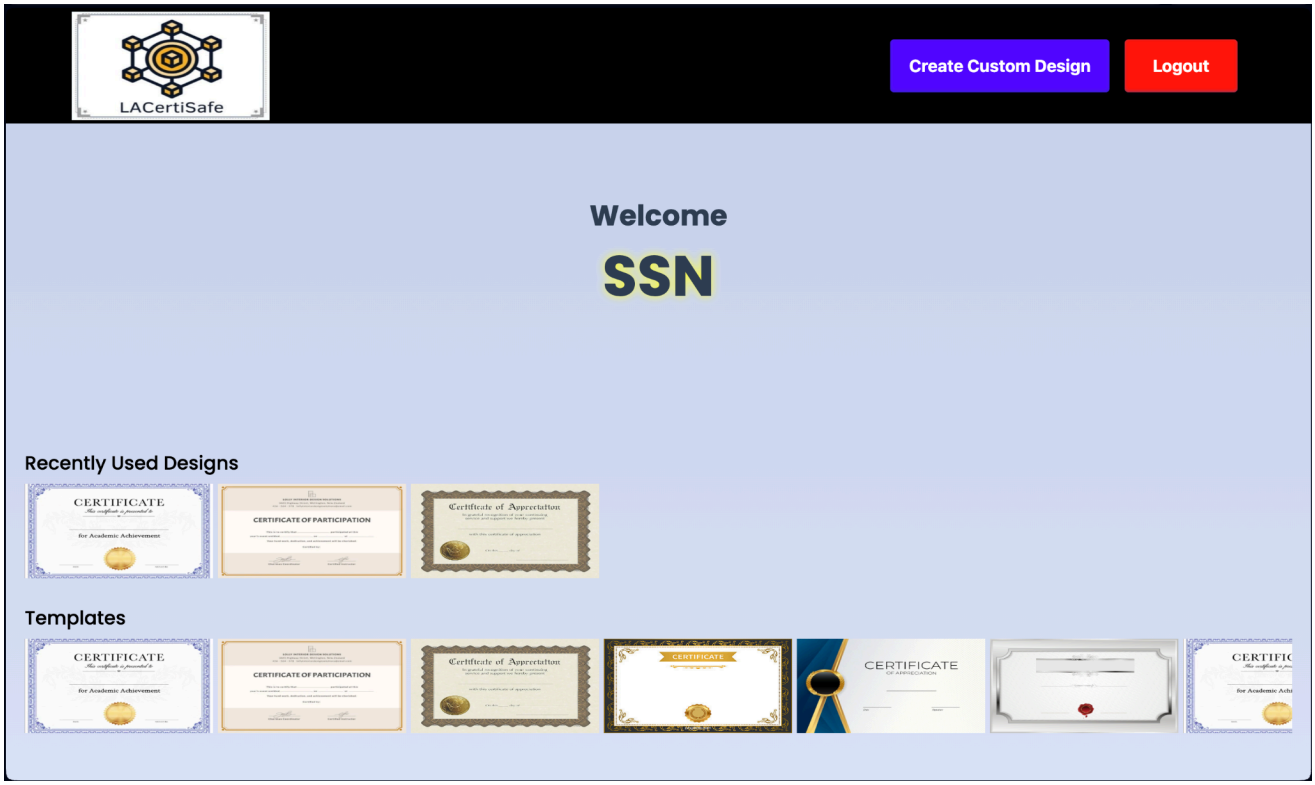
Institute login page



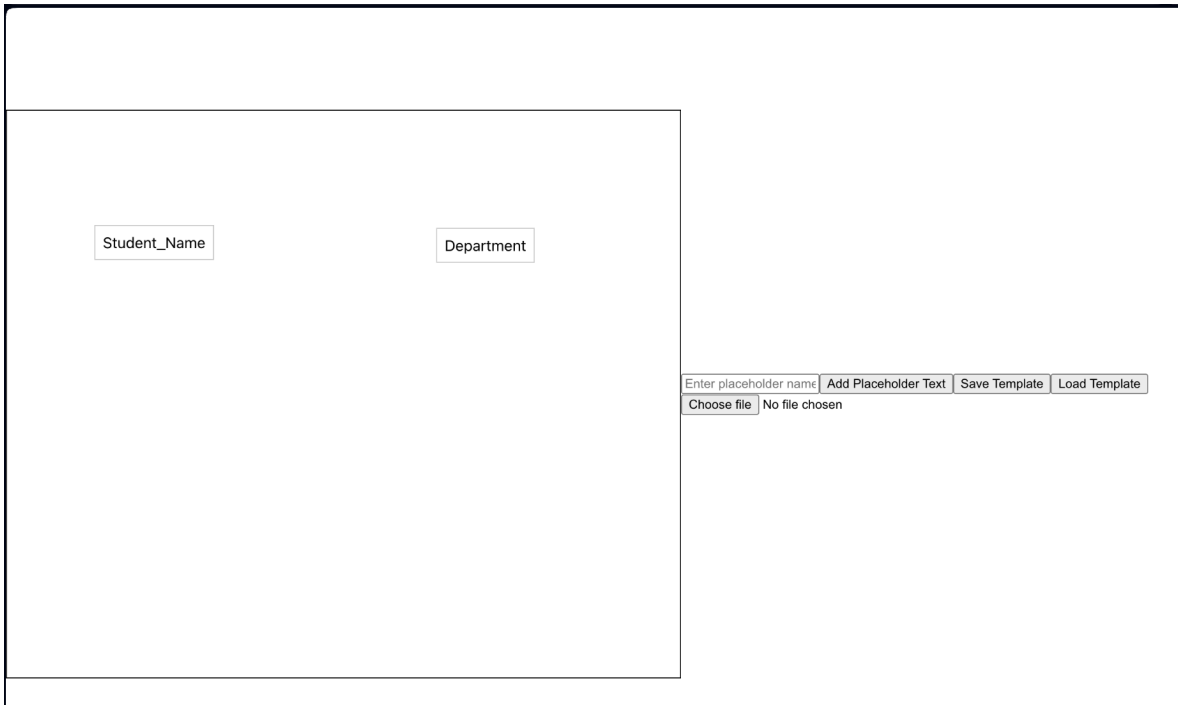
Institute table

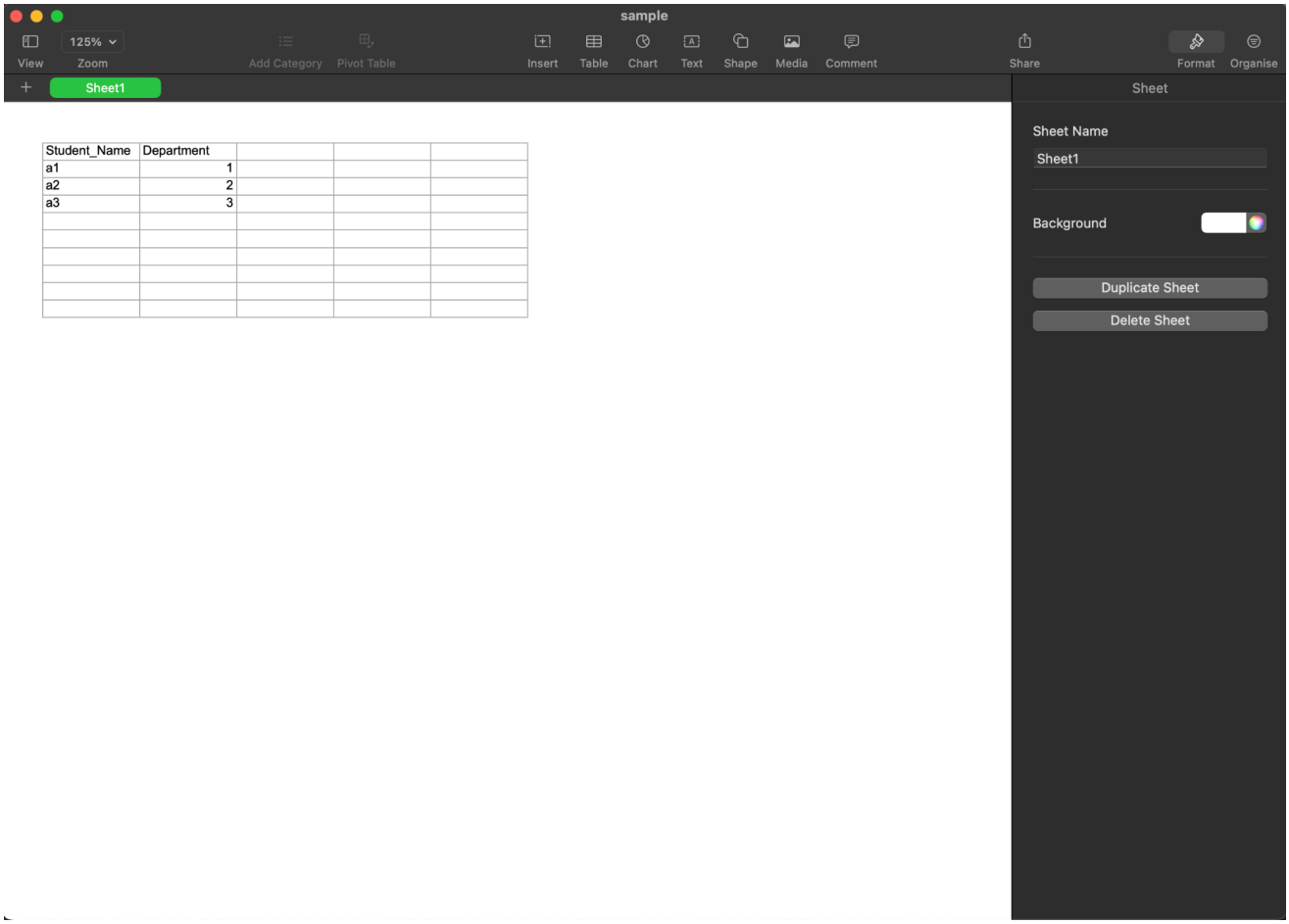


Design dashboard page



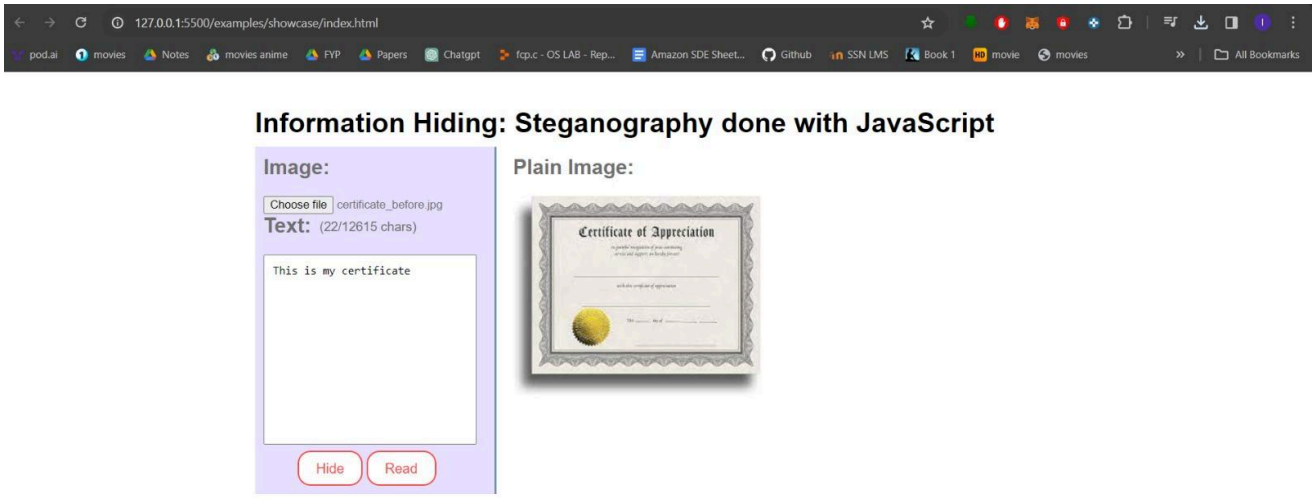
Placeholder mapping sample module

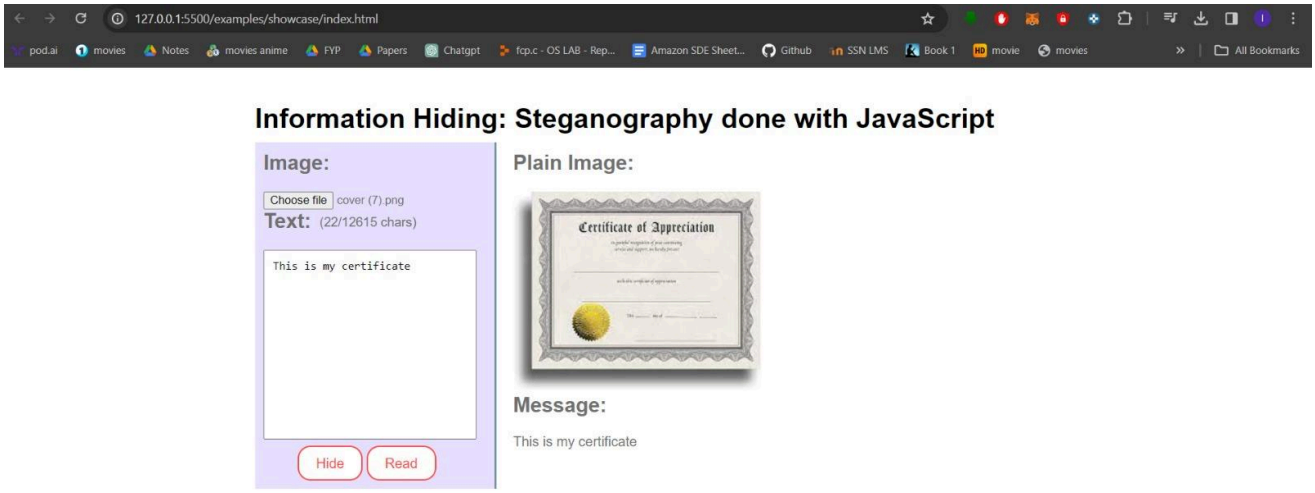



sample
125%
View
Zoom
Add Category
Pivot Table
Insert
Table
Chart
Text
Shape
Media
Comment
Share
Format
Organise
Sheet1
Sheet
Sheet Name
Sheet1
Background
Duplicate Sheet
Delete Sheet
Student_Name
Department
a1
1
a2
2
a3
3

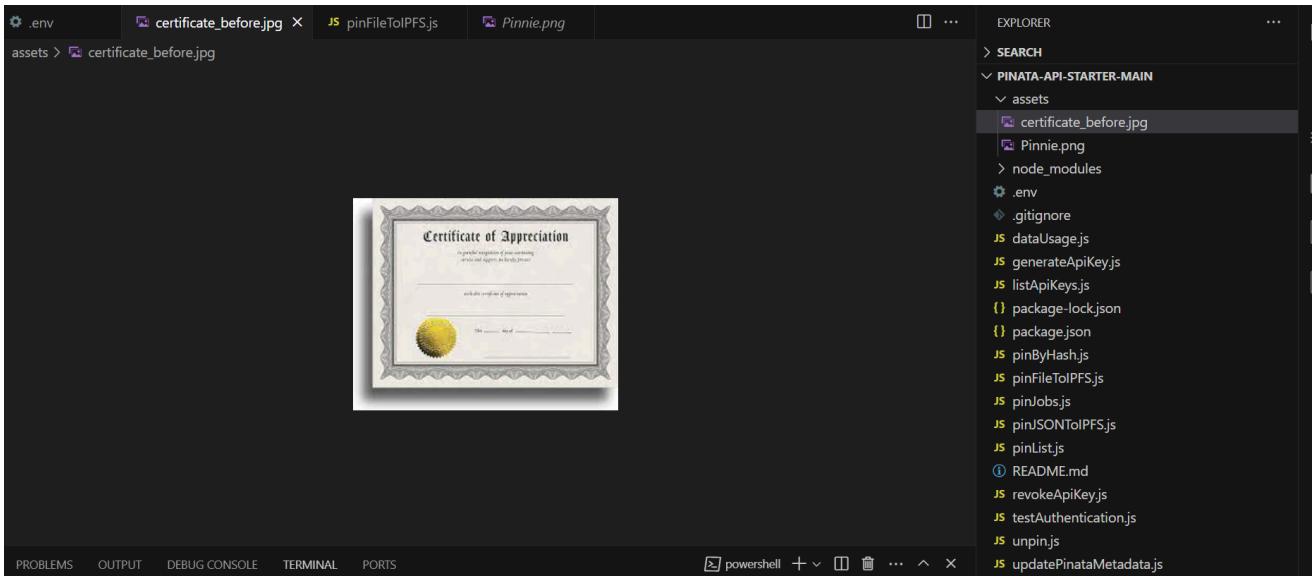

certificate_1.png
certificate_2.png
certificate_3.png

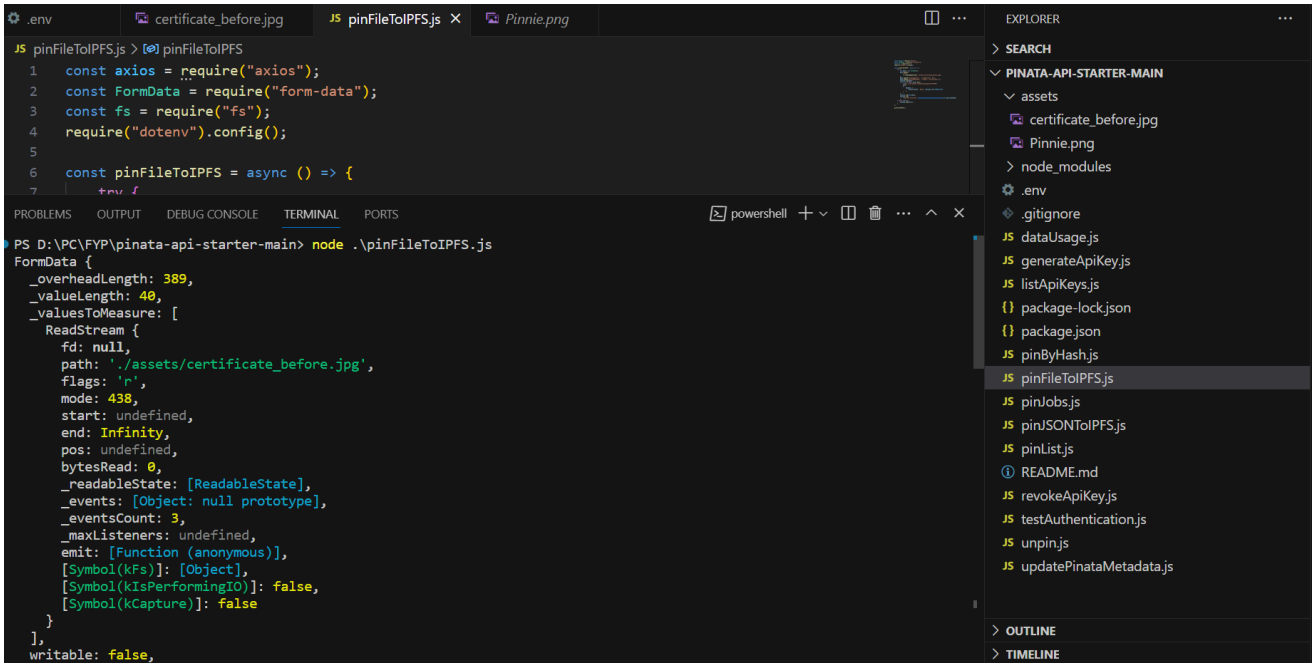
Embedding and Extracting information using Steganography module

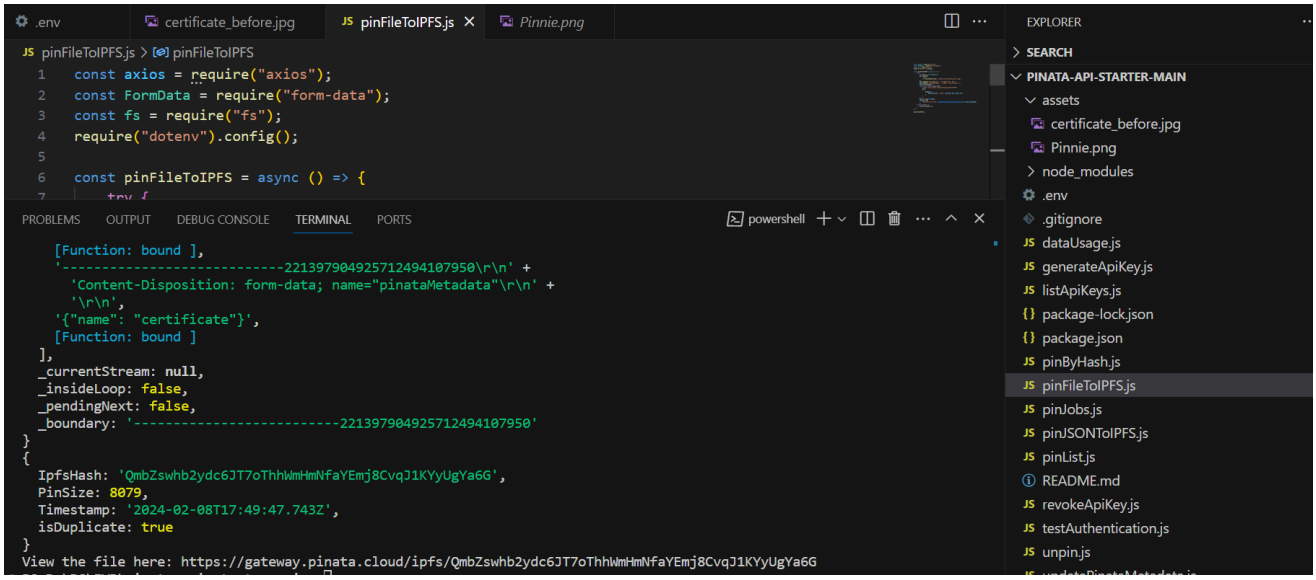




IPFS sample module







The file in the IPFS with
Hash :QmbZswhb2ydc6JT7oThhWmHmNfaYEmj8CvqJ1KYyUgYa6G
To Access the file: [IPFS link]

8.2 Remaining

- **Generation module**
  Completing the design template tool.
  Backend node API for storing the certificates generated into the IPFS.
  Deployment of the smart contract.

- **Retrieval module**
  API for retrieving the certificates of the particular user.
  API for downloading the certificate.

- **Verification module**
  Implementation of 2FA test module.
  Implementation of mail service module.
  Server routes to retrieve files from IPFS.
  Hash comparison module for verification.

Overall Integration of three modules and testing with use cases.

9. Feasibility Study

Creating an application like the one described is entirely feasible with a dedicated timeframe and minimal budget constraints. The project can be realized without significant financial overhead, thanks to the availability of various free tools and resources. Test networks like the Ethereum Rinkeby testnet can be employed for blockchain development, eliminating the need for actual cryptocurrency expenditures. We students can leverage open-source technologies, such as IPFS, and benefit from comprehensive documentation and online communities to aid in the development process. Additionally, the project's educational nature makes it an ideal learning experience, offering us hands-on experience in blockchain, decentralized storage, and web development. With teamwork, commitment, and access to the wealth of online resources and our guidance from our mentor we believe we have the potential to bring this innovative project to life without excessive costs.

10. References

[1] T.S.Raja Rajeswari & Sk Khaja Shareef, *Generating and Validating Certificates Using Blockchain*,2021 6th International Conference on Communication and Electronics Systems (ICCES)
https://ieeexplore.ieee.org/document/9489105

[2] Justin S. Gazsi & Sajia Zafreen, VAULT: A *Scalable Blockchain-based Protocol for Secure Data Access and Collaboration*, 2021 IEEE International Conference on Blockchain
https://ieeexplore.ieee.org/document/9680475

[3] Manjula K Pawar & Prakashgoud Patil, *Performance Analysis of E-Certificate Generation and Verification using Blockchain and IPFS*, IEEE International Conference on Inventive Computation Technologies (ICICT 2022)
https://ieeexplore.ieee.org/document/9850830

[4] Bharti Chikankar & Siddhant Jaiswal, *Certificate Generation System*, IJREAM-2020. International Journal of Research in Engineering, Science and Management Volume-3, Issue-8, August-2020journals.resaim.com/ijresm | ISSN (Online): 2581-5792 | RESAIM Publishing
https://journal.ijresm.com/index.php/ijresm/article/download/251/229

[5] Gururaj Harinahalli Lokesh & Vignesh Vijay Kumar, *Providing Authentication and Privacy for University Certificates Using Smart Contracts in Blockchain Technology*, INDECS-2022.
researchgate.net

[6] Rohan Hargude & Ghule Ashutosh, *Generating E-Certificate and Validation using Blockchain*, IJCRT-2021 | Volume 9, Issue 7 July 2021 | ISSN: 2320-2882.
https://ijcrt.org/papers/IJCRT2107013.pdf

[7] A. Rustemi, Fisnik Dalipi & Vladimir Atanasovski, A *Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification*, IEEEAccess-2023 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10163764

[8] Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85. https://ieeexplore.ieee.org/document/8029379

[9] M. J. M. Chowdhury, A. Colman and P. Sarda, " Blockchain Versus Database: A Critical Analysis," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering
https://ieeexplore.ieee.org/document/8456055