CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Examinations are essential in assessing academic achievement and intellectual development within educational systems. They uphold the integrity of learning outcomes and guide educational progress. However, examination malpractice remains a persistent challenge, especially in physical examination halls, where unethical practices such as whispering answers, impersonation, unauthorized material use, or covert gestures are commonly observed (Akinola & Yusuf, 2023).

Although human invigilators have traditionally been responsible for maintaining order during exams, their effectiveness is increasingly compromised. Large examination halls filled with dozens or even hundreds of students present a significant challenge for manual supervision. Human invigilators are often limited by fatigue, distractions, and human error, making it difficult to monitor multiple candidates simultaneously and detect subtle acts of cheating in real-time (Oladipo et al., 2022).

Recent advancements in artificial intelligence (AI) and computer vision offer a promising solution to this problem. By using system cameras integrated with intelligent detection systems, institutions can now automate parts of the examination monitoring process. These AI-based systems are capable of identifying multiple faces, tracking head movements, detecting unauthorized behaviors, and capturing audio cues such as whispering or verbal communication—actions that would otherwise be difficult for a single invigilator to catch during a crowded examination session.

Unlike online proctoring solutions that monitor individual students through personal webcams, this project focuses on physical examination environments where one or more centrally placed surveillance cameras are used to monitor all students in the examination hall simultaneously. The system employs machine learning models such as BlazeFace for detecting and counting faces, FaceMesh for tracking eye and head orientation, Coco-SSD for detecting prohibited objects (such as mobile phones or books), and audio signal processing for identifying suspicious sounds.

The key objective is to support human invigilation by providing real-time alerts and storing recorded evidence of suspected malpractice, allowing invigilators to respond promptly or review incidents after the examination. This approach reduces reliance on large numbers of invigilators, enhances the accuracy of exam surveillance, and improves the scalability of monitoring, especially in institutions with limited personnel or resources.

By adopting this AI-enhanced system camera solution, educational institutions can reinforce academic integrity and discourage misconduct through increased visibility and accountability. This research contributes to ongoing efforts to integrate intelligent technologies into physical examination settings to promote fair, secure, and transparent assessment conditions (Emeka & Ajayi, 2025).

1.2 Problem Statement

The shift toward improved educational technology has uncovered new vulnerabilities in physical exam settings, especially where human invigilation is the primary method of monitoring. Despite being in a controlled environment like an exam hall, examination malpractice remains prevalent due to several factors that limit the effectiveness of traditional proctoring.

1. Limited Human Supervision Capacity

Physical examination halls often host dozens to hundreds of students at once, making it difficult for invigilators to observe every individual simultaneously. Human invigilators are prone to fatigue, distractions, and blind spots**,** allowing students to exploit gaps in supervision to engage in malpractice such as whispering, passing notes, or showing unauthorized materials to peers (Adewale & Hassan, 2023).

2. Subtle and Undetectable Malpractices

Many forms of malpractice in physical exam halls—like covert gestures, head turns, or eye signaling—are difficult to detect in real-time without technological support. These behaviors often go unnoticed, especially in large rooms where visibility is restricted.

3. Inadequacy of Manual Video Monitoring

Some institutions attempt to record physical exam sessions using CCTV or simple camera setups. However**,** manual review of long video footage is time-consuming, subjective, and often lacks timely detection, making it difficult to respond during the exam or gather solid evidence afterward.

4. Lack of Real-Time Alert Systems

Traditional surveillance systems do not provide instant alerts when suspicious activities occur**,** meaning invigilators are unaware of ongoing malpractice until after the fact—if at all. This delayed response compromises the credibility of the assessment.

5. Absence of Audio Monitoring

Current physical proctoring solutions rarely include audio surveillance**,** allowing students to engage in verbal collaboration or whispering without detection. This leaves a critical gap in monitoring communication-based cheating.

6. Scalability and Consistency Issues

Institutions with limited staff or infrastructure struggle to maintain consistent invigilation standards across multiple examination halls or campuses. The human-centered model doesn't scale well for high-capacity exams, leading to inconsistencies in supervision quality and increased opportunities for malpractice.

1.3 Objectives of the Study

The primary objective of this research is to develop an intelligent E-Crime Identification System that automatically detects and reports examination malpractice in physical exam halls through the use of AI-enhanced video and audio surveillance.

This system will assist institutions in conducting secure, scalable, and transparent examinations by automating the monitoring of student behaviors using system-installed cameras and microphones.

Specific Objectives:

1. **To develop a real-time surveillance system** (web-based or standalone) that connects to hall-installed cameras and microphones for monitoring student activities during physical examinations.
2. **To integrate advanced AI and computer vision models**, including:

   - **BlazeFace** for detecting and counting faces within the exam hall.
   - **FaceMesh** for tracking eye movements and head orientation to detect gaze shifts or suspected communication.
   - **Coco-SSD** for identifying unauthorized objects such as mobile phones, textbooks, or earpieces.

3. **To implement an audio analysis module** that:

   - Detects voice activity or spoken communication among students.
   - Flags background noise patterns such as whispering or group conversation.

4. **To design a real-time alert and evidence system** that:

   - Notifies invigilators or system administrators immediately upon detecting suspicious activity.
   - Captures and stores short video/audio clips or images as evidence of potential malpractice.

5. **To build a secure and structured back-end system** that:

   - Manages examination sessions, student records, and configuration settings.
   - Encrypts and stores flagged media securely to protect integrity and user privacy.
   - Enables administrative tools for reviewing, tagging, and exporting violation reports.

6. **To create a user-friendly dashboard for exam supervisors** that:

- Displays detected incidents in real time.
- Allows sorting/filtering of events by student, time, or violation type.
- Generates detailed reports for institutional use.

7. **To ensure system scalability and institutional adaptability**, allowing seamless integration with:

    - Existing hall surveillance infrastructure.
    - Examination management platforms or student identity databases.

8. **To evaluate system performance** based on key metrics such as:

    - Detection accuracy, speed of response, and false positive/negative rates.
    - Reliability under varying hall conditions (e.g., lighting, camera angles, and noise levels).

9. **To promote ethical surveillance and privacy compliance**, by:

    - Incorporating consent protocols for student awareness.
    - Ensuring the system aligns with privacy regulations such as GDPR or national data protection laws.

1.4 Scope of the Study

This project focuses on the detection of visual and auditory examination malpractice in physical examination halls using surveillance cameras and microphones installed within the environment. The system is designed to assist human invigilators by providing real-time alerts and recorded evidence whenever suspicious behavior is detected during in-person, paper-based, or computer-based assessments conducted in classrooms or halls.

The scope includes:

1. The use of **system-installed cameras** to monitor multiple students simultaneously, enabling the detection of:

    - Multiple faces or heads grouped closely.
    - Irregular head movements or turning suggestive of cheating behavior.
    - Temporary or prolonged absence of a student’s face from camera view.
2. **Integration of object detection models** (e.g., Coco-SSD) to recognize unauthorized physical items such as:
    - Mobile phones, books, earphones, and other prohibited materials.
3. **Audio surveillance and analysis**, using hall microphones to detect:
    - Verbal communication, whispering, or background voices that indicate collaboration or assistance.
4. **Real-time alert and evidence capturing mechanism**, which:
    - Notifies the invigilator or system administrator when suspicious behavior occurs.
    - Automatically captures short video/audio segments or snapshots as evidence for post-exam review.
5. **Centralized session management**, logging of detected events, and metadata handling on a secure server backend.

Limitations of the Study:

- The system does not include biometric authentication or real-time identity matching.
- It relies on the correct positioning and quality of surveillance equipment; poor camera angles, lighting, or audio interference may affect accuracy.
- The system does not prevent malpractice**,** but focuses on detecting and documenting it.
- False positives or negatives may occur due to overlapping noise, occlusion, or crowd density.
- Real-time performance may be influenced by network latency **or** hardware limitations.

Despite these constraints, the system offers a scalable, cost-effective, and intelligent solution to enhancing invigilation processes in traditional examination environments.

1.5 Significance of the Study

Examination malpractice threatens the core of academic integrity and undermines the reliability of assessment outcomes. This is especially concerning in physical exam halls where the number of students per session often overwhelms available invigilation resources. As institutions seek to uphold standards while managing large candidate populations, intelligent surveillance systems become not only relevant but necessary.

This study is significant in the following ways:

1. **Advancement in Academic Integrity Monitoring**: The system introduces a technology-driven solution for real-time malpractice detection in physical examination settings. By complementing human invigilators with AI-powered surveillance, it enhances the overall reliability and fairness of the assessment process, making malpractice detection more proactive and evidence-based.
2. **Application of AI in Education Security**: The research demonstrates how machine learning techniques—such as facial detection, head tracking, object recognition, and sound analysis—can be applied in real-world academic contexts. It showcases the integration of computer vision and audio intelligence into existing institutional infrastructure to strengthen examination oversight.
3. **Cost-Effective and Scalable Deployment**: The system is built using lightweight, open-source frameworks that support deployment in resource-constrained settings. Unlike commercial platforms that require per-user licensing, this project is optimized for shared use in large physical halls, making it accessible to institutions across developing regions (Adewale & Hassan, 2023).
4. **Contribution to Research and Innovation**: This project enriches the growing field of AI in education by offering a prototype that can be further developed by researchers and policymakers. The system's modular architecture allows future enhancements such as biometric matching, attendance tracking, and integration with examination management tools.
5. **Institutional and Policy Relevance**: The solution supports institutional accountability and transparency in assessments, making it relevant for policy formulation and quality assurance in education. Its implementation can serve as a model for national education bodies seeking to modernize invigilation practices without increasing manpower demands.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The prevalence of examination malpractice poses a significant threat to the credibility and integrity of educational systems across the globe. As assessments move beyond physical classrooms into digital and hybrid environments, traditional methods of invigilation are increasingly being challenged. This shift has prompted a growing body of research into technological solutions, particularly those leveraging Artificial Intelligence (AI), computer vision, and machine learning to monitor and prevent exam-related misconduct (Okafor & Adeyemo, 2023).

The literature reviewed in this chapter focuses on four key areas: the nature and causes of examination malpractice, its consequences, the role of surveillance technologies in academic environments, and recent advancements in AI-powered monitoring tools. These insights form the theoretical foundation for the development of an intelligent camera-based surveillance system designed to detect and respond to cheating behaviors in real time.

Moreover, this chapter explores ethical concerns surrounding digital surveillance in education, especially as institutions strive to balance academic integrity with student privacy and trust (Chen et al., 2024). Understanding these tensions is crucial in designing a responsible and effective solution for mitigating malpractice in examinations.

2.2 Concept of Examination Malpractice

Examination malpractice, often described as academic dishonesty, encompasses a diverse range of unethical practices undertaken by students with the intention of gaining an unfair advantage during assessments. This persistent problem affects educational systems globally, particularly in regions where instructional resources, qualified personnel, and institutional oversight are insufficient (Olatunji & James, 2022). It distorts the process of evaluating students' academic performance and undermines the credibility of educational qualifications, ultimately posing a threat to national development and professional competence.

2.2.1 Evolution of Examination Malpractice

The nature of examination malpractice has evolved significantly over time, particularly in response to advancements in technology. Traditional forms of cheating such as using concealed paper notes, whispering answers, or copying from nearby candidates continue to exist. However, the rise of digital learning platforms and the widespread adoption of online and remote examinations have given rise to more sophisticated forms of malpractice. Students now exploit technological tools such as mobile phones, smartwatches, and earpieces to access unauthorized materials. Additionally, some engage in screen sharing or remote desktop access to receive external assistance during online tests. Impersonation—where another individual takes the test on behalf of the registered student—has become more difficult to detect in virtual settings. Browser manipulation and the use of automated software further complicate monitoring efforts. As a result, traditional invigilation strategies are proving inadequate in addressing these challenges, prompting the integration of artificial intelligence and other smart technologies into examination surveillance systems (Chen et al., 2024).

2.2.2 Causes of Examination Malpractice

The causes of examination malpractice are varied and deeply rooted in personal, institutional, and societal dynamics. One of the leading drivers is academic pressure. Students often face intense expectations from parents, guardians, or scholarship bodies to achieve high academic performance, pushing them toward dishonest behaviors when they feel unprepared. Poor study habits also play a significant role; students who procrastinate or struggle with time management may resort to cheating as a last-minute solution. Furthermore, a lack of confidence and fear of failure often compel academically weaker students to engage in malpractice, particularly when examinations are perceived as high-stakes.

Institutional weaknesses further exacerbate the issue. In many schools, especially in low-income or resource-constrained regions, invigilation systems are either poorly structured or completely ineffective. Overburdened supervisors may be unable to monitor students effectively, while some may even be complicit in enabling malpractice. Where punitive measures are either too lenient or inconsistently enforced, students are less likely to perceive cheating as a serious offense. In such environments, academic dishonesty may become normalized, and peer influence can amplify the likelihood of misconduct. Additionally, societal attitudes that downplay the seriousness of cheating further reinforce these behaviors, making examination malpractice a systemic rather than isolated issue.

2.2.3 Consequences of Examination Malpractice

The consequences of examination malpractice are far-reaching and detrimental to individuals, institutions, and society as a whole. One of the most critical implications is the devaluation of academic credentials. When students obtain qualifications through dishonest means, those credentials lose their meaning and reliability, potentially disadvantaging graduates who have earned their achievements honestly. This leads to a decline in the overall credibility of educational institutions.

At the institutional level, the presence of unchecked malpractice can damage an organization's reputation, particularly if incidents become public or result in legal or regulatory action. Such reputational harm may impact student enrollment, deter academic partnerships, and reduce the institution's appeal to employers and international bodies. In the wider context, graduates who lack the necessary knowledge and skills due to malpractice are likely to underperform in the workplace. This is particularly dangerous in sensitive fields such as medicine, engineering, and law, where incompetence can result in life-threatening consequences.

Examination malpractice also fosters a culture of corruption and unethical behavior. Students who develop dishonest habits in school may carry these tendencies into their professional lives, perpetuating a cycle of misconduct. Moreover, public trust in the educational system deteriorates when stakeholders—students, parents, educators, and employers—perceive that academic assessments do not reflect true merit. Finally, when exams fail to serve their purpose due to widespread cheating, the resources invested in planning, administering, and grading these assessments are wasted, resulting in diminished educational returns.

2.3 Surveillance Technologies in Academic Environments

The integration of surveillance technologies within academic institutions has become a pivotal response to the increasing challenge of examination malpractice. As digital transformation reshapes the educational landscape, particularly in the wake of global shifts toward remote learning, institutions are progressively adopting advanced monitoring tools to preserve the integrity of assessments. Surveillance in this context extends beyond traditional physical observation to include sophisticated digital mechanisms that incorporate artificial intelligence (AI), biometrics, computer vision, and audio analytics.

2.3.1 Traditional Surveillance Systems

Conventional surveillance approaches such as closed-circuit television (CCTV) have long been employed in physical examination centers to deter and detect misconduct. These systems function by capturing continuous video footage that can be reviewed in real time or retrospectively by human invigilators or security personnel. While effective in controlled environments, CCTV systems present several limitations. Chief among these is their dependency on manual monitoring, which makes them resource-intensive and less scalable, especially in large institutions or during high-capacity examination periods. Furthermore, violations are often detected only after the examination has concluded, reducing the immediacy of response. The lack of automation and the high demand for human oversight diminish their overall efficiency and responsiveness (Idoko & Suleiman, 2023).

2.3.2 Remote and AI-Based Proctoring

The rise of online and hybrid learning has necessitated the evolution of proctoring systems to accommodate remote examination environments. AI-powered proctoring platforms now utilize webcams, microphones, and screen-capture software to observe candidates during assessments. These systems deploy machine learning algorithms to detect anomalies such as prolonged gaze shifts, suspicious facial movements, and the appearance of unauthorized individuals or objects within the camera frame. Background noise analysis through microphone input helps identify potential verbal communication or external assistance.

Popular commercial solutions such as ProctorU, Examity, and TestReach have demonstrated the potential of remote AI-based surveillance. These platforms offer a combination of automated detection and human review, enabling institutions to scale their assessment processes without proportionally increasing invigilation staff. However, despite their capabilities, these tools often come with substantial licensing fees and raise concerns regarding user privacy, data storage, and the ethical implications of continuous monitoring. Institutions in developing regions, constrained by budgetary and infrastructure limitations, may find such solutions difficult to implement universally (Chen et al., 2024; Musa & Bello, 2025).

2.3.3 Deep Learning and Real-Time Detection

The emergence of deep learning technologies has further enhanced the sophistication and accuracy of surveillance systems in academic contexts. Research initiatives and experimental projects have employed advanced models such as Convolutional Neural Networks (CNNs), YOLO (You Only Look Once), and MediaPipe frameworks to detect specific behaviors associated with examination malpractice. These include the identification of mobile phone usage, the temporary absence of the test-taker's face from the frame, frequent head turning indicative of communication attempts, and the presence of unauthorized objects like books or handwritten notes.

What sets these systems apart is their ability to operate in real time, delivering immediate alerts to invigilators or administrators and capturing time-stamped video or audio evidence for subsequent review. The use of libraries such as TensorFlow and OpenCV enables the development of lightweight and browser-compatible models that can function effectively using standard hardware like basic webcams and microphones. This accessibility makes them a viable solution for institutions with limited access to high-end computational infrastructure.

In addition, modern surveillance models are increasingly being deployed within secure examination portals through integration with WebRTC and WebSocket protocols. This ensures low-latency communication and seamless data transmission between client devices and backend servers, allowing for the centralized management of examination sessions and violation logs. Developers are also adopting privacy-conscious design practices, ensuring that data collection complies with institutional policies and regional data protection regulations.

2.4 Related Works

The growing need to uphold academic integrity in online examinations has led researchers and technologists to explore a variety of automated surveillance systems. This section critically reviews prior work in the domains of face detection, behavior analysis, object recognition, and ethical considerations in AI-based proctoring, with particular emphasis on the methodologies adopted, the accuracy achieved, and the practical challenges encountered.

2.4.1 Face Detection and Behavior Monitoring

Ahmed and Joseph (2024) presented a prototype system that utilizes facial recognition and head pose estimation to monitor students' attentiveness during online exams. By analyzing head movement and gaze direction, the system could reliably detect when a student turned their head or looked away from the screen—behaviors commonly associated with possible malpractice. Their study demonstrated commendable accuracy in controlled settings. However, one notable limitation was the system's dependency on consistent lighting conditions. Performance significantly declined in low-light environments or when students had poor-quality webcams, limiting its reliability in diverse real-world scenarios.

Similarly, Eze et al. (2023) developed a webcam-based invigilation solution that automatically alerts proctors when more than one face is detected within the camera frame. This feature aimed to prevent impersonation and unauthorized collaboration. While their system proved effective in multi-user detection, it lacked the capability to identify contextual violations, such as the use of mobile phones, calculators, or unauthorized materials, thereby narrowing its utility in comprehensive surveillance scenarios.

2.4.2 Object Detection in Exam Environments

The application of object detection algorithms has been another significant focus in related research. Chen et al. (2024) implemented a system based on the YOLOv5 model, capable of recognizing a wide range of objects including mobile phones, books, calculators, and tablets. Their experiments reported a high classification precision exceeding 90 percent. Despite its promising accuracy, the system's real-time performance required high-end graphics processing units (GPUs), which poses a challenge for implementation in resource-constrained educational environments, particularly in developing countries where access to advanced hardware is limited.

In an effort to create a more accessible solution, Ibrahim and Aluko (2025) proposed a hybrid detection system that combined facial tracking with audio signal analysis. Their model was designed to identify students who attempted to communicate verbally during examinations. By monitoring audio volume levels and detecting deviations from predefined thresholds, the system could flag possible instances of spoken collaboration. Although this approach significantly improved the detection of voice-based malpractice, it was prone to false positives, especially in cases where ambient noise or innocent verbal exclamations triggered the system.

2.4.3 Ethical Considerations in Surveillance

Beyond the technical dimensions of examination monitoring, ethical considerations have emerged as a critical area of discourse in related literature. Okafor and Adeyemo (2023) emphasized the need for transparency and student consent in the deployment of surveillance tools. They raised concerns regarding potential infringements on students' rights to privacy, particularly when institutions implement monitoring mechanisms without adequate disclosure or opt-out options. Their work calls for the adoption of ethical design principles, including data minimization and anonymization, to foster trust and compliance.

Further advancing the ethical discussion, Chen and Zhang (2022) examined algorithmic bias in facial recognition systems. Their findings highlighted that students with darker skin tones or those in poorly lit environments were disproportionately flagged by certain detection algorithms, revealing a troubling issue of fairness in AI surveillance. They advocated for more inclusive model training and environmental calibration to ensure that AI-driven invigilation does not inadvertently discriminate against specific student demographics.

2.5 Gaps in Literature

While there has been a noticeable increase in research focused on digital proctoring and AI-driven exam surveillance, several important gaps still remain. These gaps become even more apparent when we consider the everyday realities of institutions in developing countries, where limited access to advanced technology and infrastructure can make it difficult to adopt the latest innovations. There's a growing need for solutions that are not only effective and responsive in real time but also ethical, affordable, and adaptable to a range of environments.

One of the main gaps in the literature is the lack of systems that can handle multiple types of cheating behavior at once. Most existing research tends to concentrate on just one aspect—either facial recognition and head movement monitoring, or object detection like spotting mobile phones or paper notes. But cheating is rarely that simple. In real-life situations, students might engage in a mix of behaviors—such as looking off-screen while also speaking quietly to someone off-camera. When systems fail to bring together visual and audio cues in a coordinated way, they miss out on the full picture. Important behavioral indicators like whispering, long screen absences, or even shifting eye movements can slip through the cracks if audio isn't part of the equation. This creates blind spots in detection and makes it harder for institutions to respond effectively.

Another issue is that many of the technologies discussed in academic literature rely on high-end hardware, including powerful GPUs and expensive cloud platforms. These requirements make them difficult to implement in places where schools may have only basic computers and slow internet connections. This limits their usefulness in low-resource settings—ironically, the very environments where exam malpractice is often most prevalent. There's a clear need for lightweight, browser-friendly, and open-source tools that don't require institutions to spend heavily or overhaul their existing systems just to maintain academic integrity.

A further limitation is the lack of real-time response and record-keeping in most systems. While it's helpful that some models can detect suspicious behavior, many fail to alert invigilators immediately or save video and audio clips for later review. This is a serious drawback when schools need to act quickly or provide proof of misconduct during disciplinary proceedings. Ideally, a well-designed system should not only catch cheating as it happens but also give educators a way to go back and verify what took place, ensuring transparency and fairness for everyone involved.

Adaptability is another area where many current tools fall short. Most are tested in clean, quiet environments with strong lighting and stable internet—conditions that don't reflect what many students face in their homes or rural communities. In these less-than-ideal settings, AI models often perform poorly, making false accusations or failing to detect real violations. This highlights the need for technologies that are robust and flexible enough to handle noisy rooms, poor lighting, or network interruptions without compromising performance.

Equally important, and often overlooked, are the ethical and privacy concerns tied to AI surveillance in education. In many cases, students are monitored without knowing exactly what data is being collected, how it's being stored, or who will have access to it. This lack of transparency can undermine trust and even raise legal concerns—especially in countries with strict data protection laws. An ethical surveillance system must go beyond technical performance; it should be built around student consent, data privacy, and fairness. Giving users control over their data and clearly explaining how the system works can go a long way toward building trust and acceptance.

Finally, there's a clear shortage of home-grown solutions—tools developed locally, by and for the communities that need them most. Right now, most of the available software is built by companies in wealthier countries, which can lead to a mismatch between the tool's design and the actual challenges faced in different parts of the world. Without local customization or involvement, schools may find themselves using tools that are not cost-effective, hard to modify, or culturally appropriate. Supporting open-source, community-built systems can promote innovation, empower local developers, and lead to more sustainable and relevant solutions for tackling exam malpractice.

CHAPTER THREE

SYSTEM DESIGN AND METHODOLOGY

3.1 Introduction

This chapter presents the foundation of the system design and the methodology adopted in the development of the E-Crime Identification System for Examination Malpractice Using Camera Surveillance. As online and computer-based testing continues to grow in popularity across academic and professional domains, the demand for secure, intelligent proctoring solutions has become increasingly critical. Traditional examination environments typically rely on human invigilators to monitor student behavior; however, with the shift to remote learning and virtual examinations, the integrity of these processes has been compromised due to the lack of adequate surveillance and detection mechanisms.

To address this challenge, the proposed system aims to deliver a real-time, intelligent, and automated proctoring framework capable of monitoring examinees using a standard webcam and microphone. The system leverages computer vision and machine learning technologies integrated through a web interface to identify various forms of examination malpractice. These include but are not limited to:

- **Presence of multiple faces** within the camera view, which could indicate impersonation or unauthorized assistance.
- **Head movement detection**, signaling attempts to look away from the screen, possibly at notes or another device.
- **Speech or audio analysis** using microphone input to detect communication during the examination.
- **Object detection**, including prohibited items such as mobile phones, books, or writing notes.

The system is designed with modularity, allowing each detection module (face, head movement, object, audio) to function independently while contributing to an integrated surveillance system. This modular design supports scalability, enabling future enhancements like emotion recognition or eye-tracking to be added without restructuring the entire application. Additionally, the solution is built to run entirely within a web browser using modern frontend frameworks and JavaScript-based AI libraries such as TensorFlow.js, thereby ensuring cross-platform usability and eliminating the need for software installation on the client side.

From a systems perspective, the architecture incorporates both client-side and server-side components. The client-side handles real-time detection using camera and microphone feeds, processes them through pre-trained machine learning models, and flags suspicious activities. The server-side, powered by Node.js and WebSocket technology, is responsible for storing evidence (video and audio clips), managing alerts, and enabling administrators to monitor examinee behavior through a secure interface.

Ultimately, this system addresses the urgent need for robust digital exam surveillance, offering a practical and innovative approach to reducing examination fraud. The design considerations outlined in this chapter reflect the commitment to building a system that is both technically sound and user-friendly—providing educational institutions and organizations with a scalable, web-based, and intelligent tool for maintaining examination integrity.

3.2 System Development Methodology

For the successful development of the E-Crime Identification System for Examination Malpractice Using Camera Surveillance, the Agile software development methodology was employed. This choice was driven by Agile's flexibility and iterative nature, which enabled constant refinement and seamless feedback integration throughout the development lifecycle. Given the experimental nature of integrating AI-driven detection models into a web-based environment, Agile allowed the development team to respond quickly to challenges, test innovative ideas, and refine system components without major disruptions.

Requirement Gathering

The development process began with an in-depth requirement analysis phase. During this stage, the team analyzed the limitations of traditional online examinations by consulting educators, reviewing existing online proctoring platforms, and observing real-world candidate behavior in unsupervised testing environments. The objective was to identify the most prevalent forms of examination malpractice—such as impersonation, external assistance, and the use of unauthorized materials—and define clear functional and non-functional requirements that the system should meet.

System Design

Following the requirement phase, a detailed system design process was initiated. Interface mockups were created to visualize both the student examination screen and the admin's monitoring dashboard. These mockups were used to plan the user experience and layout of core monitoring tools. At the same time, the architecture of the AI-based detection engine was drafted. This included outlining the operational flow of face detection**,** head turn analysis**,** object detection**,** and audio monitoring modules. Each module was designed to function independently, enabling parallel processing and modular upgrades, while also contributing to a cohesive and robust proctoring framework.

Implementation Phase

The implementation phase focused on building both the **f**rontend and backend using modern web development tools. The frontend was built using React.js**,** chosen for its component-based architecture and real-time rendering capabilities. The backend was implemented using Node.js**,** leveraging its event-driven and non-blocking architecture to handle WebSocket connections efficiently for real-time alert communication. This made the system suitable for simultaneous connections and fast media handling. On the frontend**,** TensorFlow.js was employed for client-side model inference, enabling AI-driven detections to run directly in the browser without additional installations. Web APIs such as MediaDevices and MediaRecorder were integrated to access and process the webcam and microphone streams in real time.

Testing and Iteration

Testing was embedded throughout the development process. Functional testing was conducted on each detection module to ensure that facial recognition, head movement tracking, object recognition, and audio analysis performed as expected under different environmental conditions.

Simulated exam sessions were organized to mimic real-life test environments. These simulations allowed the team to evaluate how the system responded to challenging scenarios such as low lighting, background distractions, or sudden movements. Performance data and user feedback from these sessions were used to identify flaws and areas for improvement.

Deployment

Once all components were successfully integrated, the system was deployed on a local server for testing. Deployment tasks included optimizing model load times, ensuring stable WebSocket communication between clients and administrators, and verifying that alerts were triggered accurately and delivered promptly. The team conducted mock examination sessions to monitor the system’s behavior and measure metrics like model inference speed, alert latency, and media evidence upload consistency. These sessions validated the system’s ability to perform under pressure and maintain real-time responsiveness.

Review and Refinement

In the final phase, a thorough review and refinement process was carried out. Logs and feedback collected from earlier testing were analyzed to identify bottlenecks and performance issues. Several improvements were implemented, including model optimization to reduce processing delay, frontend UI enhancements to improve usability for both students and admins, and backend error handling improvements for better system resilience. The iterative nature of Agile development ensured that these refinements could be implemented quickly without interrupting core functionalities.

3.3 System Architecture

The architecture of the E-Crime Identification System for Examination Malpractice Using Camera Surveillance follows a modular client-server model**,** designed for real-time monitoring, scalability, and future extensibility. The architecture ensures a clear separation of responsibilities between the client-side application**,** which runs on the student’s browser, and the server-side infrastructure**,** which handles alert processing, data management, and administrative oversight. This approach enables seamless communication between examinees and proctors during online exams.

Client Side (Frontend) – React.js with TensorFlow.js

The frontend is developed using React.js**,** a modern JavaScript library used to build interactive and responsive user interfaces. It incorporates TensorFlow.js**,** which allows for running pre-trained machine learning models directly in the browser**,** eliminating the need to send raw video or audio data to an external server—thus enhancing both performance and privacy**.**

The core function of the frontend is to monitor examinees in real-time using the device's webcam and microphone. It integrates several AI-powered modules and browser-native APIs:

- **Face Detection**: Using the BlazeFace model**,** the application continuously monitors the webcam stream for human faces. If more than one face is detected or if no face is present for a prolonged period, the system raises a violation alert.
- **Head Pose Estimation**: Implemented using FaceMesh**,** which maps 468+ facial landmarks. By analyzing the orientation and positioning of these landmarks, the system determines whether a student is turning their head away from the screen, which may indicate potential cheating behavior.
- **Object Detection**: Conducted through Coco-SSD**,** a lightweight object detection model that identifies forbidden items such as phones**,** books**,** or extra monitors. Detected objects are cross-referenced with a list of banned materials and flagged accordingly.
- **Audio Monitoring**: The Web Audio API captures microphone input and continuously measures the audio amplitude. Significant spikes in volume suggest speaking or ambient conversation, which are not allowed during an exam and are treated as potential infractions.
- **Evidence Capture**: Upon detecting any suspicious behavior, the system automatically triggers the MediaRecorder API to capture a 5-second video or audio clip. This media is compressed, timestamped, and prepared for immediate upload as supporting evidence.
- **Real-time Communication**: A WebSocket client maintains a persistent, low-latency connection to the server. This ensures that violation alerts, including timestamps, user/session data, violation type, and associated media, are transmitted to the server as soon as they occur—enabling near-instantaneous admin response.

Server Side (Backend) – Node.js with WebSocket

The backend is built using Node.js, a non-blocking, event-driven JavaScript runtime well-suited for real-time applications. A WebSocket server runs continuously to handle two-way communication with multiple student devices simultaneously.

Key responsibilities of the Node.js backend include:

- **Real-Time Alert Handling**: The WebSocket server receives structured JSON messages containing alert data and associated media files. These messages are authenticated and parsed to ensure data integrity before being logged into the system.
- **Evidence Management**: A dedicated module manages the secure storage of media files (audio and video clips), which are organized by session ID**,** violation type**,** and timestamp**.** This systematic structure facilitates efficient retrieval for review during or after the examination.
- **Admin Dashboard API**: The backend exposes RESTful API endpoints that power the admin dashboard. Administrators can log in, view alerts in real-time, review violation logs, download evidence, and monitor ongoing sessions via these APIs.
- **Session Logging and Analytics**: The backend records all session data—login times, logout times, number and type of violations, and more. This data can be exported or visualized to generate exam integrity reports for academic use.

Integration and Real-Time Operation

The client and server components work in sync to support real-time operation. By running inference directly in the browser via TensorFlow.js**,** the client avoids overloading the network with raw media streams. Instead, only summarized alert data and short media snippets are transmitted to the backend. This dramatically improves system responsiveness and privacy.

The WebSocket protocol ensures minimal latency, allowing administrators to be notified of violations the moment they occur. Alerts appear instantly on the admin dashboard with contextual media evidence, enabling swift decision-making and intervention when needed.

This architecture is designed to be scalable, secure, and extensible**.** New features—such as eye tracking**,** emotion analysis**, or** keystroke monitoring—can be integrated without a full system overhaul, thanks to its modular design. The use of a browser-based architecture and Node.js backend ensures broad compatibility, performance efficiency, and a future-ready platform for intelligent exam surveillance.

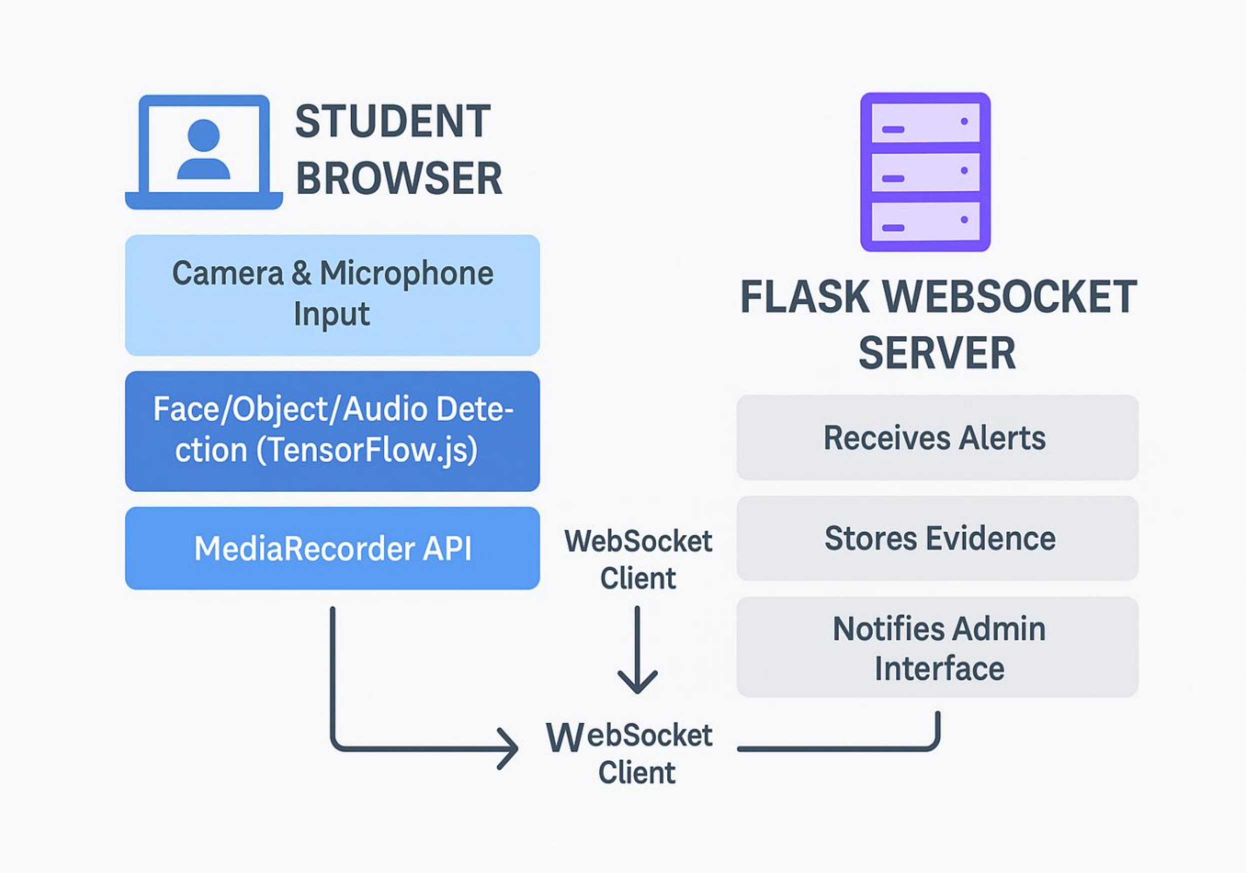

Figure 3.3: E-Crime Identification for Examination Malpractice Using Camera Surveillance System Architecture

3.4 Use Case Diagram

To better understand how different users interact with the E-Crime Identification System for Examination Malpractice, a use case diagram is used. This diagram helps map out the roles and responsibilities of each user and shows the main activities they perform within the system. It's especially helpful during system planning and testing, as it outlines what features the system must support.

Actors and Their Roles

There are two main users—or "actors"—in the system: the Admin and the Student**.**

- **Admin**: The admin is in charge of overseeing the entire exam process. They log into the system to monitor students in real time, receive alerts when the system detects suspicious behavior, and review any evidence collected. Admins also manage user access and system logs, making sure everything runs smoothly and securely.
- **Student**: The student is the one taking the exam and being monitored by the system. Once logged in, the student is automatically placed under surveillance through their webcam and microphone. Although students don't actively control the monitoring, their behavior—whether compliant or suspicious—is the main focus of the AI detection system.

Core Use Cases

Here's how both actors typically interact with the system:

- **Login**: Before anything else, users must log in securely. For students, logging in gives them access to the exam platform and triggers the monitoring process. For admins, login grants access to the dashboard, where they can oversee live sessions and manage violations.
- **Start Monitoring**: When a student starts their exam, the system automatically turns on their webcam and microphone. AI-powered models begin analyzing the video and audio streams in real time. Admins can also manually start or observe these monitoring sessions through their interface.
- **Detect Violation**: This is where the AI kicks in. Throughout the session, the system keeps watch for various forms of suspicious behavior. These include:
    - More than one face appearing on the screen
    - The student disappearing from view
    - Unauthorized objects like phones or books
    - Excessive head movement suggesting possible cheating

    - Talking or other audio signals picked up by the microphone

  Detection is powered by machine learning models such as BlazeFace (for face detection), FaceMesh (for head position), Coco-SSD (for object recognition), and built-in audio analysis tools.

- **Send Alert**: When the system flags a suspicious activity, it instantly sends an alert to the admin’s dashboard. Alongside the alert, it captures a snippet of the video, image, or audio that triggered the detection—so the admin has concrete evidence to review and decide what action to take.
- **Logout**: When the exam is over—or if a session ends for any reason—students can log out securely. Admins also have a logout feature to protect sensitive data and system access once their monitoring duties are done.

Visual Representation

While not shown in this document, the actual **use case diagram** illustrates these interactions in a simple visual format:

- **Actors** (Admin and Student) are placed on the sides.
- **Use Cases** (like "Login," "Start Monitoring," "Detect Violation") are drawn as ovals.
- Lines and arrows connect each actor to the use cases they interact with.

This visual tool is not just a technical diagram—it’s a useful planning aid. It helps developers understand what the system needs to do and ensures that the final product aligns with user expectations and goals.

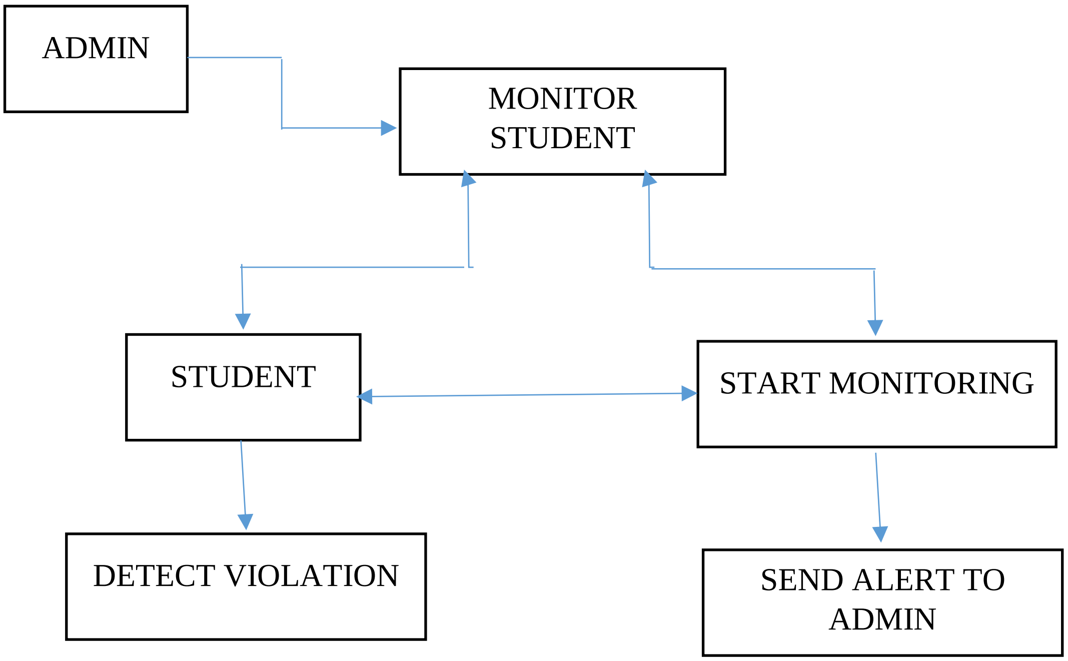

Figure 3.4: E-Crime Identification for Examination Malpractice Using Camera Surveillance Use Case Diagram

3.5 Flowchart

The flowchart illustrates the operational process of the E-Crime Identification System with two main users: the **Admin** and the **Student**.

1. **Student Flow:**
    - The student logs in to the system.
    - The system activates the webcam and microphone.
    - Monitoring begins as the student takes the exam.
    - AI continuously analyzes video and audio for suspicious behavior.
    - If malpractice is detected, an alert is generated and evidence is captured.
    - After completing the exam, the student logs out.
2. **Admin Flow:**
    - The admin logs in to the dashboard.
    - They receive real-time alerts during the exam.
    - Admin reviews flagged evidence (images/audio).

- Admin may take action or store the violation for post-exam review.
- Logs out after monitoring is complete.

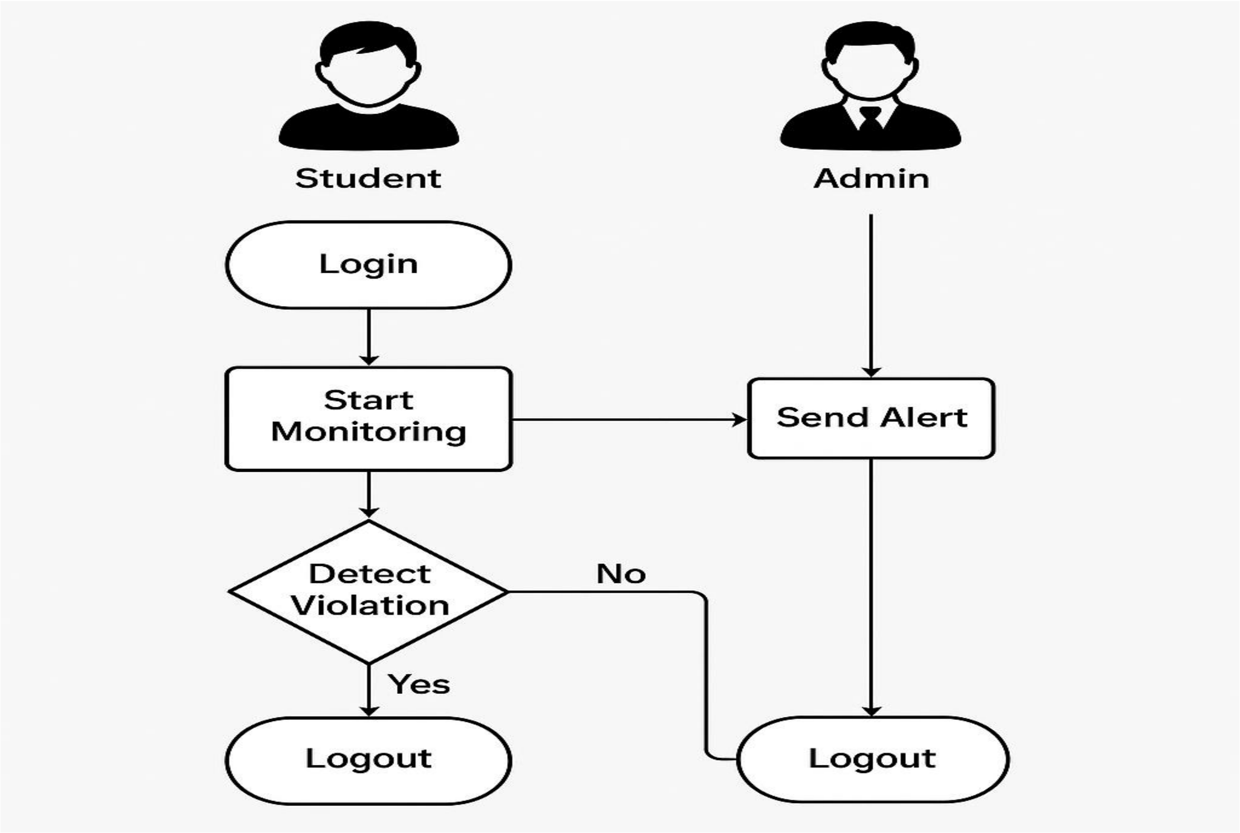

Figure 3.5: E-Crime Identification for Examination Malpractice Using Camera Surveillance Flow chart

3.6 Database Design

The **E-Crime Identification System for Examination Malpractice** employs a relational database to store and manage all critical system data, including user information, examination session logs, and violation reports. This ensures data integrity, secure user authentication, traceability of events, and efficient querying of surveillance records.

The database is structured around three primary entities: Users**,** Exam Sessions**,** and Violations**.** These tables are linked using foreign key relationships to maintain consistency and support robust data management.

Users Table

The users table holds all registered individuals who can access the system. Each user is assigned a unique identifier (user_id) and a role which determines their level of access and functionality within the platform.

- user_id: This is the primary key that uniquely identifies each user.
- username: A string representing the login name of the user (either admin or student).
- password_hash: This field stores the encrypted version of the user's password to ensure security and prevent plaintext storage.
- role: Defines the user's permissions within the system. It can either be 'admin' for administrators or 'student' for exam candidates.

This structure allows the system to implement role-based access control, where only administrators can view violations and receive alerts, while students can only start and participate in exams.

Exam Sessions Table

The exam_sessions table tracks each exam sitting undertaken by a student. It records when a student starts and ends an exam, providing the foundation for time-bound monitoring and linking violations to specific sessions.

- session_id: The primary key that uniquely identifies each examination session.
- user_id: A foreign key that links each session to the corresponding user (i.e., student) in the users table.
- start_time: A timestamp that records when the exam session began.
- end_time: A timestamp marking when the session was completed or terminated.

This table is essential for correlating violations with specific time frames and ensuring that any evidence collected is associated with a valid session.

Violations Table

The violations table is responsible for logging any suspicious or rule-breaking behavior detected by the system. It connects directly to the exam_sessions table to contextualize each violation within the appropriate exam instance.

- violation_id: A primary key that uniquely identifies each violation entry.
- session_id: A foreign key referencing the exam_sessions table, ensuring that each violation is tied to a specific student session.
- violation_type: A descriptive string indicating the type of misconduct observed, such as "Multiple Faces Detected," "Phone Detected," "Talking Detected," or "Head Turn Detected."
- timestamp: The exact date and time when the violation occurred, allowing admins to investigate based on temporal evidence.
- media_url: The file path or URL pointing to the stored media evidence (image, video, or audio clip) captured during the violation.

This table enables detailed auditing of examination behavior, with strong evidentiary support that can be referenced post-examination or in disciplinary procedures.

Database Management Considerations

- **Security**: Passwords are securely hashed (e.g., using `bcrypt`) and never stored in plaintext. Each user document includes a role field (`admin` or `student`) that is used to enforce access control throughout the application. JWT (JSON Web Tokens) or similar methods are used for secure authentication.
- **Scalability**: While the system is initially deployed with a lightweight local MongoDB instance for development and testing, its document-based structure supports seamless migration to scalable cloud-based solutions like MongoDB Atlas**.** This allows for horizontal scaling, sharding, and replica sets in production environments.
- **Performance**: Frequently queried fields such as `userId`, `sessionId`, and `timestamp` are indexed using MongoDB's native indexing features. This ensures efficient query performance even as the dataset grows with more exam sessions and violation records.