IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

SecureNEET: A Blockchain-Enabled, AI-Powered Examination Management and Learning Platform

Angel Mariya P J[1], Anupama M V[2], Devika M A[3], Fathima Shabnas U T[4], Sibi Sasidharan[5], Anjitha P[6]
Student, Department of Computer Science and Engineering[1,2,3,4]
Assistant Professor, Department of Computer Science and Engineering[5,6]
Thejus Engineering College, Thrissur, Kerala, India

Abstract: *Question paper leakage threatens the credibility of national-level examinations such as the National Eligibility cum Entrance Test (NEET). Conventional systems rely on centralized storage and manual distribution of papers, exposing them to insider threats, cyberattacks and early access, while students depend on several disconnected platforms for preparation. This paper presents SecureNEET, a blockchain-enabled, AI-powered examination management and learning platform with an Admin web application, an Exam Center web application and a Student Flutter mobile application sharing a Django backend and a MySQL database. Random NEET-format papers are generated from a Question Bank populated with Admin-approved, AI-generated questions. Each paper is protected with SHA-256 hashing and AES-256-CBC encryption, bound to an auto-decrypt time, and its hash and a unique QR token are recorded on an Ethereum blockchain through a Solidity smart contract. An Exam Center can download a paper only after the release time and after QR and 6-digit email OTP verification, and every attempt is logged for the Admin. Students are verified using face recognition with 128-dimensional dlib ResNet embeddings and ID proof, and login activity is monitored by rule-based anomaly detection. The Student application provides a Retrieval-Augmented Generation (RAG) chatbot, AI quick-revision summaries, AI mock tests and previous-year papers. SecureNEET thus combines secure examination management with continuous student preparation in a single platform*

Keywords: Blockchain, Question Paper Security, Face Recognition, Retrieval-Augmented Generation, AES-256, Examination Management, NEET

I. INTRODUCTION

The credibility of a competitive examination rests on the confidentiality of its question paper until the scheduled time. Leakage gives some candidates an unfair advantage and can lead to cancellation of the examination, financial loss, legal action and loss of public trust. Recent incidents involving NEET question papers have raised serious concern among students, institutions and authorities.

Most examination management systems focus on registration, scheduling, paper distribution and results. Papers are typically held on centralized servers and distributed manually, login relies mainly on a username and password, student identity is checked manually against ID documents, and there is no tamper-evident proof that a paper has not been altered. These practices leave the system exposed to insider threats, compromised credentials, impersonation and accidental exposure.

Advances in blockchain, cryptography, computer vision and generative AI can address these weaknesses. A blockchain provides an immutable record for integrity verification, strong encryption with time-locked release prevents early access, face recognition reduces impersonation, and AI reduces the effort of building a large question bank while supporting students with doubt solving, revision and practice [1]–[3].

This paper presents SecureNEET, designed around the NEET workflow. The main contributions are:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, November 2026 Impact Factor: 8.2

- Random NEET-format paper generation (Physics, Chemistry, Botany and Zoology) without question repetition, from an AI-assisted, Admin-reviewed Question Bank.
- Paper protection using SHA-256 hashing, AES-256-CBC encryption and a time-bound auto-decrypt mechanism, with the paper hash and a unique QR token recorded on an Ethereum smart contract.
- Controlled paper release at Exam Centers using release-time checking, QR verification and 6-digit email OTP, with every failed or early attempt logged for the Admin.
- Student verification using face recognition and ID proof, and rule-based login anomaly detection.
- An integrated Flutter student application with a RAG chatbot, AI quick revision, AI mock tests and previous-year papers.

The rest of the paper is organized as follows. Section II reviews the literature, Section III describes the system design, and Section IV concludes the work and outlines future scope.

II. LITERATURE SURVEY

We reviewed twenty studies published between 2021 and 2026. They are grouped below by the problem they address and summarized in Table I.

TABLE I: SUMMARY OF REVIEWED LITERATURE BY THEME

Theme	Refs.	Typical limitation
Blockchain-based paper protection	[1], [3], [7], [8], [10]–[13], [15], [20]	No face or ID check at the center; mostly no AI question selection or learning support
Biometric and AI-based proctoring	[2], [4]–[6], [14], [16]	Mostly online exams; off-browser cheating undetected or in-browser proctoring can be disabled
Anomaly monitoring	[18]	Tested on only about 550 synthetic logs
Reviews and result management	[9], [17], [19]	Theoretical or results only; no pre-exam paper protection

A. Blockchain-Based Paper Protection

Farhan et al. propose ASSURE-EXAM, combining Ethereum smart contracts, IPFS and time-lock release [1]. Abid et al. combine AES encryption, IPFS and time-locked smart contracts [3], and Yadav et al. use a private Ethereum chain with AES-256, IPFS, role-based access and multi-signature authentication [7]. Rahman et al. combine blockchain, digital signatures, hashing and one-time access codes [8], Kapse et al. transmit encrypted papers over blockchain and IPFS [11], and Tejashwini et al. use encryption, blockchain and time-locked access [10], with AI-generated papers via the Cohere API and client-side key handling in [12]. Pranathi et al. compare the gas efficiency of Hardhat and Truffle [13], Ahirrao et al. use Ethereum hashing with device fingerprinting that can be spoofed [15], and [20] uses Ethereum, IPFS, AES-128 and time-locks. None of these includes face-based student verification at the examination center.

B. Biometric and AI-Based Proctoring

Chaudhari et al. integrate blockchain with OpenCV face recognition [4], and Zhu and Cao combine biometrics, encryption and blockchain [6]. Fidelia uses behavioural monitoring and periodic face checks, which cannot detect off-browser cheating [5]. Wang et al. use YOLOv12 with Hyperledger Fabric and IPFS [14], and Mourya et al. use browser-based TensorFlow proctoring that a skilled candidate could disable [16]. Rama Krishna combines deep learning question generation, biometrics and blockchain but does not address centre-specific verification [2]. These works mostly target online examinations rather than pre-examination paper protection at physical centers.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

C. Anomaly Monitoring

Jalandanki and Devi use Isolation Forest anomaly detection with blockchain and IPFS for question paper leakage prevention, but test it on only about 550 synthetic logs [18].

D. Reviews and Result Management

Farooq et al. review blockchain-based online examination assessment models, all of them theoretical [17]. Abdelsalam et al. [9] and ParikkhaChain [19] address online exam data and results rather than paper protection.

E. Research Gaps Identified

The review reveals the following gaps.

1. No face and ID verification at the center. Blockchain-based paper protection works [1], [3], [7], [8], [10]–[13], [15], [20] provide no face-based or centre-level identity check of the student.

2. Online focus instead of pre-examination protection. Proctoring and biometric studies [4]–[6], [14], [16] mostly target online examinations, and [9], [19] address results rather than paper protection.

3. Limited AI support. AI-generated questions appear only in [2] and [12], the latter without server-side key storage, and none of the reviewed works offers integrated learning support such as doubt solving, revision and practice.

4. Weak monitoring and robustness. Off-browser cheating goes undetected [5], device fingerprinting can be spoofed [15], in-browser proctoring can be disabled [16], and anomaly detection has been tested on only about 550 synthetic logs [18].

5. Theoretical or partial treatment. One review finds all models theoretical [17], and [13] compares only gas efficiency, so complete implemented workflows remain scarce.

SecureNEET addresses these gaps by combining time-locked paper release, QR and OTP verification, face and ID verification at the center, login anomaly monitoring and integrated AI-based learning support in one platform.

III. DESIGN

A. System Architecture

SecureNEET has three client modules: an Admin web application, an Exam Center web application and a Student Flutter mobile application. Every client communicates only with a central Django backend, which applies the security rules, accesses the data stores and calls external services (Fig. 1). The backend contains modules for authentication and role management, question bank and exam management, AI question generation, random paper generation, AES-256 encryption and SHA-256 hashing, QR token verification, face recognition and ID verification, login anomaly detection, notifications, the RAG chatbot, and AI summary and mock tests. It connects to a MySQL database, an Ethereum blockchain through a Solidity smart contract, Google Gemini for question generation, and a local Ollama service for RAG-based learning. The encrypted paper stays in MySQL, and only its hash and QR token are stored on the blockchain.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

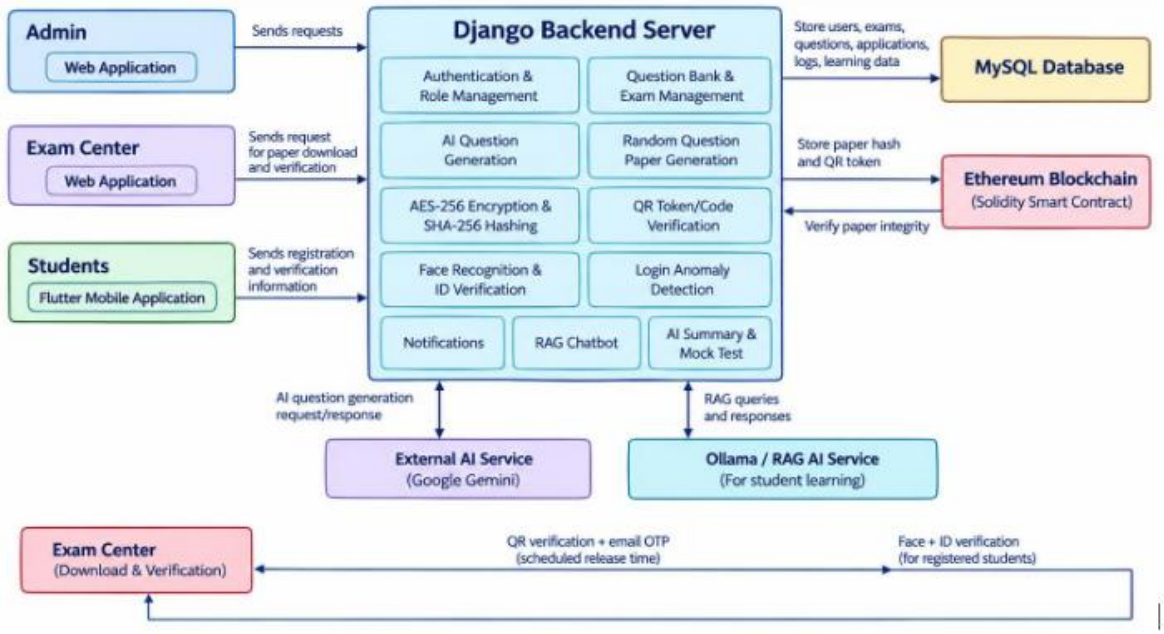


Fig. 1. System architecture of SecureNEET.

B. Question Bank and AI Question Generation

The Admin builds the Question Bank manually or uploads study material as text or PDF so that Google Gemini generates NEET-style multiple-choice questions. Near-duplicate questions are removed, and only questions approved by the Admin are added, so the quality of AI output is controlled by human review.

C. Paper Generation, Encryption and QR Token

For a chosen examination, the Admin supplies the number of questions per subject and the release time. The system selects questions randomly across Physics, Chemistry, Botany and Zoology without repetition, computes the SHA-256 hash of the paper, and encrypts it with AES-256-CBC using a random initialization vector. A unique QR token and QR code are created and an auto-decrypt time is bound to the paper. The encrypted paper is stored in MySQL, and the hash and QR token are recorded on the Ethereum blockchain through the QuestionPaperStorage smart contract.

D. Controlled Paper Download

On examination day the Exam Center can download the paper only when three checks pass: (i) the current time is at or after the release time, (ii) the QR token matches the stored paper and the blockchain record, and (iii) the 6-digit email OTP matches its stored hash and is within its 5-minute validity. Failed QR, OTP and early-access attempts are logged and visible to the Admin, and only successful verification unlocks the decrypted paper.

E. Student Verification

At the center, a live image is compared with the registered face image using 128-dimensional embeddings from the dlib ResNet model, together with ID proof verification. Image quality checks are applied, and the match score and verification status are stored.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

F. Login Anomaly Detection

Login attempts are logged and analysed by two rules: three or more failed attempts from one IP address within 30 minutes, or five or more failed attempts against one username within one hour, are flagged as suspicious. Role-based access control restricts each user to their own functions.

G. Student Learning Module

The Flutter application supports registration, examination application, admit card, notifications and complaints. Its learning features use a locally hosted language model through Ollama: a RAG chatbot answers doubts from the stored study material, quick-revision summaries are generated with an extractive fallback, mock tests default to 10 questions with 4 marks per correct answer and give improvement suggestions, and previous-year papers can be downloaded.

H. Data Flow

Fig. 2 shows the Level 0 (context) diagram, in which SecureNEET is a single process exchanging data with four external entities. The Admin sends the exam details (question count and release time), study material, and approval and allocation decisions, and receives the attempt logs that form the audit trail; the Exam Center sends the QR token, OTP and live image and receives the decrypted paper and the verification result; the Student sends registration and verification information, applications and study questions, and receives the admit card, notifications, results and learning content; and the Ethereum smart contract receives the paper hash and QR token and returns the token check.

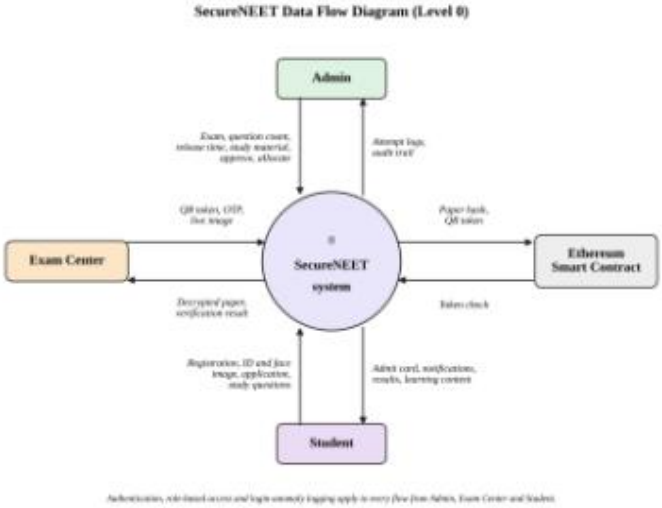


Fig. 2. Level 0 data flow diagram of SecureNEET.

Fig. 3 shows the Level 1 data flow diagram, which decomposes this context diagram into six processes: paper generation, encryption and QR token (1.0); paper download verification (2.0); student verification (3.0); question bank and AI question generation (4.0); application and allocation management (5.0); and student learning (6.0). All processes read and update the MySQL database, and authentication with login-anomaly logging applies to every user flow.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

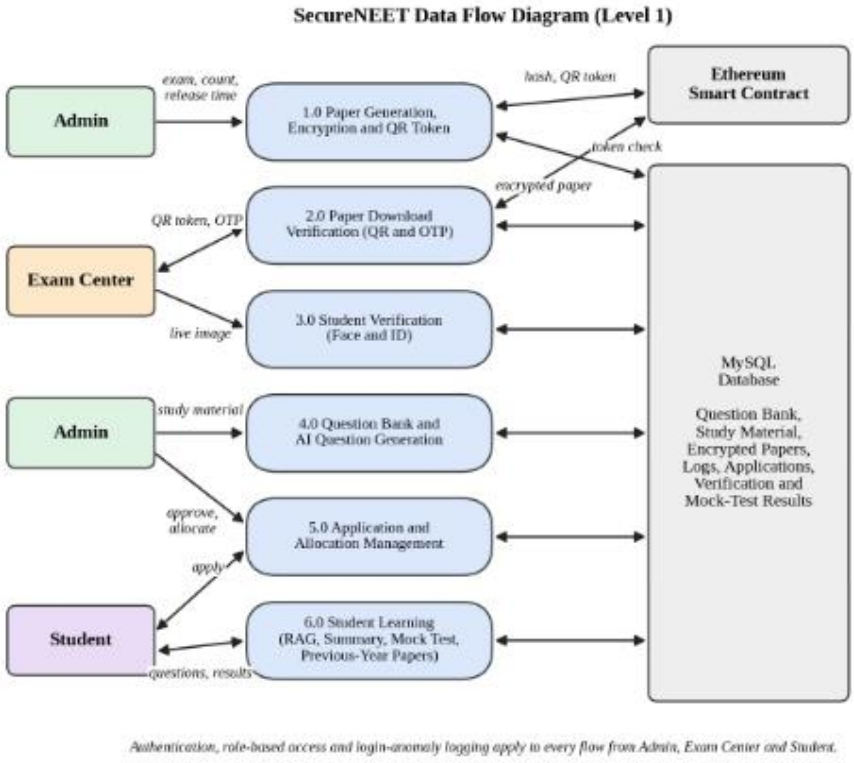


Fig. 3. Level 1 data flow diagram of SecureNEET.

I. Implementation Environment

The Admin and Exam Center modules are Django 4.2 web applications (function-based views), and the Student module is a Flutter (Dart) Android application using the same backend. Table II lists the main technologies and Table III the main security parameters.

TABLE II: IMPLEMENTATION TECHNOLOGIES

Component	Technology
Backend	Python 3, Django 4.2
Database	MySQL
Frontend	HTML5, CSS3, JavaScript
Mobile app	Flutter, Dart (Android)
Blockchain	Ethereum, Ganache, Solidity, Remix IDE, Web3.py
Cryptography	AES-256-CBC, SHA-256
Face recognition	face_recognition (dlib ResNet), OpenCV, NumPy
Email OTP	Django SMTP, Gmail, port 587, TLS
AI questions	Google Gemini, google-genai SDK, pypdf
RAG chatbot	Ollama local LLM, study material base

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

TABLE III: SECURITY AND SYSTEM PARAMETERS

Parameter	Value
Paper encryption	AES-256-CBC, random IV
Paper integrity	SHA-256 hash on blockchain
Email OTP	6 digits, valid 5 minutes
Face embedding	128-dimensional
Failed login (IP)	3 or more in 30 min
Failed login (user)	5 or more in 1 hour
Mock test default	10 questions, 4 marks each

J. Security Analysis

Premature access is blocked at three layers: the paper is encrypted at rest, decryption is bound to the release time, and download needs both the QR token and a fresh email OTP. Because the hash is on the blockchain, any change to the stored encrypted paper is detectable. Random generation without repetition reduces predictable patterns, and logging of all failed attempts gives the Admin an audit trail. Face recognition with ID proof reduces impersonation compared with manual checking.

IV. CONCLUSION AND FUTURE WORK

This paper presented SecureNEET, a blockchain-enabled, AI-powered platform that protects NEET question papers before the examination, verifies the people involved and gives students an integrated learning environment. Time-locked release, QR and OTP verification and the blockchain integrity record ensure that a paper cannot be read or silently altered before the permitted time, and every attempt is logged for the Admin. The system has limitations: the blockchain layer runs on a Ganache local testnet, AI-generated question quality depends on Admin review, face recognition has no liveness detection, RAG retrieval is not yet vector-database based, anomaly detection is rule-based, and stable internet is required. Quantitative evaluation of face matching, chatbot quality and system load is left for the next phase. Future work includes deployment of the smart contract on a public test network or permissioned blockchain, IPFS storage and digital signatures, liveness detection for face recognition, a vector database for RAG retrieval, multilingual support, SMS-based OTP, machine-learning anomaly detection, personalised study plans, and backend scaling for large numbers of students and centers.

REFERENCES

[1]. M. Farhan, M. Rajapakshe, R. B. Sulaiman and U. Butt, “Assure-Exam: A Blockchain-Based Assurance Framework for Secure and Transparent Exam Paper Distribution,” in 2025 Annual Computer Security Applications Conference Workshops (ACSAC Workshops), Honolulu, HI, USA, Dec. 2025, pp. 323–331, doi: 10.1109/ACSACW69556.2025.00042.

[2]. M. B. Rama Krishna, “A Blockchain-Integrated Decentralized Examination Framework with Deep Learning-Driven Question Generation and Intelligent Proctoring,” 2026.

[3]. T. Abid, A. K. Khan, M. J. Quadri and M. F. Ul Haq, “An Enhanced Security Model for Digital Exams: AES Encryption with Smart Contract-Based Access,” 2025.

[4]. M. A. Chaudhari, K. S. Ghodake, P. S. Aher and A. S. Borade, “Enhancing the Reliability and Security of Online Exam Systems Using Blockchain Technology,” 2025.

[5]. N. O. Fidelia, “A Risk-Aware Privacy-Preserving Online Examination System Using Behavioral Anomaly Detection Using Blockchain Technology,” 2026.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

[6]. X. Zhu and C. Cao, "Secure Online Examination with Biometric Authentication and Blockchain-Based Framework," 2021.
[7]. G. Hemanth Kumar Yadav, K. Adithya, T. Ehshanulla, M. Mokshith Srinivas Yadav and Y. Gowrishankar, "Blockchain-Powered Question Paper Leakage Prevention System," in Proc. ICRDICCT'25, SciTePress, 2025, pp. 701–706, doi: 10.5220/0013888700004919.
[8]. S. M. T. Rahman, M. N. Iftekhar, R. Alam, S. M. R. Gafur and D. Nandi, "Secured Question Paper Management System," AIUB Journal of Science and Engineering (AJSE), vol. 20, no. 1, pp. 25–32, Apr. 2021.
[9]. M. Abdelsalam, M. Shokry and A. M. Idrees, "A Proposed Model for Improving the Reliability of Online Exam Results Using Blockchain," IEEE Access, vol. 12, pp. 7719–7733, 2024, doi: 10.1109/ACCESS.2023.3304995.
[10]. Tejashwini et al., encryption, blockchain and time-locked access for question paper protection, 2026.
[11]. Kapse et al., "Blockchain Based Solution for Secured Transmission of Examination Paper," IEEE conference, Gunupur, Odisha, India, Dec. 15–17, 2022.
[12]. Y. Tejashwini, M. Farzanula, Nikhil S and S. A. Khan, "Question Paper Leakage Protection Using Blockchain," Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng. (IJIREEICE), vol. 13, no. 9, Sep. 2025, doi: 10.17148/IJIREEICE.2025.13904.
[13]. Pranathi et al., three-layer blockchain examination framework with IPFS and Hardhat vs. Truffle gas comparison, 2025.
[14]. H. Wang, Z. Shukur, K. A. Z. Ariffin, R. Xiao and L. Wang, "Online Exam Cheating Detection and Blockchain Trusted Deposit Based on YOLOv12," Sci. Rep., vol. 15, Art. no. 33236, Sep. 2025, doi: 10.1038/s41598-025-18412-0.
[15]. Ahirrao et al., Flask and SQLite examination system with Ethereum hashing, question shuffling and device fingerprinting, 2026.
[16]. Mourya et al., "SecureQuest": encrypted question bank with IPFS, Polygon blockchain and TensorFlow-based AI proctoring, 2026.
[17]. M. S. Farooq, R. Tehseen et al., "Blockchain Based Online Examination Assessment Models for Educational Institutes: A Systematic Literature Review," VFAST Trans. Softw. Eng., 2021.
[18]. Jalandanki and Gayathri Devi, blockchain, IPFS and Isolation Forest anomaly detection for question paper leakage prevention, 2025.
[19]. R. J. I. Momin, A. M. S. Rumi and R. Reaz, "ParikkhaChain: Blockchain-Based Result Processing and Privacy-Preserving Academic Record Management for the Complete Examination Lifecycle," arXiv:2604.16827, Apr. 2026.
[20]. Secure examination workflow using blockchain with Ethereum, IPFS, AES-128 and smart-contract time-locks, 2026.