VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belagavi-590018, Karnataka

Phase I Project Work Report
On

"EXAM-VAULT : REINVENTING EXAMINATION SECURITY THROUGH BLOCKCHAIN AND ENCRYPTION"

Submitted in partial fulfillment of the requirements for the award of the degree of
Bachelor of Engineering
in
Computer Science & Engineering

Submitted by

USN	Name
1BI22CS156	SHRUTI KUMARI
1BI22CS159	SNEHA R
1BI22CS184	VIBHANSH JAIN
1BI22CS194	YOGANAND

Under the Guidance of
Prof. SHRUTHI B GOWDA
Assistant Professor
Department of CS&E, BIT
Bengaluru-560004

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

BANGALORE INSTITUTE OF TECHNOLOGY

K.R. Road, V.V. Pura, Bengaluru-560004

2024-25

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belagavi-590018, Karnataka

BANGALORE INSTITUTE OF TECHNOLOGY

Bengaluru-560 004

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Certificate

This is to certify that the Major Project (BCS685) work entitled **"EXAM-VAULT : REINVENTING EXAMINATION SECURITY THROUGH BLOCKCHAIN AND ENCRYPTION"** carried out by

USN	Name
1BI22CS156	**SHRUTI KUMARI**
1BI22CS159	**SNEHA R**
1BI22CS184	**VIBHANSH JAIN**
1BI22CS194	**YOGANAND**

Bonafide students of VI semester B.E. for the partial fulfillment of the requirements for the Bachelor's Degree in Computer Science & Engineering of the **VISVESVARAYA TECHNOLOGICAL UNIVERSITY** during the academic year 2024-25. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said degree.

Prof. Shruthi B Gowda
Guide
Assistant Professor
Dept. of CSE, BIT

Dr. Suneetha K. R.
Prof. & Head,
Dept. of CSE, BIT

ACKNOWLEDGEMENT

The knowledge & satisfaction that accompany the successful completion of any task would be incomplete without mention of people who made it possible, whose guidance and encouragement helped bring our efforts to success. We would like to thank all and acknowledge the help we have received to carry out this project.

We would like to convey our thanks to Principal **Dr. Aswath M U,** Bangalore Institute of Technology, and **Dr. Suneetha K R,** Professor and Head, Department of Computer Science and Engineering, BIT for being kind enough to provide the necessary support to carry out the Mini Project.

We would like to acknowledge the support we have received from the Major Project coordinators **Prof. Prashanth Kumar K N,** Asst. Prof. and **Prof. Manjushree N S,** Asst. Prof., Department of Computer Science and Engineering, BIT for continuous co-ordination and timely deliberation of requirements at every phase of the Major Project.

We are most humbled to mention the enthusiastic influence provided by our guide **Prof. Shruthi B Gowda,** Assistant Professor on the Mini Project for the ideas, time to time suggestions, for the constant support and co-operation shown during the venture and for making this Major Project a great success.

We are very much pleased to express our sincere gratitude to the friendly cooperation shown by all the staff members of the Computer Science Department, Bangalore Institute of Technology.

1BI22CS156	**SHRUTI KUMARI**
1BI22CS159	**SNEHA R**
1BI22CS184	**VIBHANSH JAIN**
1BI22CS194	**YOGANAND**

ABSTRACT

Secure transmission of examination question papers is critical to maintaining the integrity of academic evaluations. Traditional methods, which rely heavily on physical distribution, are prone to paper leaks, unauthorized access, and tampering. “EXAM-VAULT” proposes a blockchain-based framework for safeguarding question paper delivery using end-to-end encryption and decentralized technology.

The system incorporates Ethereum, Hyperledger Fabric, IPFS, RSA encryption, and smart contracts written in Solidity to offer a tamper-proof, auditable solution. ReactJS and Django serve as the frontend and backend, respectively, while MetaMask and Firebase are used for role-based authentication and decentralized identity verification.

By employing RSA encryption and IPFS for document security and decentralized storage, and storing metadata hashes on blockchain platforms, the system ensures confidentiality, integrity, and traceability of question papers. This solution targets universities, colleges, and certification authorities, aiming to eliminate human error and security loopholes, thereby revolutionizing exam security through modern technological integration.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 Overview

EXAM-VAULT is a blockchain-based secure examination management system designed to prevent question paper leaks and unauthorized access during the transmission and storage of examination papers. The project leverages decentralized technologies such as Ethereum, Hyperledger Fabric, and IPFS, along with RSA encryption and smart contracts, to ensure confidentiality, integrity, and transparency in academic evaluations.

The system introduces role-based dashboards for key stakeholders—COE, teachers, and superintendents—with each user authenticated through Firebase and MetaMask. Papers are encrypted and uploaded to IPFS, where they are assigned unique Content Identifiers (CIDs). These CIDs are stored immutably on the blockchain to ensure verifiability and tamper-proof access control.

The front-end interface is developed using ReactJS, with a Django backend handling core logic and smart contract interactions. Transactions and activities are traceable and auditable through blockchain logs, enhancing accountability and reducing human error.

EXAM-VAULT is applicable in universities, online exam platforms, and certification bodies, and serves as a scalable, secure alternative to traditional paper distribution systems.

1.2 Motivation

In recent years, incidents of examination question paper leaks and unauthorized access have significantly undermined the credibility and fairness of academic assessments. Traditional methods involving physical transportation or centralized digital storage are highly vulnerable to human error, insider threats, and external breaches. These challenges not only disrupt academic schedules but also diminish institutional trust and student morale.

The motivation behind EXAM-VAULT stems from the need to reinforce examination integrity through technological innovation. By incorporating blockchain and encryption, we aim to create a system that ensures secure, tamper-proof transmission of question papers, with transparent and

auditable transactions. The decentralized nature of blockchain, combined with strong encryption mechanisms and role-based access control, provides a robust alternative to existing systems.

This project is driven by the vision of building a future-ready, scalable, and trustworthy platform that can be adopted by universities, certification authorities, and online exam platforms globally. It not only addresses the immediate concern of paper leaks but also sets a precedent for secure digital transformation in the education sector.

1.3 Objectives

1. Develop role-based dashboards for COE, teachers, and superintendents

- Building custom dashboards tailored to different roles:
    - COE (Controller of Examinations): Access to question paper uploads, paper assignment, and security checks.
    - Teachers: Possibly for setting or reviewing question papers securely.
    - Superintendents: Monitor exam paper receipt, distribution, and status during exams.
- Each user sees only the features relevant to their role, increasing **usability** and **security**.

2. Deploy IPFS for decentralized, encrypted paper handling

- IPFS (InterPlanetary File System) is a peer-to-peer decentralized storage system.
- Use IPFS to store question papers securely, ensuring:
    - They are encrypted, so only authorized users can access them.
    - The files are decentralized, meaning they’re not stored on a single vulnerable server.
    - This reduces the risk of tampering or data loss.

3. Develop a secure and verifiable examination paper transmission using blockchain-backed audit trails via Hyperledger Fabric and Ethereum-enabled interactions

- The goal is to secure the transmission of exam papers from one role to another.
- Create an audit trail using:
    - Hyperledger Fabric (permissioned blockchain): For internal operations, like tracking when papers were uploaded or accessed.
    - Ethereum (public blockchain): For adding verifiable events or transactional proofs that cannot be altered.

- This builds a transparent and tamper-evident system.

4. Integrate smart contracts written in Solidity on Ethereum for tamper-proof transactions

- Use Solidity (a language for Ethereum) to write smart contracts.
- These contracts will:
  - Automate certain actions (e.g., releasing a paper at a scheduled time).
  - Ensure rules are enforced without manual intervention.
  - Make all actions tamper-proof, as smart contract code and actions are immutable once deployed.

1.4 Purpose, Scope and Applicability

1.4.1 Purpose

The primary purpose of EXAM-VAULT is to create a secure, transparent, and decentralized platform for managing examination paper workflows. It aims to eliminate the risks associated with traditional paper transmission systems—such as unauthorized access, leakage, and loss of confidentiality—by introducing encryption, decentralized storage, and immutable transaction records. The system also empowers academic authorities to trace every action performed on a question paper, enhancing accountability and reducing malpractices.

1.4.2 Scope

- Secure uploading and encryption of question papers by teachers.
- Decentralized storage using IPFS and CID generation for each encrypted file.
- Recording and auditing of CID transactions on Ethereum and Hyperledger blockchains.
- Role-specific dashboards for managing workflows and access (COE, teachers, superintendents).
- Integration with smart contracts, authentication systems (Firebase, MetaMask), and blockchain simulation environments (Ganache).
- Scalable infrastructure that can be extended to various academic or legal document transmission systems.

1.4.3 Applicability

The proposed project is applicable in:

- Educational Institutions: For managing university, school, and competitive exam papers.

- Government Agencies: For national-level examinations like UPSC, banking, or board exams.
- Healthcare and Legal Sectors: To securely transmit confidential reports and documents.
- Certification Bodies: To ensure integrity in professional and technical certifications.

1.5 Organization of Report

The report is organized into the following chapters:

- Chapter 1 – Introduction: Provides an overview of the project, its motivation, objectives, scope, and applicability.
- Chapter 2 – Tools and Technologies: Describes the technical stack and frameworks used in the development of the project.
- Chapter 3 – System Design: Discusses the architectural and modular design, including blockchain integration and smart contract flow.
- Chapter 4 – Implementation: Explains the development process, code snippets, workflows, and testing scenarios.
- Chapter 5 – Results: Presents the outcome of the project including screenshots, testing metrics, and performance analysis.
- Chapter 6 – Applications & Conclusion: Lists potential applications, key conclusions, and future scope.
- References: Includes all academic and technical references used for the development of the project

Chapter 2

LITERATURE SURVEY

2.1 Introduction

Examination security has become a critical concern for educational institutions worldwide, especially with the proliferation of digital platforms. The increased risk of unauthorized access, tampering, and examination paper leaks has exposed significant vulnerabilities in traditional examination processes. Conventional methods, such as physical delivery of papers or unsecured digital transfers, lack robust protection, traceability, and transparency, making them inadequate in addressing modern security threats.

Limitations of Traditional Examination Security

Physical and Digital Risks: Traditional systems are prone to breaches, including unauthorized access, data manipulation, and result falsification. The absence of comprehensive audit trails further complicates the detection and investigation of such incidents.

Lack of Transparency and Traceability: Without secure, verifiable records, it is challenging to ensure accountability and maintain the integrity of examination processes.

Blockchain and Encryption: Advancing Examination Security

Recent advancements in blockchain and encryption technologies provide innovative solutions to these longstanding issues:

Immutability and Decentralization: Blockchain's core attributes—immutability, decentralization, and cryptographic security—make it highly suitable for securing examination records. Once data is recorded on a blockchain, it cannot be altered or deleted, preventing unauthorized modifications to question papers, scores, or student identities.

Smart Contracts: Automated protocols known as smart contracts can manage the distribution of exam papers, restrict access to authorized candidates, and facilitate transparent grading, all without human intervention. This automation enhances both security and operational efficiency.

Encrypted Storage and Retrieval: Integrating blockchain with systems like the Inter Planetary File System (IPFS) allows institutions to store and retrieve encrypted examination papers securely, mitigating the risk of tampering or premature access.

Robust Authentication: The use of cryptographic techniques and biometric verification (such as facial recognition) strengthens identity verification, reducing the risk of impersonation and unauthorized participation in online examinations.

Research and Implementation

Blockchain-Based Systems: Solutions such as TrustExaminer, built on Hyperledger Fabric, demonstrate the practical application of blockchain in examination management. These systems offer granular access control, data privacy, and scalability—key requirements for handling sensitive educational data.

Academic Credential Verification: Blockchain has also been applied to secure academic credentials, ensuring the authenticity and traceability of records while protecting against forgery and manipulation.

Security Considerations and Challenges

While blockchain offers significant security benefits, certain vulnerabilities must be addressed:

Potential Threats: Blockchain-based systems are susceptible to attacks such as 51% attacks, double spending, Sybil attacks, and smart contract exploits. Effective countermeasures include robust consensus mechanisms, multi-factor authentication, and formal verification of smart contracts.

2.2 Summary of Papers

1. Anuradha et al. (2025) – Blockchain-Based Exam Security Model

Anuradha and her team proposed a blockchain-based framework designed to secure the examination paper lifecycle. Their model focused on leveraging the immutability and traceability aspects of blockchain to prevent tampering and unauthorized modifications of question papers during transmission. However, a major shortfall of this solution was its lack of role-based access control and encryption mechanisms. In the absence of encryption, question papers were vulnerable during temporary storage or network transmission, especially in scenarios where the blockchain nodes could be compromised or observed.

Moreover, without clearly defined roles such as COE (Controller of Examinations), teacher, and superintendent, the system did not enforce layered permissions or responsibilities, making it unsuitable for institutions that require strict access boundaries. The EXAM-VAULT system addresses these limitations by introducing RSA encryption, MetaMask-based role control, and Firebase-authenticated dashboards for different stakeholders.

2. Shirke et al. (2025) – Trust Examinator

Shirke and team proposed Trust Examinator, a transparent and traceable examination system built on blockchain. It focused on decentralizing examination management and used hashes to ensure content immutability. However, the project lacked the implementation of encrypted, decentralized file storage mechanisms.

Without integrating platforms like IPFS, the Trust Examinator system remained vulnerable to centralized file manipulation and lacked scalability in handling large volumes of encrypted papers. EXAM-VAULT overcomes these limitations by splitting encrypted files into Merkle Tree-based chunks, distributing them via IPFS, and referencing the content identifiers (CIDs) in a blockchain ledger for secure retrieval.

3. Li and Han (2024) – EduRSS: Blockchain-Based Academic Record System

Li and Han proposed EduRSS, a blockchain-secured platform aimed at secure storage and sharing of academic records, such as transcripts and certificates. Their work leveraged a public blockchain to ensure the immutability and traceability of records. The solution focused primarily on the storage aspect rather than real-time dynamic interactions, such as those required during examination workflows.

Though academically significant, EduRSS was not designed to handle time-sensitive operations like exam paper distribution, which demands real-time encryption, upload, verification, and retrieval by multiple roles. The EXAM-VAULT framework overcomes this limitation by incorporating live user interaction modules (via ReactJS and Django) and real-time smart contract-triggered events for paper submission, selection, and access.

4. Chennamma et al. (2024) – SecureQ: Blockchain-Based Exam System Without Encryption

The SecureQ framework presented by Chennamma et al. was a promising concept for using blockchain to manage the distribution and logging of exam papers. However, a critical flaw in their design was the absence of any encryption mechanism.

This makes the system unsuitable for any real-world deployment where sensitive academic data needs protection. EXAM-VAULT rectifies this issue by incorporating RSA public-key encryption for securing papers before upload, ensuring that even if storage nodes are compromised, the data remains inaccessible without the decryption key.

5. Kamble et al. (2024) – Blockchain for Competitive Exams

This study by Kamble et al. focused on leveraging blockchain to combat exam malpractice in competitive and government examinations. Their architecture enabled secure question paper distribution using a single blockchain platform, primarily Ethereum. While effective in ensuring data integrity, the solution did not employ a hybrid blockchain approach, missing the opportunity to leverage the complementary benefits of private (Hyperledger Fabric) and public (Ethereum) blockchains.

The EXAM-VAULT platform uses both Ethereum and Hyperledger for storing metadata and audit logs, while actual encrypted question papers are stored securely and efficiently on IPFS, reducing blockchain bloat and transaction costs.

6. Kadam et al. (2024) – Blockchain-Enabled Exam Platform

Kadam and colleagues developed a blockchain-powered assessment platform that aimed to ensure transparency and tamper-resistance in examination evaluation. The system included question uploading, student responses, and grading logs on the blockchain. However, it relied on static storage servers to manage files, which introduced security vulnerabilities in storing and retrieving papers and answers.

This approach defeated the purpose of decentralization by reintroducing centralized storage concerns. In contrast, the EXAM-VAULT project embraces a fully decentralized data flow by integrating IPFS for file storage, RSA for encryption, and Ethereum for CID hash logging, ensuring both availability and security of the question papers.

7. Ocheja et al. (2022) – Blockchain in Education: Case Studies

Ocheja et al. conducted a comprehensive review of blockchain applications in education, covering real-world case studies and conceptual applications. Their work provided valuable insights into the practical implementation challenges and benefits of blockchain technology in learning management, credential verification, and academic recordkeeping.

However, their study remained theoretical and did not offer a concrete, implementable architecture for managing dynamic workflows like examination security. EXAM-VAULT builds upon these insights and goes a step further by providing an end-to-end solution with detailed system design, smart contract implementation, and testable modules for secure exam paper handling.

8. Badlani et al. (2022) – EduCrypto: Blockchain in Education

The EduCrypto project by Badlani et al. explored the use of blockchain for managing student data, including academic achievements and attendance records. The emphasis was on institutional transparency and digital identity management. While the project used blockchain effectively, it did not extend to the management of examination papers or paper lifecycle security. By focusing primarily on student performance data, EduCrypto missed addressing the high-risk area of question paper leaks. EXAM-VAULT specifically tackles this gap by targeting the paper-setting, distribution, and retrieval phases of examinations, ensuring end-to-end security and compliance with academic integrity protocols.

9. Rahman et al. (2021) – Secure Question Paper Management with Basic Cryptography

Rahman et al. introduced a Secure Question Paper Management System (SQPMS) utilizing basic symmetric cryptography to protect the content of question papers. Their approach involved encrypting the question papers with a shared key and allowing authorized users to decrypt the content. While this method was effective in offering confidentiality, the system lacked decentralized architecture and automated access control mechanisms.

Furthermore, their solution did not implement IPFS (InterPlanetary File System) for decentralized storage or smart contracts for workflow automation. This reliance on a central server introduced vulnerabilities such as a single point of failure and potential internal breaches. In contrast, EXAM-VAULT uses a hybrid blockchain model, smart contract-driven paper tracking, and IPFS for decentralized encrypted storage, thereby enhancing fault tolerance and transparency.

10. Islam et al. (2021) – BSSSQS: Blockchain-Based Question Sharing

Islam et al. designed the BSSSQS (Blockchain-Based Smart and Secure Question Sharing) platform, which introduced blockchain technology into academic content distribution. The model utilized a blockchain to ensure the traceability of question sets. While the system was a step in the right direction, it lacked fine-grained access control and role differentiation among users.

In real-world academic settings, different roles (e.g., COE, setter, invigilator) require varying levels of permission and data access. BSSSQS did not accommodate these hierarchical distinctions. EXAM-VAULT introduces role-based dashboards, smart contracts for workflow logic, and authentication mechanisms to enforce granular access policies, improving both usability and compliance.

Summary

Across these papers, it is evident that while blockchain offers immense potential in securing academic workflows, many of the existing systems are partial or incomplete, lacking components such as:

- Decentralized file storage (IPFS),
- Role-based access control,
- Real-time paper handling,
- End-to-end encryption.

2.3 Drawback of Existing System

- **Risk of Paper Leaks**

  Physical transportation and email-based transmission of question papers are highly susceptible to unauthorized access and leaks. There is little to no way to trace who accessed the content or when the breach occurred.

- **Lack of Auditability**

  Existing systems do not maintain a tamper-proof, immutable audit trail. If question papers are leaked or altered, there is no secure method to identify the source of the breach.

- **Centralized Vulnerabilities**

  Conventional digital systems often store examination content on centralized servers. These are vulnerable to cyberattacks, insider threats, and single points of failure that can disrupt the examination process.

- **Manual Authentication Processes**

  Verifying the identity of paper setters and superintendents is often performed manually or with basic login credentials, making it easier for impersonation or unauthorized access.

- **No Real-Time Transparency**

  The stakeholders (COE, teachers, and superintendents) lack real-time visibility into the status of the examination paper lifecycle—from submission to selection and retrieval.

- **No Encryption or Secure Handling**

  Most existing systems do not enforce end-to-end encryption, meaning that sensitive content like question papers can be intercepted or accessed in plain text during transmission or storage.

- **High Dependency on Human Intervention**

  Manual handling increases the chance of errors, delays, or mismanagement of critical assets like examination content.

2.4 Problem Statement

"To develop a blockchain-based system for secure and confidential transmission of question papers."

Input: COE's question paper requests, teacher-prepared PDF papers, user credentials, and course details.

Output: Encrypted papers on IPFS with hashes, blockchain-based metadata, secure paper delivery to superintendents, and tamper-proof, anonymous transaction records.

2.5 Proposed Solution

- COE logs into the dashboard using Firebase for secure authentication and sends paper-setting requests.
- The backend operations, including handling requests and managing workflows, are powered by Django.
- Teachers accept/reject requests via ReactJS interface, preparing papers upon acceptance.
- Question papers in PDF are encrypted with RSA and uploaded to IPFS for decentralized handling.
- IPFS generates a unique Content Identifier (CID) for the paper, recorded on the Ethereum blockchain and Hyperledger Fabric via Ganache.
- COE selects a paper anonymously, with the CID logged in Ethereum and Hyperledger Fabric via Ganache.
- Superintendent retrieves the paper's CID from Ethereum using MetaMask for secure access.
- Encrypted paper is accessed from IPFS using the CID and decrypted with RSA.
- Smart contracts, written in Solidity and deployed with Truffle on Ganache, manage transactions on Ethereum.

Chapter 3

REQUIREMENT ENGINEERING

3.1 Software and Hardware Tools Used

Hardware Requirements:

- Processor: Intel Core i5 or equivalent
- RAM: 8 GB minimum
- Storage: 256 GB SSD
- Network: Stable internet connection with 10 Mbps minimum

Software Requirements:

- Operating System: Windows 10/11 or Ubuntu 20.04
- Browser: Cross Platform
- Development Tools: Node.js, ReactJS, Truffle, Ganache
- Dependencies: IPFS, Ethereum, Hyperledger Fabric, Solidity for smart contract development

3.2 Conceptual/Analysis Modelling

3.2.1 Use Case Diagram

- The Use Case Diagram illustrates the interactions between different user roles and the system functionalities. The key actors are:
- COE (Controller of Examinations)
- Logs into the system
- Sends paper-setting requests
- Selects question papers anonymously
- Verifies audit trail
- Teacher (Paper Setter)
- Receives paper-setting request
- Uploads encrypted PDF papers to IPFS
- Accepts/rejects requests

- Superintendent
- Retrieves question paper using CID from the blockchain
- Decrypts the paper for examination
- System
- Encrypts papers using RSA
- Stores files on IPFS and generates CID
- Records CID and metadata on Ethereum/Hyperledger Fabric
- Manages role-based access using smart contracts and MetaMask

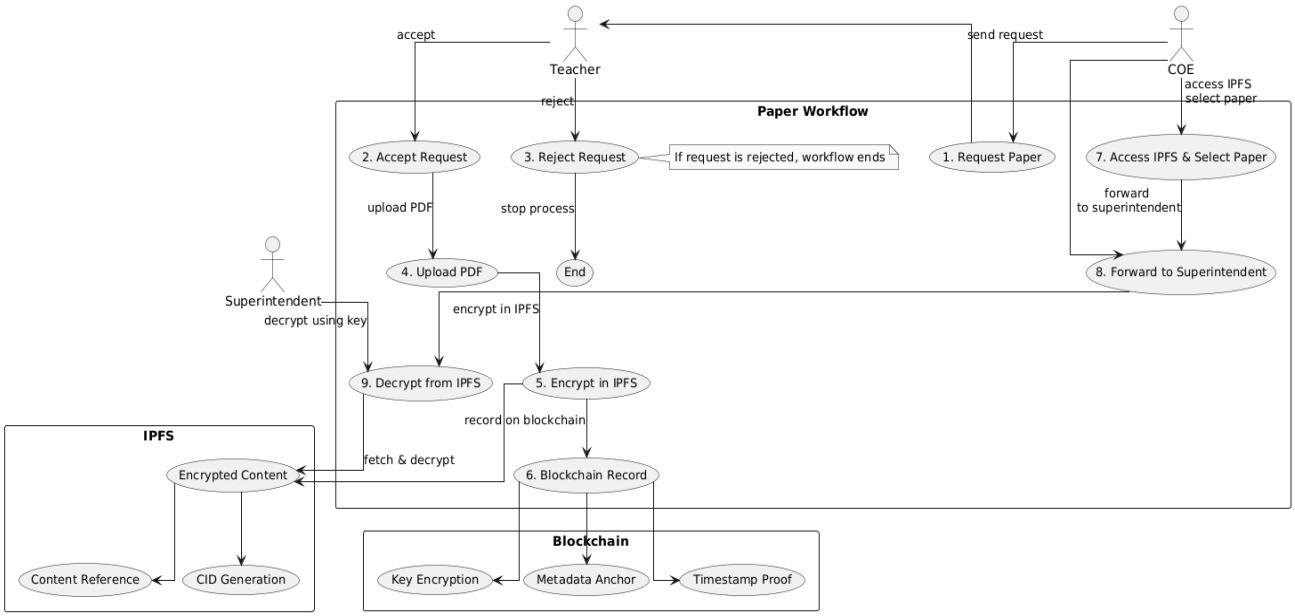


Figure 3.1: Use Case Diagram

3.2.2 Sequence Diagram

- COE logs in and sends a request to Teacher.
- Teacher accepts and uploads an encrypted PDF to IPFS.
- IPFS returns a CID, which is logged via smart contract to Ethereum and Hyperledger.
- COE selects a paper anonymously using the CID.
- Superintendent accesses the CID using MetaMask and retrieves the encrypted paper from IPFS.
- The paper is decrypted using RSA for examination purposes

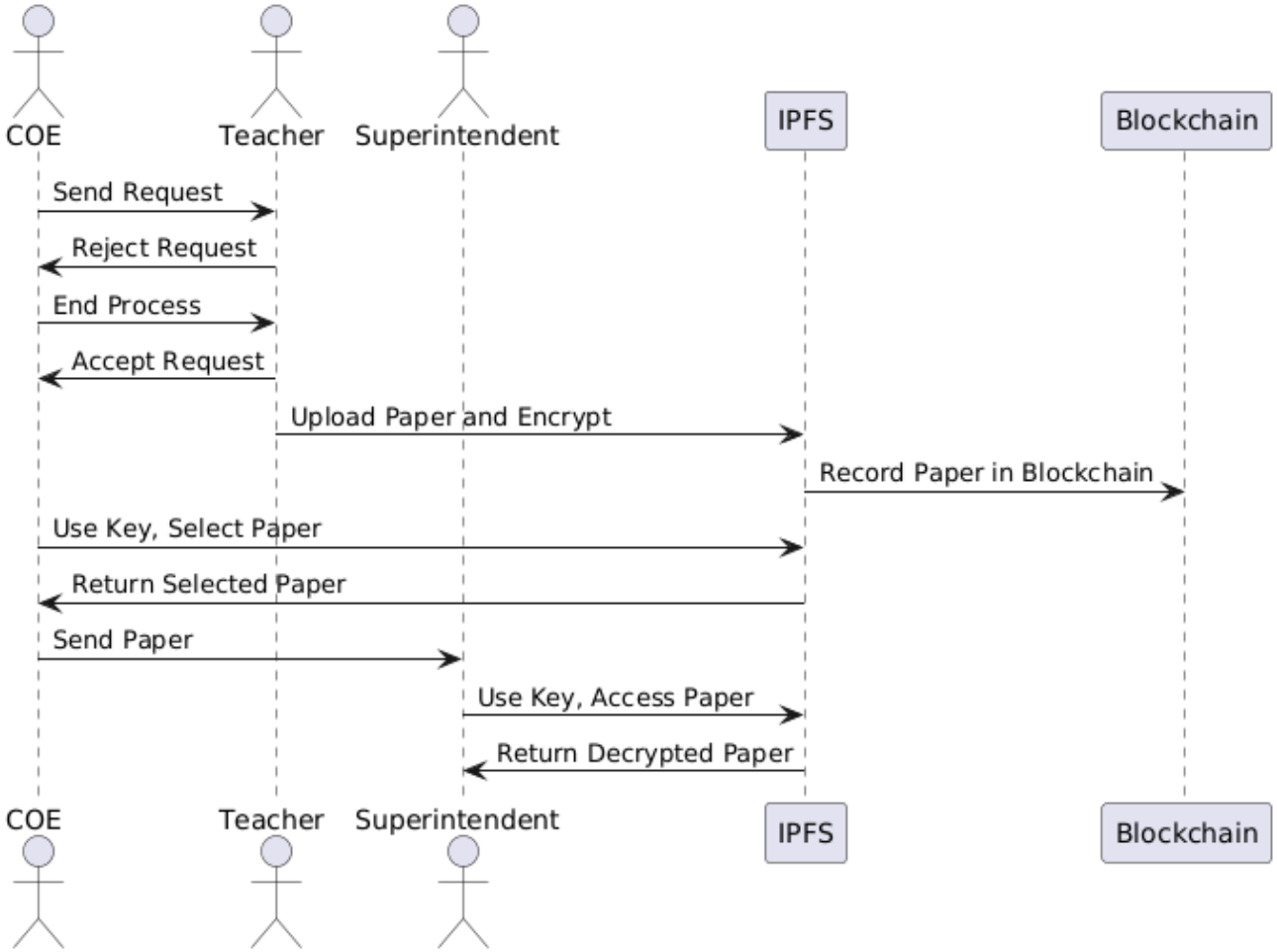


Figure 3.2: Sequence Diagram

3.2.3 Activity Diagram

The activity diagram represents the dynamic flow of the system:

- Start → Login (via Firebase) → Role Identified (COE/Teacher/Superintendent)
- COE → Send Request → Select Paper (anonymously) → Verify Hash
- Teacher → Accept Request → Encrypt Paper → Upload to IPFS → Store CID on Blockchain
- Superintendent → Fetch CID → Retrieve Paper → Decrypt Paper → End

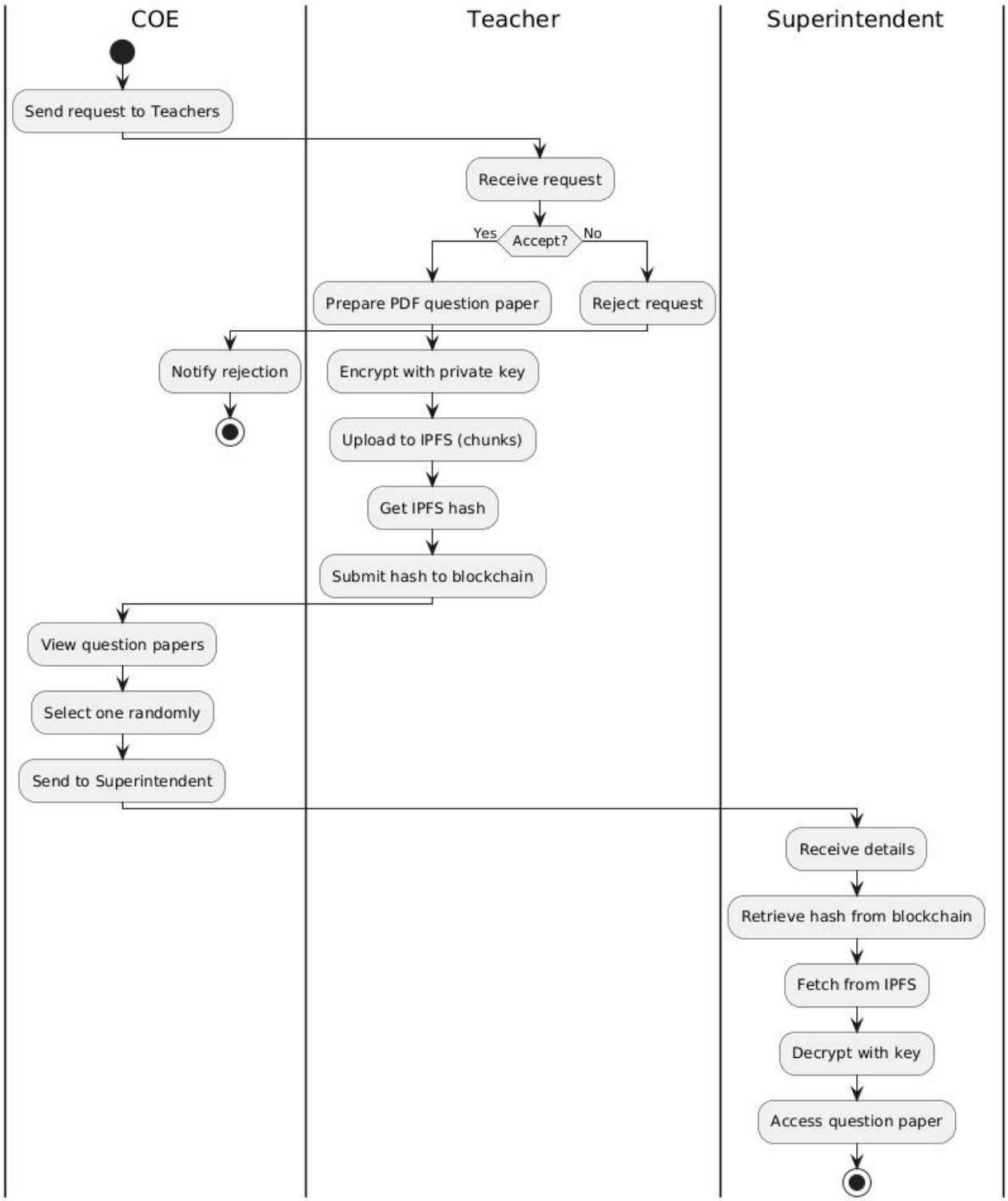


Figure 3.3: Activity Diagram

3.2.4 State Diagram

This represents the lifecycle of a question paper in the system:

- State 1: Draft (Created by Teacher)
- State 2: Encrypted (Using RSA)
- State 3: Uploaded to IPFS (CID generated)
- State 4: CID Recorded (Blockchain)
- State 5: Selected (COE selects paper)
- State 6: Retrieved (Superintendent accesses it)
- State 7: Decrypted (Paper is ready for exam)
- Each state transition is triggered by a secure and verifiable action by the authenticated user.

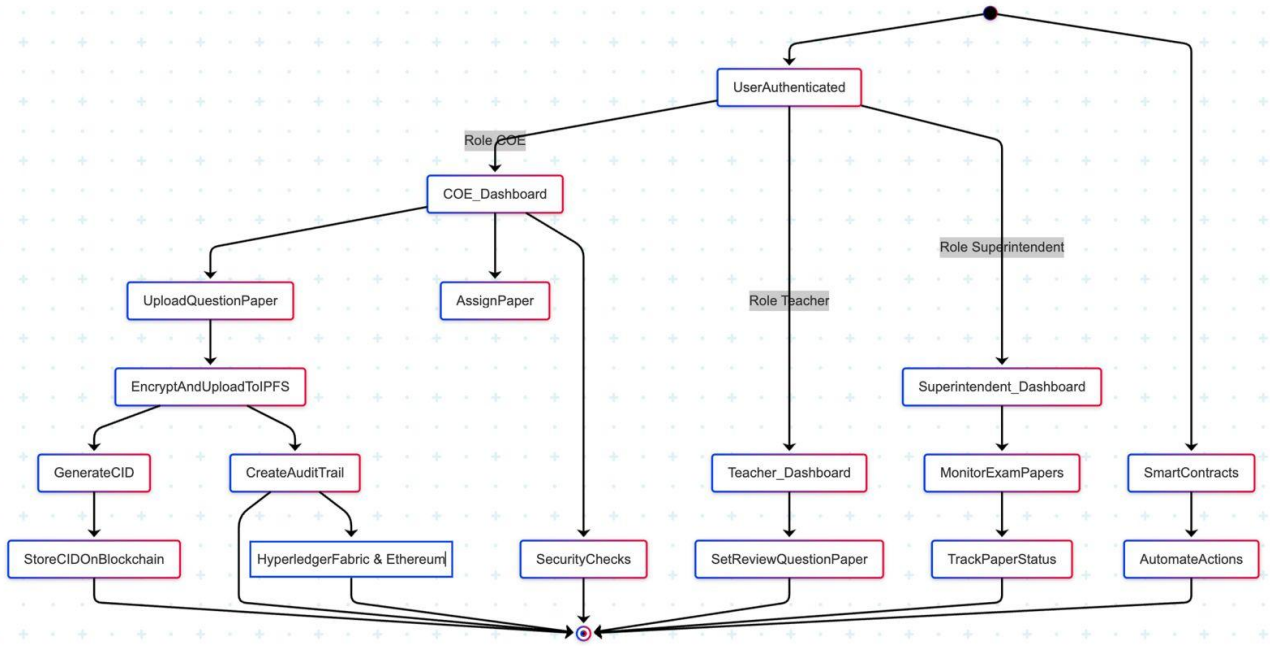
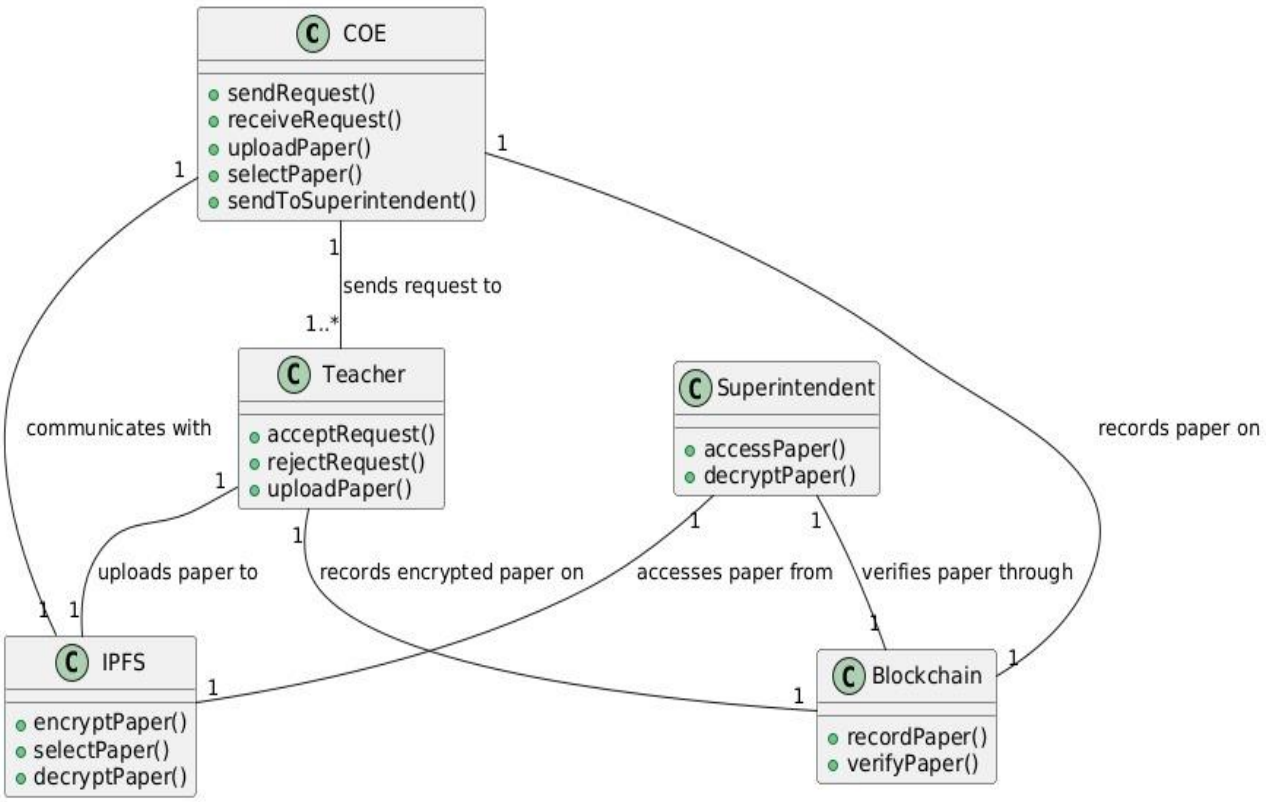


Figure 3.4: State Diagram

3.2.5 Class Diagram

- The class diagram models a secure examination paper transmission system using blockchain and IPFS technologies.
- COE (Controller of Examination) initiates the process by sending requests to one or more Teachers to set question papers and later selects and forwards a paper to the Superintendent.

- Teacher can accept or reject the request; if accepted, the Teacher prepares the paper, encrypts it, uploads it to IPFS for decentralized storage, and records the encrypted paper on the Blockchain for integrity and traceability.
- IPFS (InterPlanetary File System) handles the encryption, chunking, and decentralized storage of the examination paper, providing a hash for retrieval.
- Blockchain stores the hash and metadata of the encrypted paper, ensuring tamper-proof records and enabling verification of the paper's authenticity.
- Superintendent accesses and decrypts the selected paper from IPFS and verifies its integrity via the Blockchain before using it for the examination.
- The relationships show COE communicates with Teachers, Teachers interact with both IPFS and Blockchain, and the Superintendent retrieves and verifies papers through IPFS and Blockchain, respectively.
- This structure ensures secure, transparent, and auditable handling of examination papers, eliminating the risks of physical transmission



3.5: Class Diagram

3.3 Software Requirements Specification

3.3.1 User Requirements

- The system must securely transmit encrypted examination papers from the COE to the assigned superintendent.
- It must ensure only authorized personnel with valid decentralized identities can access the question papers.
- The solution should provide immutable and verifiable audit trails using blockchain and IPFS technologies.
- The platform must support real-time identity verification and role-based access through smart contracts and MetaMask.

3.3.2 System Requirements

- Ethereum blockchain and Hyperledger Fabric, accessed via Ganache, are used for secure transaction recording, with smart contracts written in Solidity.
- IPFS for decentralized paper handling and CID generation.
- Smart contracts written in Solidity and deployed with Truffle for Ethereum transactions.
- RSA encryption integrated with ReactJS for securing PDF papers during upload and access.

Chapter 4

PROJECT PLANNING

4.1 Project Planning and Scheduling

Project planning and scheduling are critical aspects of software development that ensure timely and efficient execution of the system. In this project, *"Secured Blockchain-Based Examination Management System,"* we adopted structured planning techniques and scheduling methodologies to manage complexity and interdependencies.

Planning involves identifying all major tasks required to develop the system and establishing dependencies among them. These tasks were broken down into smaller, manageable modules using the Divide and Conquer strategy.

Scheduling ensures the proper allocation of time and resources to each task. We used visual tools like the Gantt Chart and Program Evaluation Review Technique (PERT) to map and manage the project lifecycle.

Gantt Chart Overview

The Gantt chart below represents the major phases and their respective timelines in the ExamVault Project:

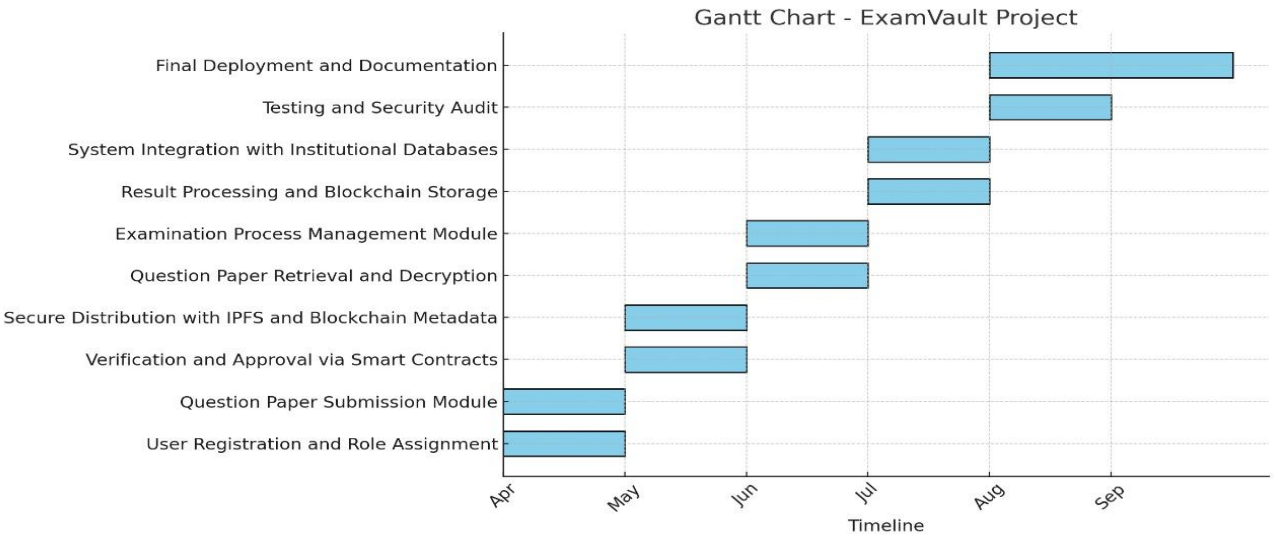


Figure 4.1: Gantt Chart of Project Planning

Project Timeline:

- **April:** User registration setup and question paper submission modules.

- **May:** Smart contract validation and secure distribution via IPFS.
- **June:** Decryption, exam process handling, and management modules.
- **July:** Blockchain storage and institutional database integration.
- **August–September:** Testing, security audit, final deployment, and documentation.

This clear distribution of work ensured smooth progress tracking and milestone achievements.

4.2 Module Breakdown and Functionality

Using the divide and conquer method, the system was split into discrete modules:

1. User Registration and Role Assignment

Enables onboarding of different stakeholders (admin, examiners, centers).

Controls access based on user roles.

2. Question Paper Submission Module

Secure interface for question setters to upload encrypted exam content.

Anonymity is preserved using encryption and identity abstraction.

3. Verification and Approval via Smart Contracts

Smart contracts validate the uploaded papers automatically.

Logs verification history securely on the blockchain.

4. Secure Distribution with IPFS and Blockchain Metadata

Encrypts papers and stores them on IPFS.

Blockchain holds the metadata and hash for integrity verification.

5. Question Paper Retrieval and Decryption

Authorized users at examination centers retrieve and decrypt papers just-in-time.

Private key-based access control is enforced.

6. Examination Process Management Module

Facilitates exam coordination and real-time status tracking.

7. Result Processing and Blockchain Storage

Ensures tamper-proof result storage.

Enables verifiable result authentication using blockchain.

8. System Integration with Institutional Databases

Syncs with academic records and user databases.

Enhances interoperability with educational infrastructure.

9. Testing and Security Audit

Validates system performance, scalability, and security.

Conducts penetration tests and encryption verification.

10. Final Deployment and Documentation

Completes final deployment.

Prepares user manuals and technical documentation.

Chapter 5

APPLICATIONS & CONCLUSION

5.1 Applications

- University & College Examinations
- Online & Remote Examinations
- Competitive & Government Exams
- E-Governance in Education
- Prevention of Paper Leaks & Exam Malpractices

5.2 Conclusion

- The project EXAM-VAULT: Reinventing Examination Security Through Blockchain and Encryption successfully addresses one of the most pressing challenges in the academic ecosystem — the secure, verifiable, and tamper-proof transmission of examination question papers. With the increasing number of exam paper leaks and unauthorized access incidents, especially in high-stakes university and government-level assessments, there is a clear and urgent need for a more secure, automated, and decentralized solution. EXAM-VAULT offers precisely that.
- By integrating decentralized technologies such as Ethereum, Hyperledger Fabric, and IPFS, the system provides a blockchain-backed audit trail, ensuring that any activity related to question papers — from creation to delivery — is recorded immutably and transparently. The use of RSA encryption guarantees end-to-end confidentiality, ensuring that question papers are not accessible or readable without the proper private key.
- Smart contracts written in Solidity automate key transactions, enforce role-based access control, and eliminate human errors or malicious intervention. Teachers upload question papers in an encrypted format, which are then stored on IPFS, with the corresponding Content Identifier (CID) recorded on the blockchain. This ensures that no one — not even system administrators — can tamper with the content or metadata without detection. The COE can anonymously select papers, while superintendents securely retrieve them using MetaMask-authenticated credentials.
- The solution is both technically robust and operationally scalable. The front end, developed using ReactJS, and the back end using Django, provide an intuitive user experience while managing complex encryption, authentication, and blockchain interactions in the background. Firebase ensures secure

role-based authentication, while Ganache simulates the Ethereum environment for local testing and validation.

- In addition to addressing the existing flaws of centralized systems — such as lack of traceability, vulnerability to tampering, and over-reliance on manual processes — EXAM-VAULT introduces a next-generation standard for how sensitive academic data should be managed. It enhances trust, reduces overhead, and mitigates the risk of academic malpractice, all while remaining extensible to other domains such as legal document transmission, digital certifications, and medical data sharing.
- In conclusion, EXAM-VAULT is not just a secure exam paper management system — it is a vision for the future of digital trust in education. It exemplifies how blockchain and cryptographic technologies, when thoughtfully applied, can bring about meaningful transformation in conventional administrative workflows. As institutions globally shift toward digital transformation, the adoption of platforms like EXAM-VAULT will become not just advantageous, but essential.

REFERENCES

[1] K. Anuradha, K. Jahnavi, P. Jahanavi, M. Bhargavi, P. Praveen, R. K. Krishnapriya, V. S. M. Shahil, and N. V. Kumar, "Enhancing Exam Security with Blockchain Technology," International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 13, no. III, pp. 1967-1971, Mar. 2025.

[2] Rahman, S. & Iftekhar, Md. Nashif & Alam, Rashedul & Gafur, S M Raihan & Nandi, Dip. (2025). Secured Question Paper Management System. AIUB Journal of Science and Engineering (AJSE).

[3] H. Li and D. Han, "EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme," in IEEE Access, vol. 7, pp. 179273-179289, 2024.

[4] Kamble, A. D., & Kamble, D. A. (2024). Blockchain-based Competitive Examination System in India: Preventing Paper Leaks and Mitigating Frauds. International Journal of Innovative Research in Science, Engineering and Technology, 13(8), 14810-14817.

[5] Kadam, Sahil & Kothalkar, Mahesh & Ambawade, Dayanand. (2024). Blockchain-Enabled Examination Platform: A Secure Approach for Academic Assessments.

[6] S. R. G, S. K N and H. R. Chennamma, "Security of Examination Question Paper Through Blockchain - SecureQ," 2023 International Conference on Innovation and Novelty in Engineering and Technology (INNOVA), Vijayapura, India, 2023, pp. 1-6.

[7] Islam Abhi, Anik & Kader, Md Fazlul & Shin, Soo. (2022). BSSSQS: A Blockchain-Based Smart and Secured Scheme for Question Sharing in the Smart Education System.

[8] P. Ocheja, F. J. Agbo, S. S. Oyelere, B. Flanagan and H. Ogata, "Blockchain in Education: A Systematic Review and Practical Case Studies," in IEEE Access, vol. 10, pp. 99525-99540, 2022.

[9] S. Badlani, T. Aditya, S. Maniar and K. Devadkar, "EduCrypto: Transforming Education using Blockchain," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2022, pp. 829-836.

[10] Chaitanya Damodar Shirke, Dr. Rakhi O. Gupta, Dhanraj Nagesh Chinta, Nashrah Gowalker (2021), Trust Examinator: A Secure, Transparent, Blockchain-Based Examination System, International Journal of Research Culture Society, Volume – 9, Issue – 2., Pp.19-27.