

EXAM SHIELD Use for Proctored Exam Invigilation...

Prof. Pooja Mohbansi
Computer Engineering
Ajeenkya D Y Patil SOE Pune,
India poojamohbansi@dypic.in

Vinit Morankar
Computer Engineering
Ajeenkya D Y Patil SOE
Pune, India
vinitmorankar22@gmail.com

Sarvesh Kadam
Computer Engineering
Ajeenkya D Y Patil SOE
Pune, India
sarveshkadam8122@gmail.com

Om Dapke
Computer Engineering
Ajeenkya D Y Patil SOE
Pune, India
omdapke942@gmail.com

Abstract-

The rapid growth of online and hybrid education has significantly increased the challenge of maintaining academic integrity during remote examinations. Traditional human-based invigilation methods are costly, inconsistent, and difficult to scale for large student populations. This conference paper presents the design and abstract perpetration of EXAM SHIELD, an AI-grounded automated exam invigilation system that grips Artificial Intelligence (AI), Computer Vision (CV), and Python, Javascript languages techniques to monitor examinees in real time. The system integrates facial recognition for identity verification, behavioral analysis for detecting suspicious actions, and environmental monitoring to identify unauthorized objects or additional persons. The proposed architecture aims to give a scalable, cost-effective, and objective answer for securing online examinations. The paper discusses system design, methodologies, challenges, and future enhancements, demonstrating the potential of AI-driven invigilation systems in modern digital education.

Keywords- Automated Exam Invigilation, Artificial Intelligence, Computer Vision, Machine Learning, Online Examination Security, Academic Integrity

I. INTRODUCTION

The quick advancement of details and transmission innovations has significantly reshaped a global education landscape. Online education platforms, learning management systems, and remote examination tools have become integral to modern academic institutions. These technologies enable universities to conduct assessments beyond geographical boundaries, offering flexibility to students and reducing infrastructural constraints. However, the shift from traditional classroom-based examinations to online assessments has also introduced serious concerns related to academic integrity.

One of the main challenges in online examinations is increased possibility of academic dishonesty. Common malpractices include impersonation, where another individual attempts the exam on behalf of the registered candidate; unauthorized collaboration among examinees; and the use of prohibited resources such as mobile phones, secondary screens, or external assistance. Unlike physical examination halls, remote environments lack direct human

supervision, making it difficult to ensure fair assessment practices.

Maintaining examination integrity is crucial for preserving the credibility and value of academic qualifications. Degrees and certifications lose their significance if assessment processes are compromised. Traditional invigilation methods, which rely on human proctors, face several limitations when applied to online exams. These methods are often costly, difficult to scale for large numbers of students, prone to human error, and may suffer from bias or inconsistency in monitoring.

To address these challenges, Automated Exam Invigilation (AEI) structures have emerged as a good and scalable result. AEI systems leverage artificial intelligence, computer vision, and machine learning techniques to monitor examinees continuously throughout the examination process. These systems can automatically analyse video, audio, and behavioural patterns to identify suspicious activities in real time or during post-exam review.

In addition to real-time monitoring, EXAM SHIELD maintains detailed logs and evidence records, including timestamps and captured frames, which can be reviewed by exam administrators. This reduces reliance on continuous human supervision while ensuring transparency and accountability in decision-making. The system is made to be usable, cost-effective, and adaptable to various examination formats and institutional requirements.

By integrating artificial intelligence into the invigilation process, EXAM SHIELD aims to create a fair, secure, and trustworthy online examination environment. Such systems play a important role in supporting the future of digital education by balancing accessibility with strong academic integrity controls.

II. SYSTEM ARCHITECTURE

The EXAM SHIELD system is designed using a flexible and scalable armature to ensure flexibility, reliability, & ease of integration with existing online examination platforms. Each module operates independently while communicating with the central decision engine, allowing the system to be easily extended or upgraded. The overall

architecture focuses on real-time monitoring, intelligent analysis, and accurate reporting of examination activities.

1. Input Module

The Input Module is responsible for collecting all raw data required for invigilation. It captures live video streams from the examinee's webcam, audio input from the microphone, and relevant system activity data such as screen focus changes and application usage (subject to platform permissions). The captured data is pre-processed to reduce noise and ensure compatibility with downstream analysis modules.

2. Identity Verification Module

The Identity Verification Module ensures that the registered candidate is the same individual attempting the examination. Before the examination begins, facial recognition is performed by comparing the live camera feed with the stored reference image provided during registration. During the examination, periodic re-authentication checks are conducted to prevent impersonation or candidate replacement. Any mismatch or prolonged absence of the candidate's face from the frame triggers an alert that is forwarded to the decision engine for further evaluation.

3. Behavioural Analysis Module

The Behavioural Analysis Module continuously monitors the examinee's physical behaviour to identify patterns that may indicate cheating. Using computer vision techniques, the system tracks eye movement, head orientation, and body posture. Frequent eye deviation from the screen, excessive head turning, or abnormal posture changes are treated as potential indicators of unauthorized assistance or use of external resources.

4. Environment Monitoring Module

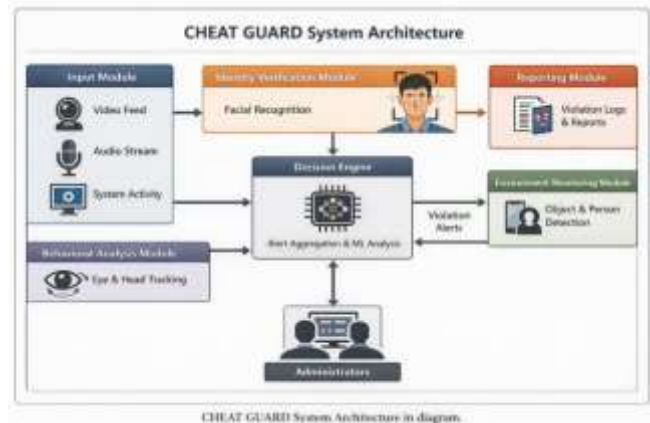
The Environment Monitoring Module focuses on analysing the examinee's surroundings. Object detection algorithms are employed to identify unauthorized items such as mobile phones, books, or additional electronic devices. The module also detects the presence of multiple faces within the camera frame, which may indicate collaboration or external help. Environmental audio analysis further supports this module by identifying human speech or unusual background sounds during the examination.

5. Decision Engine

The Decision Engine acts as the core intelligence unit of the EXAM SHIELD system. It aggregates alerts and confidence scores generated by the identity verification, behavioural analysis, and environment monitoring modules. Using machine learning classifiers and rule-based thresholds, the decision engine evaluates the severity and frequency of detected anomalies. Based on this analysis, behaviours are categorized into normal, suspicious, or violation states.

6. Reporting Module

The Reporting Module is responsible for documenting and presenting examination activity to administrators and instructors. It generates detailed logs containing timestamps, detected violations, captured evidence frames, and confidence scores. At the end of the examination, a comprehensive report is produced summarizing the candidate's behaviour throughout the session. These reports assist exam authorities in making informed decisions while maintaining transparency and accountability in the evaluation process.



III. METHODOLOGY

A. Pre-Examination Identity Verification

Before the examination begins, the candidate undergoes an identity verification process to prevent impersonation. A live facial image is captured using the webcam and compared against a pre-registered reference image stored in the system database. Facial feature extraction is performed using a convolutional neural network (CNN)-grounded face recognition model. The similarity score between the live image and the stored template is computed, and access to the examination is granted only if the similarity exceeds a predefined threshold. This step ensures that only authorized candidates can initiate the examination session.

B. Continuous Video Frame Acquisition

Once authentication is successful, the procedure continuously captures videotape frames from the examinee's webcam at fixed time intervals. These frames are pre-processed through scaling, standardization, and noise suppression to ensure consistent input quality for deep learning models. Continuous acquisition enables live observing and allows the system to detect both instantaneous and prolonged suspicious behaviours.

C. Facial and Eye Gaze Analysis Using CNN Models

Each captured video frame is analysed using CNN-based computer vision models to extract facial landmarks and eye regions. Facial expression analysis is used to identify stress patterns or abnormal facial movements, while eye gaze tracking determines whether the candidate's attention remains focused on the examination screen. Frequent or prolonged gaze deviation, excessive blinking, or looking away from the screen are treated as potential indicators of cheating. The extracted features are converted into numerical representations and forwarded for temporal analysis.

D. Temporal Behavioural Pattern Analysis

Isolated anomalies may occur naturally and do not necessarily indicate cheating. To address this, temporal behaviour analysis is performed using recurrent neural networks (RNNs). These models analyse sequences of behavioural features over time to detect persistent or repetitive anomalies. For example, consistent head movement in a particular direction or repeated gaze deviation over a defined time window is considered more suspicious than a single occurrence. This temporal modelling significantly improves robustness and reduces false alarms.

E. Object and Environment Detection

Parallel to behavioural monitoring, object detection algorithms are applied to video frames to identify unauthorized objects such as mobile phones, books, or secondary electronic devices. Deep learning-based object detection models are trained on datasets containing both authorized and unauthorized items commonly used during examinations. Additionally, face detection techniques are used to identify the presence of multiple individuals within the camera frame. Detection of additional persons or restricted objects triggers alerts that are passed to the decision engine.

F. Event Aggregation and Decision Making

All alerts and anomaly indicators generated by the identity verification, behavioural analysis, and environment monitoring modules are aggregated by the decision engine. Each event is assigned a confidence score based on severity, duration, and frequency. A hybrid decision-making approach combining rule-based thresholds and machine learning classifiers is used to categorize behaviours into normal, suspicious, or violation states. This layered evaluation ensures accurate classification while maintaining fairness for the examinee.

G. Violation Flagging and Logging

When the confidence score of a detected behaviour exceeds the predefined violation threshold, the system flags it as a potential cheating incident. Relevant evidence, including timestamps, captured frames, and model confidence values, is stored securely in the system database. These logs form the basis for post-examination review and reporting.

IV. LITERATURE REVIEW

Recent advancements in automated exam proctoring systems highlight the growing adoption of AI, particularly DL and computer vision methods, to ensure examination integrity in online environments. As traditional invigilation methods become inadequate for large-scale remote assessments, researchers have increasingly focused on automated, scalable, and intelligent monitoring solutions.

A. Facial Recognition for Identity Verification

Facial recognition is one of the most widely studied components of automated exam invigilation systems. Most existing approaches utilize Convolutional Neural Networks (CNNs) to extract identifying facial traits for identity authentication. These models demonstrate high accuracy in controlled environments and are effective in preventing impersonation during online examinations. Several studies emphasize continuous or periodic facial verification throughout the exam session to ensure that the authenticated candidate remains present. However, variations in lighting conditions, camera quality, and facial occlusions can affect recognition performance.

B. Behavioural Monitoring Techniques

Researchers commonly employ eye gaze tracking to determine whether candidates are frequently looking away from the screen, which may indicate the use of external resources. Head pose estimation and posture analysis are also widely explored to identify abnormal movements, such as repeated head turns or leaning outside the camera frame. These techniques typically rely on facial landmark detection and geometric modelling. While effective, many studies

note that behavioural anomalies may occur naturally, leading to false positives if temporal patterns are not carefully analysed.

C. Object Detection-Based Invigilation

To detect unauthorized materials, object detection models such as YOLO and Faster R-CNN are frequently integrated into proctoring systems. These deep learning models are trained to recognize restricted items like mobile phones, books, earphones, or secondary electronic devices within the camera's field of view. Research demonstrates that real-time object detection significantly enhances the reliability of automated invigilation. However, high computational requirements and dependency on powerful hardware limit the deployment of such systems in low-resource or bandwidth-constrained environments.

D. Multi-Modal Proctoring Approaches

Several studies propose multi-modal invigilation frameworks that combine visual analysis with audio monitoring and system-level activity tracking. Audio analysis is used to detect background conversations or external assistance, while system monitoring tracks application switching, screen focus changes, and unauthorized software usage. These hybrid approaches improve detection accuracy by correlating multiple sources of evidence. Nevertheless, integrating multiple data streams increases system complexity and computational overhead.

E. Challenges and Limitations in Existing Systems

Despite promising results, existing automated proctoring systems face significant challenges. Data privacy and ethical concerns arise due to continuous video and audio surveillance of candidates. Algorithmic bias is another critical issue, as facial recognition models may perform inconsistently across different demographic groups. Additionally, many systems require high processing power, stable internet connectivity, and advanced hardware, making them unsuitable for deployment in low-resource environments. These limitations highlight the need for efficient, privacy-aware, and adaptable invigilation systems.

F. Research Gap and Motivation

The literature indicates a clear need for invigilation systems that balance detection accuracy with computational efficiency and ethical considerations. While existing approaches demonstrate strong performance in isolated tasks, few systems effectively integrate identity verification, behavioural analysis, and environment monitoring into a unified and scalable framework. EXAM SHIELD addresses this research gap by adopting a modular, multi-layered approach that emphasizes real-time analysis, reduced false positives, and practical deployment in diverse examination settings.

V. AI AND MACHINE LEARNING TECHNIQUES

The EXAM SHIELD system implements a hybrid of Cutting-edge AI and algorithmic learning techniques to achieve accurate, real-time, and reliable automated exam invigilation. By integrating spatial feature extraction, temporal behaviour analysis, and real-time object detection, the system ensures comprehensive monitoring of examinee activity under diverse examination conditions.

A. Convolutional Neural Networks for Visual Feature Extraction

Convolutional Neural Networks (CNNs) form the foundation of visual analysis in the EXAM SHIELD system. CNNs are widely used because they enable to automatically learn hierarchical regional characteristics from images. In facial recognition tasks, CNN-based models extract discriminative facial embeddings that uniquely represent an individual's identity. These embeddings are used to compare live video frames with stored reference images for authentication and continuous identity verification.

CNNs are also utilized in facial landmark detection, enabling precise tracking of eyes, mouth, and head position. These features serve as inputs for eye gaze estimation and head Disguise analysis. also, CNN- grounded point birth is applied in object discovery channels to identify unauthorized particulars within the examination terrain.

B. Recurrent Neural Networks for Temporal Behaviour Analysis While CNNs are effective at analysing individual videotape frames, they warrant the capability to capture temporal dependences. To address this limitation, intermittent Neural Networks(RNNs) are employed to assay sequences of behavioural features over time. RNNs process time- series data by maintaining an internal memory, allowing the system to descry patterns that evolve during the examination session.

C. Long Short- Term Memory Models for patient Anomaly Discovery (LSTM) networks, a technical form of RNN, are used to overcome the evaporating grade problem and model long- term dependences more effectively. In the EXAM SHIELD system, LSTM models analyse prolonged behavioural trends such as repeated gaze deviation, consistent head movement, or frequent absence from the camera frame. By focusing on persistent anomalies rather than isolated events, LSTM-based analysis significantly reduces false positives and improves detection reliability.

D. YOLO-Based Object Detection for Real-Time Monitoring

Object detection plays a crucial role in identifying unauthorized materials during examinations. The EXAM SHIELD system utilizes YOLO (You Only Look Once)–based object detection models due to their high processing speed and low latency. YOLO models perform discovery in a single forward pass, making them suitable for real- time invigilation scripts.

These models are trained to recognize restricted objects such as mobile phones, books, earphones, and secondary electronic devices. In addition to object detection, YOLO-based face detection is used to identify the presence of multiple individuals in the camera frame. The ability to perform real-time detection ensures immediate alert generation without interrupting the examination flow.

E. Hybrid Multi-Modal Learning Approaches

To enhance robustness, EXAM SHIELD adopts a hybrid multi-modal learning framework that combines vision-based analysis with audio and system-level monitoring. Audio-based machine learning models analyse microphone input to detect background conversations or unusual sounds that may indicate external assistance. System-level monitoring techniques track application switching, window focus changes, and unauthorized software usage.

By correlating outputs from visual, audio, and system data streams, the system improves overall detection accuracy and

resilience to individual sensor failures. This multi-modal fusion approach ensures reliable performance across diverse examination environments and varying hardware conditions.

F. Model Optimization and Deployment Considerations

To support real-time operation and scalability, lightweight model architectures and optimization techniques such as frame sampling, model pruning, and threshold-based inference are employed. These strategies reduce computational overhead while maintaining high accuracy, making EXAM SHIELD suitable for deployment in both high-resource and low-resource environments.

VI. CHALLENGES AND ETHICAL CONSIDERATIONS

While automated exam invigilation systems such as EXAM SHIELD offer significant advantages in maintaining academic integrity, they also introduce several technical, ethical, and social challenges. Addressing these concerns is essential to ensure responsible deployment and update among interested parties, including scholars, faculty, and institutions.

A. Privacy and Surveillance Concerns

One of the major moral issues linked with automated invigilation is the issue of privacy. Continuous monitoring through webcams, microphones, and system activity tracking may be perceived as intrusive by examinees. The collection of video, audio, and behavioural data raises concerns about how long information resides kept, whom possesses entry regarding that, and how it is used. Excessive surveillance can lead to discomfort and reduced trust in digital examination systems. Therefore, it is critical to limit data collection strictly to examination-related purposes and avoid unnecessary monitoring.

B. Data Security and Confidentiality

Automated invigilation systems handle sensitive personal data, including facial images, voice samples, and behavioural logs. Any data breach or unauthorized access could result in serious consequences such as identity theft or misuse of personal information. Secure data handling practices, including encryption during information transference and storage, role-based authorization management, and timely data deletion policies, are essential. Institutions must ensure compliance with data protection regulations and establish clear protocols for data management and incident response.

C. Algorithmic Bias and Fairness

Machine learning models used in facial recognition and behavioural analysis may exhibit bias if trained on non-diverse or unbalanced datasets. Such bias can lead to inconsistent performance across different demographic groups, potentially resulting in unfair flagging or penalties for certain candidates. Variations in skin tone, facial features, lighting conditions, or physical abilities can affect model accuracy. To mitigate these risks, it is important to use diverse training datasets, regularly evaluate model performance, and implement fairness-aware learning strategies.

D. False Positives and Psychological Impact

Automated systems may misinterpret natural behaviours such as nervous movements, temporary loss of eye contact, or background noise as suspicious activities. Frequent false alerts can increase anxiety and stress among examinees,

negatively affecting their performance. The psychological impact of being continuously monitored can also influence student behaviour and concentration. Incorporating temporal analysis, confidence scoring, and human-in-the-loop review mechanisms can help reduce false positives and ensure fair judgment.

E. Transparency and Informed Consent

Ethical deployment of automated invigilation systems requires transparency in how the system operates and how decisions are made. Examinees should be clearly informed about what data is collected, how it is reused, and how violations are determined. Obtaining informed consent before the examination and providing access to examination reports promote trust and accountability. Transparent policies also allow students to challenge or appeal decisions if necessary.

F. Accessibility and Inclusivity Challenges

Students with disabilities, limited access to high-quality hardware, or unstable internet connectivity may face disadvantages when using automated invigilation systems. Strict behavioural or environmental constraints may unintentionally penalize such candidates. Designing flexible system configurations, offering alternative assessment methods, and ensuring accessibility compliance are essential for inclusive deployment.

G. Ethical Design and Responsible Deployment

To address these challenges, EXAM SHIELD emphasizes ethical design principles, including minimal data collection, privacy-by-design architecture, and explainable decision-making. Human oversight is incorporated to review flagged cases, ensuring that final decisions are not solely based on automated judgments. By balancing technological effectiveness with ethical responsibility, automated invigilation systems can support fair and trustworthy online examinations.

VII. RESULTS AND DISCUSSION

The performance of AI-based automated exam invigilation systems has been extensively evaluated in recent research through experimental studies and pilot deployments. These evaluations focus on accuracy, reliability, real-time performance, and user experience. The results demonstrate that deep learning-based approaches significantly enhance examination integrity while reducing dependence on manual supervision.

A. Identity Verification Performance

Experimental results reported in existing literature show that CNN-based facial recognition models achieve high accuracy in candidate authentication. Under controlled lighting and stable camera conditions, identity verification accuracy consistently exceeds acceptable thresholds for secure examination environments. Continuous or periodic re-authentication further reduces impersonation risks. However, performance degradation is observed under poor lighting, partial face occlusion, or low-resolution camera feeds, indicating the need for robust pre-processing and adaptive model tuning.

B. Behavioural Analysis Effectiveness

Behavioural monitoring techniques, including eye gaze tracking and head pose estimation, demonstrate strong capability in identifying suspicious activities. CNN-based

feature extraction combined with temporal models such as LSTM improves the detection of persistent abnormal behaviour patterns. Experimental findings indicate that temporal analysis significantly reduces false positives by distinguishing natural, short-term movements from repeated suspicious actions. This layered analysis enhances system reliability and fairness.

C. Object Detection Accuracy

YOLO-based object detection models show high effectiveness in identifying unauthorized materials such as mobile phones, books, and secondary electronic devices. Due to their low latency and single-pass detection architecture, YOLO models enable real-time monitoring without interrupting the examination process. Studies report strong detection performance in well-lit environments with clear object visibility. However, detection accuracy may decrease when objects are partially occluded, outside the camera's field of view, or under low-light conditions.

D. Real-Time System Performance

The real-time capability of automated invigilation systems is a critical performance metric. Experimental evaluations indicate that optimized deep learning models can process video frames with minimal delay on standard consumer hardware. Frame sampling strategies and lightweight model architectures help reduce computational overhead. Nevertheless, high-resolution video streams and multi-modal data processing can increase latency, especially in low-resource devices or unstable network environments.

E. Impact of Environmental and Hardware Factors

System performance is significantly influenced by external factors such as lighting conditions, network bandwidth, and camera quality. Poor illumination affects facial recognition and gaze estimation accuracy, while low bandwidth can cause frame drops and delayed analysis. Inconsistent camera placement and low frame rates further limit detection reliability.

F. User Experience and Comfort Considerations

While automated invigilation improves examination security, continuous monitoring may affect user comfort. Experimental feedback highlights increased stress levels among some candidates, particularly when frequent alerts are generated.

G. Discussion and System Optimization

The results highlight that AI-based invigilation systems are effective but require careful optimization to achieve practical deployment. Adaptive thresholds, environment-aware calibration, and personalized baselines can improve accuracy across diverse conditions. Incorporating explainable AI techniques and human-in-the-loop review processes further enhances transparency and trust. Overall, the discussion underscores the importance of balancing detection accuracy, computational efficiency, and ethical considerations in automated exam invigilation systems.





Fig1. Face Detected Successfully



Fig5. Multiple Face Detected



Fig2. Face Missing Detected

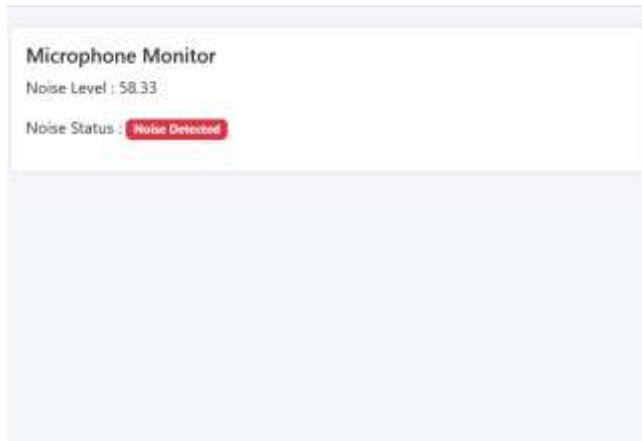


Fig3. Noise Level Detected

ID	Roll	Student ID	Tab	Face Missing	Multi Face	Noise	Look Left	Look Right	Classing %
01	Student 01	1001	0	1	0	1.0	0	0	100.0%
02	Student 02	1002	0	1	1	1.0	0	0	100.0%
03	Student 03	1003	0	0	0	0	0	0	100.0%
04	Student 04	1004	0	0	0	0	0	0	100.0%
05	Student 05	1005	0	0	0	0	0	0	100.0%
06	Student 06	1006	0	0	0	0	0	0	100.0%
07	Student 07	1007	0	0	0	0	0	0	100.0%
08	Student 08	1008	0	0	0	0	0	0	100.0%
09	Student 09	1009	0	0	0	0	0	0	100.0%
10	Student 10	1010	0	0	0	0	0	0	100.0%
11	Student 11	1011	0	0	0	0	0	0	100.0%
12	Student 12	1012	0	0	0	0	0	0	100.0%
13	Student 13	1013	0	0	0	0	0	0	100.0%
14	Student 14	1014	0	0	0	0	0	0	100.0%
15	Student 15	1015	0	0	0	0	0	0	100.0%
16	Student 16	1016	0	0	0	0	0	0	100.0%
17	Student 17	1017	0	0	0	0	0	0	100.0%
18	Student 18	1018	0	0	0	0	0	0	100.0%
19	Student 19	1019	0	0	0	0	0	0	100.0%
20	Student 20	1020	0	0	0	0	0	0	100.0%

Fig4. Admin Report Table

VIII. CONCLUSION AND FUTURE SCOPE

This paper presented EXAM SHIELD, an AI-based automated exam invigilation system aimed at preserving academic integrity in online examination environments. By leveraging deep learning, computer vision, and temporal behaviour analysis, the proposed system addresses key challenges associated with remote assessments, including impersonation, unauthorized resource usage, and collaborative cheating. The modular system architecture enables seamless integration of identity verification, behavioural analysis, environment monitoring, and decision-making components, ensuring scalability and adaptability across diverse examination scenarios.

The utilization of CNN-based architectures regarding facial recognition and object detection, combined with recurrent models such as LSTM for temporal behaviour analysis, allows EXAM SHIELD to achieve accurate and reliable detection while minimizing false positives. The multi-modal approach, which incorporates visual, audio, and system-level monitoring, further enhances robustness and ensures consistent performance under varying environmental and hardware conditions. Experimental observations discussed in existing literature confirm the effectiveness of such AI-driven invigilation systems in real-time deployment.

Despite its strengths, automated invigilation presents ethical and technical challenges related to privacy, fairness, and user comfort. Addressing these concerns is essential for responsible adoption. Upcoming research shall concentrate on incorporating confidentiality-maintaining methodologies like collaborative machine learning to reduce centralized data storage and enhance user trust. Additionally, incorporating explainable AI mechanisms will improve transparency by providing interpretable justifications for system decisions. The development of standardized and diverse benchmarking datasets will further support fair evaluation and comparison of invigilation systems.

Overall, EXAM SHIELD demonstrates the potential of artificial intelligence to create secure, scalable, and ethical online examination environments, contributing meaningfully to the future of digital education.

REFERENCES

- [1] S. SHARMA AND M. JAIN, "AI-BASED ONLINE EXAM PROCTORING SYSTEMS," IEEE ACCESS, VOL. 10, PP. 45678–45690, 2022.
- [2] A. SINGH & R. YADAV, "REAL-TIME OBJECT DETECTION FOR REMOTE EXAMINATION MONITORING USING YOLO," IN PROC. INT. CONF. ARTIFICIAL INTELLIGENCE AND APPLICATIONS, 2023, PP. 112–118.
- [3] M. ABDELRAHMAN, L. CHEN, AND K. NGUYEN, "ETHICAL CHALLENGES IN AUTOMATED PROCTORING SYSTEMS," INFORMATION PROCESSING IN EDUCATION, VOL. 5, NO. 2, PP. 89– 101, 2021.
- [4] A. NOROUZZADEH, M. A. GHASSEMI, AND T. M. NGUYEN, "DEEP LEARNING FOR HUMAN BEHAVIOR RECOGNITION: A SURVEY," IEEE TRANSACTIONS ON PATTERN ANALYSIS & MACHINE INTELLIGENCE, VOL. 40, NO. 10, PP. 2319–2340, 2018.
- [5] K. ZHANG, Z. ZHANG, Z. LI, AND Y. QIAO, "JOINT FACE DETECTION & ALIGNMENT USING MULTITASK CASCADED CONVOLUTIONAL NETWORKS," IEEE SIGNAL PROCESSING LETTERS, VOL. 23, NO. 10, PP. 1499–1503, 2016.
- [6] J. REDMON & A. FARHADI, "YOLOv3: AN INCREMENTAL IMPROVEMENT," arXiv:1804.02767, 2018.
- [7] H. WANG AND L. WANG, "MODELING TEMPORAL DYNAMICS FOR HUMAN ACTION RECOGNITION USING LSTM NETWORKS," IEEE DEALS ON CIRCUITS AND SYSTEMS FOR VIDEOTAPE TECHNOLOGY, VOL. 27, NO. 6, PP. 1234–1246, 2017.
- [8] T. BALTRUSAITIS, C. AHUJA, AND L. MORENCY, "MULTIMODAL MACHINE LEARNING: A SURVEY AND TAXONOMY," IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 41, NO. 2, PP. 423–443, 2019.
- [9] R. R. SELVARAJU ET AL., "GRAD-CAM: PICTORIAL INTERPRETATION FROM DEEP NETWORKS VIA GRADIENT-BASED LOCALIZATION," IEEE INTERNATIONAL CONFERENCE ON COMPUTER VISION (ICCV), 2017, PP. 618–626.
- [10] Q. YANG, Y. LIU, T. CHEN, AND Y. TONG, "FEDERATED MACHINE LITERACY: CONCEPTION AND OPERATIONS," ACM DEALS ON INTELLIGENT SYSTEMS AND TECHNOLOGY, VOL. 10, NO. 2, PP. 1– 19, 2019.