

Intelligent Video Proctoring System Using MediaPipe and DeepFace

Jarugulla Saranya¹, Bh. VijayaLaxmi², G. Rajasekharam³

¹M.Tech Student, Department of Computer Science & Engineering, Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagaram - 535216, Andhra Pradesh, India

²Assistant Professor, Department of Computer Science & Engineering, Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagaram - 535216, Andhra Pradesh, India

^{3,4,5,6}Assistant Professor, Department of Computer Science & Engineering, Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagaram - 535216, Andhra Pradesh, India

Email: jarugullasaranya@gmail.com

Abstract - This paper discusses the design of an intelligent video proctoring system aimed at securing remote evaluations and interviews. This multi-faceted platform incorporates artificial intelligence, computer vision, and modern web technologies (to provide real-time continuous identity verification and monitoring for behavioral anomalies) in order to facilitate secure remote assessments. At the core of the system is a facial recognition algorithm (DeepFace) utilizing the ArcFace algorithm for face matching. MediaPipe is utilized to perform gaze tracking, head pose estimation, and facial landmark recognition. Anomalies are detected based upon browser level activity such as tab switching or screen interruption and are flagged for atypical behavior based upon these same events. An instant fraud alert is sent to the administrator via a WebSocket after evaluating all of the signals from the three location anomaly sources using a weighted assessment score. The application's architecture employs React, TypeScript, FastAPI and Python to enable low latency, distributed processes with scalable capabilities. User management with role-based access control (RBAC), JWT authentication, encrypted session communication, event-based audit logging, etc. enhance the remote assessment's integrity, limit impersonation, create transparency during on-line assessments and provide reliability in employment decisions.

Key Words: Intelligent Video Proctoring, DeepFace, MediaPipe, Behavioral Analysis, Real-Time Fraud Detection

1.INTRODUCTION

Due to the significant growth in online education, remote recruiting, and virtual certification programs, there is an ever-increasing need for digital assessment platforms that are secure and reliable. Many of the traditional online testing platforms are poorly equipped with adequate systems to verify identity continuously and monitor behavior, which leaves open the opportunity for impersonation, cheating, or receiving assistance from someone other than themselves [1]. The challenge of maintaining the integrity and transparency of remote interviews and examinations in the academic and corporate environment has become a major issue as they continue to grow in popularity [2]. The current methodologies of online proctor solutions generally consist of basic forms of monitoring, such as web-based camera recording and browser

activity tracking, which are not sufficient to detect sophisticated forms of fraudulent behavior in real-time [3].

The recent advances in the areas of artificial intelligence (AI), computer vision (CV), and machine learning (ML) have allowed for the development of smart proctoring systems that are able to perform automated behavioral analysis and identity verification [4]. Technologies such as facial recognition, gaze tracking, and head-pose estimation allow for the continuous monitoring of candidates while they are taking assessments and can identify suspicious activity with a much higher degree of accuracy [5]. Deep learning-based face recognition systems, such as DeepFace and ArcFace, are effective at identifying faces even in unevenly lit or poorly lit environments [7]. Likewise, MediaPipe provides both fast and light facial landmark detection suitable for large-scale monitoring applications [8].

The Intelligent Video Proctoring System builds upon the integration of the latest web technologies and the analytics of AI and has built a highly secure and scalable methodology to remotely monitor activities that occur during video conferencing. The front end of the Intelligent Video Proctoring System uses the React and Typescript frameworks for the user interface, while FastAPI and Python are used to build the backend using high-performance asynchronous programming techniques [9]. The Intelligent Video Proctoring System utilizes DeepFace for identity verification and uses MediaPipe to track facial landmarks, determine gaze direction, and conduct head-pose analysis by continually capturing and analyzing webcam frames [10]. Any actions deemed suspicious, such as detecting multiple faces or abnormal gaze direction, switching tabs while taking an online exam, and interrupting a screen share, will automatically trigger an escalating fraud score based on a weighted fraud score mechanism [11]. All functionalities are offered from a centralized platform that allows for events to be logged, audit trails maintained, and tapes with timestamped evidence set aside for analysis after interviews and to comply with institutional regulations [12]. Secure access control for data through the use of Role-Based Access Control and authentication of users through a JSON Web Token (JWT) method will also help protect user privacy and the data they generate [13].

One of the greatest benefits of the proposed system is its ability to integrate several behavioural indicators into a single, complete fraud assessment model [14]. By assigning weighted contributions to different types of suspicious activity, as opposed to traditional systems that only produce a binary decision (pass/fail), it is possible to improve the accuracy of a decision and decrease the number of false positives [15]. The

design of the architecture lends itself to multiple simultaneous interview sessions via the use of asynchronous processing pipelines, thus creating opportunities for expanding to larger-than-normal school systems and recruiting agencies [16]. Intelligent proctoring systems enhance the integrity of an exam by furthering the ability of an institution to conduct their operations transparently and efficiently [17]. By monitoring an exam electronically, the need for human monitors is reduced, as well as the cost of providing monitoring through an individual [18]. Additionally, ongoing behavioural analysis allows an institution to detect subtle deviations from acceptable behaviour that may be missed by traditional monitoring techniques [19]. Future developments may expand upon this foundation by adding machine learning methods that ensure privacy, utilize GPU technology to speed up processing, and create more advanced anomaly detection techniques to enhance both the efficiency and the accuracy of the proctoring process [20].

1.1 BACKGROUND

The need for effective digital proctoring solutions has become increasingly more urgent as online learning platforms, e-recruitment systems, and virtual certification programs have all rapidly been adopted over these past months. Currently, the majority of online testing systems primarily use manual observer and low-level video monitoring which provides little to no protection against impersonation, cheating, or unauthorized assistance during an exam. Recent advances in artificial intelligence (AI) and computer vision have led to the development of intelligent proctoring systems that enable machine-based identity verification and behaviour analysis in real-time. Technologies such as DeepFace and MediaPipe provide the capability to achieve both accurate facial recognition and eye gaze estimation and head pose estimation to allow for continuous monitoring of a candidate throughout the duration of an exam. Moreover, new web technologies such as FastAPI, WebRTC and WebSockets now provide the capacity for scalable, low-latency communications for remote assessments. Intelligent video proctoring systems take advantage of these technologies to enhance examination integrity, reduce the need for human supervision of testing, and offer an audit-ready monitoring framework. The proliferation of these systems in academic, recruitment, and professional certification environments requiring remote evaluation processes that are secure and transparent is evident.

1.2 PROBLEM STATEMENT

Due to the growing number of candidates trying to cheat on their assessments (via impersonation or having someone take the test for them), there are great challenges in providing safe, secure, equitable, and reliable assessment methods. Assessment systems also continue to develop greater amounts of assessment fraud due to increased reliance on remote methods to complete assessments. Many of the traditional systems being used to help reduce fraud will not be able to adequately detect impersonation (potentially fraudulent activity) or offer the needed level of assessment integrity. Generally speaking, many of the current online assessment systems do not offer sufficient identity verification, limited ability to monitor/test behavior or the ability utilize real-time

monitoring of test-taker behavior to score potential fraud, and to generate immediate alerts in case of detected fraud. Added to these issues are privacy, security, and issues related to allowing for appropriate levels of protection against potential fraud. As a result, there is a strong need for a more intelligent, scalable, and AI-based video proctoring solution that will provide the following capabilities: continuous proof of identity through biometric capability; real-time behavior analysis to help identify potentially fraudulent activity; and immediate alerts when potential fraudulent activity is detected to ensure the assessment process is secure, transparent, and reliable.

2. LITERATURE REVIEW

As online education, virtual hiring, and remote certifications gain steam, an increasing need exists for secure and intelligent proctoring solutions that protect examination integrity and transparency [1]. Historically, proctoring on the internet has relied on manual oversight, recording your webcam while you take an exam, and monitoring your browser activity. However, these methodologies often fail to provide continuous verification of a test taker's identity and accurate assessments of their behavior during remote testing [2]. As such, the majority of studies being conducted today are focused on combining computer vision, artificial intelligence, and machine-learning technologies to create automated and scalable proctoring systems [3].

Recent developments in facial recognition systems have made the verification of individuals in a remote assessment setting much more reliable than ever before [4]. Modern face recognition systems using deep learning (e.g., neural networks) produce high-dimensional "embeddings," which allow for the precise identification of a person even when there is a variance in light and/or the person being tested is at an angle relative to the camera and there may be noise from other sources in the environment [5]. They are therefore increasingly becoming one of the important functions of intelligent proctoring systems as they reduce the risk of impersonation and increase the accuracy of authentication from the time the exam begins until its end [6]. Continuous facial verification techniques are now preferred to single-event verification techniques as they provide the ability to monitor in real-time and identify the change of identity of a person being tested while the exam is in progress [7].

The use of the computer vision framework has had a positive impact on many different aspects of behavioral monitoring as well as indicating suspicious activities [8]. For example, systems use facial landmark detection, gaze tracking, and head pose estimation to identify candidate behaviors that demonstrate abnormality such as an excessive amount of time spent looking away from their screen, multiple faces on screen at the same time, and excessive head movement [9]. The lightweight computer vision pipelines can provide real-time inference and scalable deployments supporting several concurrent users

[10]. With the incorporation of facial analysis via behavioral monitoring it allows for more reliable fraud detection because it provides multiple independent signals to create one unified signal for assessment purposes [11].

As modern online proctoring continues to develop, proctoring systems are utilizing web-based architectures for increased scalability and low-latency communication [12]. The frontend technologies used (i.e., React and TypeScript) provide responsive interfaces for both candidates, administrators, and interviewers, while backend frameworks support asynchronous processing and real-time processing events of requests [13]. WebRTC technology allows for low-latency video streaming to facilitate continuous monitoring, while WebSocket communications will provide immediate notifications of any fraudulent behavior to appropriate parties [14]. Collectively, these technologies will enhance operational effectiveness and allow for seamless interactions between monitoring components and end-users [15].

Intelligent proctoring system research has revealed the significance of a Risk-Based Anomaly Assessment (RBAS) approach for assessing anomalies [16]. With an advanced system (as opposed to traditional systems that produce only binary outcomes), scoring will instead assign a weighted score (to a range of severity and frequency) for each suspicious activity [17]. The use of a multimodal fraud scoring system – which utilizes a range of sources, i.e., face verification, gaze behavior, browser activity, and environmental analysis – can lead to greater accuracy in decision-making, and reduce false positives through evaluation of subjects from multiple sources [18]. By adopting this methodology, proctoring standards can facilitate greater confidence in candidate evaluations, as well as develop more effectively transparent processes for making decisions about remote interviews and assessments [19].

Security and confidentiality are paramount to contemporary remote proctoring systems [20]. A large percentage of these systems use encrypted channels for communication/control of the system; role-based access/control; secure/authenticating mechanisms; and create a formalized audit trail of events, thus protecting sensitive candidate information and providing regulatory compliance. Additionally, by utilizing work logs and timestamped evidence collection/storage systems, remote proctoring systems provide a level of transparency that allows for post-process review/investigation. The architecture of remote proctoring systems is also being developed to ensure scalability and concurrent processing without negatively impacting performance due to the use of asynchronous marker processing and architecture. More recent research has also begun to explore techniques such as privacy-preserving machine learning; GPU acceleration, and different anomaly

detection models that will provide for improved efficiency, scalability, and reliability in future intelligent proctoring systems.

2.1 RESEARCH GAPS

- Existing systems lack continuous real-time identity verification during remote assessments.
- Traditional proctoring methods generate high false-positive fraud detection results.
- Many platforms fail to integrate multi-modal behavioral analysis effectively.
- Current systems provide limited scalability and insufficient audit transparency

2.2 RESEARCH OBJECTIVES

- To develop an AI-based real-time intelligent video proctoring system.
- To implement continuous facial verification using DeepFace and MediaPipe.
- To design a weighted fraud-scoring mechanism for anomaly detection.
- To ensure secure, scalable, and transparent remote assessment monitoring.

3 METHODOLOGY

The Intelligent Video Proctoring System proposed in this research focuses on creating a secure, scalable, and artificial intelligence (AI)-based platform for conducting online examinations and remote interviews. It combines current web technologies with artificial intelligence and computer vision to provide continuous identity verification, behavioral monitoring, and the ability to track fraudulent actions in real-time. The methodology consists of system architecture design, facial authentication, analysis of eye gaze, analysis of head pose, monitoring of browsers, creation of fraud scores, and creation of centralized audit logs. DeepFace, MediaPipe, FastAPI, React, WebRTC, and WebSockets are all examples of technologies that are included in the solution to provide low-latency communication and reliable monitoring performance. This proposed system improves the integrity of assessments, reduces the possibility of impersonation, and provides clear monitors for academic and hiring environments, as shown in Fig. 1.

Step 1: System Design and User Management

The Intelligent Video Proctoring System (IVPS) is built on a distributed web architecture, allowing users to participate in remote interviews and testing securely via the internet. The system's frontend utilizes React + TypeScript to generate responsive dashboards for candidates, interviewers, and administrators, while the backend leverages FastAPI + Python to provide asynchronous processing and high-performance API management.

The system employs role-based access control (RBAC) to manage user privileges and provide secure interaction among users. Users log into the system through JSON Web Token (JWT) authentication using bcrypt to hash passwords. Administrators can schedule interviews, observe live activity during interviews, and access the session logs; meanwhile, candidates have secure access to examination portals.

To further secure the data sent between the various components of this more modular architecture, the IVPS provides encryption of all communications between users to ensure the privacy and integrity of the data. The distributed architecture used by the IVPS also provides for greater scalability, reliability, and maintainability while allowing for many simultaneous users interacting with their own respective interview/testing processes in both educational and employment environments.

Step 2: Real-Time Identity Verification

The second phase in the process involves ongoing identity validation through the use of Artificial Intelligence and Computer Vision Technologies. When a new session is started with a user, facial images are collected and stored securely within the system as part of Session Initialization. As all of this happens, the system continuously processes real-time video images captured from the user's webcam by way of DeepFace with the ArcFace model in order to perform facial authentication, comparing real-time facial embeddings to those of the stored references, to verify the identity of the user throughout their assessment period.

During real-time processing, MediaPipe is integrated into the delivery of service to the user via the collection of video frames processed for Face Detection, Face Landmark Extraction, Gaze Tracking and Head Pose Estimation. By employing MediaPipe's capabilities, evidence of possible activity based on their primary purposes of Authenticate a Service User includes; the user being absent from the screen, the presence of multiple faces, abnormal gaze movement, and presence of people who may be helping the user accessing their credentials. Using MediaPipe's very lightweight Inference capability provides the system with a low-latency processing environment for Real-Time Application Use. By using continuous validation of identity, impersonation risks are greatly reduced, and the integrity of the assessment is protected by ensuring only an authenticated service user remains present throughout the duration of the interview or testing session.

Step 3: Behavioral Monitoring and Fraud Detection

In the third stage of intelligent behavioral analysis and fraud detection, multi-modal monitoring techniques are used to continuously verify browser event occurrences such as tab conversions, window blurs, interruptions to screen sharing, and unauthorized browser

activity. In addition to monitoring events at the browser level, computer vision algorithms are utilized to assess the candidate's behaviors through analysis of facial expressions and gaze directions, as well as the candidate's head movements. Each anomalous behavior identified by the biometric and/or computer vision algorithms is assigned a weighted score based on the level of severity and the occurrence frequency. The weighted contributions are then combined to generate a cumulative score that represents the overall candidate behavior throughout the session. A multi-signal evaluation technique increases the reliability of detection and decreases the number of false-positive results compared to traditional single-factor monitoring techniques. Annotations in WebSocket format will enable the interviewer and administrator to receive live fraud alerts with minimal latency. The methodology described above provides for rapid response to detected suspicious behaviors and allows for secure, transparent, and fully automated monitoring of remote assessments and interviews.

Step 4: Data Logging, Audit, and System Scalability

In the final phases of the event, system logging, auditing, and scaling for large-scale deployment are completed. These logs contain all of the suspicious events that were detected during the event within a central repository that includes date/time, metadata, score of fraudulence, and if applicable, a copy of the captured video images to track the suspected fraud cases. These logs provide post event analysis, institutional compliance, and provide transparent procedures for conducting investigations that can occur after the conclusion of the event. The use of asynchronous processing pipelines allows the system to handle concurrent sessions efficiently without causing any degradation in system performance. WebRTC technology allows for low-latency streaming of video and FastAPI provides an incredibly scalable means of handling requests and conducting real-time communications. Methods for improving database storage efficiency and retrieval times for large volumes of monitoring data have been implemented. Additionally, the architecture has been designed to accommodate potential future enhancements, including GPUs for acceleration, advanced algorithms for detecting anomalies, and machine learning techniques that discover privacy-preserving ways for tracking individuals throughout an entire event. This scalable framework ensures reliable operation across all academic institutions, organizations that conduct recruitment, and environments that require professional certification, utilizing virtual monitoring systems providing secure performance standards.

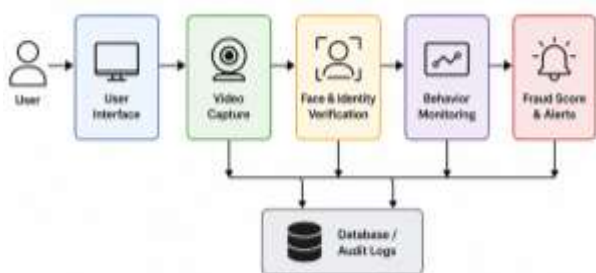


Fig -1: Methodology Block Diagram of the Intelligent Video Proctoring System

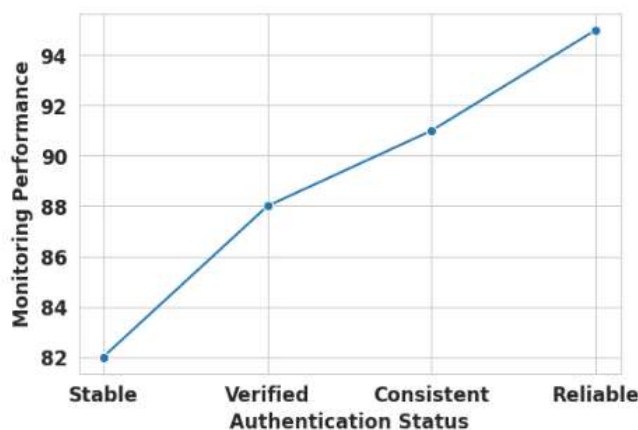


Fig. 3. Monitoring Performance Based on Authentication Status

4 RESULTS AND DISCUSSION

Figure 2 demonstrates a steady upward direction in the observations produced from each module of the security analysis process. The alert signal phase of the system is followed by a phase for evaluating those actions through actual behaviour observations, creating summary activities, and mapping the security of those same actions. The increase from module to module illustrates how much more valuable each module's output is for your monitoring and evaluation efforts. The rapid increase in the observations created once user action is examined as opposed to the mere capture of the user's signal. The final output at the security mapping actually demonstrates that all of the collected indication produce the maximum amount of data for review each day or time period. Therefore, Figure 2 provides verification that the overall step-by-step analysis process is an effective tool for detecting potentially fraudulent activity in a systematic manner.

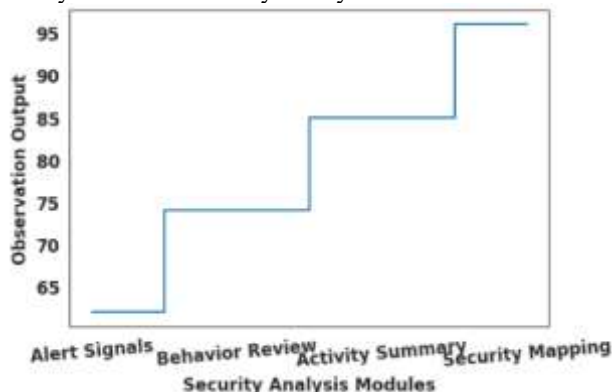


Fig. 2. Observation Output Across Security Analysis Modules

As demonstrated in Fig 3, all categories of authentication show a steady improvement in terms of monitoring performance (from stable to verified to consistent to reliable). Each level of authentication improves upon the last when using continuous authentication as a strength of the proctoring process. This allows for improved performance overall after completing the identity reinsurances of the users being tested, with reliable performance subsequently achieved at that highest level. Thus, continuous verification of one's identity as well as continuous assessment of behavior is essential to maintain a secure remote monitoring environment.

5 CONCLUSION

Intelligent Video Proctoring System (IVPS) will offer a viable, expandable, and AI-based solution that provides secure monitoring of online tests and remote interviews; it will offer seamless integration between current online technologies and the application of artificial intelligence and computer vision to continually verify a person's identity, monitor one's behavior and provide real-time detection of fraud. A major component of facial recognition and tracking (marking eye movement) and head posture is via DeepFace/MediaPipe—this allows for accurate surveillance of all methods used by candidates to take the exam.

The combination of analysis of browser activity and an overall fraud score for all of the fraud children of each participant provides further security and anomaly detection through improved reliability and reduced limitations compared to previously used online proctoring methods, when many methods of monitoring were combined together. The architecture of this development has shown evidence that real-time communications, alerting, and centralized logging via ;with WebRTC and WebSocket show effective performance. In terms of combining multiple monitoring and observational methods will greatly enhance the effectiveness of providing quality monitoring results..

REFERENCES

1. R. D, H. C, E. S, H. A, and K. R.: Smart Proctor: Lightweight, Privacy-Centric Remote Exam Monitoring. International Journal For Multidisciplinary Research (2025)
2. J. R. Pansare: Proctoring Using AI. International Journal For Science Technology And Engineering 13(6) (2025) 1825–1835
3. S. S. Benazer, S. K. Ramamoorthy, and S. M. Kamali: An AI-Based Intelligent Exam Proctoring System for Secure and Fair Online Assessments. (2024)
4. A. Patil, P. A. Chavan, S. R. Jadhav, A. U. Phodkar, M. B. Gulame, and A. P. Pimpalkar: Online Exam Proctoring Application Using-AI. International Journal of Science and Research Archive 15(2) (2025) 1228–1234
5. P. Shrivastav, S. Mishra, S. S, and S. K. G: AI-Powered Multimodal Approach for Secure Online Examinations. (2025) 1520–1525
6. V. L. Priya, A. G. Naidu, I. M. Manikanta, C. S. Kumar, B. I. Preetham, and S. Muthumeena: Proctonix AI - Smart Exam Proctoring using AI and Webcam. (2025) 1762–1768
7. M. P and V. K: AI-Powered Real-Time Proctoring System for Secure Online Examinations. (2025)

8. S. A. Pascual: AI-Powered Online Exam Proctoring System for Secure and Scalable Assessment. *Indian Scientific Journal Of Research In Engineering And Management* 09(06) (2025) 1–9
9. S. S. Benazer, S. K. Ramamoorthy, and S. M. Kamali: An AI-Based Intelligent Exam Proctoring System for Secure and Fair Online Assessments. (2024)
10. V. R, P. P. Rao, M. S. N, and N. A: Virtual Overseer for Examination Using Artificial Intelligence. *Indonesian Journal of Information Systems* (2024)
11. D. Mewada, S. Gaikwad, B. Gharat, and P. Kamble: An AI Powered Exam Proctoring: Comprehensive Monitoring for Integrity. (2024) 1–5
12. O. Malekar, A. Karale, P. Pawara, and R. A. Gharat: Real-Time Exam Monitoring. *International Journal of Advanced Research in Science, Communication and Technology* (2025) 288–294
13. S. Sharma, A. Manna, and N. Arunachalam: Analysis on AI Proctoring System Using Various ML Models. (2024)
14. M. Chougule, S. Bagul, M. Gharat, S. Malve, and D. Kayande: ProctoXpert – An AI Based Online Proctoring System. (2024) 1–8
15. R. Zod, A. Dongarwar, L. Mandurkar, Y. Narad, and H. Bhagat: Elevating Online Assessment Security: A Comprehensive AI-Based Examination Hosting and Proctoring System by Integrating Flask and AI Technologies. (2025) 1–7
16. N. Akber, N. Neha, R. PK, S. Shinas, and S. CS: Online Exam Proctoring System Using Machine Learning. *Indian Scientific Journal Of Research In Engineering And Management* 09(03) (2025) 1–9
17. X. Chen et al.: Effective Exam Cheating Detection via Large-Small Model Collaboration. (2025) 233–238
18. S. Rao, A. Krishna, S. Rao, and A. Krishna: Autonomous Proctoring Software: A Comprehensive Framework for Ensuring Academic Integrity in Remote Examinations. *International Journal of Latest Technology in Engineering Management & Applied Science* 14(10) (2025) 540–548
19. D. Hariprawira: Artificial Intelligence in Online Proctoring: Algorithmic Bias, Accountability, and the Limits of Automated Final Decision-Making. (2026)
20. S. J. Evangeline, S. A. M P, R. T, and S. K. M: Smart Exam Hall Invigilation with Biometric Authentication and AI-based Malpractice Detection. (2025) 348–353