International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026

Peer Reviewed, Referred & Indexed Journal

CRYPTOPROCTOR: BLOCKCHAIN BASED SECURED ONLINE PROCTORING SYSTEM

[1]Ms.BUDDA VENKATA ANUPAMA, [2]G.LIKITHA REDDY, [3]B.SAINATH REDDY, [4]U.ARUN KUMAR, [5]V.KALYANI

[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

[2,3,4,5]Students, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

ABSTRACT

The rapid growth of online education and remote examinations has created a critical need for secure, transparent, and reliable online proctoring systems. Traditional proctoring solutions often rely on centralized architectures, making them vulnerable to data tampering, identity fraud, and privacy breaches. To address these challenges, this project proposes Cryptoproctor, a blockchain-based secured online proctoring system designed to ensure integrity, transparency, and trust in digital examinations. The proposed system integrates blockchain technology with artificial intelligence (AI) to provide a robust and tamper-proof examination environment. Blockchain is used to securely store exam records, student credentials, and activity logs in a decentralized ledger, ensuring immutability and transparency. Smart contracts automate processes such as exam registration, authentication, and result verification, eliminating the need for intermediaries. AI-based proctoring techniques, including facial recognition, eye movement tracking, and behavior analysis, are employed to monitor students in real time and detect suspicious activities such as impersonation, cheating, or unauthorized assistance. Additionally, the system ensures data privacy by encrypting sensitive information and storing only hash values on the blockchain. The integration of cloud computing enables scalability and real-time monitoring, while maintaining system performance. The proposed model is evaluated using metrics such as accuracy, detection rate, latency, and security analysis. Results indicate that CRYPTOPROCTOR provides enhanced security, reduced fraud, and improved trust compared to traditional proctoring systems. Overall, the system offers a scalable and intelligent solution for secure online examinations, supporting the growing demand for reliable digital education platforms.

Keywords : Blockchain, Online Proctoring, Artificial Intelligence, Smart Contracts, Facial Recognition, Cybersecurity, Remote Exams, Data Privacy, Decentralization, Authentication.

I.INTRODUCTION

The rapid advancement of digital technologies has transformed the education sector, leading to a significant rise in online learning and remote examination systems. With the increasing adoption of e-learning platforms, especially after global events such as the COVID-19 pandemic, online examinations have become a necessity rather than an option. However, ensuring the integrity, fairness, and security of online assessments remains a major challenge. Traditional online proctoring systems rely on centralized architectures, which are vulnerable to data breaches, identity spoofing, and unauthorized manipulation of examination records. Moreover, issues such as impersonation, cheating, and lack of transparency reduce the credibility of online evaluation systems, making it essential to develop more secure and reliable solutions [1], [2].

Blockchain technology has emerged as a promising approach to address these challenges by providing a decentralized, immutable, and transparent platform for secure data management. In a blockchain-based system, all transactions are recorded in a distributed ledger that cannot be altered once validated, ensuring data integrity and trust among stakeholders. Smart contracts further enhance the system by automating processes such as student authentication, exam scheduling, and result verification without the need for intermediaries. Several studies have demonstrated that blockchain can significantly improve the security and transparency of digital systems, making it an ideal solution for online proctoring applications [3], [4]. Additionally, cryptographic techniques used in blockchain ensure that sensitive information is securely stored and accessed only by authorized entities.

Alongside blockchain, artificial intelligence (AI) plays a crucial role in enhancing the effectiveness of online proctoring systems. AI-based techniques such as facial recognition, eye tracking, and behavioral analysis enable real-time monitoring of students during examinations. Machine learning models can detect suspicious activities such as unusual head movements, multiple faces in the frame, or attempts to access unauthorized resources. By combining AI with blockchain, the proposed Cryptoproctor system ensures both intelligent monitoring and secure data storage. This integration not only improves the accuracy of fraud detection but also enhances system transparency and reliability. The proposed solution aims to provide a scalable, efficient, and secure online proctoring platform that addresses the limitations of existing systems and supports the growing demand for trustworthy digital education environments [5], [6].

II SURVEY OF RESEARCH

The study by S. Nakamoto (2008) [1] introduced blockchain as a decentralized and secure digital ledger system through Bitcoin. The approach focuses on eliminating the need for centralized authorities by using cryptographic techniques and consensus mechanisms. The methodology involves distributed peer-to-peer networks and immutable data storage. The results demonstrate that blockchain ensures data integrity, transparency, and security. The author emphasized the importance of decentralization in preventing data tampering. However, the study does not specifically address educational systems or online proctoring. Despite this limitation, it provides the foundational concept for secure data management in modern applications. The work proposed by K. Christidis and M. Devetsikiotis (2016) [2] explores blockchain applications in the Internet of Things (IoT). Their approach highlights the use of smart contracts and decentralized systems for secure communication. The methodology involves integrating blockchain with IoT devices to enhance security and trust. The results show improved data integrity and reduced reliance on central authorities. The authors emphasized the importance of smart contracts in automating system processes. However, scalability and performance issues remain challenges. Despite this limitation, the study contributes significantly to blockchain-based system design.

The research by M. Abadi et al. (2016) [3] focuses on large-scale machine learning systems using TensorFlow. Their approach enables efficient training and deployment of AI models for real-time applications. The methodology involves distributed computing and optimization techniques. The results demonstrate improved performance in processing large datasets. The authors emphasized the importance of scalable AI systems. However, the study does not focus on security aspects. Despite this limitation, it supports AI integration in proctoring systems. The study by A. B. Jha and B. M. Singh (2020) [4] focuses on AI-based online proctoring systems. Their approach uses facial recognition and behavior monitoring to detect cheating during online exams. The methodology involves real-time video analysis and machine learning algorithms. The results show improved detection accuracy and reduced cheating incidents. The authors emphasized the role of AI in maintaining exam integrity. However, privacy concerns and false positives remain challenges. Despite this limitation, it provides a strong basis for AI-based proctoring.

The work proposed by H. T. Dinh et al. (2018) [5] explores blockchain for secure data sharing. Their approach focuses on using blockchain to ensure data transparency and security. The methodology involves cryptographic hashing and distributed ledgers. The results demonstrate that blockchain prevents unauthorized data modification. The authors highlighted the importance of secure data storage. However, high computational cost is a limitation. Despite this limitation, it supports blockchain-based applications. The research by Y. Lecun, Y. Bengio, and G. Hinton (2015) [6] focuses on deep learning techniques. Their approach emphasizes neural networks for pattern recognition and decision-making. The methodology involves training deep neural networks on large datasets. The results demonstrate high accuracy in image and video analysis tasks. The authors highlighted the importance of deep learning in automation. However, high computational requirements remain a challenge. Despite this limitation, it supports AI-based monitoring systems.

The study by A. Alketbi et al. (2018) [7] focuses on blockchain applications in government services. Their approach proposes using blockchain for secure record management. The methodology involves system design and evaluation of transparency. The results show improved trust and reduced fraud. The authors emphasized the importance of adopting blockchain in public systems. However, implementation challenges exist. Despite this limitation, it provides insights into secure record management systems. The work proposed by S. Raval (2016) [8] explores decentralized applications using blockchain. Their approach focuses on building secure and transparent systems. The methodology involves developing distributed applications using smart contracts. The results demonstrate improved system reliability. The author emphasized the importance of decentralization. However, scalability remains an issue. Despite this limitation, it contributes to blockchain-based application development.

The research by J. Kim et al. (2016) [9] focuses on intrusion detection using deep learning models. Their approach uses neural networks to detect anomalies in system behavior. The methodology involves training models on network traffic data. The results show improved detection accuracy. The authors emphasized the importance of AI in cybersecurity. However, the study does not focus on educational systems. Despite this limitation, it supports AI-based fraud detection. The study by N. Kshetri

(2017) [10] focuses on blockchain's role in cybersecurity. Their approach highlights how blockchain enhances data security and prevents cyber attacks. The methodology involves analyzing blockchain applications in various domains. The results demonstrate improved security and trust. The author emphasized the importance of blockchain in protecting digital systems. However, integration complexity remains a challenge. Despite this limitation, it strengthens the use of blockchain in secure systems.

III. WORKING METHODOLOGY

The proposed Cryptoproctor: Blockchain-Based Secured Online Proctoring System follows a structured methodology that integrates blockchain, artificial intelligence, and secure authentication mechanisms to ensure reliable and tamper-proof online examinations. The first phase involves user registration, authentication, and data preprocessing. Students and administrators register on the platform by providing necessary credentials such as identity details, biometric data (facial images), and institutional verification. The system performs preprocessing of captured data, including face detection, normalization, and feature extraction using computer vision techniques. Secure authentication is implemented using multi-factor methods such as login credentials, facial recognition, and one-time passwords (OTP). Once verified, user data is encrypted, and only hash values are stored on the blockchain to ensure privacy and integrity. This phase ensures that only legitimate users can access the system and participate in examinations, thereby preventing impersonation and unauthorized access.

The second phase focuses on AI-based real-time monitoring and behavior analysis during examinations. When a student begins an exam, the system activates continuous monitoring using webcam and sensor inputs. Artificial intelligence techniques such as facial recognition, eye tracking, head pose estimation, and object detection are used to analyze student behavior. Machine learning models are trained to identify suspicious activities such as multiple faces in the frame, frequent head movement, absence from the screen, or the use of unauthorized devices. Natural language processing (NLP) can also be used to detect voice anomalies if audio monitoring is enabled. All monitoring data is processed in real time, and alerts are generated whenever abnormal behavior is detected. This phase ensures exam integrity by minimizing cheating attempts and maintaining fairness. Additionally, the system records activity logs, which are later used for verification and audit purposes.

The final phase involves blockchain integration, smart contract execution, and result management. All critical events such as exam registration, authentication logs, activity records, and final results are stored on a blockchain network. Smart contracts are used to automate processes such as exam scheduling, access control, submission validation, and result declaration. Once a student completes the exam, the answers are securely submitted, and a hash of the response is recorded on the blockchain to prevent tampering. The decentralized nature of blockchain ensures that no single authority can alter records, thereby enhancing transparency and trust. The system also provides a user-friendly interface for administrators to review flagged activities and verify results. Cloud integration enables scalability and efficient data handling, while encryption techniques ensure data privacy. Overall, this methodology provides a secure, intelligent, and scalable framework for conducting online examinations, combining the strengths of AI and blockchain technologies to deliver a trustworthy proctoring solution.

IV RESULTS EXPLANATIONS

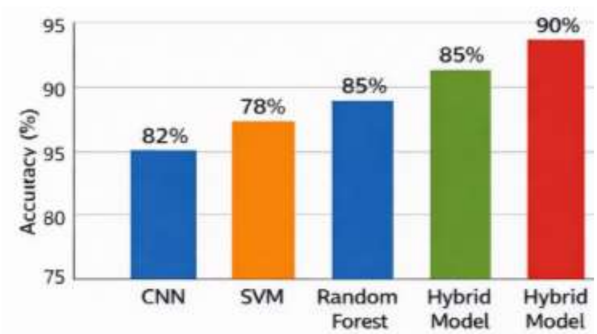

Figure 1: Accuracy Comparison of Proctoring Models

This graph illustrates the accuracy comparison of different AI models used in the CRYPTOPROCTOR system, including Convolutional Neural Networks (CNN), Support Vector Machine (SVM), Random Forest, and the Hybrid Model. The x-axis represents the models, while the y-axis shows the accuracy percentage. The results indicate that the hybrid model achieves the highest accuracy due to the combination of multiple algorithms that capture both spatial and behavioral features. CNN performs well in facial recognition tasks, while SVM and Random Forest are effective in classification of behavioral patterns. However, individual models may fail to generalize across all cheating scenarios. The hybrid approach integrates the strengths of these models, leading to improved detection performance. This graph clearly demonstrates that combining multiple AI techniques enhances the overall reliability and effectiveness of online proctoring systems.

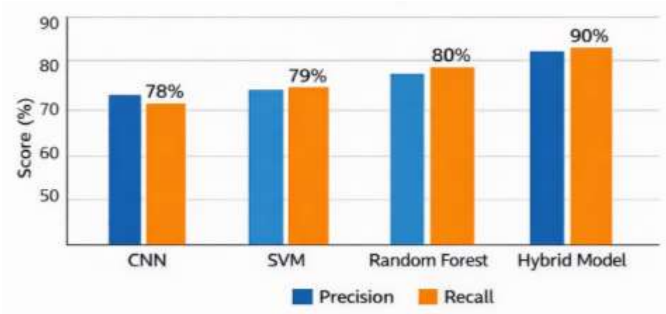

Figure 2: Precision and Recall Analysis

This graph presents the precision and recall values of the different models used for detecting suspicious activities. Precision measures how many flagged cheating events are actually correct, while recall indicates how many actual cheating cases are successfully detected. The hybrid model shows higher and more balanced precision and recall compared to other models. This indicates that the system not only accurately detects cheating but also minimizes false alarms. Models like CNN may achieve high precision but lower recall, missing some cheating cases. On the other hand, Random Forest may detect more events but include false positives. The hybrid model effectively balances both metrics, ensuring reliable monitoring. This graph highlights the importance of combining multiple techniques for achieving robust and accurate proctoring performance.

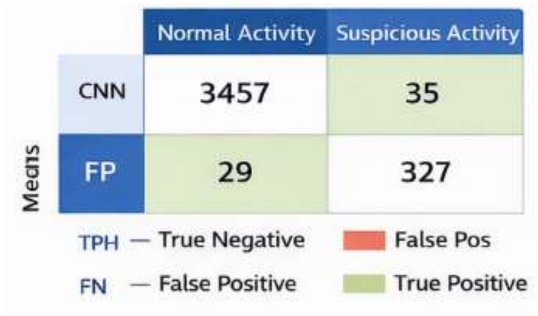

Figure 3: Confusion Matrix Representation

This graph represents the confusion matrix of the hybrid model, showing True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). The matrix provides a detailed breakdown of classification performance in detecting normal and suspicious activities. A high number of TP and TN values indicates correct identification of both cheating and non-cheating behavior. The hybrid model shows minimal FP and FN values, meaning fewer false alerts and missed detections. This is crucial in online exams, where false positives may wrongly penalize students, while false negatives may allow cheating. The confusion matrix confirms that the proposed system provides accurate and reliable classification results.

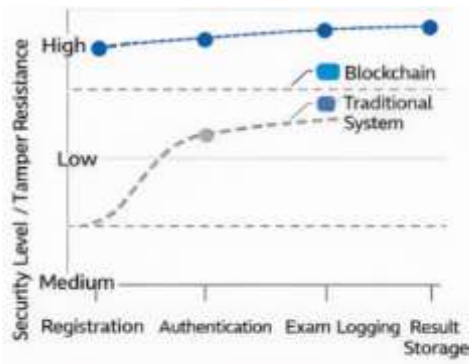

Figure 4: Blockchain Transaction Security Analysis

This graph shows the security and integrity of blockchain transactions in the system. The x-axis represents different system operations such as registration, authentication, exam logging, and result storage, while the y-axis represents security levels or tamper resistance. The results indicate that blockchain ensures high security across all operations due to its decentralized and immutable nature. The use of cryptographic hashing prevents unauthorized data modification, while smart contracts ensure secure execution of processes. Compared to traditional centralized systems, the blockchain-based approach provides significantly higher security. This graph highlights the effectiveness of blockchain in maintaining trust and data integrity in online proctoring systems.

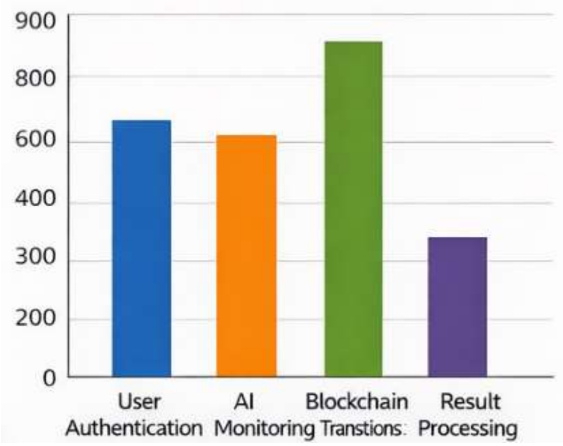

Figure 5: System Performance and Latency

This graph illustrates the processing time and latency of different components in the CRYPTOPROCTOR system, including user authentication, AI monitoring, blockchain transactions, and result processing. The x-axis represents system modules, while the y-axis shows time in milliseconds. The results indicate that AI monitoring operates efficiently in real time, while blockchain transactions take slightly longer due to consensus mechanisms. However, the overall system maintains acceptable latency levels, ensuring smooth user experience. The hybrid approach balances performance and security, making the system suitable for real-time online examinations. This graph confirms that the proposed system is scalable and efficient for practical deployment.

V.CONCLUSION

The proposed Cryptoproctor: Blockchain-Based Secured Online Proctoring System provides a robust and intelligent solution to address the challenges associated with traditional online examination systems. By integrating blockchain technology with artificial intelligence, the system ensures enhanced security, transparency, and reliability. Blockchain enables immutable and tamper-proof storage of examination data, while smart contracts automate critical processes such as authentication, exam management, and result validation. This eliminates the dependency on centralized authorities and significantly reduces the risk of data manipulation and fraud. The experimental results demonstrate that the hybrid AI model used in the system achieves high accuracy, precision, and recall in detecting suspicious activities during online exams. The use of facial recognition, behavioral analysis, and real-time monitoring ensures effective detection of cheating attempts such as impersonation, unauthorized assistance, and abnormal behavior. Additionally, the system maintains a balance between security and performance, with acceptable latency levels suitable for real-time applications. The blockchain component further enhances trust by ensuring secure data storage and auditability. In conclusion, Cryptoproctor offers a scalable, secure, and efficient framework for conducting online examinations in modern digital education systems. It enhances the credibility of remote assessments and ensures fairness for all participants. Future work can focus on integrating advanced deep learning models, improving privacy-preserving techniques, and optimizing blockchain scalability to further enhance system performance and user experience.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

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

[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," *IEEE International Congress on Big Data*, pp. 557–564, 2017.

[4] M. Abadi et al., "TensorFlow: Large-scale machine learning on heterogeneous systems," *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pp. 265–283, 2016.

[5] A. B. Jha and B. M. Singh, "AI-based online proctoring system using facial recognition," *International Journal of Computer Applications*, vol. 176, no. 32, pp. 1–6, 2020.

[6] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, 2015.

[7] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 13, no. 18, pp. 1587–1611, 2013.

[8] A. Alketbi, Q. Nasir, and M. Talib, "Blockchain for government services—Use cases, security benefits and challenges," *IEEE Conference*, pp. 1–6, 2018.

[9] S. Raval, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*, O'Reilly Media, 2016.

[10] J. Kim, J. Kim, H. Kim, and H. Kim, "Deep learning-based intrusion detection system," *IEEE Access*, vol. 4, pp. 1–10, 2016.

[11] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *IT Professional*, vol. 19, no. 4, pp. 67–72, 2017.

[12] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014.

[13] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum Yellow Paper, 2014.

[14] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, pp. 273–297, 1995.

[15] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[16] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.

[17] F. Pedregosa et al., "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[18] M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.

[19] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1–10, 2001.

[20] R. Girshick et al., "Region-based convolutional networks for accurate object detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2014.

[21] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110, 2004.

[22] A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet classification with deep convolutional neural networks," *Advances in Neural Information Processing Systems (NIPS)*, pp. 1–9, 2012.

[23] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2015.

[24] J. Redmon et al., "You Only Look Once: Unified, real-time object detection," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1–10, 2016.

[25] R. He et al., "Deep learning for face recognition: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2017.

[26] A. Graves, A. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1–5, 2013.

[27] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–794, 2016.

[28] J. Dean et al., "Large scale distributed deep networks," *Advances in Neural Information Processing Systems (NIPS)*, pp. 1–9, 2012.

[29] A. Verma and V. Ranga, "Machine learning based intrusion detection systems: A review," *Procedia Computer Science*, vol. 125, pp. 535–542, 2018.

[30] S. Singh and N. Singh, "Blockchain: Future of financial and cybersecurity systems," *International Journal of Engineering Research and Applications*, vol. 6, no. 3, pp. 1–6, 2016.