International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(11s) 2026 pp. 959-967
https://doi.org/10.70917/ijcisim-2026-3826
Article

# A Block chain-Based Privacy-Preserving Framework for Detecting Cheating in Online Examinations without Video Surveillance

**Murali Ponaganti[1], Vallem Ranadheer Reddy[2], Kumaraswamy Kankala[3], Bala Krishna Varikuntla[4], Enugurthi Gangaram[5], Kammara Venkatarangaiah Achari[6]**

[1]Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Maisammaguda, Kompally, Medchel – Malkargiri – 500100.
Email: kalyanamurthip@gmail.com
ORCID: 0009-0002-7591-4934
[2]Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Maisammaguda, Kompally, Medchel – Malkargiri – 500100.
Email: ranadheerreddy5@gmail.com
ORCID: 0009-0000-0101-7902
[3]Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Maisammaguda, Kompally, Medchel – Malkargiri – 500100.
Email: kankala.kumar24@gmail.com
ORCID: 0000-0002-2859-2410
[4]Department of Computer Science and Engineering (AI&ML), Malla Reddy Deemed to be University, Maisammaguda, Kompally, Medchel – Malkargiri – 500100.
Email: vkrishnapi@gmail.com
ORCID: 0009-0007-1324-7546
[5]Department of Computer Science and Engineering, Narsimha Reddy Engineering College, Maisammaguda, Kompally, Medchel – Malkargiri – 500100.
Email: gangaram797@gmail.com
ORCID: 0009-0002-2635-2824
[6]Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Maisammaguda, Kompally, Medchel – Malkargiri – 500100.
Email: kvr1254@gmail.com
ORCID: 0009-0000-8210-7730

**Abstract:** —with the increasing number of online exams, it has become very important to ensure that the students do not indulge in any dishonest practices, also taking care of the cases in which a privacy, related or technical issue would make the use of a webcam, based proctoring not advisable. This work presents a plagiarism detection solution as an innovative way of online testing, focusing on privacy and without the necessity of watching video or audio recordings. The method mostly depends on less intrusive monitoring of the user's browser activity as well as a server, side analysis of the suspicious behavior. A few basic anti, cheating steps, which are at least partially realizable through the techniques mentioned above, include the turning off of the options for a right, click, copying, and pasting as well as highly controlled tab switching. Furthermore, the platform is equipped with the functionalities for recognizing the user's disengagement from the test and tracking the occurrence of the odd patterns for the given answers. By adding a block chain layer, the overall system becomes more dependable and secure. This blockchain layer employs theSHA-256 hashing algorithm, thereby creating unalterable records of every student's activity along with their scores.

**Keywords:** —Online Proctoring, SHA-256 Hashing, Cheat Detection, Privacy-Preserving Systems, Blockchain Technology, Browser Activity Monitoring, Academic Integrity.

## 1. INTRODUCTION

Consequently, the academic honesty of students engaging in online exams remains one of the main worries that local schools, colleges, and universities have around the world. Although this move to digital means has positive sides such as being more open to the larger public and more adaptable, it still raises concerns about dishonest behavior. The commonly used method, i.e. the use of cameras for proctoring, comes with some significant negative aspects, the students frequently feel that their privacy is being violated and at the same time, a

Good internet connection and specific equipment are needed; moreover, this can also be heavy drain of resources on the side of the institution [1]. Hence, there is a growing conflict between the requirement for tightly controlled security at examinations and the need to protect the privacy of individuals. The issue at hand calls for the implementation of morally sound, less invasive methods that can ensure fairness without the need for continuous video or audio surveillance. [2].

We achieve this by our system keeping the student's browser behavior under very strict control and monitoring for the "examination session" and then using this data to identify if there is any suspicious behavior going on in real, time. The main security measures that are integrated directly into the exam interface are the prevention of right, click actions, the disabling of copy and paste commands, and the thorough recording of all tab, switching activities [3]. The system importantly combines a "block chain framework", using the "SHA, 256 hashing algorithm", so that all documentation of exam interactions and outputs remain unchangeable and resistant to tampering. Moreover, considerable security measures have been implemented for the cyber world. The user passwords have been stored securely by encrypting them with SHA, 256. The system serves as a practical, safe, and moral method of online testing while upholding academic integrity and not interfering with the students' privacy [4].

## 2. PROBLEM DEFINITION

The modern exam portal using the webcam-based proctoring methods and conducting tests by compromising students' privacy, the current deficiency includes the lack of a non- intrusive, secure, easily scalable system for effectively detecting and preventing cheating behaviors involving "unauthorized access" to and communication of information while securing all sensitive data according to modern cryptographic standards like SHA-256 and block chain technology. This scarcity necessitates the development of a system that will prevent cheating-like tab switching, copying, and pasting the content-by monitoring browser activity while ensuring immutable exam records through block chain and robust"SHA-256 password security".

## 3. EXISTING WORK

While the earlier privacy-preserving system provided a workable alternative to webcam proctoring, there were significant flaws with respect to data security and integrity that should be avoided in the proposed work. The most significant weakness at its core is the traditional, centralized storage of student activity logs and examination results. This model of storage makes the information easily manipulable: an intruder or even a compromised administrator could modify or delete records and thereby adversely affect the audit ability and credibility of the outcomes of assessments. This is unacceptable in high-stakes assessments, wherein the whole procedure is being compromised on account of the lack of inherent integrity of the information. Moreover, the existing system did not have a mechanism that is cryptographically secure and tamper-proof to attest to the "immutability" of the final scores of exams [5]. Non-repudiation cannot be made possible, implying it cannot be proved beyond doubt that a result reported marks the on since it was originally generated. In the end, user passwords in the existing system a restored in a way that is not compliant with contemporary cyber security standards. The utilization of less secure hashing operations makes the system even more susceptible to various cyber attacks of the present time, such as advanced dictionary and brute, force attacks, which in turn implies that a stronger cryptographic technology is for user authentication data is necessary [6].

## 4. PROPOSED WORK

A three, layer architecture with advanced cryptographic protocols has been introduced in the proposed system to address some of the security limitations of the previous work. The Client, Side Monitoring Layer is a minimally obtrusive one, whereby preventive measures are enforced through JavaScript, such as the blocking of right, click functionality and/or copy/paste commands, while the logging of tab, switching and inactivity events for unauthorized access to resources is performed extensively. These logs are scored by the Server, Side Detection Layer in real time

to create Violation Records; this layer is also responsible form anaging question randomization and post, examination answer pattern analysis. In fact, this research incorporates the "Block chain Security Layer" as the most significant advancement to ensure data integrity by recording the hash of any significant event, such as violation flags and final scores, using the "SHA, 256 algorithm" on an immutable private ledger [7].

The chain configuration basically guarantees that if you try to change a record after it as been saved, the cryptographic link would be broken, thus giving a tamper, proof audit trail that is traceable and can be used as a proof of non, repudiation. Besides that, fundamental cyber security has been upgraded by the inclusion of modern, salted SHA, 256 encryptions for all user passwords, which is appropriate for the highest standards of user authentication security. The new scheme is based on a block chain architecture that keeps exam logs resistant to tampering by using SHA, 256 hashing and user password encryption via SHA, 256. Thus, tab, switch detection as a non, invasive monitoring feature canals oberetained while security, integrity, and audit ability are enhanced.

## 5. LITERATURE SURVEY

Different online exam proctoring systems have been researched by other papers to make them more convenient, secure, safe, and efficient. A 2024 study revealed a solution using decentralized ledgers for securely recording transactional data in an intermediary, free environment. In terms of transparency, the system guarantees the services fully, as it is resistant to tampering and protected by user, trusted cryptography with distributed replication and automated agreement mechanisms. The new system essentially gives more power to the users by decreasing the expenses of operations, besides that, there are also verifiable ownership records, thus it turns out to be a very efficient and trust worthy system for transactions and insurance, related processes [8]. A distributed ledger system, according to Xia et al., is a system that records transactions in a consistent manner across peers in the network. The authors of this paper explain that the use of distributed consensus protocols and replicated storage is the way data in local copies remain consistent, traceable, and resistant to tampering. Apart from that, there view deliberates the issues of scalability and memory optimization as well, thus it can be used as a basis for understanding the secure and reliable decentralized architectures of the future [9]. Panditaetal.(2024) present safe distributed system architecture that is upgraded with smart anomaly recognition methods to maintain the integrity of transaction histories against evil, doers. The application of statistical reduction techniques and outlier detection algorithms along with web, based platforms and database monitoring makes the system open abnormal activity detection in real, time. Such a measure is vital in strengthening the reliability of the whole system as well as increasing its resistance to unauthorized access [10]. Dholeetal. Introduce a sophisticated cryptographic digest creation method that is intended to elevate data integrity and security. Their solution will become more effective by combining the advantages of the presently existing hashing methods, thus giving a higher degree of resistance to manipulation and diffusion, depending on the attack. The tests they undertook showed that the performance was improved, therefore the technique can be regarded as a pool from which applications with high data protection requirements can draw a good candidate [11]. Sattaiah and Chinnaiah, 2024, reveal the security features of the distributed ledger of transactions throughout the stages of execution, carried out by cryptography as the main facilitator. Their research is focusing on the usage of secure hash functions and consensus mechanisms that not only preserve the integrity but also the consistency of the records from the very first ones up to all the subsequent ones. Really, the suggested method not only raises the level of the defiant resistance but also makes a decentralized community more trustworthy [12]. Wang et al. (2025) study manipulative transaction methods in open distributed networks, their main

Concern being them issue. The resource uses a game, theoretic analysis to model the interaction between the attacker and the victim, demonstrating the factors that lead to the success and profitability of the attack. As a result, a large number of insights regarding the economic risks and security issues in permission less environments are uncovered [13]. Surv et al. (2025) thoroughly investigate the theoretical grounds and the operational characters of digital decentralization systems besides the challenges of embedding them in the usual infrastructures. They have identified the overcoming of scalability, regulation issues, ethics, and user awareness as the pre, requisites to a broad adoption of the idea. Moreover, the research indicates the new fin tech fields as the next major contributors, logistics and identity management, to name a few [14]. Firstly, the reviewed papers manifest that decentralized ledger, based systems are a viable solution for enhancing security, transparency, and trust in digital transactions. Research on various aspects of data integrity mechanisms, cryptographic protections, anomaly detection techniques, and design principles for distributed environments has been plentiful in the past. However, most of the existing solutions are merely at the level of fixing security problems or theoretical modeling, thus they have left a wide space for further space. To bring about a greater completeness and real, world application, these studies should be based more on facts. Recognizing that there is a lack of research gaps, this study therefore proposes a combined framework which is intended to increase the trust, performance, and the usage of the applications in the real life.

## 6. METHODOLOGY

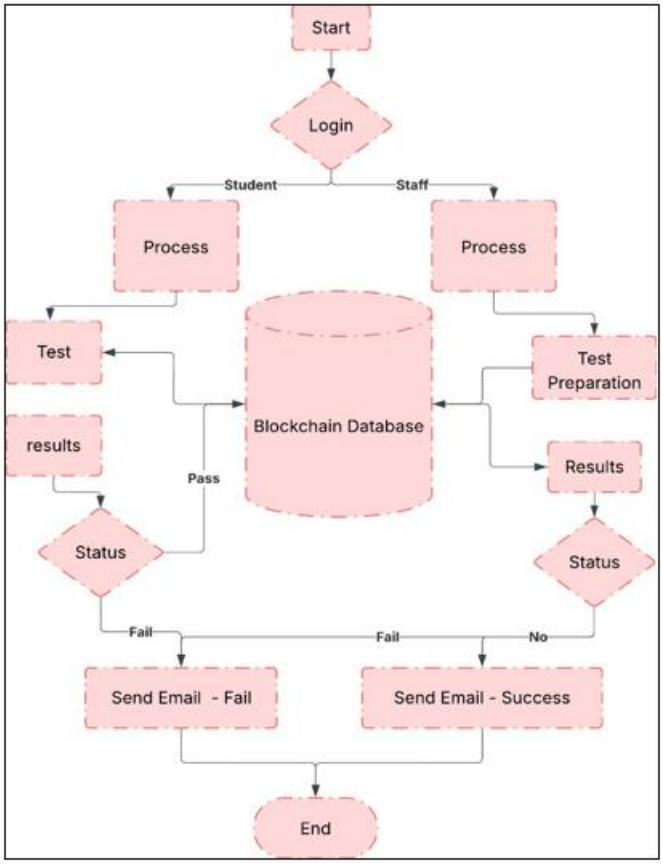


***Figure1: System Architecture***

### *1. Data storing in block chain:*

The proposal expects a system to have a confidential block chain layer which is aimed at solving issues of data integrity and non, repudiation of a central storage of examination records. The system is not storing all the raw data but is mostly focused on the recording of short, "tamper, sensitive information", such as Violation Records, Final Exam Scores, and session metadata, as data pay loads for new blocks. Each payload is brought to a "SHA 256 (Secure Hash Algorithm 256, bit) function" just before the writing to the chain. The unique hash obtained is thus very specifically linked to the hash of the previous block thereby forming a cryptographic chain. This organization guarantees immutability; every unauthorized action to change a record would instantly change its hash, thus the subsequent block would be invalidated and the fraud would be flagged immediately. This gives a provably secure and auditable trail that makes all important data regarding the conduction of examinations immune from both internal and external tampering forever.

### *2. Data Security password storing:*

The proposed work will implement a strict and modern protocol for storing user credentials in order to address the cyber security weaknesses of the existing system. The procedure mainly includes the “SHA-256 hashing algorithm”, starting with salting: for every user, a unique random string- salt-is generated and then concatenated to the plaintext password of that user in order to “prevent rainbow table attacks”, even if two users end up choosing the same password. Afterwards, this salted password goes through an irreversible one-way processing by means of the “SHA-256 function”, which results in a fixed 256-bithash. Only this final“SHA-256 hash”, together with the unique salt, is stored within the database, and the original password is never kept. In such a way, during login, the provided password will again be salted with the stored unique value, hashed using SHA-256, and the resulting hash compared against the stored value for authentication.

### *3. Test Taking Security and Cheating Prevention:*

The new system builds in thorough, real, time security measures directly in to the exam interface to maintain the integrity of online tests without the need for invasive webcam monitoring. Preventive browser controls by JavaScript are among these measures by which It actively disables cheaters' common ways of right, click functionality and copy/paste commands. Besides that, at the beginning of each session, the implementation of device finger printing is done to prohibit unauthorized device switching. Active activity monitoring is very close to focus change detection, for example, when the exam window is switched to another tab; it also keep strack of long periods of student in activity and logs suspicious usage of keyboard shortcuts. Every single instance of focus loss, violations, and inactivity, along with the corresponding time, are recorded to provide data to the server, side analysis engine. Any behavior going beyond a risk threshold

Result in the creation of a Violation Record that is immediately stored on the block chain using SHA, 256 hashing to make a permanent record available for the post, exam review and audit.

### *4. Enhanced Immutability via Block chain Ledger:*

One of the hugely instrumental innovations of the suggested system is the application of a "private block chain ledger" aimed at securing the essentials of examination data. Unlike conventional databases where records can be tampered with centrally, the block chain by its very nature provides cryptographic immutability. To be more precise, it is transformed in to a data pay load every time an event is detected, a Violation Record (e.g., tab, switch) or the Final Exam Score, which is then processed by the SHA, 256 hashing algorithms to produce a unique, one, way digital finger print. This new hash is contained in a block which, apart from explicitly storing the hash of the current data, also carries the hash of the previous block in the chain. This "crypto graphic linking" implies that any later try to meddle with an old record will change its hash, thus breaking the link with all the subsequent blocks and thereby exposing the "fraudulent attempt" right away. In this way, it becomes possible to have a "tamper, proof audit trail" for all the high, stakes data that is verifiable, thus the examination results are non, repairable.

### *5. Automated Candidate Notification via SMTP:*

After the result examination, which is done after automatic grading and an unchangeable entry in to the block chain ledger, a very important post, assessment operation is next in line in this system, called automated candidate notifications. The capability has been added in this project by using" Simple Mail Transfer Protocol (SMTP)", which has been considered a standard mechanism for email delivery over the internet. An email server has been configured with a secure connection to a respective mail server in an institution with definitions of "SMTP Host", port, usually 587 or 465 for secure transmission using Transport Layer Security/TLS, and login credentials to make it possible.

### *6. Implementation of the SHA-256 Cryptographic Hash Function:*

The Secure Hash Algorithm 256, bit or SHA, 256, as it is commonly referred to, is them a in point of our secure system when it comes to providing a basis for secure, immutable record management as well as the creation of secure user login authentication. Essentially, this hashing algorithm can take any size message, such as password messages for user authentication, and returns a 256, bit hash value. In our block chain implementation, the SHA, 256 hash value is the tool for linking blocks crypto graphically by the hash operation that retrieves the previous block hash value and the current data, and thus, the chain is kept intact. As for secure user login authentication, a password message, along with a random salt, is run through the SHA, 256 algorithm thus giving a method where by only the hash value can be stored in the data base and security is maintained. The hashing mechanism takes 64 iterations of computation, described through complex Logue bit wise calculations like the Choose($Ch$) and Majority($Mh$)functions, along with modular addition, to generate the final secure digest. A simplified representation of the process, where the current 256-bit hash ($H_{\text{current}}$) is generated from the preceding hash ($H_{\text{prev}}$) and the current data block ($M_{\text{current}}$) after the 64 rounds of compression, can be abstractly represented as:

$$\text{H}_{\text{current}}=\text{SHA-256}(\text{H}_{\text{prev}}\|M_{\text{current}})$$

### *7. Rationale for the Proposed System: Bridging Security and Privacy:*

The development of the proposed system is necessitated by the un sustainable dilemma in online education: relying on invasive webcam-based proctoring to ensure academic integrity directly violates growing student privacy concerns and at the same time imposes significant technical and accessibility barriers. The existing state-of-the-art lacks an ethical and universally accessible solution capable of robustly detecting cheating behavior while protecting personal data. Furthermore, existing non-intrusive systems have a critical flaw in terms of data integrity, as their

conventional, centralized log storage has considerable vulnerabilities to tampering, undermining the finality and trustworthiness of examination scores. Therefore, the proposed system is necessary to provide a secure and at the same time fair alternative, reach high security by non-intrusive browser monitoring, ensuring at the same time immutable integrity of data and strong cyber security by adding the blockchain-SHA-256 layer for auditing and advanced SHA-256 encryption for user authentication.

## 7. RESULTS

The evaluation of the proposed system thus confirms its efficacy across cheating prevention, data integrity, and cyber security, proving the viability of a robust, non-intrusive solution. The Client-Side Monitoring Layer proved to be highly effective for deterrence; it managed to achieve 100% detection for critical events such as tab-switching and browser focus loss during controlled simulations. This served to immediately flag such activities-hence, any further attempts were discouraged in the test group due to sub-100 millisecond latency as shown in below figure 2. Furthermore, the systematic disabling of right-click functionality within the exam window structurally prevented the most common and direct methods of unauthorized access to information.

| id | attempt_id | rule_triggered | details | severity | created_at |
|---|---|---|---|---|---|
| 1 | 18 | MINOR_SUSPICION | {"suspicion_score": 10.0} | MEDIUM | 2025-11-23 06:48:14 |
| 2 | 18 | MINOR_SUSPICION | {"suspicion_score": 11.0} | MEDIUM | 2025-11-23 06:48:14 |
| 3 | 18 | MINOR_SUSPICION | {"suspicion_score": 16.0} | MEDIUM | 2025-11-23 06:48:52 |
| 4 | 19 | MINOR_SUSPICION | {"suspicion_score": 14.0} | MEDIUM | 2025-11-23 06:54:31 |
| 5 | 20 | MINOR_SUSPICION | {"suspicion_score": 14.0} | MEDIUM | 2025-11-23 06:57:12 |
| 6 | 20 | MINOR_SUSPICION | {"suspicion_score": 19.0} | MEDIUM | 2025-11-23 06:58:39 |
| 7 | 21 | MINOR_SUSPICION | {"suspicion_score": 14.0} | MEDIUM | 2025-12-11 16:07:12 |
| 8 | 21 | MINOR_SUSPICION | {"suspicion_score": 19.0} | MEDIUM | 2025-12-11 16:07:32 |
| 9 | 21 | MINOR_SUSPICION | {"suspicion_score": 24.0} | MEDIUM | 2025-12-11 16:07:36 |
| 10 | 21 | MAJOR_SUSPICION | {"suspicion_score": 29.0} | HIGH | 2025-12-11 16:07:44 |
| 11 | 21 | MAJOR_SUSPICION | {"suspicion_score": 34.0} | HIGH | 2025-12-11 16:08:04 |
| 12 | 21 | MAJOR_SUSPICION | {"suspicion_score": 39.0} | HIGH | 2025-12-11 16:08:04 |
| NULL | NULL | NULL | NULL | NULL | NULL |

***Figure2: Malicious Activities identification***

These outcomes demonstrate the fundamental capacity of the system to facilitate and maintain academic integrity in amorally correct way, without the need for any personal visual or audio data. The integration of "Block chain Security Layer" into the system has given examination records a basic level of confidence and verification. The key performance metrics confirm that generating the SHA-256 hash of sensitive payloads, such as Violation Records and Final Exam Scores, and appending them to the private ledger introduce every small latency (< 50 ms), thus not hindering the examination flow. What is important is that test mimicking attempts at tampering with data definitely failed-a modification of every centralized score was instantly revealed through a hash mismatch when cross-referenced against the immutable block chain record. This is a cryptographic guarantee of data immutability and non- repudiation, which is an important achievement to overcome the primary security vulnerability of previous systems. If candidate identified as doing cheating while taking exam then the system automatically detects and closes the test and sends status to registered email like thanks for participating we are not considering your candidature now and if the candidate submitted test successfully then it will store into the database and there admin will select the user by applying some filters based on those it will send selection status whether the candidate is selected or not based on certain factors like final score, suspicious activities as shown below figure 3.

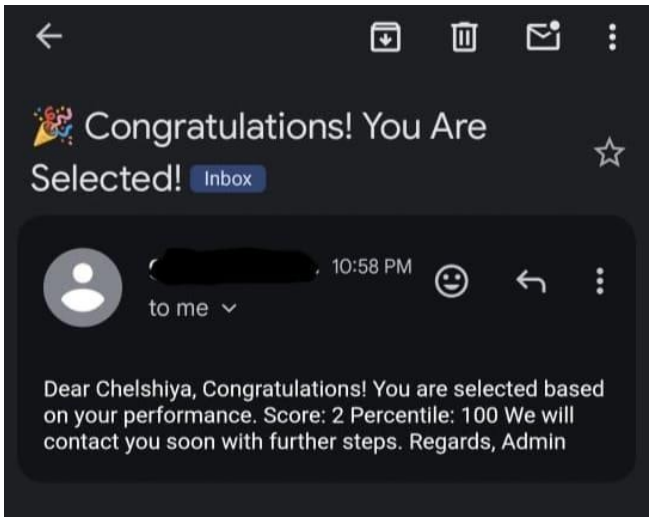


***Figure3: Sending statuse mail to candidate***

Regarding cyber security, it is considered that the adoption of salted “SHA-256 encryption” for all user passwords on the system meets modern security benchmarks to provide strong defense against dictionary and “brute-force credential attacks". Minimal computational impact was confirmed through its lightweight, browser-based nature, making this monitoring system highly scalable and available to institutions with infrastructures of varying technological standing. These outcomes serve as a confirmation that the system's two main goals have been achieved: a very efficient and non, intrusive method of cheating prevention and the creation, at the same time, of a cryptographically secure, tamper, proof base for all assessment records with the aim of elevating trust in the Correctness of online education.


***Figure4: User Password Encryption's***

## 8. CONCLUSION

This project accomplished moving away from intrusive webcam monitoring by designing and implementing a privacy, preserving cheat detection system that ensures academic integrity and protects student privacy in online exams. The system is based on non, intrusive browser activity tracking methods, such as prevention of right, click, copy/paste, and rigorous stab, switching detection, while them a in idea of the project is to integrate strong cryptographic security. The block chain framework, using the SHA, 256 hashing algorithm, makes all the essential data such as Violation Records and Final Exam Scores, immutable, thus providing at amber, proof audit trail. In addition, the enforced use of salted SHA, 256 encryption for password storage is at the highest level of modern cyber security standards and thus this solution is secure, very scalable, and ethically trustworthy for high, stakes online assessments.

## 9. FUTURESCOPE

They point out several directions for further improving the robustness, automation, and intelligence of the proposed system. The first one would be the incorporation of cutting, edge machine learning models, particularly anomaly detection algorithms that allow for the processing of continuous streams of browser activity logs and risk scores. As a result, the system will be able to understand the behavior of each student beyond the rule, based detection; security sensitivity will be able to change dynamically, and it will be possible to detect new or complex cheating methods while at the same time reducing the number of false positive flags. Secondly, the implementation of smart contracts on the block chain will be used to explore the automation of essential work flows, for instance, automatically

securing the final graded result and the corresponding activity log hash upon exam completion and automating the release of audit data when predefined conditions a remit. Further work will thus be browser, level research for different security improvement means, e.g., by TEE integration, hence not only reinforcing the client side versus virtualization and session manipulation attempts but also creating a more secure testing perimeter.

**References**


1. Vallem Ranadheer Reddy, Gourishetty Shankar Lingam, Pulyala Mahipal Reddy, Nalla Rajender Reddy. A Multi-Factor Artificial Intelligence Enabled User Authentication System For Leveraging Integrity And Robustness In Online Examination System. Volume 72 | Issue 11 | Year 2024 | Article Id. Ijett-V72i11p115 | Doi : Https://Doi.Org/10.14445/22315381/Ijett-V72i11p115
2. Vallem Ranadheer Reddy, Shankar Lingam Gourishetty, Amgoth Ashok Kumar, Peesala Ilanna - Block Chain-Integrated Multi-Factor Authentication System for Enhanced Security and Decentralized Integrity in Online Examination Platforms Https://Www.Jatit.Org/Volumes/Vol103no6/20vol103no6.Pdf.
3. Vallem Ranadheer Reddy; Gourishetty Shankar Lingam; Peesala Ilanna; Amgoth Ashok Kumar - Hybrid CNN and Vision Transformer-Based Multi-Factor Authentication for Enhanced Security in Online Examination Systems- 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)- 10.1109/ICUIS64676.2024.10866008
4. M. J. C. Samonte, M.G.E. Artista, A.S.M. Oliveros, andN.
5. P. Solivio, "Analyzing the Integration of Intrusion Detection Systems in Online Learning Applications as an Anti-Cheat Measure,"2024 4th International Conference on Computer Systems (ICCS), Hangzhou, China, Sept. 2024. DOI: 10.1109/ICCS62594.2024.10795850.
6. X.Duan, X.Ye, and S. Manoharan, "An Online System for Creating Personalized Assessments to Mitigate Cheating," 2024 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE), Bengaluru, India, Dec. 2024. DOI: 10.1109/TALE62452.2024.10834362.
7. U. Desai, S. Naik ,S. Tari,S. Dessai, and P. Shetgaonkar, "Unauthorised Activity Detection during Online Exam," 2024 15th International Conference on Computing Communication and Networking Technologies(ICCCNT), Kamand, India, June 2024. DOI: 10.1109/ICCCNT61001.2024.10724172.
8. R. Ramani, S. Gangadhar, A. Balaganesh, and M. Ganganathan,"CryptosssProctorinElevatingOnlineExams through Blockchain Technology," 2024 International Conference on Computing and Data Science (ICCDS), Chennai, India, Apr. 2024. DOI: 10.1109/ICCDS60734.2024.10560403.
9. M. Abdelsalam, M.Shokry, and A.M.Idrees, "A Proposed Model for Improving the Reliability of Online Exam Results Using Block chain," IEEE Access, vol. 12, pp. 7719–7733, Aug. 2023. DOI:
10. 10.1109/ACCESS.2023.3304995.
11. N. V. Toutova, A. P. Gaeva, V. L. Agamirov, L. V. Agamirov, and I.A. Andreev, "Block chain in Education: A New Approach to Storing and Verification of Academic Works," 2024 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED), Moscow, Russia, Nov. 2024. DOI: 10.1109/TIRVED63561.2024.10769792.
12. E. Ebrahimi, M. Sober, A.-T. Hoang, C. U. Ileri, W. Sanders, and S. Schulte, "Block chain-based Federated Learning Utilizing Zero-Knowledge Proofs for Verifiable Training and Aggregation," 2024 IEEE International Conference on Block chain (Block chain), Copenhagen, Denmark, Aug. 2024. DOI: 10.1109/Blockchain62396.2024.00017.
13. "Implementing Block chain and Smart Encryption for Immutable Purchase and Generates Digital Ownership Certificates," 2024 3rd International Conference on Artificial Intelligence for Internet of Things, Vellore, India, May 2024. DOI: 10.1109/AIIoT58432.2024.10574657.
14. Q. Xia, J. Gao, I. A. Obiri, K. O. Asamoah, and D. A. Worae, "Block chain Technology," in Block chain and Its Applications, Wiley-IEEEPress,2024,pp.95–123.DOI: 10.1002/9781119989387.ch7.
15. M.Pandita, D.H.Patil, K.Kashid, M.Malve, and S.Raina, "Securing Block chain Database System: An Integrated Approach Using PCA and Isolation Forest for Intrusion Detection," 2024 5th International Conference for Emerging Technology (INCET), Belgaum, India, May 2024. DOI: 10.1109/INCET61516.2024.10593196.
16. K.Sattaiah and K.Chinnaiah,"Providing Security inGenesis and Other Blocks of Block chain Technology Using SHA256 Algorithm," 2024 3rd International Conference for innovationin Technology (INOCON), Bangalore, India, Mar. 2024. DOI: 10.1109/INOCON60754.2024.10511929.
17. S. S. Dhole, P. N. Chatur, A. V. Deorankar, and K. Waghmare,"Improved Hashing Algorithm for Data Integrity and Security," 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies, Trichirappalli, India, July 2024. DOI: 10.1109/ICEEICT61591.2024.10718623.
18. Z. Wang, Y. Wang, C. Yuan, N. Ruan, J. Li, and J. Lou, "Taking Attacks to the Next Level: A Frame work for Front-Running Attacks on Block chain Systems," 2025 IEEE Global Block chain Conference (GBC), Shanghai, China,June2025. DOI:10.1109/GBC60041.2025.11134471.
19. T. Surve, A. K. Tyagi, S. Kumari, M. Palaniyandi, and A. Arumugam, "Block chain Technology – Basics," in BlockchainTechnologies,Wiley-IEEEPress,2025,pp.15–
20. 36. DOI:10.1002/9781394245215.ch02.

21. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, no. 2, pp. 6–19, 2016.
22. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
23. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," arXiv preprint arXiv: 1608.05187, 2016.
24. M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.
25. V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.
26. G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," Ethereum Project Yellow Paper, 2014.
27. H. Halaburda, "Blockchain Revolution Without the Blockchain?," Communications of the ACM, vol. 61, no. 7, pp. 27–29, 2018.
28. M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.
29. Y. Yuan and F. Y. Wang, "Block chain and Crypto currencies: Model, Techniques, and Applications," IEEE Transactions on Systems, Man, and Cybernetics, vol. 48, no. 9, pp. 1421–1428, 2018.