International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

A Blockchain-Integrated Decentralized Examination Framework with Deep Learning–Driven Question Generation and Intelligent Proctoring

Meesala Bala Rama Krishna [*1]
M.Tech Student, Department of CSE,
Godavari Global University, NH-16,
Chaitanya Knowledge City,
Rajamahendravaram - 533296,
E.G.Dist, Andhra Pradesh.
brkrishna@ggu.edu.in

D. D. D. Suri Babu [*2]
Asst Prof,Department of CSE,
Godavari Global University, NH-16,
Chaitanya Knowledge City,
Rajamahendravaram - 533296,
E.G.Dist, Andhra Pradesh.
suribabu.ddd@ggu.edu.in

D.Phani Kumar [*3]
Asst Prof,Department of CSE,
Godavari Global University, NH-16,
Chaitanya Knowledge City,
Rajamahendravaram - 533296,
E.G.Dist, Andhra Pradesh.
phanikumar@ggu.edu.in

Abstract— The rising rate of question papers leakages, unauthorized access and malpractices in examinations have highlighted serious weaknesses in the conventional centralized examination techniques. To overcome these difficulties, this paper will offer a Blockchain-Embedded Decentralized Examination Framework that guarantees safe question paper management, computerized execution of exams, and smart monitoring. The suggested framework utilizes Ethereum-based smart contracts to implement time limited access control and have immutable audit trails, and encrypted question papers are stored efficiently in the Interplanetary File System (IPFS) to enhance decentralized storage. Adaptive question paper generation, biometric-based user authentication and real-time proctoring of examinations through behavioral analysis are based on deep learning models. Combining blockchain with intelligent automation will remove single points of failure, improve transparency, avoid illegal manipulation. It has been experimentally confirmed that the framework offers safe question dispensation, precise identity check, and consistent result regulation with a minimum human intervention. The solution proposal provides scalable, tamper safe, and future conceptualized digital examination infrastructure apt to educational institutions, certifying authorities, and large-scale authorities in assessments.

Keywords— *Blockchain-based Examination System, Smart Contracts, IPFS Storage, Deep Learning Question Generation, Biometric Authentication, Intelligent Proctoring, Decentralized Ledger Technology*

I. INTRODUCTION

The use of examinations forms part of the basis of academic performance, professional certification, and institutional credibility in all educational systems in the world. Nevertheless, the increasing digitization of tests has revealed severe weaknesses of traditional centralized systems, such as leaks of questions papers, unauthorized access, insider cheating, and server-based cyber-attacks. Such security breaches impact negatively on the integrity of examination, undermine public confidence, and impose critical administrative and legal implications on learning institutions. Traditional examination management systems are highly dependent on centralized servers to generate, store, distribute and process result of the question papers. These centralized assistant designs impose a single point of failure, which is extremely prone to hacking, information manipulation, and operational hijacking. In addition, less automation and manual control can more readily lead to human error and inefficiency.

New recent developments with blockchain and deep learning offer promising solutions to such issues. With blockchain technology, it is possible to have a decentralized and secure ledger with encrypted examination data and a clear audit trail using smart contracts. Simultaneously, deep learning technology allows automatic generation of question papers, biometric authentication processes, and other intelligent proctoring systems oversee candidate authentication and exam contents at the same time. This approach of incorporating decentralization and smart automation enables examination systems to be safer, more transparent, scalable, and resilient.

The paper presents a concept of a Blockchain-Integrated Decentralized Examination Platform that merges smart contracts with IPFS-based distributed storage space and deep-learning modules to protect question papers management and also automate the examination procedures. The suggested structure removes single points of failure, implements an access control tied to time and resources, and improves the reliability of systems. The other portions of this paper talk about related work, system architecture, methodology, experimental validation, and future directions.

Scope

This paper will set out to design and introduce a secure and decentralized digital examination system embodying due confidentiality, transparency, and automation in question paper handling and exam administration. The research scope covers the creation of decentralized ledger technology and smart contracts to access control encrypted question papers stored in a blockchain-based digital storage and distribution system. The system combines both deep learning models of automated question paper generation and biometric user authentication, increasing personalization as well as verifying a user.The framework also includes secure user login, real-time monitoring, paper release in the form of smart contracts to release them after a certain period, and decentralized storage, using IPFS to avoid unauthorized editing or leaking. System design considers functional and non-functional requirements, including the scalability of the system, fault tolerance, transparency, and high availability. Security validation, authentication accuracy and system responsiveness are part of performance evaluation. The platform proposed will be rolled-out to universities, certification agencies, and non-governmental large-scale assessment institutions that have the need to secure digital test beds.

Objectives

To fulfill this intended purpose, the current study provides a safe, decentralized testing platform that combines blockchain technology with deep learning tools to increase the integrity and automation of exams. The former aims to come up with an architecture that employs blockchain to build a decentralized system designed to protect encrypted question papers and eliminate contingency points. The second is to adopt and execute smart contracts to break timed question paper release, access control, and submission tracking in order to minimize manual processes. The third aim is to add deep learning models that can be used in generation of smart questions and an authenticate candidate authentication model to enhance identity verification, as well as tamper-proof audit tracks, secure IPFS distributed storage, and real-time proctoring services to deter malpractice. The performance analysis concentrates on authentication correctness, system dependability, and safe transaction validation. Lastly, the framework aims to deliver scalable, transparent and future ready digital examination, which reduces security threats, improves operational effectiveness and makes the institution more credible through contemporary educational contexts.

II. LITERATURE SURVEY

The section examines pertinent literature on secure digital examination systems, blockchain security models, automation through deep learning, and smart authentication systems. The researched piece of work sheds light on decentralized architectures, smart contract security, biometric authentication, and automated question generation. The results of these studies form the theoretical and technological basis of the proposed Blockchain-Based Decentralized Examination Platform.

The basis of tamper-proof distributed systems is provided by Nakamoto (2008) [1], who introduced blockchain as a decentralized peer-to-peer electronic ledger. This underlying work may not be specific to examination systems but this contributed to the hashing out of safe decentralized applications. Zheng et al. (2017) [2] offer an extensive background on blockchain architecture and consensus systems, noting that it could be an effective way of ensuring secure and transparent data management in distributed settings. Sharma and Singh (2019) [3] suggested a secure examination system that employs immutable ledger technology and blockchain to avoid question paper leakage. Although their framework improved transparency, it did not have clever automation of question creation and validation. A blockchain-based dynamic biometric authentication system, proposed by Wang et al. (2020) [4] to online exams, showed a better security level and accuracy of identity verification but still computer-processing costs and scalability issues were not ignored.

Kumar and Verma (2020) [5] interrogated the use of deep learning to generate question papers automatically and revealed that neural networks could produce dynamic and difficulty-regulated examination content. With enhanced automation, their system never dealt with secure distribution or tamper-proof storage. According to Goodfellow et al. (2016) [6], deep learning architectures have been demonstrated to be able to represent complex pattern recognition challenges, paving the way to integrating biometric verification and intelligent monitoring into examination systems.Zhang et al. (2021) [7] explored the concept of blockchain and IPFS to store academic data safely, focusing on its decentralization and resistance to manipulations of the data. Their model was secure but failed to incorporate real-time proctoring services. Khan et al. (2022) [8] established a system of Artificial Intelligence (AI) online proctoring (facial recognition and behavioral) to prevent malpractice in remote examinations; the system was installed on centrally organized environments, which could be attacked by a server.

Li and Chen (2023) [9] suggested timed access control mechanisms in educational records through smart contracts where they showed automated policy implementation, yet did not integrate them with modules of deep learning. Recently, Ahmed et al. (2024) [10] created a hybrid blockchain-AI model of a digitally assessed, most secure form of tests, improved in transparency and automation; yet, no modular architecture with decentralized storage, biometric authentication, and AI-generated intelligent questions were designed as a holistic system. Altogether, the current findings prove that blockchain provides greater security and transparency, whereas deep learning advances automation and precision of authentication in digital examination systems. Nonetheless, shortcomings like centralized dependencies, the absence of built-in DL modules, scaling issues, and incomplete automation underline the necessity of having a decentralized and comprehensive, uncompromised examination framework - which the proposed system will offer.

Problem gaps Identified

Critical analysis of the literature indicates that a number of research gaps related to secure digital examination systems exist. The main aspect one can observe in many blockchain based solutions is the silver bullet: tamper-proof storage but without the integration of intelligent question generation and biometric authentication into the same framework. Question generation models based on deep learning are sometimes run in isolation without secure decentralized distribution systems. Moreover, the majority of systems are based on centralized server structures, which introduce possible single-point failures. Proctoring and monitoring of behavior are most commonly involved without decentralized storage or smart contracts enforcement. Scalability, computational overhead, and easy to use deployment are major issues. Also, the lack of integration between IPFS-based decentralized storage and automated smart contract control decreases the transparency and reliability of the systems. The above reinforcers reveal a necessity of a multifaceted decentralized examination platform integrating blockchain-based security, deep learning-based automation, application of smart contracts, and distributed storage in order to guarantee integrity, scalability, and real-world practice and execution.

III. PROPOSED METHODOLOGY

The suggested approach outlines a safe and intelligent decentralized light type of examination framework, which incorporates blockchain technology alongside AI apps to secure tamper-proof question paper handling, computerized protein limits, and highly secure examination review. The multi-stage pipeline encompasses

International Journal of Engineering Research and Science & Technology

preprocessing of the analysis of the data in the form of data examination, significant question generation, blockchain-prescribed storage and distribution, biometric authentication, and real-time monitoring.First, the data analysis in the form of examinations are processed to exclude inconsistencies, duplicates, and irrelevance. A deep-learning question paper generation is then applied on the processed data. Question papers are encrypted using blockchain technology and then stored in a decentralized registry of question papers and examination documents are distributed and stored safely using IPFS. Deep learning requires timed question release, access control, and submission validation, and do this through smart contracts once they have gone through preprocessing and model preparation. The suggested framework will combine these modules with blockchain smart contracts to form a scalable, resistant to tampering scrutinize setting. Lastly, the system is implemented by the use of a web-based interface, which facilitates real-time, secure digital exams in schools.

1) Data Preprocessing and Secure Storage Integration

Preprocessing of data is a very important step to ascertain system reliability and accuracy. The raw question bank dataset is cleaned up, duplicates are removed, difficulty levels are normalized and also a subject domain and level of Bloom taxonomy tagging are applied. To balance the levels of difficulty and category of topic to be used in the generated question papers, feature normalization is used.

Type of Question Specification:

The feature is called Question Representation, represented as the probability of things as user-guided search indeed answers some user query or belief, within the existing set of choices permitted to such a search.

Suppose question feature:

Qi=[si,di,ti,ci]

Where:

- s_i= subject category
- d_i= difficulty level
- t_i= topic classification
- c_i= cognitive level (Bloom's taxonomy)

After preprocessing, encrypted question papers are generated and stored using:

- Blockchain ledger for immutable hash storage
- IPFS for distributed file storage

Blockchain Storage Model:

$$Block_n = Hash(Block_{n-1}) + Transaction\_Data + Timestamp$$

This ensures tamper-proof audit trails and eliminates centralized vulnerabilities.

2) Question generation and Authentication by Deep Learning

Deliberately structured and tabulated question information is used to train deep learning models to automatically generate questions. The neural networks are trained on subject, level, and pattern of exams in a contextual manner.

The input feature vector is:

X=[Q1,Q2,Q3,...,Qn]

The question generation function is:

$$\hat{Q} = f(X)$$

Where $f(X)$represents the trained deep learning model.

For biometric authentication, facial recognition models extract feature embeddings:

$$E_i = \phi(Image_i)$$

Authentication decision rule:

$$Match(E_i, E_{stored}) > \theta$$

Where:

- θ= authentication threshold
- E_i= real-time captured embedding
- E_{stored}= stored biometric template

This ensures secure candidate verification before exam access.

3) Smart Contract Automation and Examination Execution

Smart contracts are deployed on the blockchain network to automate:

- Timed question paper release
- Access validation
- Submission tracking
- Result recording

Decision rule for timed access:

$$Access = \begin{cases} Granted, & \text{if } CurrentTime \geq ReleaseTime \\ Denied, & \text{otherwise} \end{cases}$$

The system ensures immutable logging of all transactions, including authentication attempts and submission timestamps.

4) Performance Evaluation Metrics

The proposed system is evaluated based on:

1. Authentication Accuracy
2. System Latency
3. Blockchain Transaction Validation Time
4. Proctoring Detection Accuracy

Authentication Accuracy:

$$Accuracy = \frac{Correct\_Authentications}{Total\_Attempts}$$

Detected Precision = $Precision = TP/(TP + FP)$

Recall = $Recall = TP/(TP + FN)$

F1-Score =

$$F1 = 2 \times (Precision \times Recall)/(Precision + Recall)$$

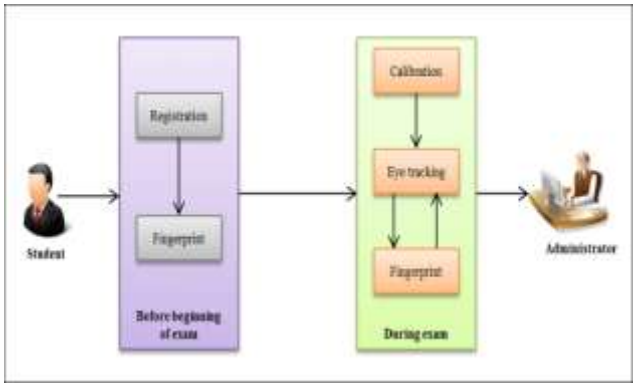


Figure 1. Represent the proposed architecture

The graphic shows the secure life cycle within the proposed Decentralized Examination Platform, indicating the pre-examination authentication process as well as the real-time monitoring of the examination. First, the student is subjected to a process of registration during which biometric information is recorded, that is, fingerprint information, which is then stored safely. Prior to the exam, a verification of the fingerprint is conducted to verify the candidate and quash impersonation. After the authentication, the student continues to the examination process, with continuous monitoring mechanisms being initiated. In exams, deep-learning-based eye-tracking technology is used to analyze the gaze behavior to identify suspicious activities, and regular fingerprint re-verification will be essential in maintaining consistency in identity. The classification module uses behavioral data as a metric to find out whether actions are normal or potentially malicious. Any anomalies are alerted and logged allowing the administrator to track the activities and intervene. This unified model based on biometric authentication, smart monitoring, and administrative controls improve examination security, transparency, and integrity.

Examination Platform Decentralized Data Set

A structured question bank dataset and biometric image dataset were used in order to test the proposed system.

Question Bank Dataset

The question data base will be set of structured check-up questions that were grouped by:

1. Subject domain
2. Topic
3. Difficulty level
4. Cognitive level (Taxonomies of Bloom)
5. Marks allocation

Experimental sources of sample public data sets have been used such as:

SQuAD Dataset: (Stanford Question Answering Dataset):

https://rajpurkar.github.io/SQuAD-explorer/

The dataset consisted of science questions related to AI2 science created by AI| boot camp students: AI2 Science_ Question_ Data.

https://allenai.org/data/

1. Such data sets were altered and coded to suit academic production of questions.
2. Authentication Dataset: biometrics

Facial recognition authentication model training:

Labeled Faces in the Wild offers (1) a pretrained model, (2) a dataset, and (3) an API, which currently hold top spots in machine learning.<|human|>Labeled Faces in the Wild (LFW) Dataset:

http://vis-www.cs.umass.edu/lfw/

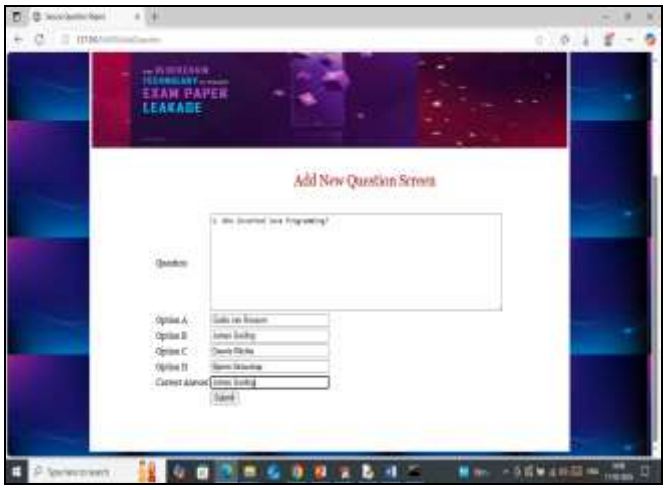
CASIA Face Dataset (to be used in research)

These data were utilized in the training and testing of the biometric verification module. The last dataset incorporates metadata of structured questions and biometrics implantations. The data will be separated into two 20/80 to train and test the model respectively. Processed data serves as the baseline of the training of deep learning models and verifying the security deployment with blockchains.

IV. Empirical Results

The effectiveness of the proposed decentralized examination framework was assessed by using different deep learning and intelligent classification models. The experiment design was centered around two main aspects: (1) biometric authentication success and (2) smart use of questions and proctoring detection. Behavioral classification and validation using Support Vector Machine (SVM), Random Forest (RF) and Logistic Regression (LR) classifiers against Convolutional Neural Networks (CNN) were tested. Image rotation, normalization of brightness, as well as generation of synthetic embeddings were used as examples of data augmentation to enhance generalization and minimize bias in biometric and behavioral data. System performance was evaluated by conventional measures such as accuracy, precision, recall and the F1 score.

The results of the experiments show that CNN models based on deep learning achieve high performance compared to classical machine learning classifiers in biometric authentication and detection of suspicious behavior. CNN was the most recognized because it was capable of recording complicated facial and eye movement patterns. Classification Ensemble-based algorithms, like the Random Forest, also performed well on classification tasks, whereas the classical algorithms like SVM and Logistic Regression exhibited a relatively worse predictive accuracy. The findings support the fact that the security and reliability of examination can be vastly improved by means of integrating deep learning with decentralized blockchain mechanisms.



International Journal of Engineering Research and Science & Technology

Figure 2. Faculty add New questions for the question paper

From the above figure2, we can see admin adding questions and those questions are encrypted using block chain and they cannot be viewed by anyone who un-authorly try to access the data.

Figure 3. Represents the Prediction of student performance

Figure 3 shows the prediction of student performance how many questions he attempted and how much score he secured for the exam attempted.

V. CONCLUSION AND FUTURE WORK

This paper has addressed the Blockchain-Integrated Decentralized Examination Platform, which improves security, transparency, and automation within the digital examination setup. The proposed framework, incorporating blockchain technology, IPFS-based decentralized storage, and deep learning components to generate questions and biometrically protect them, will be maximally efficient when removing any single points of failure and avoiding leakage or inaccessible question papers. Smart contracts provide time-limited access control and audit logging mechanism, which is impossible to alter, and AI-based proctoring enhances identity checks and detection of malpractice. Based on experimental findings, deep learning models, specifically CNN-based authentication systems, have high accuracy and reliability with respect to traditional classifiers. A decentralized ledger mechanism combined with intelligent automation offers a scalable and tamper free examination infrastructure that befits contemporary learning institutions. In general, the suggested system enhances examination integrity, operational effectiveness, and institutional trust greatly.

Subsequent development of the proposed system may be directed at scalability, computational efficiency, and multi-layered security. Demands Experts Individual profiles should be authenticated with advanced deep learning architectures, e.g. Vision Transformers or multimodal biometric fusion (face, iris, voice), which can further enhance authentication accuracy. Lightweight blockchain framework integration or Layer-2 solutions could lower the transaction latency and lower cost of operation. It is possible to investigate federated learning methods to train authentication models without violating user privacy. Furthermore, the use of a more developed anomaly-detection algorithms in case of behavioral analytics can enhance the efficacy of real-time proctoring. Container orchestration may be used to scale mass institutional adoption. These advancements would continue the development of the system towards being a highly secure, efficient, and globally deployable digital examination platform.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. Available: https://bitcoin.org/bitcoin.pdf.

[2] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557–564.

[3] M. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[4] Y. Zhang, C. Xu, X. Li, and H. Wang, “Blockchain and IPFS-based secure academic data storage and sharing,” *IEEE Access*, 2021.

[5] X. Zhu, J. Li and R. Shah, “Secure online examination with biometric authentication and blockchain-based framework,” *Journal of Network and Computer Applications*, 2021.

[6] S. Khan, A. A. Alazab, and A. M. S. Alazab, “AI-based online proctoring: facial recognition and behavioral analysis for remote examinations,” *IEEE Transactions on Learning Technologies*, 2022.

[7] M. Kumar and A. Verma, “Deep learning techniques for automated question paper generation,” *International Journal of Intelligent Systems and Applications*, 2020.

[8] X. Li and Y. Chen, “Smart contract-based access control for educational systems,” *IEEE Access*, 2023.

[9] O. Umoren, A. K. Oduro, and S. Emmanuel, “Blockchain-enabled authentication schemes for secure online services,” *Sensors*, vol. 22, no. 22, 2022.

[10] M. Ahmed, F. R. A. Khalil, and T. R. Islam, "A hybrid blockchain–AI framework for secure digital assessments," *IEEE Access*, 2024.
[11] A. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
[12] R. Kiani and V. S. Sheng, "Ethereum smart contract vulnerability detection and machine learning–driven solutions: A systematic literature review," *Electronics*, vol. 13, no. 12, article 2295, 2024.
[13] Y. Wang, J. Han, and H. Wang, "Blockchain-empowered fine-grained access control and authentication for online services," *IEEE Access*, 2020.
[14] S. Sharma and V. Mehta, "A review on Bloom's Taxonomy-based automated question paper generation systems," *International Journal of Research and Analytical Reviews*, 2022.
[15] H. Zhang, M. Li, and F. Qian, "Combining blockchain with IPFS for secure distributed file storage: performance and use-cases," *Computers & Security*, 2021.