iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79920

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

AI-Based Online Examination Proctoring System

Mrs. Banupriya K. M.[1], Rayeesa Anjhum H.[2], Soundharya M.[3], Nishanthi S.[4], Nandhitha G.[5]
[1]*Assistant Professor, Department of Computer Science and Engineering, Arunai Engineering College, Tamil Nadu, India*
[2, 3, 4, 5]*Department of Computer Science and Engineering, Arunai Engineering College, Tamil Nadu, India*

Abstract: ***Online examinations have become a cornerstone of modern education, yet they are increasingly vulnerable to sophisticated threats such as cheating, impersonation, and the illicit use of AI-generated content. Traditional proctoring solutions often suffer from high human dependency and significant privacy risks due to centralized data storage. To address these challenges, this paper proposes a next-generation, AI-based privacy-preserving online examination proctoring system. The framework utilizes Federated Learning to ensure that sensitive student data is processed locally, thereby maintaining strict data confidentiality.***

Integrity is further reinforced through a multi-layered monitoring approach: remote Photoplethysmography (rPPG) is employed to analyze physiological stress signals via a webcam to detect suspicious behavior , while Keystroke Dynamics provides continuous identity verification based on unique typing patterns. Additionally, the system incorporates a voice-based AI Proctor Agent for real-time automated warnings and Large Language Model (LLM)-based plagiarism detection to identify AI-generated or copied answers in real-time. By integrating these advanced AI and machine learning techniques, the proposed system offers a secure, fair, and scalable solution that reduces the burden of manual invigilation while ensuring the overall reliability of the examination environment.

Keywords: Artificial Intelligence , Machine Learning , Federated Learning , Online Proctoring , rPPG (Remote Photoplethysmography) , Keystroke Dynamics , Privacy-Preserving AI , LLM-based Plagiarism Detection , Behavioral Biometrics , Cheating Prevention.

I. INTRODUCTION

A. Overview

This project introduces an AI-powered, privacy-preserving intelligent proctoring system belonging to the domain of EdTech. The system aims to create a secure, fair, and trustworthy environment for remote assessments, university internal assessments, and competitive exams. By utilizing advanced AI and Machine Learning techniques like **Federated Learning**, the system ensures that student data is processed locally, maintaining high levels of privacy. The integration of multi-modal monitoring, including behavioral biometrics and physiological analysis, sets this framework apart from traditional solutions.

B. Problem Statement

Current online examination systems face several critical limitations that undermine their reliability:

- Detection Gaps: Inability to detect AI-generated answers and limited cheating detection techniques.
- Resource Dependency: High dependency on human invigilators for monitoring.
- Privacy Risks: High risk of student data privacy violations due to centralized data processing.
- Identity Issues: Weak mechanisms for continuous identity verification during the exam.

C. Objectives

The primary objectives of this proposed system are:

- To Preserve Privacy: Implementing Federated Learning to keep student data on local devices.
- To Enhance Security: Utilizing Keystroke Dynamics and rPPG-based stress monitoring for continuous authentication and behavioral analysis.
- To Automate Monitoring: Deploying a voice-based AI Proctor Agent to provide real-time warnings and reduce manual supervision.
- To Combat AI Misuse: Integrating LLM-based plagiarism detection to identify copied or AI-generated content instantly.

II. LITERATURE REVIEW

1) Prof. Bharath Kumar B S et al. (2025) proposed a CNN-based multi-modal monitoring system integrating facial recognition and gaze tracking for real-time behavior analysis. However, its dependence on centralized high-bandwidth video processing limits accessibility and increases false positives in low-connectivity areas.
2) Pushpendra Kumar Sahure & Vipin Kumar (2025) and Neeraj S (ProctorEdge, 2025) introduced dual-layer audio-video monitoring using deep learning for voice and noise detection. Although secure, the system requires high-end hardware and raises privacy concerns due to centralized storage of sensitive data.
3) Dr. Jayshree R. (2025) and Tejaswini H S et al. (2025) implemented head-pose and eye-gaze tracking to monitor student focus. While effective, performance drops significantly under poor lighting conditions.
4) Aditya Pawar et al. (2025) and Kondreddi Lakshmi Narayana et al. (2025) focused on detecting digital cheating through tab-switching and unauthorized application monitoring. However, these approaches do not address impersonation or secondary device usage.
5) Sathish Kumar et al. (2025) proposed a hybrid CNN-LSTM model for detecting temporal behavioral anomalies such as posture shifts and eye movements. Despite improved detection accuracy, the system suffers from high latency during peak usage.
6) J. Lee and M. Kumar (2025) and L. Zhang et al. (2025) introduced Federated Learning with FedAvg to process biometric data locally, sharing only encrypted gradients. This approach significantly improves privacy, scalability, and bandwidth efficiency.
7) Dr. Tripathi et al. (2025) developed a multi-modal AI proctoring system integrated with the Gemini AI engine for context-aware anomaly detection. The system automates reporting but increases architectural complexity.
8) Vishal A S et al. (2025) proposed a CNN-based real-time object detection framework. However, reliance on centralized video streaming leads to bandwidth issues and deployment challenges in unstable network environments.

III. PROPOSED SYSTEM

A. *Key Functional Modules*

1) AI Proctor Agent: The AI Proctor Agent is the main monitoring component of the system. It continuously supervises the exam using video and audio analysis and generates alerts when suspicious behavior is detected.
2) Federated Learning (FL): Federated Learning processes student data locally on their device. Only encrypted model updates are sent to the server, ensuring strong privacy protection.
3) rPPG Stress Monitoring: The rPPG module uses webcam input to estimate heart rate and stress levels. Sudden stress changes may indicate unusual or suspicious behavior.
4) Keystroke Dynamics: This module analyzes typing speed and rhythm. It helps in verifying student identity continuously during the exam.
5) Wearable & AR-Glass Detection: AI-based object detection identifies hidden gadgets like smart glasses and mobile phones. It prevents the use of unauthorized devices during exams.
6) Encrypted Updates: All sensitive data is converted into encrypted updates before transmission. This prevents direct exposure of raw biometric information.
7) Cloud Server & Analytics: The cloud server aggregates model updates and performs centralized analysis. It stores reports and improves overall detection accuracy.
8) LLM-Based Plagiarism Detection: The system checks answers using AI-based plagiarism detection. It identifies copied or AI-generated content in real time.

B. System Architecture

The system follows a Decentralized Edge-AI model. Instead of streaming video to a server, all heavy AI processing happens on the student's local device to ensure speed and privacy.

1) Client-Side (Local) Layer

This layer handles all data collection and immediate analysis without sending video to the cloud.

- Vision Module: Uses YOLOv8 for object detection (phones/books) and MediaPipe for gaze tracking.
- Physiological Module: Employs rPPG to calculate heart rate from facial skin color changes.
- Behavioral Module: Monitors Keystroke Dynamics to verify the user's typing rhythm.

2) Privacy & Communication Layer

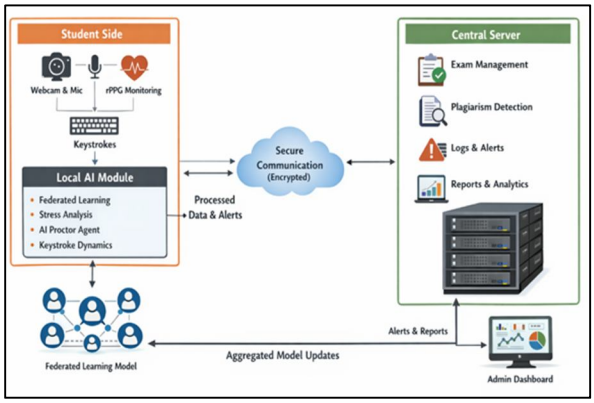
This layer manages the flow of information using Federated Learning.

- Local Inference: The device checks for cheating locally.
- Encrypted Updates: Instead of raw video, only "Model Weights" or "Violation Alerts" are sent to the server.
- Bandwidth Efficiency: Saves significant internet data by avoiding video streaming.

3) Server-Side (Admin) Layer

The central server acts as the final decision-maker and reporting hub.

- Integrity Dashboard: Compiles local alerts into a final "Integrity Score" for the teacher.
- LLM Plagiarism Check: Analyzes submitted answers to detect if they were generated by ChatGPT or other AI tools.



C. Tools and Technologies

Programming Languages

- Python – For AI model development and backend processing

Frontend Technologies

- HTML
- CSS
- JavaScript

Backend Technologies

- Flask
- REST API Integration

Artificial Intelligence & Machine Learning

- TensorFlow / PyTorch
- OpenCV (for face & object detection)
- Scikit-learn (for behavioral analysis)

Biometric & Monitoring Modules

- rPPG Algorithm (Physiological stress monitoring)
- Keystroke Dynamics Model
- Object Detection Model (YOLO / CNN)

Security & Privacy
- Federated Learning Framework
- AES Encryption / Secure HTTPS

Cloud & Database
- Firebase / AWS / Azure
- MySQL

Plagiarism Detection
- LLM-based Text Analysis
- NLP Techniques (SpaCy / NLTK)

IV. METHODOLOGY

1) User Authentication & Registration: The system verifies identity using facial recognition with liveness detection to prevent impersonation. Keystroke dynamics provides continuous authentication by analyzing typing behavior throughout the exam.

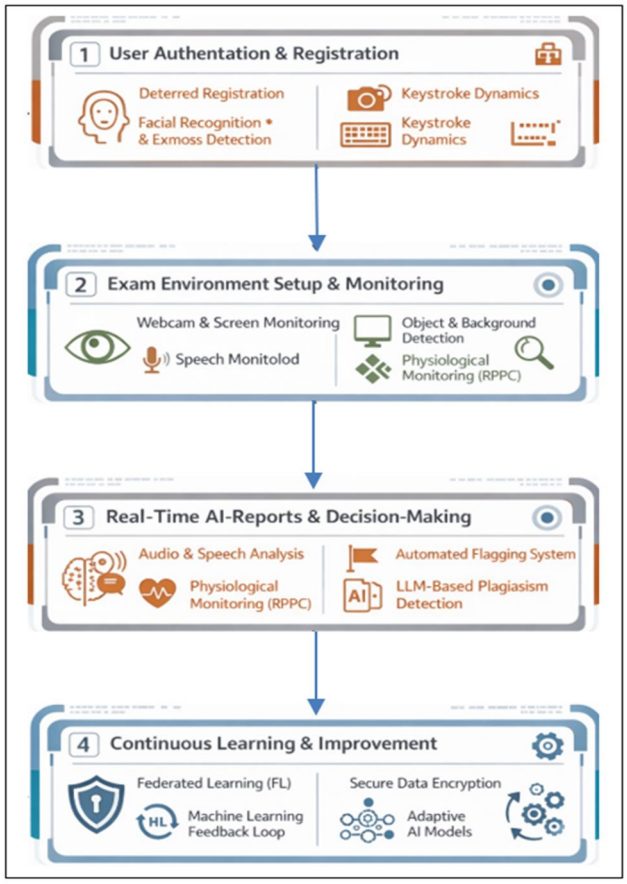
2) Exam Environment Monitoring: Webcam and screen monitoring track facial activity and surroundings in real time. AI-based object detection identifies unauthorized devices and additional persons in the environment.

3) Real-Time AI Proctoring: A voice-based AI agent performs audio monitoring to detect suspicious communication. rPPG-based physiological analysis monitors heart rate variations to identify abnormal behavior.

4) Proctoring & Decision-Making: An AI-driven anomaly detection model generates automated flags and proctoring scores. LLM-based plagiarism detection evaluates responses for AI-generated or copied content.

5) Data Security & Privacy: Federated Learning ensures local data processing, sharing only encrypted model updates. Secure encryption protocols protect all communications between client and server.

6) Continuous Model Improvement: A federated feedback loop refines the global model using aggregated updates. Adaptive AI models continuously improve detection accuracy and reduce false positives.



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

V. IMPLEMENTATION AND RESULT

A. Implementation

1) Environment Setup & Tool Configuration

The first step is setting up the development environment on the machine.

- Language: Python is installed as the primary language for AI and backend logic.
- Framework: Flask is configured to manage web requests and API integrations.
- Database: MySQL is used to store student data, exam questions, and proctoring logs.
- IDE: Tools like Spyder or VS Code are used for writing and debugging scripts like main.py, vision.py, and qachat.py.

2) User Interface (Frontend) Development

The frontend is designed using HTML, CSS, and JavaScript to create a user-friendly and intuitive experience.

- Login Page: Built with integrated webcam access for facial recognition.
- Exam Interface: A secure window that displays questions, a countdown timer, and the live proctoring status.
- Warning System: Pop-up alerts and audio cues (integrated via JS) provide instant feedback if the AI detects a violation.

3) Database Schema & SQLyog Integration

Using SQLyog, the MySQL database is structured to handle high-concurrency access.

- Tables: Separate tables are created for Students, Teachers, Exams, Questions, and Proctoring_Logs.
- Security: Queries are optimized for speed, and sensitive data like passwords and biometric hashes are stored using SHA-256 encryption.

4) Exam Engine & AI Algorithm Implementation

The core engine is developed in Python to retrieve data from MySQL and present it to the student.

- Cheating Detection: This is the heart of the engine, where AI Algorithms are implemented.
- Vision AI: YOLOv8 is integrated to detect unauthorized objects (phones, books).
- Identity AI: Keystroke Dynamics algorithms monitor typing rhythms to prevent impersonation.

5) Proctoring System & Video Monitoring

The video monitoring system is integrated using Flask and OpenCV.

- Webcam Integration: The webcam feed is processed locally to track Gaze (Eye Movement) and Head Pose.
- Physiological Layer: The rPPG module is implemented to extract heart rate signals from facial video frames to monitor stress levels.
- Gemini AI Integration: High-risk frames are sent to the Google Gemini API for deep reasoning, ensuring that complex cheating scenarios are accurately identified.

6) System Testing & Debugging

Thorough testing is conducted to ensure the system is "Exam-Ready."

- Functionality Testing: Verifying that all buttons, timers, and questions load correctly.
- Stress Testing: Checking if the system can handle multiple local AI modules running simultaneously.
- Accuracy Validation: Measuring the False Positive Rate of the AI to ensure students aren't wrongly accused of cheating.

7) Deployment

The final step is deploying the system on a secure web server (such as AWS or Google Cloud). This allows students and educators to access the platform from anywhere while maintaining the decentralized Federated Learning architecture to keep local data private.

B. Result

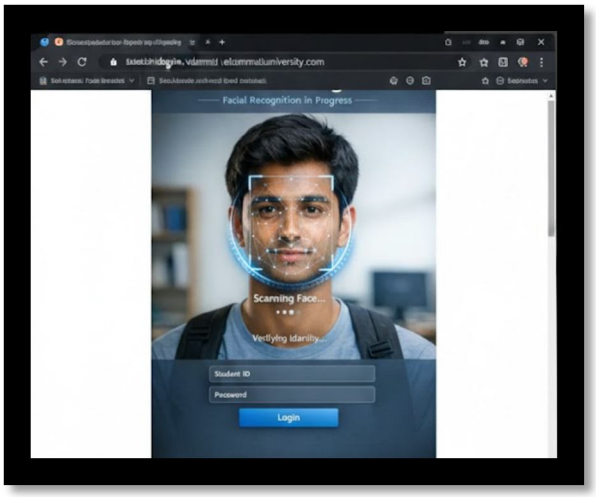


Fig 1: Facial Recognition Login Page

Fig 2: Live Proctoring Dashboard

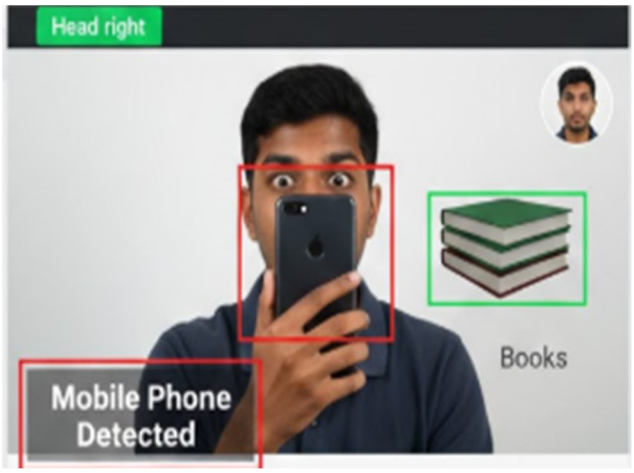


Fig 3: Object Detection

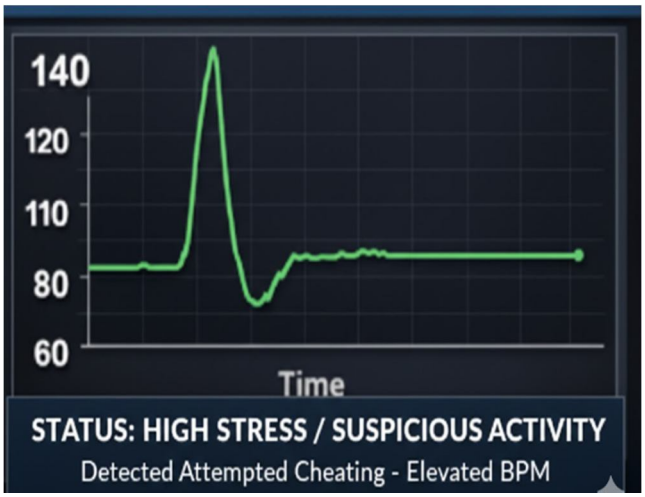


Fig 4: Heart Rate Monitoring

Fig 5: AI Warning Alert

Fig 6: AI Warning Report

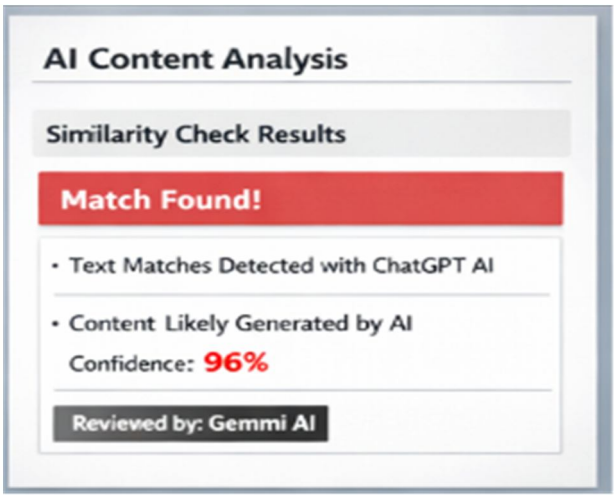


Fig 7: AI-Generated Content Check

VI. CONCLUSION

In conclusion, the AI-Based Online Examination Proctoring System provides a privacy-preserving, multimodal framework that ensures exam integrity while protecting sensitive student data. Leveraging Federated Learning, all biometric and behavioral information—including facial features, eye gaze, typing patterns, and rPPG-based heart rate monitoring—is processed locally, minimizing centralized data risks and ensuring compliance with data protection standards. The system integrates physiological monitoring, Keystroke Dynamics, and YOLOv8 object detection to detect stress, continuously verify identity, and monitor for prohibited devices such as mobile phones, smartwatches, and AR-glasses in real time. An AI Proctor Agent evaluates live webcam feeds to track gaze, posture, and environmental compliance, while LLM-based content verification identifies AI-generated or plagiarized responses to uphold academic honesty. Combined with a dynamic Trust Score that quantifies behavioral consistency and adherence to exam protocols, the system delivers high detection accuracy with minimal latency. Its scalable, modular architecture allows deployment across diverse online exam platforms and supports future integration of advanced AI models, additional sensor inputs, and adaptive assessment formats. Overall, this framework establishes a robust, secure, and ethical solution for modern remote examinations, providing transparency, accountability, and a next-generation standard for trustworthy digital education.

VII. FUTURE SCOPE

While the current iteration of AI-Based Online Examination Proctoring System establishes a strong security foundation, several advancements are envisioned for future development:

1) 5G-Enabled Edge Orchestration: Integrating 5G technology to facilitate ultra-low latency synchronization of global model updates in massive-scale federated environments.

2) 3D Gaze Estimation and Attention Mapping: Incorporating advanced eye-tracking algorithms to provide deeper insights into student cognitive engagement and focus without requiring specialized hardware.

3) Adaptive Emotional Intelligence: Utilizing Affective Computing to detect extreme student anxiety or burnout, allowing the system to provide supportive interventions during high-pressure exams.

4) Stealth Device Recognition: Enhancing the object detection library to identify miniaturized and subcutaneous communication devices using Transformer-based vision architectures.

REFERENCES

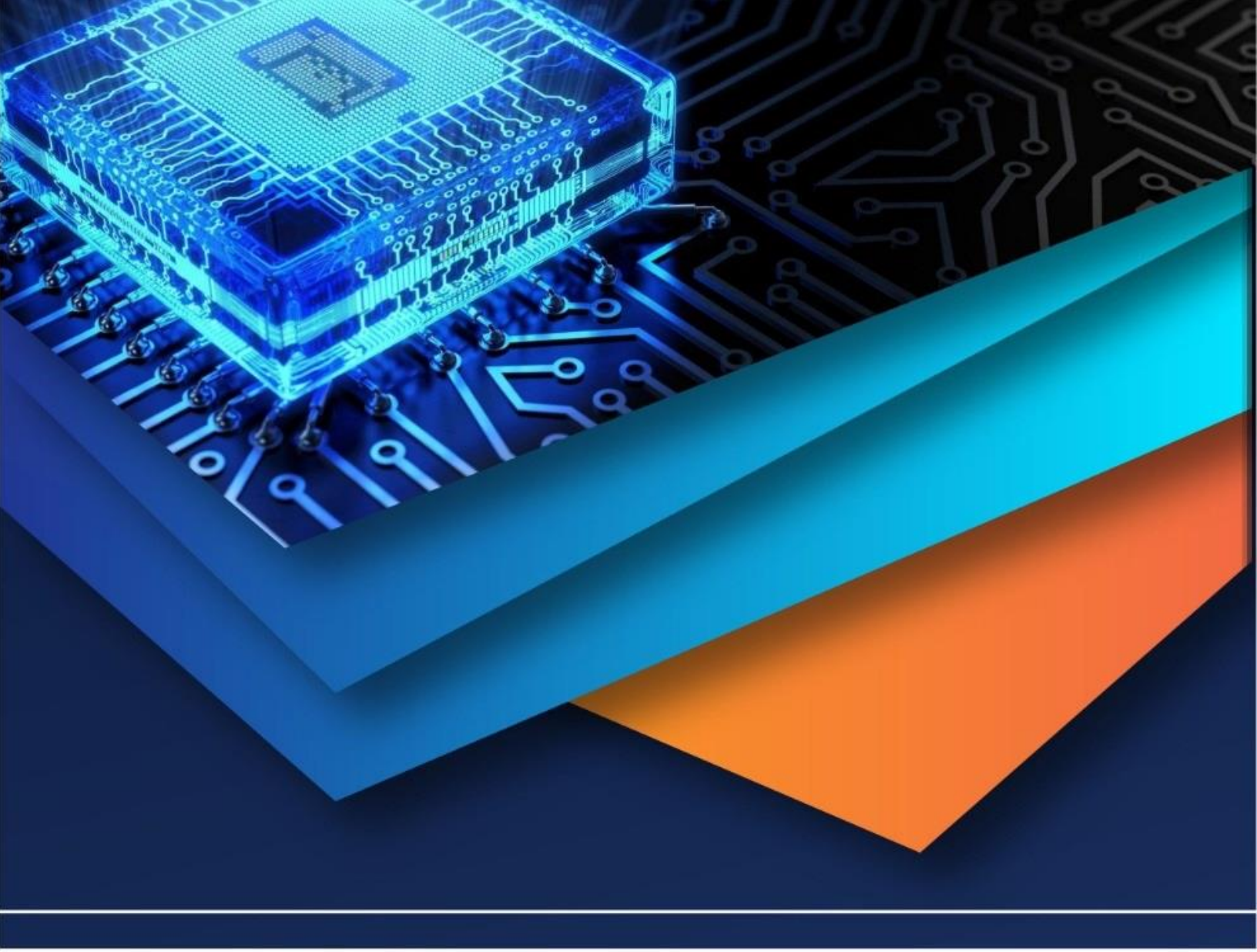
[1] J. Lee and M. Kumar, “Privacy-Preserving AI-Based Online Examination Proctoring Using Federated Learning,” IEEE Access, vol. 13, pp. 14567–14579, 2025.

[2] R. Sharma, P. Verma, and S. Iyer, “Real-Time Cheating Detection in Online Exams Using Deep Learning and Computer Vision,” in Proceedings of the IEEE International Conference on Artificial Intelligence and Data Engineering (AIDE), 2025, pp. 210–216.

[3] L. Zhang et al., “Federated Learning for Secure and Scalable Remote Assessment Systems,” Journal of Information Security and Applications, vol. 78, 2025.

[4] T. Ahmed and K. Rahman, “Keystroke Dynamics-Based Continuous Authentication for Online Examination Security,” IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 7, no. 1, 2025.

[5] G. Akçapınar, "Detecting AI-Assisted Cheating in Online Exams through Behavior Analytics," arXiv preprint arXiv:2510.18881, 2025.
[6] A. K. Naveen, B. Singla, R. Wankhade, S. M., R. S. Ramu, and R. M. Reddy Guddeti, "AutoOEP — A Multi-modal Framework for Online Exam Proctoring," arXiv preprint arXiv:2509.10887, 2025.
[7] N. S., K. Rohith, and A. R., "ProctorEdge: Advanced AI Examination Monitoring and Security System," SciTePress – Science and Technology Publications, 2025.
[8] E. Xu, J. Lu, S. Xu, et al., "Cheating Recognition in Examination Halls Based on Improved YOLOv8," Discover Computing, vol. 28, article 256, 2025.
[9] S. G. Satpute and T. S. Babasaheb, "Real-Time AI Solutions for Preventing Academic Cheating and Malpractices in Examinations," International Journal of Advanced Scientific Research, vol. 10, no. 3, pp. 72–75, 2025.
[10] "Behavioral Biometrics for Remote Exam Integrity: Continuous Authenticity Assessment via Keystroke Dynamics," Procedia Computer Science, vol. 274, pp. 402–411, 2025.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY