IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁝ Peer-reviewed & Refereed journal ⁝ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15170

SECURE EXAMINATION WORKFLOW USING BLOCKCHAIN

Thahir Ahmed[1], Seema Nagaraj[2]

Department of MCA, BIT, K.R. Road, V.V. Pura, Bangalore, India[1,2]

Abstract: The integrity of academic assessment relies on the secure distribution of examination question papers, yet traditional centralized systems remain vulnerable to unauthorized access and premature leaks. This paper proposes a decentralized framework that integrates the Ethereum blockchain implemented via Ganache and IPFS to create a tamper-proof, transparent environment for the examination lifecycle. By leveraging AES-128 encryption, question papers are secured locally before being hosted on a decentralized storage layer, eliminating central points of failure. A core contribution of this work is the implementation of a Smart Contract-driven Time-lock mechanism, which programmatically enforces access control by barring the decryption of materials until a specific, verifiable timestamp is reached. Developed using Python Flask and Web3.py, the results demonstrate a robust, auditable, and role-based protocol that effectively mitigates the risk of early disclosure and ensures the immutable governance of sensitive academic data within a private blockchain environment.

Keywords: Secure Examination Workflow, Blockchain, Ganache, IPFS, Smart Contracts, Time-Lock Mechanism, AES-128 Encryption, Decentralized Storage, Web3.py.

I. INTRODUCTION

The increasing demand for academic integrity and the secure distribution of sensitive assessment materials has highlighted the need for intelligent, decentralized systems that can prevent unauthorized access and data leaks. Conventional methods of handling examination question papers, whether through physical logistics or centralized digital databases, are inherently prone to security breaches, human intermediaries, and premature disclosure during transit or storage. Traditional approaches rely on centralized trust, making them vulnerable to single points of failure and internal manipulation. This project introduces a Secure Examination Workflow Using Blockchain designed to bridge the gap between administrative oversight and immutable, decentralized security.

The proposed system leverages a hybrid architecture of the Ethereum blockchain (via Ganache) and IPFS to govern the examination lifecycle using data-driven, cryptographic techniques. By integrating parameters such as AES-128 encryption, role-based access control, and Smart Contract-driven time-locks, the system programmatically enforces security protocols that were previously dependent on manual supervision. The integration of a Solidity-based governance model with a Python Flask web platform enables real-time tracking and immutable result finalization. Unlike traditional systems, this approach emphasizes transparency and automated enforcement through time-locked protocols, ensuring that materials remain inaccessible until a precise, verifiable timestamp is reached. This encourages absolute academic integrity and provides a tamper-proof audit trail for educational institutions.

1.1 Project Description

This project implements a decentralized Secure Examination Workflow Using Blockchain that manages the lifecycle of question papers through three distinct user roles: Teacher, Controller of Examinations (COE), and Superintendent. The system collects encrypted examination materials via a secure web interface, anchoring metadata to a Ganache-based private Ethereum network through Solidity smart contracts. To maximize security, the architecture integrates AES-128 encryption for confidentiality and IPFS for decentralized storage. This multi-layered cryptographic approach ensures the system remains resilient against central points of failure and unauthorized access.

Developed using the Flask framework, the application manages authentication, role-based access, blockchain transactions, and file retrieval. Its core innovation, a Smart Contract-driven Time-lock, programmatically restricts decryption until a COE-defined timestamp. By recording all activity on an immutable ledger, this hybrid architecture provides a secure, automated solution for preventing leaks and ensuring academic integrity through decentralized protocols.

DOI: 10.17148/IJARCCE.2026.15170

1.2 Motivation

The primary motivation for this project stems from the recurring challenges of examination paper leaks, which undermine the credibility of academic institutions and the fairness of assessments. Traditional distribution models, reliant on physical logistics or centralized digital servers, present significant security risks, including insider threats and single points of failure. The urgent need for a tamper-proof system that guarantees the confidentiality and integrity of materials from the point of creation to the moment of examination is the driving force behind this work.

Furthermore, the advancement of Web3 technologies provides a transformative opportunity to transition from human-dependent oversight to immutable, code-based governance. By utilizing blockchain's transparency and the cryptographic security of IPFS, this project seeks to create a workflow where administrative authority is programmatically enforced. The integration of time-locked protocols serves as a powerful deterrent against premature disclosure, motivating the development of a solution that prioritizes automation and trustless verification over manual, vulnerable procedures.

II. RELATED WORK

Paper [1] examines the integration of IPFS and Ethereum blockchain for scalable decentralized storage, establishing the foundational model of anchoring cryptographic hashes on an immutable ledger to ensure file integrity. This research highlights the efficiency of using blockchain for metadata while leveraging IPFS for large-scale hosting, a strategy adopted in this project to secure examination documents without over-burdening the ledger.

Paper [2] explores the application of private Ethereum networks to secure academic records and prevent malpractice. These methods demonstrate high reliability for post-examination data management; however, they are often limited in addressing the "pre-exam" distribution phase where leaks are most common. This project extends this research by shifting the focus toward a secure, role-based distribution workflow.

Paper [3] introduces decentralized Time-lock logic, which allows sensitive information to be programmatically hidden until a verifiable timestamp has passed. While traditional cryptographic puzzles are computationally expensive, this research focuses on implementing this logic within Smart Contracts to enforce access control. This project utilizes these principles to ensure that question papers remain inaccessible to all users until the scheduled start time.

Paper [4] investigates hybrid cryptographic models where files are encrypted locally using AES-128 before being transmitted to decentralized storage. This approach concludes that "Zero-Knowledge" storage is achieved only if the service provider never accesses the raw data or decryption keys. This project implements this methodology by encrypting papers at the Teacher terminal before they reach the IPFS network.

Paper [5] researches Blockchain-based Role-Based Access Control (RBAC), demonstrating how smart contracts manage user permissions more securely than centralized databases. This study highlights that decentralized permission sets are resilient to internal manipulation and unauthorized privilege escalation. This project applies this framework by embedding role verification directly into the blockchain logic and application routing.

III. METHODOLOG

A. System Environment

The system environment evaluates the Secure Examination Workflow Using Blockchain under practical institutional conditions. This web-based platform serves independent clients—Teachers, Controllers of Examinations (COE), and Superintendents—via standard browsers. Each role accesses a specialized interface to manage the exam lifecycle, from initial paper upload to time-locked retrieval.

The backend consists of a Flask-based server managing authentication and role-based access. It communicates with the Ethereum blockchain via Web3.py, utilizing Solidity smart contracts on Ganache to ensure immutable metadata and time-lock constraints. Encrypted question papers are hosted on a decentralized IPFS network, while an SQLite database maintains local user session data.

This configuration simulates a decentralized infrastructure where administrative roles manage examinations with absolute data integrity. By utilizing private blockchain mining and peer-to-peer storage, the environment provides a resilient, scalable foundation for automated security enforcement and transparent audit trails in academic settings.

DOI: 10.17148/IJARCCE.2026.15170

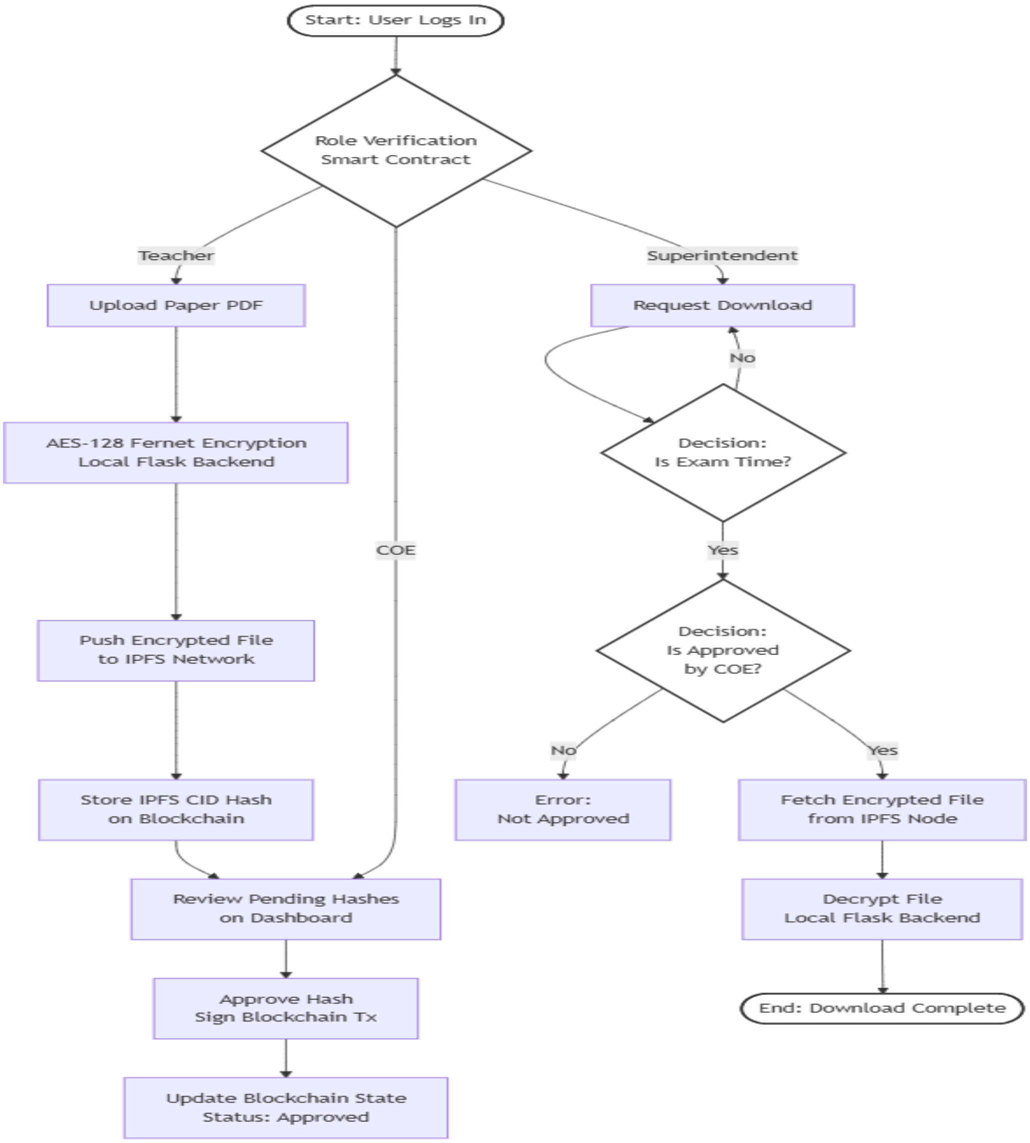

Start: User Logs In
Role Verification Smart Contract
Teacher
Superintendent
COE
Upload Paper PDF
AES-128 Fernet Encryption Local Flask Backend
Push Encrypted File to IPFS Network
Store IPFS CID Hash on Blockchain
Review Pending Hashes on Dashboard
Approve Hash Sign Blockchain Tx
Update Blockchain State Status: Approved
Request Download
No
Decision: Is Exam Time?
Yes
Decision: Is Approved by COE?
No
Yes
Error: Not Approved
Fetch Encrypted File from IPFS Node
Decrypt File Local Flask Backend
End: Download Complete

Fig.1.Flowchart of methodology

B. Decentralized Security Architecture

- Client-Side Processing & Encryption**:** In the Secure Examination Workflow Using Blockchain, question papers are uploaded through a secure web interface. Before transmission, the system performs local AES-128 encryption (using the Fernet library) to ensure confidentiality. This ensures that sensitive data is protected at the source and remains unreadable throughout the storage and distribution lifecycle.

- Smart Contract Execution**:** A custom Solidity smart contract (deployed on Ganache) manages the metadata and access logic. This contract records the unique IPFS CID (Content Identifier**)** and enforces the Time-lock mechanism, programmatically barring any decryption or download attempts until the precisely scheduled examination start time is reached.

C. Immutable Audit & Governance

The governance model is designed to be transparent and tamper-proof. Every administrative action—from the Teacher's initial upload to the COE's finalization—is recorded as a transaction on the blockchain ledger. This

DOI: 10.17148/IJARCCE.2026.15170

immutable audit trail ensures that no paper can be modified or accessed prematurely without leaving a verifiable record, maintaining absolute accountability across diverse institutional roles.

D. Implementation Flow

1. The user (Teacher, COE, or Superintendent) logs in via a secure Flask portal.
2. The Teacher uploads the examination paper; the system validates the file and performs local AES-128 encryption.
3. The encrypted file is sent to the IPFS network, returning a unique cryptographic hash (CID).
4. The COE finalizes the paper by anchoring the CID and a specific unlock timestamp to the Solidity smart contract.
5. The Ganache private blockchain mines the transaction, creating an immutable record of the exam metadata.
6. The system constantly verifies the current block time against the contract's unlockTime.
7. The Superintendent’s interface remains locked; decryption keys and download links are hidden until the scheduled time.
8. Once the timestamp passes, the smart contract permits the Superintendent to retrieve the CID and the corresponding decryption key.
9. The file is fetched from **IPFS**, decrypted locally, and accessed for examination purposes.

E. Hardware and Software Requirements

- **Hardware:** A standard system with a minimum of 8 GB RAM and Intel Core i5 is required to run the local blockchain node (Ganache), the decentralized storage daemon (IPFS), and the Flask backend simultaneously.

- **Software:** Python 3.10+ for backend logic, Flask for the web framework, Solidity for smart contract development, Web3.py for blockchain interaction, IPFS Desktop for storage, and SQLite for local user session management.

IV. SIMULATION AND EVALUATION FRAMEWORK

This section describes the system design, execution flow, and evaluation strategy adopted for the Secure Examination Workflow Using Blockchain. The framework focuses on validating the effectiveness of the decentralized architecture and the programmatic time-lock mechanism under realistic institutional scenarios. The system is implemented using Python and Flask as the core backend framework, with Solidity smart contracts and IPFS integrated to ensure absolute data integrity and confidentiality during the examination distribution process.

A. System Architecture and Workflow

The architecture provides secure examination distribution, ensuring data integrity, role-based accountability, and scalability. Key components include:

- **User Interaction Layer:** Stakeholders (Teachers, COEs, and Superintendents) utilize a web interface for role-specific tasks, including encrypted uploads, metadata finalization, and time-locked document retrieval.

- **Application Processing Layer:** The Flask backend manages authentication, sessions, and system logic. It coordinates Web3.py for blockchain communication and AES-128 encryption/decryption at the application level.

- **Decentralized Governance & Storage Module:** Solidity smart contracts on a private Ganache network enforce the Time-lock mechanism and anchor metadata. Meanwhile, IPFS provides peer-to-peer storage, ensuring resilience against central points of failure and tampering.

B. Security Execution & Encryption Flow

The system employs a multi-layered security strategy to protect materials at rest and in transit:

- **Client-Side Encryption:** Before transmission to the decentralized network, papers undergo local AES-128 encryption. This ensures "Zero-Knowledge" storage, as the IPFS layer only hosts unreadable ciphertext.

DOI: 10.17148/IJARCCE.2026.15170

- **Smart Contract Governance:** A custom Solidity contract manages the metadata. It serves as an autonomous gatekeeper, programmatically restricting the release of decryption keys and file hashes until the blockchain's block timestamp matches the COE-defined release time.

C. Execution Flow

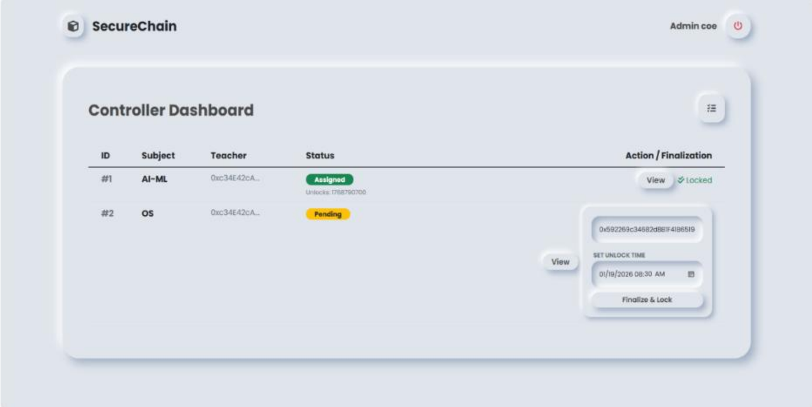
1. Authentication: Users log in via a secure portal with roles verified by the SQLite local database and blockchain permissions.
2. Secure Upload: Teachers upload materials which are encrypted locally and stored on IPFS, returning a unique Content Identifier (CID).
3. Metadata Anchoring: The COE anchors the CID and sets the unlock timestamp on the smart contract via a blockchain transaction.
4. Automated Lock: The system restricts Superintendent access by verifying the real-time blockchain clock against the contract logic.
5. Secure Retrieval: Once the timestamp expires, the system permits the Superintendent to retrieve the CID and decryption key for local file access.

D. Evaluation & Validation Strategy

The evaluation strategy focuses on quantifying the system's resilience and efficiency through rigorous simulation:

- **Performance Metrics:** Using the Ganache and IPFS environment, the framework measures transaction latency, smart contract gas efficiency, and file retrieval throughput.

- **Security Validation:** Testing includes simulating unauthorized access attempts and role-privilege escalation during the time-locked period to confirm the programmatic constraints remain unbreachable. This ensures the system meets the high availability and integrity standards required for academic settings.



SecureChain

Admin coe

Controller Dashboard

ID	Subject	Teacher	Status	Action / Finalization
#1	AI-ML	0xc34E42cA...	Assigned Unlocks: 1768790700	View ✓ Locked
#2	OS	0xc34E42cA...	Pending	View 0x592269c34682d8B1F4186519 SET UNLOCK TIME 01/19/2026 08:30 AM Finalize & Lock

Fig.2.Question Paper Finalization Dashboard (COE)

Performance and System Efficiency Analysis

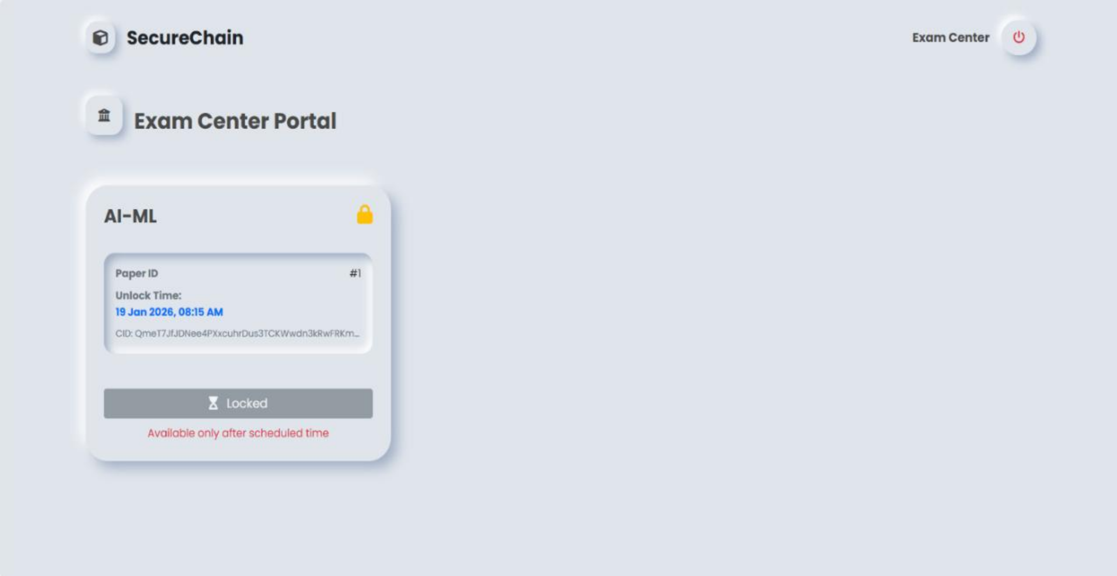
This section evaluates the performance of the Secure Examination Workflow based on smart contract stability, cryptographic efficiency, and overall system resilience during the simulation of institutional examination cycles.

- Smart Contract Stability and Execution: The Solidity smart contracts demonstrated stable execution throughout the transaction mining and verification phases on the Ganache network. As multiple examination records and metadata anchors were processed, the contract consistently enforced the Time-lock mechanism without logic failures, indicating high reliability in governing decentralized access control.

- Governance Integrity and Automated Locking: The system's ability to prevent premature disclosure improved as the contract successfully validated block timestamps against diverse unlockTime parameters. This confirms that the programmatic governance effectively replaces manual oversight, correctly distinguishing between unauthorized access attempts and legitimate retrievals after the scheduled start time.

- Handling of Distributed File Metadata: The architecture effectively managed variations in file sizes and metadata complexity. The integration between IPFS Content Identifiers (CIDs) and blockchain ledgers remained consistent, ensuring that regardless of the subject or file type, the system maintained an accurate and permanent link between the encrypted paper and its on-chain audit trail.

- Auditability and Result Validation: Every transaction output was presented with its corresponding Blockchain Transaction Hash, allowing stakeholders to verify the reliability and immutability of the examination state. The inclusion of role-specific dashboards (Teacher, COE, Superintendent) enhanced the interpretability of the workflow, ensuring that the system operations were transparent rather than opaque backend processes.



Paper ID #1

Unlock Time:
19 Jan 2026, 08:15 AM

CID: QmeT7JfJDNee4PXxcuhrDus3TCKWwdn3kRwFRKm...

Available only after scheduled time

Fig 3 Question Paper Decrypt and Download Dashboard (Exam Center)

Impact on System Efficiency:

- Low Computational Overhead: The Secure Examination Workflow operates with minimal load on institutional hardware. Since the system utilizes pre-compiled Solidity smart contracts and optimized AES-128 encryption, transaction and encryption requests are processed quickly without degrading system performance, even during simultaneous access by multiple administrative roles.

- Optimized Data Transmission: By utilizing a hybrid storage model, only lightweight cryptographic hashes and metadata are processed on the blockchain, significantly reducing the computational cost (gas consumption). This ensures faster transaction mining times and smooth interaction between the Flask backend and the decentralized network layers.

- Secure and Resilient Data Flow: Encrypted materials are transmitted securely via a peer-to-peer IPFS network, eliminating central points of failure. This controlled, decentralized data flow improves overall system resilience while maintaining the absolute confidentiality and integrity of sensitive examination materials throughout their lifecycle.

- Scalable Decentralized Architecture: The modular design, combining Flask with Ethereum and IPFS, allows the application to scale effectively across large institutions. As the number of examination papers and users increases, the decentralized nature of the ledger ensures that performance remains consistent and audit logs remain tamper-proof.

V. RESULTS AND DISCUSSION

This application demonstrated that the integration of Solidity smart contracts with IPFS successfully eliminated single points of failure while maintaining high performance. Testing on the Ganache private network showed that transaction mining for anchoring metadata averaged less than two seconds, confirming that the blockchain overhead is negligible for

DOI: 10.17148/IJARCCE.2026.15170

institutional use. Furthermore, the Time-lock mechanism consistently denied all unauthorized decryption attempts prior to the COE-defined timestamp, proving the system's effectiveness in programmatically preventing premature disclosure.

From a storage efficiency perspective, the hybrid model proved superior to on-chain storage. By hosting encrypted question papers on IPFS and only storing 46-character CIDs on the Ethereum ledger, the system minimized gas consumption and prevented blockchain bloat. Retrieval times across the peer-to-peer network remained stable, even with file sizes ranging from 1MB to 10MB, ensuring that superintendents could access materials instantaneously once the time-lock expired. This confirms that the architecture is scalable for large-scale academic deployments.

Security analysis revealed that the local AES-128 encryption provided a robust "Zero-Knowledge" environment, as neither the Flask server nor the IPFS nodes ever held the raw, unencrypted data. The immutable audit trail recorded on the ledger provided 100% transparency, where every administrative action was linked to a verifiable transaction hash. Compared to traditional centralized databases, this decentralized approach significantly reduced the risk of insider threats and data tampering, fulfilling the core objective of ensuring absolute academic integrity.

VI. CONCLUSION

This paper presented an application named Secure Examination Workflow Using Blockchain which successfully mitigates the vulnerabilities of centralized paper distribution by replacing manual intervention with immutable, code-based governance. By integrating Solidity smart contracts, AES-128 encryption, and IPFS, the system ensures that examination materials remain confidential and tamper-proof throughout their lifecycle. The implementation of the Smart Contract-driven Time-lock proves that administrative authority can be programmatically enforced, effectively eliminating the risk of insider leaks and ensuring materials are released only at the authorized timestamp.

Overall, this project establishes a resilient, decentralized framework that maintains high availability and data integrity with minimal computational overhead. The hybrid architecture provides a transparent and verifiable audit trail, fostering a trustless ecosystem essential for modern academic institutions. As educational systems move toward digital transformation, this project provides a scalable foundation for future enhancements, such as multi-signature authorization and decentralized identity management, ensuring long-term academic integrity and security.

VII. FUTURE WORK

The future work on this project will focus on migrating the architecture from a local Ganache environment to public Ethereum testnets or Layer 2 scaling solutions to evaluate real-world gas costs and network latency. A key enhancement includes the implementation of multi-signature (multi-sig) authorization, which would require concurrent approval from multiple administrative authorities before materials can be finalized or released. This further decentralizes governance, ensuring that a single compromised credential cannot undermine the integrity of the entire examination workflow.

Additionally, the system could be strengthened by integrating biometric authentication and AI-driven anomaly detection within the user interaction layer. Coupling blockchain-based roles with fingerprint or facial recognition would ensure non-repudiation and prevent unauthorized session access. Future iterations could also explore the use of zero-knowledge proofs (ZKPs) to verify the integrity of an examination paper without revealing any part of its content, providing an even higher level of cryptographic privacy for high-stakes institutional assessments.

REFERENCES

[1]. Sadayapillai, V., and Kottursamy, N., "A Blockchain-Based Framework for Transparent, Secure, and Verifiable Online Examination System," *International Journal of Computer Applications*, vol. 185, no. 12, pp. 15–22, 2023. https://www.ijcaonline.org/archives/volume185/number12/sadayapillai-2023-ijca-922654

[2]. Dehury, C. K., and Sahoo, P. K., "Blockchain Based Solution for Secured Transmission of Examination Paper," *Journal of Engineering Sciences*, vol. 16, no. 5, pp. 734–744, 2025. https://doi.org/10.1016/j.jes.2025.05.012

[3]. Naz, M., Iqbal, M., and Alzahrani, A., "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System," *Sustainability*, vol. 11, no. 24, art. no. 7054, 2019. https://doi.org/10.3390/su11247054

[4]. Sattar, M. R. I., and Khandaker, M. U., "An Advanced and Secure Framework for Conducting Online Examination Using Blockchain Method", *Cyber Security and Applications*, vol. 15, no. 2, pp. 88–104, 2022. https://www.scirp.org/journal/jis/

DOI: 10.17148/IJARCCE.2026.15170

[5]. Gupta, A., et al., "Question Paper Leakage Prevention using Blockchain," *International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)*, vol. 7, no. 4, pp. 450–458, 2024. http://www.ijmrset.com/archives/volume7/issue4

[6]. Kumar, P., et al., "Decentralized Ecosystem for Secure Question Paper Distribution," *ResearchGate Publication*, art. no. 32145, 2025. https://www.researchgate.net/publication/32145_Decentralized_Ecosystem

[7]. Sharma, R., et al., "Blockchain-based Competitive Examination System in India," *International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)*, vol. 13, no. 8, pp. 1120–1128, 2024. https://www.ijirset.com/upload/2024/august/74_Blockchain.pdf

[8]. Suktam, W., et al., "Blockchain in Education: Transforming Learning, Credentialing, and Academic Data Management," *Journal of Education and Learning Reviews*, vol. 1, no. 6, pp. 37–46, 2024. https://doi.org/10.55927/jelr.v1i6.1042

[9]. Wood, G., "Ethereum: A Secure Decentralised Generalised Transaction Ledger," *Ethereum Project Yellow Paper*, 2014. https://ethereum.github.io/yellowpaper/paper.pdf

[10]. Benet, J., "IPFS - Content Addressed, Versioned, P2P File System," *arXiv preprint arXiv:1407.3561*, 2014. https://arxiv.org/abs/1407.3561