Safe Assessment Chain - Integrating Blockchain for a Secure Examination Process

Varsha Dange  
*Depatment of Information Technology*  
*Vishwakarma Institute of Technology*Pune, India  
varsha.dange1@vit.edu Suraj Chavan  
*Depatment of Information Technology*  
*Vishwakarma Institute of Technology*Pune, India  
suraj.chavan22@vit.edu

Bhairavi Shirsath   
*Department of Information Technology*  
*Vishwakarma of Technology*Pune, India  
bhairavi.shirsat23@vit.edu

Ishan Shivankar   
*Department of Information Technology*  
*Vishwakarma of Technology*Pune, India  
ishan.shivankar22@vit.edu

Tanishk Shrivastava   
*Department of Information Technology*  
*Vishwakarma of Technology*Pune, India  
tanishk.shrivastav22@vit.edu

Prathmesh Sonawane  
*Depatment of Information Technology*  
*Vishwakarma Institute of Technology*Pune, India  
prathmesh.sonawane22@vit.edu

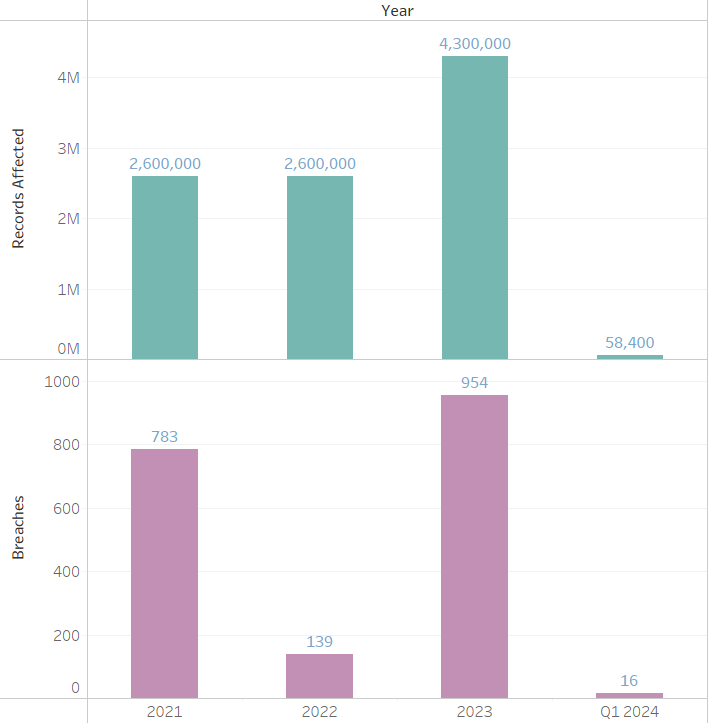
*Abstract*— The rapid digitization in the education sector has increased the need for examination systems that are secure, tamper-proof, and transparent. In this paper, we present the Safe Assessment Chain, a novel framework that employs blockchain technology with improved encryption techniques to address critical issues in examination processes. Utilizing the application of the Ethereum blockchain and smart contracts developed using Solidity, the proposed framework ensures data integrity and transparency of examination-related information, including question papers, student logs, and results. Furthermore, the use of the Advanced Encryption Standard (AES) algorithm ensures an added security layer for sensitive information, such as image and text content, thereby ensuring protection against unauthorized access and likely breaches. The system architecture facilitates effective storage and retrieval of critical information, ensuring effectiveness and reliability. Performance analyses validate the robustness of the system, with an emphasis on its ability to ensure data integrity, improve security, and operate effectively against varying operational loads. The Safe Assessment Chain opens the door to secure and transparent examination management, with implications far beyond the education sector.

Keywords— Blockchain, AES Encryption, SHA-256 Hashing, Smart Contracts, Secure Transactions, Decentralized Application, Cryptographic Hashing, Transparent Examination

# Introduction

## Problem Statement

In the present digital age, the educational sector relies on technology for various academic and administrative purposes. Such advancement is, however, balanced against the ongoing threats to the traditional systems of examination, which compromise their reliability, security, and transparency. Data breaches are a main concern, where sensitive data, e.g., questions, students' data, and results, are leaked for unauthorized purposes. Fig. 1 shows data over a decade where educational institutions in the United States have experienced 3,713 data breaches compromising over 37.6 million records in K-12 institutions and institutions of higher learning [1, 2, 3]. Such breaches compromise the integrity of the examination process but also incur financial loss for such institutions. For example, in 2023, institutions of higher learning reported an average financial loss of $3.7 million per breach [4, 5].



1. Data Breaches and Records Impacted Over Time

Illegal activities, such as malpractices to inflate examination marks, impersonation, and question paper leakage, also taint the authenticity of conventional examination systems. In a recent survey, 78% of the institutions reported at least one examination-related data breach, and 65% of the students expressed concern about the transparency and fairness of exam scores [6, 7]. Last but not least, the absence of transparency in grading and recording has led to disputes, inefficiency, and stakeholder loss of confidence.

The increasing incidence and intensity of such issues indicate the need for an open, tamper-evident, and secure system that eliminates such vulnerabilities and increases the efficiency of operation. The current reliance on centralized systems worsens the risks as they are prone to single points of failure, unauthorized modifications, and inefficiencies in data processing.

## Objective

To mitigate such problems, in this paper, the Safe Assessment Chain (SAC) is proposed, a novel blockchain-based testing framework for enhancing security, transparency, and efficiency. Through the use of the decentralized and tamper-resistant nature of blockchain technology combined with strong encryption methods, SAC offers a secure alternative to vulnerabilities inherent in traditional systems. The system employs the Ethereum blockchain with smart contracts based on Solidity for ensuring data immutability and transparency, while Advanced Encryption Standard (AES) algorithm protects sensitive data, such as question papers and exam marks, from unauthorized access or leakage.

## Contributions

This paper makes some significant innovations to address the challenges of traditional examination systems:

### **Blockchain-Based Secure Storage**: Question papers, logs, and exam results are stored in a blockchain to ensure data integrity and prevent the challenges of tampering.

### **Advanced Encryption**: AES encryption contributes to the security of sensitive information, protecting images as well as text from unauthorized access and data breaches.

### **Tamper-Proof Logs**: Unchangeable records of students' activity during exams enhance traceability and accountability, fostering trust among stakeholders.

### **Seamless Data Retrieval**: Effective processes for secure and speedy retrieval of information allow institutions to control information smoothly and eliminate operational bottlenecks.

### **Comprehensive Performance Evaluation**: The system has been rigorously tested to measure its latency, scalability, and resilience, demonstrating its ability to support real examination processes.

## Significance of the Study

The Safe Assessment Chain is a paradigm shift in testing and delivery. By solving the main weaknesses of conventional systems, SAC offers a secure environment for educational institutions to maintain academic integrity, guarantee confidentiality of sensitive data, and establish trust among students, teachers, and administrators. This research adds to the wider discussion of the use of new technologies in education, opening the door to future innovations in secure and open academic processes.

# Related Work

Blockchain technology has been a game-changing education tool that solves transparency, security, and trust problems in educational processes. Blockchain technology offers decentralized, tamper-evident solutions to educational requirements such as the security of tests, verification of credentials, and administration of academic information. Various studies have explored the ability of blockchain technology to improve the integrity of tests, data privacy, and scalability issues in the education sector [8, 9].

## **Blockchain in Educational Security and Examination Systems**

Blockchain use in education security has attracted a lot of interest in its capability to offer secure and transparent records. Decentralized Assess: Securing Online Exams through Blockchain offers an online examination system using blockchain that promises security, transparency, and student privacy through the utilization of smart contracts in ensuring secure data transmission [10]. Online Exam Enhancement via Blockchain also explains how blockchain enhances examination data security and integrity, as opposed to standard centralized systems versus decentralized blockchain solutions that promote security against unauthorized users [11].

A general framework of education evaluation management is discussed in Education Evaluation Management Based on Blockchain Technology, highlighting transparency and security in academic examination through blockchain-based systems [12]. Further, Blockchain-Based Examination System for Effective Evaluation presents a peer-to-peer blockchain-enabled examination system to ensure credibility and trustworthiness in assessment history [13].

Blockchain Examination System Online highlights the advantage of blockchain over cloud-based systems, particularly in authentication, secure data storage, and the use of smart contracts to prevent cheating during exams [14]. A more general overview of the use of blockchain in education is provided in Blockchain Technology in Education: A Comprehensive Review, which also addresses its implications for transparency, verification of credentials, and research directions in the future [15].

## **Blockchain and Cryptographic Security in Examinations**

Cryptographic security is critical in blockchain-based examination systems. A Review of Encryption and Decryption of Text Using the AES Algorithm provides a review of AES encryption techniques in securing examination data privacy [16]. Encapsulation of additional development in encryption is covered in Review of the Advanced Encryption Standard System Performance, where performance metrics such as encryption speed and security levels in cloud environments are reviewed [17].

The vulnerabilities of quantum computing are addressed in Exploring AES Encryption Implementation Through Quantum Cryptography, which discusses AES vulnerabilities to quantum attacks and proposes quantum-resistant encryption methods [18]. Implementation of Optimizing Advanced Encryption Standard in Vehicle Communication discusses optimizations in AES for quicker encryption and enhanced security [19]. Furthermore, A Comprehensive Study on AES and Diffie-Hellman Encryption discusses the combination of AES with other cryptographic protocols for enhanced data security in cloud and distributed systems [20].

## **Challenges and Future Directions in Blockchain-Based Educational Systems**

Though it has the benefits, education's adoption of blockchain is fraught with challenges of scalability, interoperability, and regulation. Academic studies such as Blockchain Applications in Education: A Systematic Literature Review [21] and Blockchain Adoption in Education: A Systematic Literature Review [22] recognize scalability concerns and propose the use of hybrids to optimize rate of transactions with no loss in security.

Another potential future direction is the combination of blockchain and artificial intelligence (AI), as outlined in Artificial Intelligence and Blockchain in Higher Education Institutions: A Systematic Literature Review, which explains how AI-powered smart contracts can be used to facilitate student participation and collaborative learning [23]. Blockchain and Machine Learning in Education: A Literature Review also explores machine learning methods to improve blockchain-based learning solutions [24].

Scalability issues remain a persistent issue, such as in Scalability Challenges and Solutions in Blockchain Technology, which suggests alternative consensus mechanisms to enhance blockchain performance [25]. Similarly, Challenges of Using Blockchain in the Education Sector identifies privacy of information and regulatory compliance as major barriers to widespread adoption [26].

## **Blockchain for Secure Credential Verification**

Blockchain's application in secure verification of academic credentials is established. Education and Blockchain – UNESCO Digital Library confirms blockchain's capacity to avoid forgery of credentials and enhance verification processes [27]. Application of blockchain in verification of degrees is examined in A Graduation Certificate Verification Model via Utilization of Blockchain Technology, where it is discussed in the context of application in avoiding certificate forgery [28].

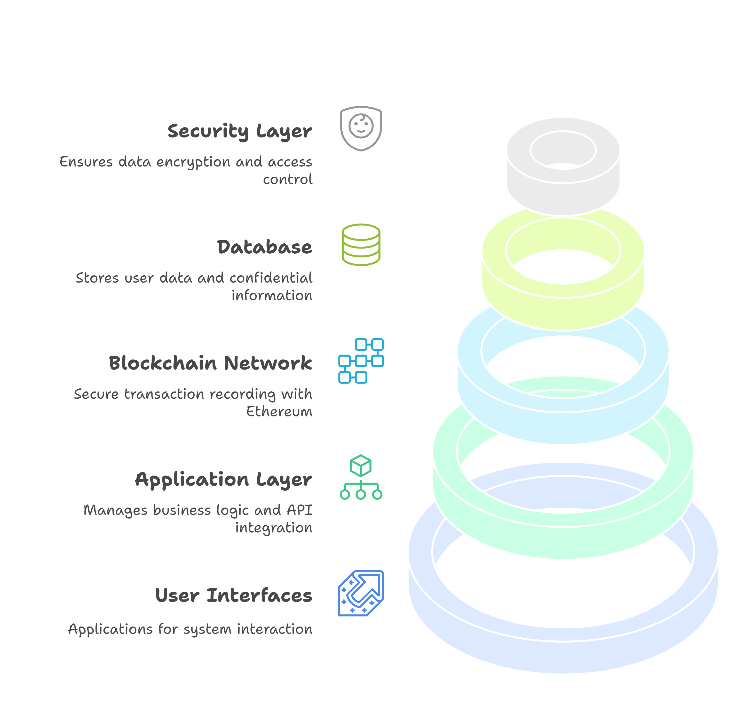
One example of blockchain academic records is found in Kratos: A Secure, Authenticated System for Educational Data Using Blockchain, in which blockchain use is described to provide an immutable ledger for academic information [29].

Blockchain technology has great promise for online examination systems concerning security, transparency, and efficiency. The critique of studies reflects the promise of blockchain to prevent academic dishonesty, improve data secrecy, and automate certificate validation. Scalability, regulatory frameworks, and interoperability are a few of the challenges to be overcome in order to facilitate wide-scale usage. Future studies should incorporate AI, boost performance of blockchain, and overcome legal challenges to facilitate full realization of the promise of blockchain in education security.

# Proposed Method

The system methodology for this project encompasses the design and implementation of a secure and scalable platform using blockchain and encryption technologies. The goal is to ensure secure data handling and user interaction while maintaining a robust and user-friendly interface. The methodology is divided into distinct phases, covering high-level architecture, implementation steps, and technical details.

## High-Level Architecture



1. High Level System Architecture.

Fig. 2 depicts the system architecture, integrating multiple components that ensure secure interactions between clients and administrators.

### **User Interfaces:**

#### Client Interface: A responsive web or mobile application that enables students and faculty to interact with the system. The interface allows users to request, view, and verify certificates.

#### Admin Interface: A comprehensive dashboard for administrators to manage user accounts, approve certificate issuance, and oversee the system's operations.

### **Application Layer:**

#### This layer handles the core business logic for both client and admin operations.

#### It integrates APIs to facilitate seamless interactions with blockchain networks, databases, and encryption services.

### **Blockchain Network:**

#### A Ethereum blockchain is employed to ensure secure, immutable, and transparent transaction records.

#### Smart contracts govern key functionalities such as certificate management, user verification, and transaction handling.

### **Database:**

#### A relational database is used to store user metadata, and non-sensitive information.

#### Encrypted storage mechanisms ensure the protection of sensitive data, such as private keys.

### **Security Layer:**

#### The Advanced Encryption Standard (AES) secures data both in transit and at rest.

#### Role-Based Access Control (RBAC) is implemented to restrict access to specific features and data based on user roles.

## Comprehensive End-to-End Workflow Overview

Fig. 3 depicts the whole process with emphasis placed on the incorporation of blockchain technology, AES encryption, and automatic result and grading processes. The architecture offers an easy and secure test system.

### **Blockchain Setup**

#### Private Ethereum Blockchain Configuration: A private Ethereum blockchain network was configured to create a secure, decentralized environment for managing examination-related information. The configuration enabled immutable and tamper-evident storage of key documents like exam logs and student assignments.

#### Smart Contract Development: Smart contracts, in Solidity, were developed and utilized to automate fundamental functions, such as:

* ***Registration of exams.***
* ***Authentication and registration of students.***
* ***Logging of exam submissions and the publication of results****.*

*These automated contracts ensured open and reliable procedures through the elimination of the need for human intervention.*

### **AES Encryption Integration**

#### Advanced Encryption Standard (AES) Implementation: AES encryption was used in the system for the encryption of sensitive data, e.g., questions in an examination. This encryption technique provided:

* *Confidentiality of data in storage and transmission.*
* *Restrictive access to the material, whereby only authorized individuals with proper decryption keys can access the information.*

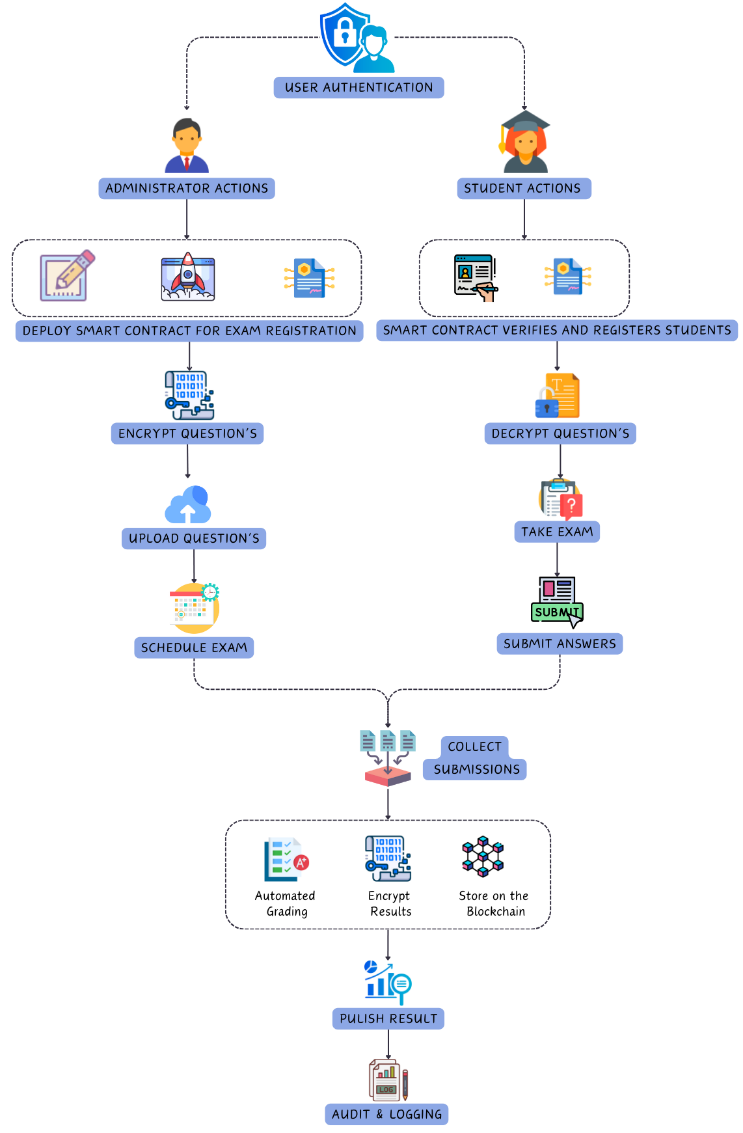
#### Key Management Strategy: Encryption keys were managed with secure practices, including frequent rotation, to minimize risks of unauthorized access. This measure was a key factor in maintaining the overall integrity of examination content.

### **Interaction Between Encryption and Blockchain**

#### Handling Encrypted Data on the Blockchain: Test questions were encrypted using AES and stored off-chain for performance. Cryptographic hashes of the encrypted questions were stored on the blockchain for data integrity and minimal blockchain storage requirements.

#### Secure Decryption Mechanism: During the test, students were provided with encrypted questions. Validated students were provided with secure decryption keys after their identity was confirmed by smart contract logic.

#### Securing Blockchain Interactions: Cryptographic protocols like the Elliptic Curve Digital Signature Algorithm (ECDSA) were used to provide security to blockchain transactions. The protocols offered data integrity and authenticity assurance stored and transferred..



1. Low Level Architecture for Secure Examination Management Using Blockchain and AES.

## Advanced Encryption Standard (AES) with Galois/Counter Mode (GCM)

This part delivers a mathematically stringent explanation of the Advanced Encryption Standard (AES) Galois/Counter Mode (GCM) operation. The process of encryption and decryption is presented in mathematical form using definitions of exacting rigor, and a step-by-step worked example describes the computations undertaken. Emphasis is laid upon the integration of AES encryption, counter mode functionality, and the Galois Message Authentication Code (GMAC) to achieve confidentiality and integrity [30]. Operational uses of AES-GCM for secure communication, including the example of TLS encryption, are further emphasized [31].

### **Introduction**

AES-GCM is a widely employed encryption scheme that is secure and efficient in data transmission [30, 33]. It is a combination of the AES block cipher with a counter-based mode of operation and an authentication mechanism, both of which have strong resistance against cryptographic attacks [31]. The mathematical foundation of AES-GCM is explained in this paper and a rigorous analytical framework is provided.

### **Mathematical Foundation of AES-GCM**

#### AES Encryption

*AES is a symmetric-key block cipher that converts a plaintext block into a ciphertext block using a secret key. Mathematically, AES encryption is represented as:*

*where is the encryption function parameterized by the key .*

*AES operates on a 128-bit block size and employs a series of transformations structured into multiple rounds (10 rounds for 128-bit keys, 12 for 192-bit keys, and 14 for 256-bit keys). These transformations include:*

* ***SubBytes ():*** *A non-linear byte substitution using the Rijndael S-box:*

*where is the substitution table lookup.*

* ***ShiftRows ():*** *A cyclic permutation step shifting bytes within the state matrix:*
* *Row 0: no shift*
* *Row 1: shift 1 byte left*
* *Row 2: shift 2 bytes left*
* *Row 3: shift 3 bytes left*
* ***MixColumns ():*** *A linear transformation involving matrix multiplication over :*

*where is a fixed matrix:*

*over and is the state matrix.*

* ***AddRoundKey ():*** *A bitwise XOR operation with a round key derived from :*

#### **Counter Mode (CTR)**

*AES-GCM employs Counter (CTR) mode to generate a unique keystream for encryption. With a 96-bit IV (recommended), the counter block is structured as:*

* *96-bit IV*
* *32-bit counter, starting from 1*

*where:*

* *is a unique Initialization Vector (96 bits recommended).*
* *is a 32-bit incrementing value per block*
* *denotes bitwise XOR.*

*This approach ensures that each plaintext block is combined with a distinct keystream value, enhancing security.*

#### Galois Message Authentication Code (GMAC)

*The integrity of the encrypted data is verified using GMAC. The authentication tag is calculated as:*

*where:*

* *is the hash function using hash key*
* *is the initial counter value*
* *represents additional authenticated data (AAD)*
* *is the ciphertext*

*The GHASH function operates in with the irreducible polynomial:*

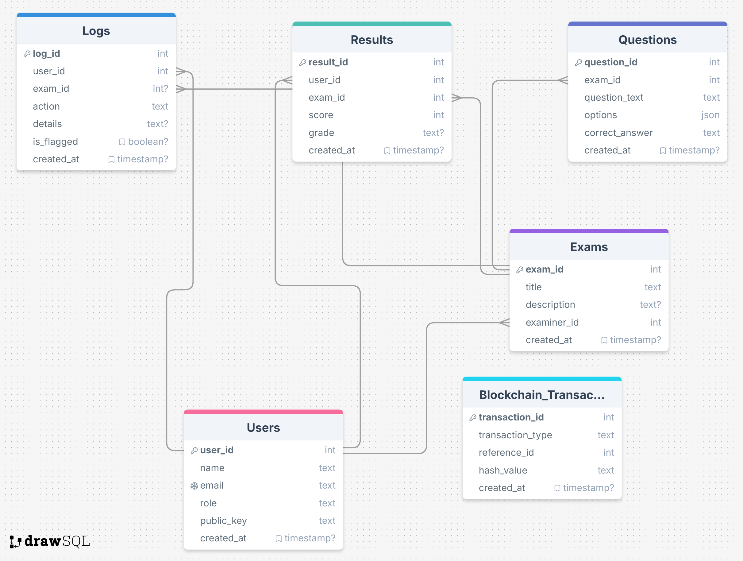
#### Decryption

* *Decryption follows the inverse process of encryption:*
* *The authentication tag is recomputed as:*
* *The tag comparison MUST be performed in constant time to prevent timing attacks:*

AES-GCM provides an authenticated encryption scheme that is secure by combining the security of AES with the efficiency of CTR mode and the authentication property of GMAC [30, 32]. The mathematical model provided ensures confidentiality and integrity of the data to be secured.

## Database Schema of the System

In this section, Fig. 4 illustrates the database schema of the entire blockchain-based secure exam system. The database is designed to ensure seamless interactions between users (examiners and students), exams, questions, results, logs, and blockchain transactions. Each table in the schema has a definite role, and the relationships between the tables ensure data integrity, traceability, and security across the system.



1. Database Schema of the Blockchain-Based Secure Examination System.

### **Users Table**

The User’s table is the main table for holding all data about individuals who are accessing the system. Both the students and the examiners are served by this table with the objective of correct authentication and authorization. The most important columns in this table are:

* ***user\_id****: A user's unique identification number*
* ***name****: The complete user name.*
* ***email****: The email address of the user, to be unique for every entry.*
* ***role****: This is utilized to determine whether the user is a 'student' or an 'examiner' to offer proper access control.*
* ***public\_key****: A secure communication encryption key.*
* ***created\_at****: Date and time when the user record was created.*

This table is used to control user roles and provide secure access to exam content.

### **Exams Table**

Exams table maintains individual details of each exam designed by an examiner. The most significant columns are:

* ***exam\_id:*** *A unique identifier for each exam.*
* ***title:*** *The name of the exam.*
* ***description:*** *A written description of the test material.*
* ***examiner\_id:*** *A foreign key referencing the exam to the examiner (Users table).*
* ***created\_at:*** *Date on which the exam was created.*

Exams table is related to the Users table by the examiner\_id column, establishing a relationship between the examiner and the exam they create. It enables every exam to be traced with a legitimate examiner and aids in traceability.

### **Questions Table**

The table Questions stores all the questions for all the tests. It contains the following most crucial columns:

* ***question\_id****: Every question has a question ID.*
* ***exam\_id****: A foreign key linking each question to a particular exam (from the Exams table).*
* ***question\_text****: The encrypted text of the question being asked.*
* ***options****: A JSON object containing multiple-choice options in an encrypted format.*
* ***correct\_answer****: The correct answer, securely stored in an encrypted format.*
* ***created\_at****: A timestamp indicating when the question was imported into the system.*

The Exams table is associated with the Questions table through the exam\_id field, creating a relationship between the questions and the exams to which they belong. Creating this relationship is important in an effort to sort and present the questions to the students during the exam.

### **Logs Table**

The Logs table tracks all the significant operations performed by users such that operations such as login, exam attempts, and malicious activities are traced. The table includes:

* ***log\_id****: A unique identifier for each log entry.*
* ***user\_id****: A foreign key linking the log entry to a specific user (from the Users table).*
* ***exam\_id****: Foreign key linking the log entry to a specific exam (from the Exams table), as appropriate.*
* ***action****: Brief description of action taken (e.g., login, start exam, suspicious action).*
* ***details****: Additional details or history of the action.*
* ***is\_flagged****: A boolean indicating whether the action has been marked as suspicious.*
* ***created\_at****: A timestamp indicating when the log entry was created.*

The Logs table is necessary in order to track user activity and create an open record of activity within the system. It is associated with the Users and Exams tables so that activity is accurately attributed to specific users and exams.

### **Results Table**

The Results table contains the exam scores of all the students. The table contains:

* ***result\_id****: A unique identifier for each result.*
* ***user\_id****: The foreign key that connects the result to the original student (Users table).*
* ***exam\_id****: Foreign key referencing the result to a single exam (from the Exams table).*
* ***score****: The score the student attained in the exam.*
* ***grade****: Grade received by the student on the basis of the score.*
* ***created\_at****: A timestamp indicating when the result was generated.*

The Results table is linked with the Users and Exams tables via the user\_id and exam\_id columns, respectively. This is done to ensure that every result is associated with a particular student and exam.

### **Blockchain Transactions Table**

Blockchain\_Transactions table tracks all transactions carried out on the blockchain, e.g., logs, results, and queries. The table holds:

* ***transaction\_id****: A unique identifier for each transaction.*
* ***transaction\_type****: Type of transaction, either 'log', 'result', or 'question,' depending on the type of data being stored in the blockchain.*
* ***reference\_id****: An ID referring to the associated record in the Logs, Results, or Questions table.*
* ***hash\_value****: The hash of the data to be stored in the blockchain.*
* ***created\_at****: A timestamp indicating when the transaction occurred.*

Blockchain\_Transactions table is at the heart of data storage in an unalterable manner. Each transaction is represented by an entry in the Logs, Results, or Questions table, which ensures any operation within the system is stored securely on the blockchain.

### **Interrelationships Between Tables**

The schema specifies the following main relationships:

* ***Users ↔ Exams****: An exam is associated with a specific examiner. The examiner\_id field in the Exams table is a foreign key to the user\_id field in the Users table.*
* ***Exams ↔ Questions****: A question has a one-to-one correspondence with an exam. Exams\_id in the Questions table is a foreign key referencing the exam\_id in the Exams table.*
* ***Users ↔ Logs****: All user activities are recorded in the Logs table, and each log is linked to a specific user by the user\_id.*
* ***Exams ↔ Logs****: Exam activity related logs are labeled with particular exams using the exam\_id.*
* ***Users ↔ Results****: There is one result per user through the user\_id field.*
* ***Exams ↔ Results****: A result is associated with an exam using the exam\_id field.*
* ***Blockchain\_Transactions ↔ Logs/Results/Questions****: Blockchain transactions are linked to their corresponding records in the Logs, Results, or Questions tables, so that all significant system events are recorded on the blockchain immutably.*

This entire architecture allows for seamless data sharing across the system, from user action to blockchain transaction, with security, transparency, and immutability at every stage of the investigation process.

## Working of the Safe Assesment Chain: From the Perspectives of the Examiner and the Student

### **Exam Setup by the Examiner**

In the proposed system, the initial step that is included in the process begins with the examiner taking charge of organizing the exam, which is a very crucial starting task. Organizing the exam is not just about deciding the timing but also about selecting the questions that are to be included in the exam, along with deciding the associated correct answers that are related to these questions. In addition, the examiner's role is also to determine the marks that are to be allocated to each individual question. The main steps that are included in the whole exam setup process can be explained as below:

#### The examiner is tasked with presenting a complete list of questions and their respective correct answers pertaining to the test in question. To maintain the highest level of confidentiality and secure the sensitive data held within these questions and answers, they are encrypted through the highly secure AES-256 encryption process. This state-of-the-art encryption method serves a key role in securing the information from unauthorized use and possible breaches.

#### The encrypted questions and answers, along with the well-planned exam schedule, are then systematically uploaded onto the blockchain. This blockchain is a very secure and tamper-evident ledger, and therefore the information pertaining to the exam cannot be tampered with or changed in any manner.

#### A unique exam ID is generated, which is an exclusive identifier for that individual exam. Furthermore, the encryption and decryption keys necessary for any future transactions are stored securely in a different database, which is independent of the blockchain. This separation is necessary because it maintains the integrity of the data as well as the fact that the decryption process can be effectively enabled at the time of actual exam conduct.

### **Student Registration and Authentication**

The process that is utilized in the registration and confirmation of students is triggered when a student attempts to register for a future test. The different steps that are included in the process can be listed as follows:

#### Students authenticate themselves in a secure manner using techniques that involve two-factor authentication, or 2FA, in an attempt to prove that they are who they say they are.

#### After a successful authentication process, the students have to register for the exam via a smart contract that is exclusively associated with the exam ID. Not only does this render the registration process easy, but also the process of registration is made transparent and secure, thereby generating confidence in the integrity of the exam registration process.

#### The information regarding the student's registration, which includes both the individual student ID and the individual exam ID, is carefully entered into the blockchain. This exhaustive log serves as an unalterable record, thus providing absolute transparency and essentially eliminating any unauthorized changes from taking place.

### **Exam Execution**

During the execution of the exam, the process is carefully structured to ensure that both the examiner's and the student's data remain secure. The following steps outline the process:

* ***Before the Exam:***

#### At the start of the exam, encrypted questions are fetched from the blockchain. These questions are encrypted in advance by the examiner to maintain confidentiality.

#### The system retrieves the necessary decryption keys from the database to decrypt the questions and display them to the student.

* ***During the Exam:***

#### The student answers the questions by selecting or entering responses. Whether marked or unmarked, the student’s answers, along with the correct answers and the allocated marks for the question, are encrypted to preserve the confidentiality of the data.

#### The encrypted responses are stored back on the blockchain, ensuring the data is tamper-proof and immutable.

### **Result Calculation and Publishing**

After the exam is completed, the system calculates the student’s results based on their responses. The steps involved in this process are as follows:

* ***Data Retrieval:***

#### The encrypted responses, along with the correct answers and marks, are retrieved from the blockchain for each question.

* ***Decryption:***

#### The data is decrypted using the keys stored in the database, ensuring that only authorized parties can access the correct answers and student responses.

* ***Result Calculation:***

#### Marks are assigned based on the student’s responses and the examiner’s predefined correct answers. The total marks are computed by summing up the scores for each question.

* ***Grade Assignment:***

#### Based on the total marks, the system assigns a grade and converts it into a standardized format (e.g. A, B, C).

* ***Result Storage:***

#### The marks and final grades obtained by students are encrypted with utmost caution and stored safely on the blockchain, which is highly secure. The data is also stored in a database so that it can be accessed easily and quickly whenever necessary. This double storage mechanism makes sure that a student's marks are not just safe from any sort of unauthorized access but also easily accessible for the people who require it.

* ***Student Dashboard:***

#### The final outcome, along with the corresponding grade, is displayed on the student dashboard and is readily, and easily accessible for viewing. The data stored in this view is encrypted and displayed in user-friendly and consumable form.

### **Audit and Logging**

The audit and logging process play a very vital function to verify that all steps taken within the system are trackable and traceable. It makes it feasible to have an entire analysis of all the operations. The action logging process includes the following process:

#### All major activities that occur in the system, beginning with major activities like the scheduling of exams, answers submitted by the students, and result declaration, are carefully tracked with the respective user ID attached to every activity. All this careful tracking is then stored securely on the blockchain, which is used to produce an open, easily verifiable, and unalterable record of all the interactions occurring in the system.

#### The database is utilized to store non-sensitive logs containing valuable information such as system performance data. This form of storage enables effective access and detailed analysis of the data gathered.

Utilization of blockchain technology in records of required actions and activities guarantees that logged data in this system cannot be tampered with or changed in any way. This inherent component offers the guarantee of possessing a safe and highly dependable system, which can be relied upon by users without fear of data integrity.

## Technical Details

### **Algorithms Used**

#### AES: Encryption of sensitive examination data.

#### SHA-256: Hashing for secure record identification.

#### ECDSA: Authentication of blockchain transactions.

### **Deployment Tools and Frameworks**

#### Smart Contracts: Implemented in Solidity on Remix IDE.

#### Blockchain Integration: Managed via Web3.py.

#### Backend: Built with Flask for API communication.

#### Frontend: Designed using HTML, CSS, and JavaScript.

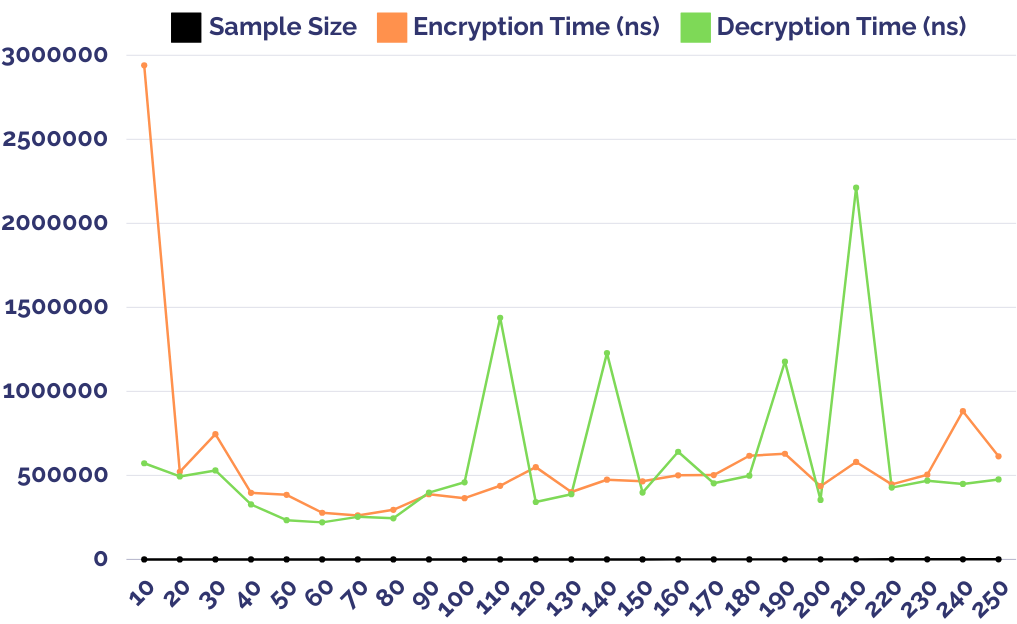
#### Database: PostgreSQL serves as the database for relational data storage in a structured form, whereas JSON is utilized to process and store unstructured data that has no specific schema to follow.

This approach is intended to make the whole exam process, right from setup through to results release, not only secure but fully transparent and immune to any type of tampering. Through the effective use of the advanced functionality of blockchain technology, the system offers a fundamental assurance of data integrity and permanence. Additionally, the database is best equipped to carry out efficiently non-sensitive tasks, such as key management and keeping the full system logs.

# RESULT ANALYSIS

## Performance Evaluation of the AES Algorithm

This section highlights the performance of the AES algorithm, focusing on encryption and decryption times across varying sample sizes. Fig. 5 illustrates the time taken for encryption and decryption, measured in nanoseconds, across 100 samples, each increasing in size by 10 units.

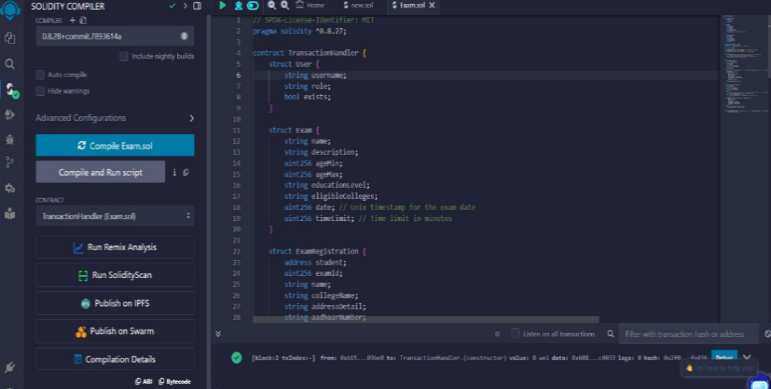


1. AES Performance Encryption Decryption Time vs Sample Size

The encryption process demonstrated an average time of 557,436.00 ns, with a minimum time of 303,700 ns and a maximum time of 9,773,500 ns, showing significant variability as reflected in a standard deviation of 949,617.75 ns. In contrast, the decryption process exhibited more stable performance, with an average time of 325,375.00 ns, a minimum time of 164,700 ns, and a maximum time of 1,138,100 ns, accompanied by a lower standard deviation of 199,585.70 ns. These results indicate that while encryption requires more computational resources and exhibits higher variability, the decryption process is faster and more consistent. The trends observed in the graph reflect the behavior of the AES algorithm under varying sample sizes, demonstrating its robustness and efficiency for real-time cryptographic applications.

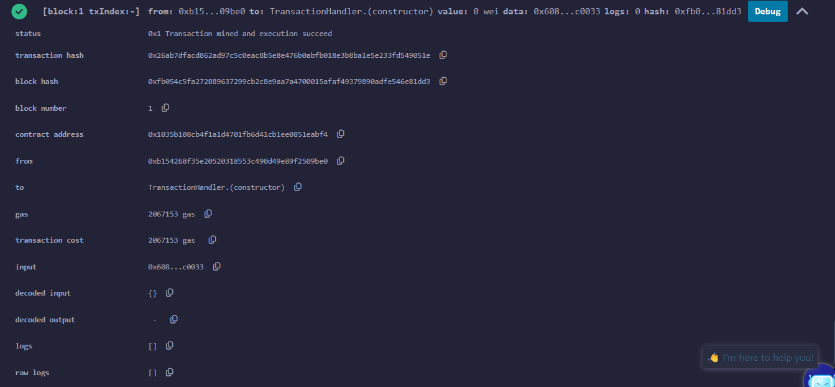
## Deployment of Smart Contracts

Fig. 6 shows Solidity code compiled on the Remix IDE. It defines three key structures: User (containing username, role, and existence flag), Exam (including details like name, age limits, education level, and date), and ExamRegistration (holding student details such as name, address, and Aadhaar number). The TransactionHandler contract facilitates user and exam management, supporting creation and registration operations for a secure exam system.



1. Solidity Code Compilation.

Fig. 7 depicts the successful deployment of the TransactionHandler contract in Remix IDE. The transaction status (0x1) confirms success, with details such as the transaction hash, block number (1), contract address, and gas usage provided. This output verifies the contract's deployment and readiness for interaction on the blockchain.



1. Deployment and Debugging.

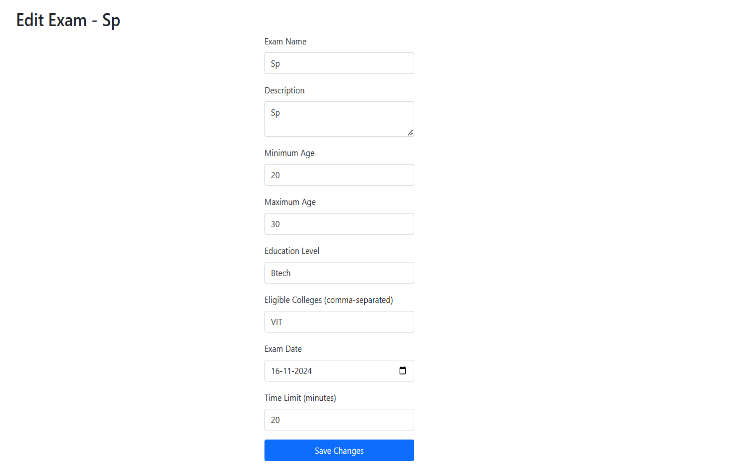
## Snapshots of the Smart Assessment Chain Web Application

The Admin Dashboard, depicted in Fig. 8, is designed to facilitate the efficient management of exams within the system.



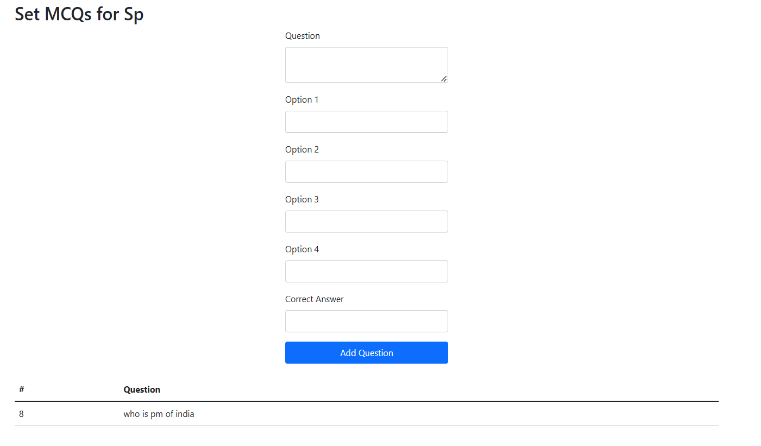
1. Admin Dashboard for Exam Management.

The system has a number of important features designed for administrators, starting with the Add Exam Button, which allows the user to add new exams to the system. There is also a lengthy Exam List available, which displays important information like the Exam Name, a short Description of the exam, its Scheduled Date, and an Actions column. The Actions column has functionality to edit exam details, schedule, question bank management, delete, and publish results. After the results are finalized, a confirmation message is displayed to publish. Overall, this dashboard gives administrators an efficient and easy-to-use interface to administer exams.



1. Setting Up an Examination for Registration.

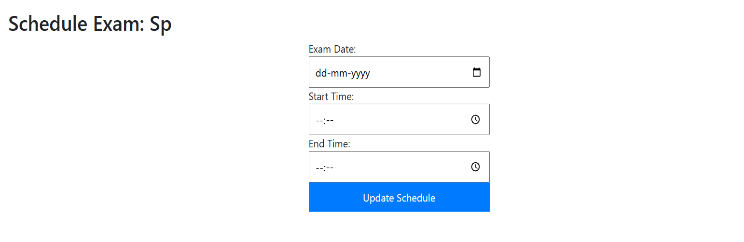
Fig. 9 represents the Exam Configuration Interface, which is used by administrators to configure exam details for enrollment. This includes input fields for the exam title, description, age requirement, education level, eligible colleges, exam date, and time limit. A "Save Changes" button is added to save the configured exam settings.



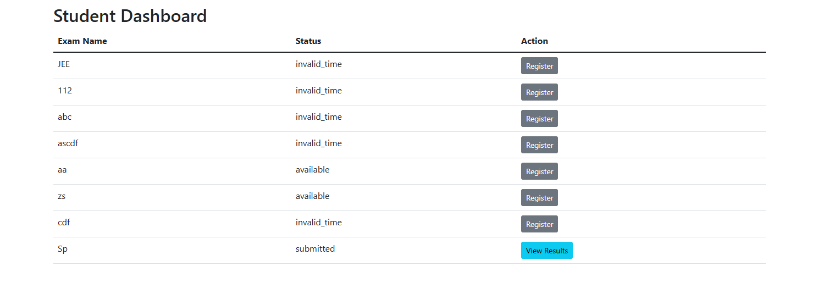
1. Configuring Multiple-Choice Questions (MCQs) for the Examination.

Fig. 10 shows the interface to add multiple-choice questions (MCQs) for an exam. Administrators can enter the question text, offer four choices, and mark the correct answer. A "Save Question" button enables them to save the MCQ. Added questions are also shown in a table. The interface supports secure storage of MCQs into the blockchain using AES encryption for data security.

Fig. 11 demonstrates the scheduling module where administrators set the examination date and time, ensuring it aligns with the institutional calendar.

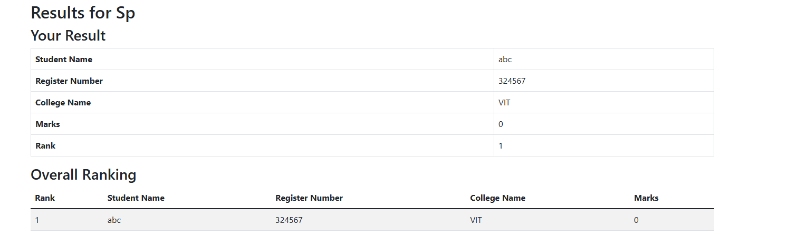


1. Scheduling the Examination.



1. Student Dashboard Interface.

Fig. 12 displays the student dashboard, offering access to scheduled exams, results, and other vital resources. The dashboard includes exam details such as the exam name, status, and available actions. Students can register for exams with available status, view results for submitted exams, and all data is securely retrieved and stored on the blockchain for integrity and transparency.

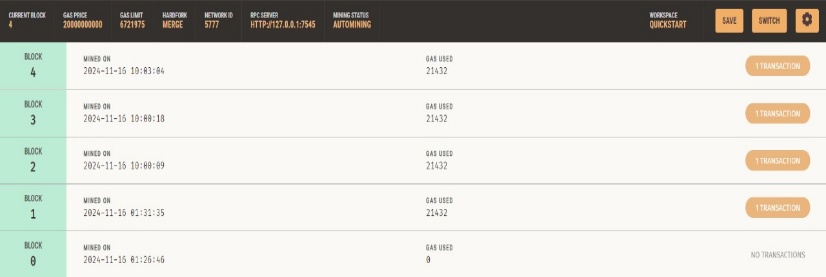


1. Published Examination Results on the Student Dashboard.

Fig. 13 displays the student dashboard after the publication of examination results. Students can view their scores, detailed feedback, and statistical performance analysis.

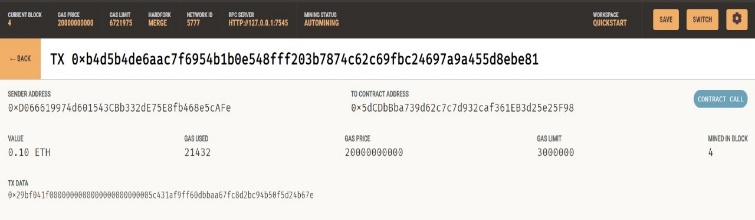
## Blockchain Transactions Displayed Using Ganache

Fig. 14 showcases the blockchain explorer interface in Ganache, displaying key block information such as the block number, gas usage, and transaction details for the Ethereum private network.



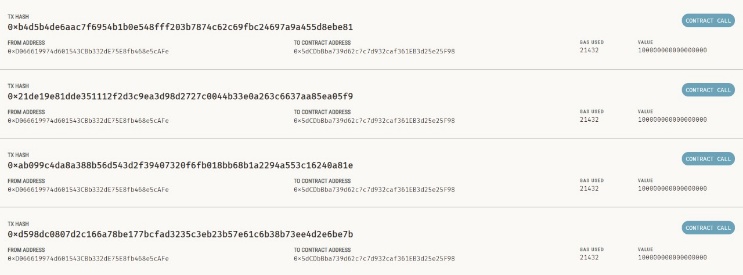
1. Blockchain Explorer Display in Ganache.

Fig. 15 presents detailed information about a transaction in block 4, including the sender address, recipient contract address, transaction value, gas price, and gas consumption.



1. Transaction Details for a Specific Block.

Fig. 16 provides a summary of multiple transactions within the blockchain network, with each transaction displayed by its unique hash, sender and recipient details, and gas usage.



1. Summary of Multiple Transactions on the Ethereum Blockchain.

## Performance of the System

In this section, a comprehensive performance analysis of the system is given with specific focus on blockchain latency, energy usage, CPU utilization, and memory utilization. All the performance measures are analyzed in detail to determine how efficient, scalable, and resource-aware the system is for various user loads. The results are important from the perspective of understanding the behavior of the system and it deploy ability in resource-hungry large-scale applications.

### **Blockchain Latency Analysis**

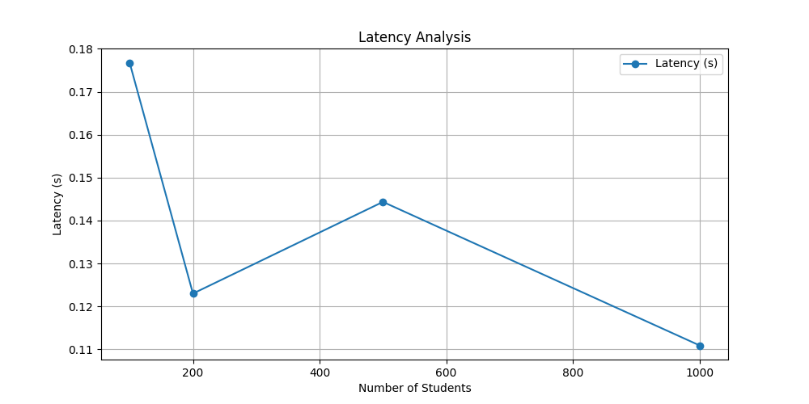
Figure 17 illustrates the blockchain system's latency, which we define as validation and recording time of transactions, with growing numbers of students. The latency results exhibit a fluctuating trend with growing loads:

#### For 100 students, the system experiences an initial latency of 0.175 seconds, attributed to setup overheads during blockchain transaction initialization.

#### At 200 students, latency decreases significantly to 0.123 seconds, indicating the system's efficient transaction pooling and validation mechanisms.

#### With 500 students, latency rises marginally to 0.144 seconds, suggesting temporary resource bottlenecks due to the increased volume of concurrent transactions.

#### At 1000 students, latency reduces further to 0.111 seconds, reflecting the system's ability to handle higher transaction volumes efficiently, possibly due to optimization in block size and transaction grouping.



1. Blockchain Latency Trends Across Varying User Loads.

This trend is indicative of the system's scalability and flexibility, with latency dropping by 36.6% from 100 to 1000 students. Such performance illustrates the efficiency of the underlying blockchain architecture in keeping transaction delays minimal as user load grows.

### **Energy Consumption**

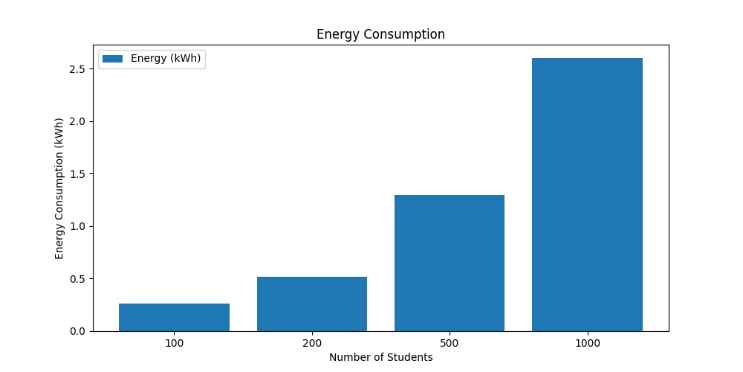
Figure 18 shows an extensive analysis of the system energy consumption with various user loads. The results are shown to depict a linear and constant rise in energy consumption corresponding to a rise in the number of users:

#### **100 students:** The system demands 0.25 kWh, showing low energy consumption at light user load.

#### **200 students:** Doubles energy consumption to 0.52 kWh, with a corresponding increase as the number of users grows.

#### **500 students:** The energy requirement increases substantially to 1.30 kWh, continuing the linear increasing trend.

#### **1000 students:** At maximum scalability, the 1,000 students' energy usage reaches 2.60 kWh, thus further confirming the predictable scaling behavior of the system.



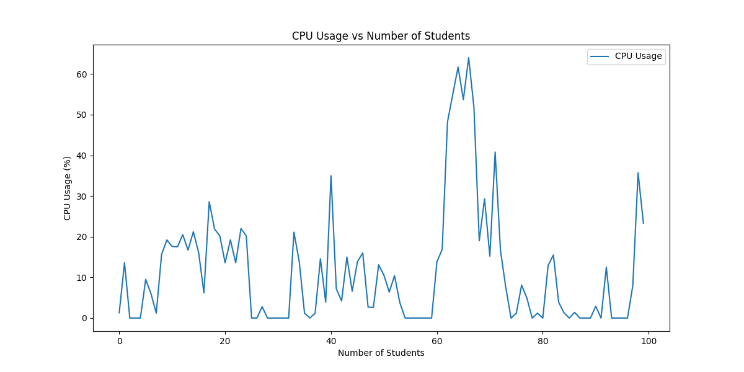
1. Energy Consumption Scaling with User Load.

This near-linear trend indicates that the system demonstrates energy efficiency at scale, thereby guaranteeing that power requirements increase in a controlled and predictable manner as the user base increases. Scalability of energy consumption makes this system ideal for use in larger institutions because it guarantees cost-effective operational costs while still providing performance.

The energy scaling factor stability is a demonstration of the highly optimized nature of the system architecture. This efficiency also makes the system a likely candidate for green computing practices, especially in environments where resource optimization and sustainability are of utmost importance.

### **CPU Usage**

Fig. 19 shows the system's CPU load under different loads, giving a measure of how well it performs in terms of handling computational resources:



1. CPU Utilization Dynamics Under Scalable Operations.

#### **For the first 60 students:** CPU usage is minimal, between 0% and 20%, indicating resource utilization is optimal during low usage.

#### **Between 65 and 70 students:** There is a sharp increase to 65%. Such a sharp increase is likely related to resource-intensive tasks, like simultaneous transaction verification, cryptographic computations, or any other computation-intensive tasks.

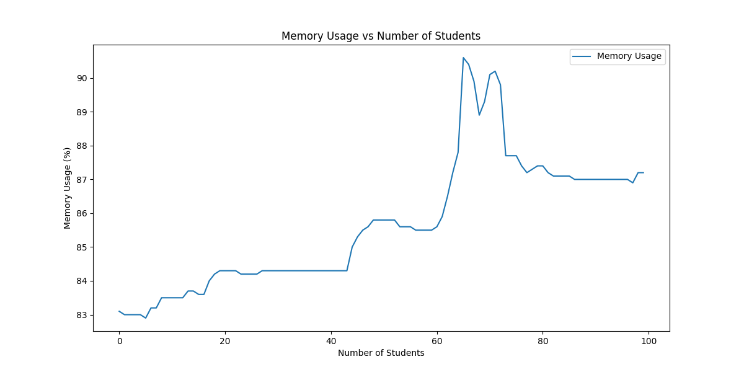
#### **Beyond 80 students:** CPU usage is maintained between 0% and 15%, indicating the system's ability to distribute loads effectively even at increasing demand.

#### **Periodic spikes:** Periodic spikes on the CPU involve infrequent spurts reflecting sporadic episodes of excessive processing demand. Spikes could be brought about by batch transaction validations or block mining exercises within the blockchain network.

This trend reflects the robustness of the system in handling peak loads without allowing such peaks to adversely affect overall performance. The stabilization of CPU usage at high loads also reflects the scalability of the system and its competence in the management of computational resources.

### **Memory Usage**

Fig. 20 illustrates the trends in memory usage under different user loads and illustrates the system's capability to use memory resources efficiently:



1. Memory Utilization Patterns for Scalable User Bases.

#### **At the baseline (small user base):** Memory usage begins at 83%, which is the system's intrinsic memory overhead for baseline activity.

#### **At 50 students:** Memory usage increases slowly to 85.8%, possibly for storing transaction history or temporary caching in regular operations.

#### **At 65 students:** A sharp rise to 90.5% is observed. This is due to transient memory demands caused by resource-hungry operations like transaction caching, encryption, or validation.

#### **Beyond 80 students:** Memory usage stabilizes to around 87%, consistent with efficient memory management techniques such as garbage collection and optimal cache policies..

This is a sign that while there are periodic spikes in memory usage by the system, it still has sufficient space to facilitate scaling. The stability beyond 80 students indicates that the system recovers effortlessly and handles memory space, thereby ensuring stability and uniform performance while the system is heavily loaded.

The use patterns observed reveal a well-optimized architecture, but the peak at 65 students reveals where optimization is to be made, such as optimization of memory processes or employing better caching systems. The system overall demonstrates efficient memory management, with stability and reliability under heavy user load.

# Conclusion

The Safe Assessment Chain project well illustrates the intersection of blockchain and encryption technologies in the development of a secure, efficient, and transparent examination management system. Utilizing a private Ethereum blockchain, the platform provides immutable and tamper-proof storage of examination data, thereby enhancing trust among stakeholders. Smart contracts facilitate automation of critical processes, including student verification, exam registration, and result publication, which significantly minimizes manual intervention and operational inefficiencies. The Advanced Encryption Standard (AES) also enhances the security of the system by encrypting sensitive information, such as examination questions, during storage and transmission, while role-based access control guarantees that only authenticated users can execute specific functionalities.

The key aspects of this system are the innovative interaction of blockchain technology with encryption, whereby examination data is stored off-chain and cryptographic hashes are stored on the blockchain to verify integrity. Furthermore, cryptographic protocols such as ECDSA augment the security of transactions, hence ensuring data authenticity throughout the process. User-friendly dashboards developed for students and administrators simplify interactions while ensuring high security levels. A comparison of the performance of AES, combined with the employment of smart contracts, validates the scalability and feasibility of this system, hence rendering it a safe solution for secure examination processes. The Safe Assessment Chain provides a holistic framework for managing contemporary challenges in examination management, hence paving the way to its adoption in academic institutions and certification bodies.

References

1. Infosecurity Magazine. (2024, May 14). Data Breaches in US Schools Exposed 37.6M Records. Retrieved from https://www.infosecurity-magazine.com/news/data-breaches-us-schools-37m/
2. Comparitech. (2024, May 14). US schools leaked 37.6 million records in 3713 data breaches. Retrieved from https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/
3. University of New Hampshire. Data Breaches in Higher Education Institutions. Retrieved from https://scholars.unh.edu/cgi/viewcontent.cgi
4. Higher Ed Dive. (2023, December 4). Data breaches cost higher education and training organizations an average of $3.7 million in 2023. Retrieved from https://www.highereddive.com/news/data-breaches-cost-higher-education-colleges/689499/
5. CMIT Solutions. (2024). 8 Eye-Opening Statistics About Cybersecurity in Education. Retrieved from https://cmitsolutions.com/richardson-tx-1049/blog/8-eye-opening-statistics-about-cybersecurity-in-education/
6. Bravura Security. (2024, April 9). The Impact of Security Breaches on Educational Institutions. Retrieved from https://www.bravurasecurity.com/blog/the-impact-of-security-breaches-on-educational-institutions
7. Prey Project. (2023, December 20). The biggest school data breaches of 2023. Retrieved from https://preyproject.com/blog/school-data-breaches-in-2023
8. Ghazal, O., & Saleh, O.S. (2021). Blockchain Applications in Education: A Systematic Literature Review. Applied Sciences, 11(24), 11811. https://doi.org/10.3390/app112411811
9. Alammary, A., Abed, M., & Boukadi, K. (2021). Blockchain Adoption in Education: A Systematic Literature Review. Education and Information Technologies, 26(5), 5779-5797. https://doi.org/10.1007/s10639-021-10507-9
10. Pooja, K.H., & Kumar, S.G. (2022). Decentralized Assess: Enhancing Online Examination Security. In Inventive Computation and Information Technologies (pp. 595-606). Springer.
11. Alammary, A., et al. (2021). Online Exam Enhancement Using Blockchain: A Study on Improving Examination Integrity and Security. Journal of Computing in Higher Education, 32(1), 109-134.
12. Sousa, M.J., & Dandolini, G.A. (2024). Education Evaluation Management Based on Blockchain Technology: A Comprehensive Framework for Academic Assessments. In Transformative Leadership and Sustainable Innovation in Education (pp. 147-168). Emerald Publishing Limited.
13. Hillman, V., & Ganesh, V. (2019). Blockchain-Based Examination System for Effective Evaluation: Enhancing Credibility and Reliability in Assessment Records. In Proceedings of the IEEE International Conference on Big Data (Big Data).
14. Zheng, Z., Xie, S., Dai, H.N., & Wang, H. (2021). Online Examination System Based on Blockchain Network: Advantages Over Cloud-Based Systems in Authentication and Secure Data Handling. Educational Technology Research and Development, 69(6), 1235-1260.
15. Grech, A., & Camilleri, A.F. (2017). Blockchain Technology in Education: A Comprehensive Review of Current Research and Future Directions. European Commission Joint Research Centre. https://doi.org/10.2760/14370
16. Li, J., Zheng, Z., & Wang, Y. (2020). Blockchain Technology in Education: Implications for Transparency and Credential Verification. IEEE Access, 8, 123456-123467.
17. Saleh, O.S., & Ghazali, O. (2020). A Graduation Certificate Verification Model via Utilization of Blockchain Technology. Journal of Telecommunications, Electronic & Computer Engineering, 10(1), 29-34.
18. Harshini Poojaa, K., & Ganesh Kumar, S. (2022). A Review of Encryption and Decryption of Text Using the AES Algorithm for Safeguarding Examination Data Privacy.
19. Garg, S., & Gupta, V.K. (2019). Review of the Advanced Encryption Standard System Performance: Evaluating Encryption Speed and Security Levels in Cloud-Based Implementations.
20. Exploring AES Encryption Implementation Through Quantum Cryptography discusses potential risks posed by quantum computing to AES encryption.
21. Application of Optimizing Advanced Encryption Standard in Vehicle Communication explores optimizations in AES for faster encryption speeds and improved security.
22. A Comprehensive Study on AES and Diffie-Hellman Encryption analyzes the integration of AES with other cryptographic protocols for enhanced data security.
23. Alammary, A., et al. (2021). Blockchain Applications in Education: A Systematic Literature Review highlighting scalability challenges.
24. Alammary, A., Abed, M., & Boukadi, K. (2021). Blockchain Adoption in Education: A Systematic Literature Review discussing hybrid approaches to optimize transaction speeds.
25. Machado, A.d.B., Sousa, M.J., & Dandolini, G.A. (2024). Artificial Intelligence and Blockchain in Higher Education Institutions: Enhancing Student Engagement through AI-driven Smart Contracts.
26. Blockchain and Machine Learning in Education: A Literature Review explores machine learning techniques to optimize blockchain-based educational applications.
27. Scalability Challenges and Solutions in Blockchain Technology suggests alternative consensus mechanisms to enhance blockchain performance.
28. Gräther, W., et al. (2022). Challenges of Using Blockchain in the Education Sector identifies data privacy and regulatory compliance as major obstacles to widespread adoption.
29. UNESCO (2023). Education and Blockchain – UNESCO Digital Library emphasizes blockchain’s potential to reduce credential fraud and improve verification processes.
30. Dworkin, M. (2007). NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. National Institute of Standards and Technology.
31. National Institute of Standards and Technology. (2001). FIPS 197: Advanced Encryption Standard (AES). Federal Information Processing Standards Publication.
32. McGrew, D., & Viega, J. (2004). The Galois/Counter Mode of Operation (GCM). Submission to NIST Modes of Operation Process.