

BANGALORE INSTITUTE OF TECHNOLOGY

K.R. Road, V.V. Pura, Bengaluru-560 004



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Project Synopsis

VI – Sem
2025(Even)

MAJOR PROJECT GROUP:

Sl. No.	USN	NAME	Sec.	Email-Id	Phone No	Signature
1	1BI22CS156	SHRUTI KUMARI	C	shrutirajput5827@gmail.com	9014809178	
2	1BI22CS159	SNEHA R	C	sneharaju2004@gmail.com	8123050008	
3	1BI22CS184	VIBHANSH JAIN	C	vibhanshjainn@gmail.com	7976814946	
4	1BI22CS194	YOGANAND	C	yoganandmaskalle@gmail.com	7676833092	

MAJOR-PROJECT DETAILS:

Title:	ExamVault : Reinventing Examination Security Through Blockchain & Encryption
Domain:	Blockchain

For office use only:

Group ID:	
Guide:	Shruthi B Gowda
Status:	Accepted / To be modified / Rejected

Signature of the Major Project Co-Ordinator

Title - ExamVault : Reinventing Examination Security Through Blockchain & Encryption

Abstract

Blockchain technology is utilized to establish a secure and transparent framework for handling examinations. By integrating Ethereum/Hyperledger, IPFS (InterPlanetary File System) for decentralized storage, and cryptographic techniques such as RSA, AES, and SHA-256, confidentiality and integrity of question papers, approvals, and result processing are ensured. Critical operations, including question paper submission, verification, approval, secure distribution, and retrieval, are automated through smart contracts written in Solidity. Role-based authentication is implemented for COEs, teachers, and superintendents, with public-private key pairs generated for encryption and decryption. Question papers are encrypted using AES encryption, uploaded to IPFS, and retrieved securely with blockchain-stored metadata and timestamps. The verification and approval process by COE ensures authenticity before distribution. Answer sheets and results can be stored on the blockchain to maintain integrity, fairness, and prevent tampering. Technologies such as Node.js, React.js, MongoDB, OpenSSL, Truffle, and Web3.js contribute to a secure, decentralized, and scalable approach to conducting examinations while eliminating traditional vulnerabilities.

Introduction

In the digital age, ensuring security, transparency, and efficiency in examination processes has become a critical challenge. Traditional methods of handling examinations often involve paper-based procedures and centralized digital systems, both of which are prone to security breaches, unauthorized access, and inefficiencies. Issues such as question paper leaks, result manipulation, and tampering create significant concerns for educational institutions and organizations conducting exams. To address these vulnerabilities, blockchain technology presents a decentralized, immutable, and tamper-proof approach to enhancing the confidentiality and integrity of examination-related activities.

Blockchain operates on a distributed ledger mechanism, ensuring that all transactions and records are securely stored, time-stamped, and verifiable. By leveraging Ethereum/Hyperledger, cryptographic encryption techniques, and decentralized storage solutions like IPFS (InterPlanetary File System), examination workflows can be managed with a high degree of security. The adoption of smart contracts written in Solidity automates key operations such as question paper submission, verification, approval, and result processing, thereby reducing reliance on intermediaries and minimizing the risk of human errors or misconduct.

A critical aspect of this approach is the role-based authentication model, where stakeholders—including COEs, teachers, and superintendents—are assigned cryptographic key pairs for secure data exchange. AES encryption is applied to protect question papers before uploading them to IPFS, while blockchain stores essential metadata and timestamps, ensuring traceability. Once verified and approved, question papers are securely distributed using public-private key encryption, allowing only authorized personnel to retrieve and decrypt them. This method eliminates risks associated with traditional distribution channels and ensures that examination materials remain confidential until the intended time.

Beyond question paper security, this framework extends to answer sheet verification and result processing. Answer scripts can be securely referenced on the blockchain, enabling digital verification and preventing post-exam alterations. Furthermore, results can be digitally signed and stored on a blockchain network, ensuring fairness, transparency, and resistance to tampering. By integrating Node.js, React.js, MongoDB, OpenSSL, Truffle, and Web3.js, a scalable, decentralized, and robust infrastructure is established, addressing long-standing security concerns in examinations.

Problem Statement

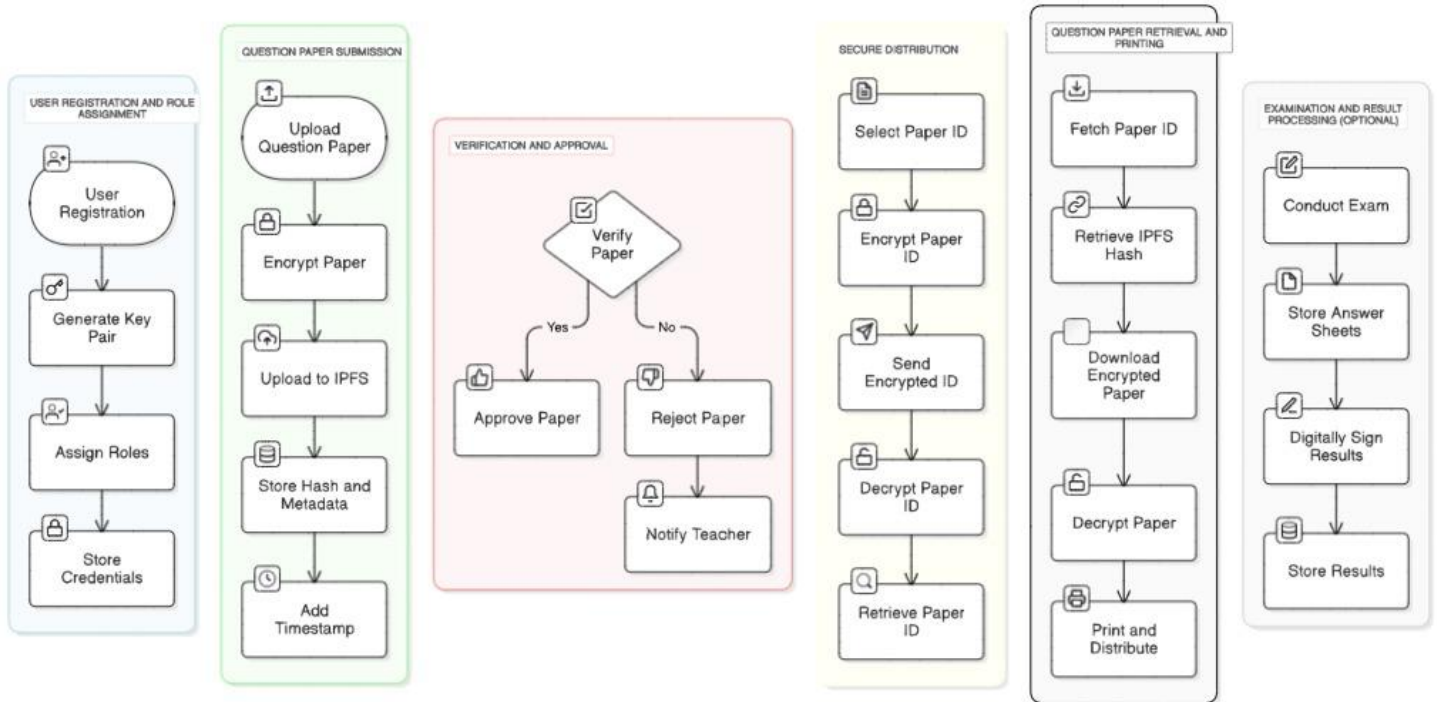
To develop a blockchain-based solution for secure and cost-effective question paper handling.

Objectives

- Secure exam materials with blockchain.
- Encrypt question papers and answer scripts.
- Automate verification with smart contracts.
- Store data securely using decentralized storage.
- Reduce human involvement with encryption.

Block Diagrams/Architecture

ExamVault: Reinventing Examination Security Through Blockchain & Encryption



Modules/Component Description

1. User Registration and Role Assignment

This module handles user authentication and role management within the system.

- Users register in the system, and unique cryptographic key pairs are generated for encryption and security.
- Different roles, such as teachers, examiners, and administrators, are assigned.
- Credentials and role-based access permissions are securely stored.

2. Question Paper Submission

This module ensures the secure submission of question papers by encrypting and storing them on a decentralized system (IPFS - InterPlanetary File System).

- Teachers upload the question paper, which is encrypted before storage.
- The encrypted document is uploaded to IPFS, ensuring tamper-proof storage.
- A unique hash value and metadata are generated for verification.
- A timestamp is added to maintain a record of submission time.

3. Verification and Approval

This module ensures that the uploaded question paper meets security and content guidelines before distribution.

- Examiners verify the integrity of the submitted paper.
- If the paper is valid, it is approved for further processing.
- If rejected, the system notifies the teacher to submit corrections.

4. Secure Distribution

This module ensures the secure transmission of question papers to authorized personnel.

- The Paper ID is selected and encrypted before being shared.
- The encrypted Paper ID is transmitted securely to designated users.
- Authorized users decrypt the Paper ID to retrieve the correct exam paper.

5. Question Paper Retrieval and Printing

This module facilitates the retrieval and printing of exam papers while maintaining security.

- The encrypted Paper ID is fetched for retrieval.
- The corresponding IPFS hash is retrieved to access the stored paper.
- The encrypted paper is downloaded and decrypted securely.
- The decrypted paper is printed and distributed for examination.

6. Examination and Result Processing

This module extends the system to securely conduct exams and store results.

- The examination is conducted based on the securely distributed papers.
- Answer sheets are securely stored for evaluation.
- Results are digitally signed to prevent tampering.
- Final results are stored securely for future reference.
- Examiners verify the integrity of the submitted paper.
- If the paper is valid, it is approved for further processing.
- If rejected, the system notifies the teacher to submit corrections.

Expected Outcomes

1. Enhanced Security in Question Paper Management

- Eliminates risks of question paper leaks through encryption and decentralized storage.
- Ensures tamper-proof storage using IPFS (InterPlanetary File System) and blockchain for immutable records.
- Provides role-based access control, preventing unauthorized modifications or retrievals.

2. Integrity and Transparency in Exam Process

- Timestamped submission and verification prevent unauthorized edits and ensures accountability.
- Audit trails on the blockchain allow tracking of every interaction with the question papers.
- Examiners and authorities can verify question papers without exposing sensitive data.

3. Efficient and Secure Distribution of Question Papers

- Encrypted question paper distribution ensures that only authorized personnel can access them.
- Prevents man-in-the-middle attacks and unauthorized decryption of question papers.
- Reduces dependency on manual paper distribution, minimizing logistical challenges.

4. Fraud Prevention and Tamper Detection

- Digital hashing techniques enable automatic detection of any modifications or tampering.
- Ensures confidentiality and authenticity of the question paper throughout the process.
- Blockchain records serve as evidence in case of disputes or suspected malpractice.

5. Secure Result Processing and Storage

- Enables secure storage of answer sheets using blockchain-based verification.
- Digitally signed results ensure authenticity and prevent grade manipulation.
- Long-term storage of results with immutable records, preventing any unauthorized changes.

6. Reduced Administrative Overhead and Human Errors

- Automation of verification, encryption, and distribution reduces manual intervention.
- Lowers the chance of human errors in handling sensitive examination materials.
- Quick and seamless retrieval of question papers and results through decentralized storage.

References

- [1] Kiwelekar, Arvind & Patil, Yogesh & Deosarkar, Shankar & Netak, Laxman. (2021). A Decentralized and Autonomous Model to Administer University Examinations.
DOI: 10.1007/978-981-33-4122-7_6.
- [2] Islam Abhi, Anik & Kader, Md Fazlul & Shin, Soo. (2018). BSSSQS: A Blockchain Based Smart and Secured Scheme for Question Sharing in the Smart Education System.
DOI: 10.48550/arXiv.1812.03917.
- [3] S. Kapse, M. Umalkar, A. Gajbe, K. Vrudhula, R. Gour and S. Telrandhe, "Blockchain Based Solution for Secured Transmission of Examination Paper," *2022 IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, Gunupur, Odisha, India, 2022, pp. 1-6
DOI: 10.1109/iSSSC56467.2022.10051340.
- [4] A. Jain, A. Kumar Tripathi, N. Chandra and P. Chinnasamy, "Smart Contract enabled Online Examination System Based in Blockchain Network," *2021 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2021, pp. 1-7
DOI: 10.1109/ICCCI50826.2021.9402420.
- [5] Chaitanya Damodar Shirke, Dr. Rakhi O. Gupta, Dhanraj Nagesh Chinta, Nashrah Gowalker (2025), Trust Examiner: A Secure, Transparent, Blockchain-Based Examination System, International Journal of Research Culture Society, ISSN(O): 2456-6683, Volume – 9, Issue – 2., Pp.19-27
DOI: 10.2017/IJRCS/202502004.
- [6] Muneeb, Muhammad & Raza, Zeeshan & Haq, Irfan & Shafiq, Omair. (2021). SmartCon: A Blockchain-Based Framework for Smart Contracts and Transaction Management.
DOI: 10.1109/ACCESS.2021.3135562.
- [7] L, Jegatha & Rawal, Bharat. (2019). Secure Online Examination System for e-learning.
- [8] S. Yadav, S. Singh, and A. K. Luhach, "Blockchain-Based Secure Examination System for Educational Institutions," *IEEE Access*, vol. 8, pp. 182855-182866, 2020.
DOI: 10.1109/ACCESS.2020.3028698.
- [9] Schär and Mösl, "Decentralized Autonomous Organizations: Concept, Examples, and Legal Analysis," *Journal of Banking and Financial Law*, vol. 34, no. 1, pp. 1–20, Mar. 2019.
- [10] A. Kumar and R. Gupta, "A Blockchain-Based Smart Contract Towards Developing Secured University Examination System," *Journal of Medical Internet Research*, vol. 23, no. 7, pp. e8284418, Jul. 2021. DOI: 10.2196/8284418.