**FACIAL RECOGNITION TECHNOLOGY (FRT) IN THE AUTHENTICATION SYSTEM OF THE COMPUTER BASED TEST (CBT)**

**BY**

**ADETOLA JOSHUA YINKA**

**UIL/PG2023/1826**

**BEING A PROPOSAL SUBMITTED TO**

**DEPARMENT OF COMPUTER SCIENCE**

**FACULTY OF COMMUNICATION AND INFORMATION SCIENCE**

**UNIVERSITY OF ILORIN**

**SUPERVISOR:**

**DR. GHANIYYAT B. BALOGUN**

**JUNE, 2025.**

**Abstract**

The increasing need for secure and reliable authentication methods in academic assessments has led to the exploration of biometric technologies in Computer-Based Testing (CBT) systems. This study presents the development and implementation of a facial recognition-based authentication system for the CBT platform at the University of Ilorin. The system utilizes Python-based tools, including Streamlit for the interface and facenet-pytorch with OpenCV for facial detection and verification, to enhance the integrity of online examinations. The modules include facial enrollment, authentication, exam administration, and result management, all integrated into a unified web-based platform. The system was evaluated using real-user datasets, and performance metrics such as authentication accuracy, usability, and administrative efficiency were recorded. Comparative analysis with traditional password-based systems revealed significant improvements in security, user experience, and impersonation prevention. Challenges such as environmental lighting and user onboarding were addressed through interface feedback and design considerations. The findings demonstrate the feasibility and effectiveness of facial recognition in academic authentication, offering a scalable solution for secure digital assessments in higher institutions.

**Keywords:** Facial Recognition, Biometric Authentication, Computer-Based Test (CBT), University of Ilorin, Streamlit, Deep Learning, Security.

**CHAPTER ONE**

**INTRODUCTION**

**1.1 Background to the Study**

Facial recognition technology (FRT) is becoming more common in the authentication systems of Computer Based Tests (CBT) as an effective measure against examination malpractices, especially impersonation. Conventional assessment techniques sometimes depend on credentials like identification through identity cards or passwords, which are susceptible to forgery or theft. Conversely, FRT employs distinct biometric information obtained from an individual's facial features, providing a more secure and dependable method for identity verification. This technology strengthens the integrity of the examination process and aligns with modern demands for efficient and user-friendly authentication techniques (Adebayo et al., 2022).

The incorporation of facial recognition in CBT systems mitigates substantial issues related to examination security. Research reveals that impersonation is one of the most widespread forms of test fraud, eroding the legitimacy of academic assessments. By incorporating FRT into CBT frameworks, educational institutions can establish a multi-tiered security architecture that utilizes biometric verification as a principal authentication technique. Research indicates that these systems can markedly diminish cases of impersonation, with certain implementations documenting a zero percent incidence of this malpractice during trials (Olaoye & Olaniyan, 2022).

Furthermore, the operational benefits of employing FRT in CBT systems are significant. The technique enables for quick and contactless authentication, which is particularly advantageous in high-stakes testing contexts where time efficiency is critical. For instance, candidates can be validated in their respective test table without the need of physical verification. This efficiency is reinforced by the inclusion of the system's ability to produce alerts for questionable behaviors, so further ensuring the integrity of the inspection process.

However, the introduction of facial recognition technology is not without its obstacles. Concerns about privacy, data security, and algorithmic bias must be addressed to enable ethical deployment. Research reveals that while FRT can considerably strengthen security measures, it is vital to create these systems with transparency and fairness in mind. This involves employing different datasets for training algorithms to eliminate biases that could harm particular demographic groups (Adebayo et al., 2022). Furthermore, constant review and refinement of FRT systems are important to maintain their effectiveness and reliability.

In conclusion, the incorporation of facial recognition technology into Computer Based Test systems gives a transformative opportunity to enhance examination security and integrity. While it offers great benefits in terms of minimizing impersonation and enhancing operational efficiency, careful thought must be given to ethical issues and any biases related with its use. As educational institutions progressively use this technology, continuous study will be crucial in addressing these difficulties and guaranteeing fair access to secure testing environments.

**1.2 Statement of Problem**

The rise of examination malpractice, particularly impersonation, poses a substantial danger to the integrity of academic assessments at the University of Ilorin (UNILORIN). Impersonation happens when one student, referred to as Student A, sits an examination on behalf of another student, Student B. This unethical activity weakens the educational system by allowing unqualified persons to receive certificates they have not earned. Recent instances at UNILORIN demonstrate the severity of this issue; in February 2024, the institution dismissed fourteen students for various sorts of misconduct, including examination malpractices such as impersonation. Such acts not only affect the integrity of academic qualifications but also weaken public trust in the educational system.

The repercussions of imitation extend beyond individual incidents; they indicate a greater culture of dishonesty that might impair student motivation and academic achievement. Research reveals that students who engage in such behaviors generally do so due to a perceived lack of preparation and a desire for achievement without effort (Onyechere, 2004). This trend is concerning, as it encourages an environment where academic dishonesty becomes commonplace, leading to a decrease in academic standards. Moreover, the consequences of these activities can be severe, potentially resulting in expulsion and a ruined reputation for both the individuals involved and the school itself.

Tackling test malpractice through the adoption of facial recognition technology at UNILORIN is vital for protecting academic integrity. By attacking mimicry head-on, the university can strengthen the legitimacy of its examinations and develop a culture of honesty among students. As educational institutions increasingly battle with concerns of academic dishonesty, implementing new solutions like FRT will be important in defending the future of education.

**1.3 Aim and Objectives**

The aim of this study is to develop and evaluate a machine‑learning‑based model that seamlessly integrates Facial Recognition Technology (FRT) into the authentication system of a computer‑based Test (CBT) platform, using the University of Ilorin as a case study.

The objectives of the study are to:

1. Analyze the existing CBT login system at the University of Ilorin for current strengths and weaknesses.
2. Develop a machine‑learning model employing facial recognition to enhance student identification accuracy.
3. Implement robust security protocols to protect biometric data and ensure compliance with privacy regulations.
4. Integrate the developed FRT model into the existing CBT platform for seamless authentication.
5. Evaluate the integrated system’s real‑time performance in preventing impersonation.

**1.4 Significance of the Study**

The use of Facial Recognition Technology (FRT) into the Computer-Based Test (CBT) system presents substantial potential for enhancing academic integrity at the University of Ilorin. By substituting conventional identification verification with biometric authentication, facial recognition technology can significantly diminish impersonation and various sorts of examination misconduct. Recent occurrences at UNILORIN, when numerous students encountered disciplinary measures for wrongdoing, highlight the pressing want for more dependable authentication systems. With FRT implemented, stakeholders may restore confidence in the evaluation process, guaranteeing that conferred qualifications appropriately represent each student's knowledge and effort.

In addition to enhancing integrity, FRT provides significant improvements in operating efficiency. The technology's swift, contactless face-matching functionality expedites the pre-examination verification process, alleviating the administrative load on invigilators and reducing waiting times for students. This automation enables examination officers to redirect resources towards enhancing teaching and learning activities instead of doing routine identity verifications. The optimized procedure improves the overall student experience by facilitating prompt exam commencements and alleviating stress linked to human verification.

This study will address the ethical and privacy problems associated with the implementation of biometric technology. We will formulate and record comprehensive security methods to protect sensitive face data and guarantee adherence to current privacy standards. Special emphasis will be made to reducing algorithmic bias so that no demographic group is unduly disadvantaged. By pairing technical innovation with transparent governance, the project will develop a model for responsible FRT deployment. Moreover, the findings will create groundwork for future study on biometric applications in education, advising other institutions as they seek secure, fair methods to sustain academic standards.

**1.5 Scope and Limitations**

This study focuses on the creation and evaluation of a machine learning model integrating face recognition technology (FRT) into the Computer Based Test (CBT) system at the University of Ilorin (UNILORIN). The scope involves creating a powerful facial recognition system capable of accurate student identification, ensuring real-time authentication to prevent impersonation during examinations. The study will leverage biometric data collection, machine learning techniques, and advanced algorithms for assessing facial features. Integration with current CBT systems is a major component, emphasizing seamless and user-friendly authentication operations. The system's performance will be tested by empirical data collecting during mock testing to measure its correctness, dependability, and operational efficiency. Moreover, the project will create tight security mechanisms for biometric data storage, assuring compliance with privacy legislation to address ethical concerns. By concentrating on the unique issue of impersonation in CBT, this research gives a targeted and practical approach to strengthen academic integrity at UNILORIN.

**1.6 Definition of Key Terms**

1. Facial Recognition Technology (FRT): A biometric technology that identifies people by analyzing their unique facial features using advanced algorithms.
2. Computer-Based Test (CBT): A testing method where exams are taken on a computer, allowing fast scoring and efficient delivery.
3. Biometric Authentication: A security method that verifies identity using unique physical traits, such as facial features.
4. Impersonation: When someone takes an exam for another person, undermining test integrity.
5. Machine Learning: A technology where computers learn from data to improve tasks like facial recognition.
6. Convolutional Neural Network (CNN): A type of machine learning model that processes images to recognize patterns like facial features.
7. Dataset: A set of data, like facial images, used to train and test recognition systems.
8. Feature Extraction: The process of identifying key facial details, like eye distance, for recognition.
9. Data Privacy: Keeping personal information, like biometric data, safe from misuse or theft.
10. Ethical Considerations: Moral issues, like fairness and privacy, raised by using technology.
11. Liveliness Detection: A check to ensure a facial scan comes from a live person, not a fake image.

**CHAPTER TWO**

**LITERATURE REVIEW**

**2.1 Introduction**

This chapter introduces important concepts involved in the integration of facial recognition technology (FRT) into the Computer Based Test (CBT) system. It also contains a number of related works that were carried out on integration of facial recognition technology (FRT) into the Computer Based Test (CBT) system.

**2.2 Review of Concepts Relating to the Work**

**2.2.1 Overview of Computer-Based Tests (CBT)**

According to Sarjiyus (2019) Computer-based testing (CBT) is the application and usage of electronic system in place of manual paper-and-pen approach for any assessment related activity. Computer based testing system enables educational institutions and other organizations that need some form of assessment to conduct and schedule surveys, quizzes, tests and examinations to be administered through a computer system and responses/ results are electronically recorded and assessed.

The objective is to make testing or assessment process fair, faster and reliable (Adebayo & Adulhamid, 2014). The Paper based testing (PPT) approach is characterized by massive leakages, impersonation, and demand for gratification by teachers, invigilators etc. hence, the necessity for computer-based testing.

The evolution of new technology has radically affected the style of learning and assessment of students’ performance. This does not prohibit the practice of selection of candidates for matriculation into any Nigerian tertiary institution by the Joint Admissions and Matriculations Board (JAMB). Before the year 2015, the conduct of entrance selection examinations called Unified Tertiary Matriculation Examination (UTME) was paper-based. The former registrar of JAMB, Prof. Dibu Ojerinde, detailed the grounds behind the proposal of Computer-based Tests (CBT) for the conduct of the examination (Okoronkwo, 2019). These include security issues, high expense of transporting the test materials and controlling examination malpractices among the examinees.

CBT has a number of major advantages compared to traditional paper-based exams (PBT) such as efficiency, instant scoring and feedback in the case of multiple-choice question tests (Boevé et al., 2015). Also, e-examination can increase the standard of student’s examination whereas the conventional examination system utilizing the pen and paper demands more effort on the side of students and invigilators (Ibrahim et al., 2017).

Despite these advantages, CBT is not without its own obstacles. Ensuring that examinees do not search computer directories or surf online to get answers is a challenge. In addition, guaranteeing that examinees do not engage in examination impersonation is virtually impossible. Again, since the birth of e-learning, there has been a security breach as it poses numerous hazards especially when tests are held electronically (online). Security is one of the issues of both traditional and online-based testing systems.

One technique to reduce security breach during online test is to identify, authenticate and monitor applicants during online assessment (Ibrahim et al., 2017).

There is therefore the requirement to uniquely identify examinees in the process of examination done. Over the decades, biometrics especially the fingerprint biometrics and facial recognition has been used to successfully identify and verify the unique identity of individuals. However, the successful implementation of the facial recognition with CBT in Nigerian higher institutions has limited applicability.

**2.2.2 Introduction to Biometric Authentication**

Biometrics (ancient Greek: bios ="life", metron ="measure") refers to two very different fields of study and application. The first, which is the older and is utilized in biological studies, including forestry, is the gathering, synthesis, analysis and management of quantitative data on biological communities such as forests. Biometrics in connection to biological sciences has been researched and applied for multiple generations and is rather simply seen as "biological statistics" (Alliance, 2009).

European adventurer Joao de Barros first documented fingerprinting in China in the 14th century. Alphonse Bertillon's Bertillonage method, used by the police, was later abandoned due to false identifications. Karl Pearson, an applied mathematician, studied biometric research at University College of London, making key findings on statistical history and correlation. In the 1960s and '70s, signature biometric authentication processes were created, but the field remained fixed until military and security services developed biometric technology beyond fingerprinting (Bhattacharyya et al., 2009).

Biometrics authentication is a growing and controversial topic in which civil liberties groups express worry over privacy and identification issues. Today, biometric legislation and regulations are in process and biometric industry standards are being evaluated. Face recognition biometrics has not achieved the ubiquitous level of fingerprinting, but with constant technological pushes and with the fear of terrorism, researchers and biometric developers will stimulate this security technology for the twenty-first century. In current approach, Biometric features can be separated in two primary classes:

1. Physiological are tied to the shape of the body and hence it differs from person to person Fingerprints, Face recognition, hand geometry and iris recognition are some examples of this sort of Biometric.
2. Behavioral are related to the behavior of a person. Some examples in this situation are signature, keystroke dynamics and of voice. Sometimes voice is also considered to be a physiological biometric as it differs from person to person. (Bhattacharyya et al., 2009).

Recently, a new trend has been developed that connects human perception to computer database in a brain-machine interface. This method has been referred to as cognitive biometrics. Cognitive biometrics is based on distinct responses of the brain to stimuli which could be used to initiate a computer database search (Bhattacharyya et al., 2009).

A biometric system can provide two functionalities. One of which is verification and the other one is Authentication. So, the approaches employed for biometric authentication ought to be stringent enough that they can employ both these features simultaneously. Currently, cognitive biometrics systems are being developed to exploit brain response to odor stimuli, facial perception and mental performance for search at ports and high security areas. Other biometric techniques are being explored such as those based on gait (way of walking), retina, Hand veins, ear canal, facial thermogram, DNA, odor and scent and palm prints. In the near future, these biometric techniques can be the solution for the existing problems in realm of information security (Bhattacharyya et al., 2009).

**2.2.3 Facial Recognition Technology (FRT)**

Face Recognition Technology (FRT) is a biometric technology that identifies or confirms individuals by evaluating their unique face traits. This technique utilizes artificial intelligence (AI) and machine learning (ML) algorithms to map and compare facial structures against a database. FRT operates by collecting an image, extracting distinctive face traits, and comparing them with stored data to validate identity. It is widely acknowledged for its non-invasive, contactless capabilities, making it a favored tool for authentication across multiple domains (Jain et al., 2021).

The development of FRT extends back to the 1960s, when academics began researching facial feature extraction for automated recognition. Early approaches depended mainly on hand measurements and crude algorithms, such as the Eigenfaces technique launched in the 1980s. With developments in computer power and AI in the 21st century, FRT grew into a sophisticated instrument. Modern systems utilize deep learning models, such as convolutional neural networks (CNNs), to increase accuracy and robustness. A landmark example is the deployment of FRT at major international airports for security screening, exhibiting its reliability in high-pressure conditions (Zhao & Chellappa, 2018).

FRT relies on two primary principles: feature extraction and face matching. Feature extraction involves detecting and encoding key facial landmarks, such as the distance between the eyes, nose shape, and jawline, into a unique numerical representation called a facial signature. Face matching compares this signature to stored templates in a database to identify or verify an individual. Modern FRT systems enhance accuracy using deep learning models, which adaptively learn complex patterns in facial data. These principles underpin the functionality of real-world systems like Apple’s Face ID, which uses infrared sensors and neural networks for authentication.

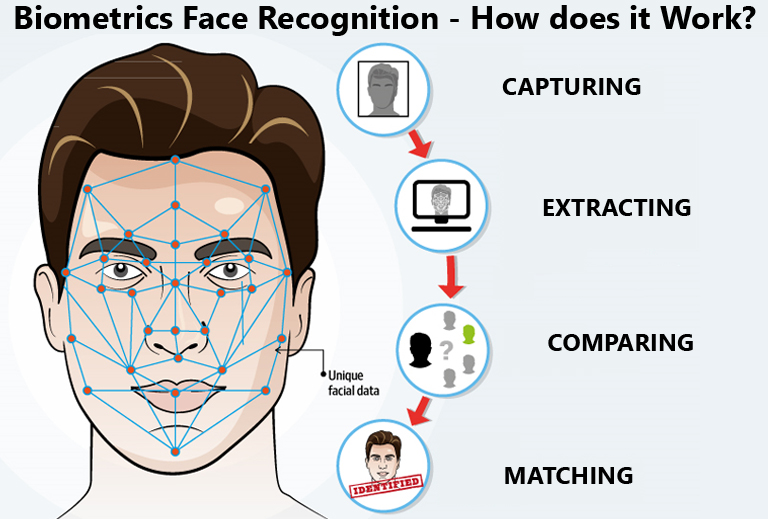


Figure 2.1 Facial Recognition Process

FRT has found significant uses in both security and education areas. In security, law enforcement agencies deploy FRT to trace offenders through surveillance footage and identify individuals in public settings. This technology supports in investigations by offering quick access to prospective suspects' identities based on visual data obtained from multiple sources. In educational environments, FRT is widely employed for campus security and attendance tracking. Schools deploy these technologies to increase safety measures against illegal entrants and streamline administrative tasks like roll calls (Andrejevic & Selwyn, 2020). However, these uses create ethical considerations surrounding privacy and surveillance.

**2.2.4 Machine Learning in Facial Recognition**

Facial recognition technology (FRT) has substantially evolved with the introduction of machine learning methods, particularly convolutional neural networks (CNNs). CNNs are adept at processing visual data due to their capacity to grasp spatial hierarchies in images, making them suitable for facial recognition tasks. By learning and extracting detailed information from facial photos, CNNs have increased the accuracy and reliability of FRT systems. For instance, the VGG-Face model, developed by the Visual Geometry Group at the University of Oxford, achieved outstanding performance in face identification by adopting a deep CNN architecture trained on a huge dataset of facial pictures (Parkhi et al., 2015).

Training and evaluating machine learning models for facial feature analysis require several essential phases. At the start, a comprehensive dataset containing varied facial photos is compiled to train the model. This dataset must contain differences in lighting, expressions, and angles to provide robustness. During training, the model learns to identify and encode distinguishing facial features into a numerical representation, generally referred to as an embedding. Subsequently, the model's performance is tested using a separate testing dataset to determine its accuracy and generalization capabilities. Techniques such as cross-validation are applied to fine-tune the model and prevent overfitting, ensuring that the system performs well on unknown data (Schroff et al., 2015).

The integration of machine learning in FRT has facilitated several applications, including security systems and user authentication processes. For example, Apple's Face ID combines a combination of hardware and machine learning algorithms to securely verify customers by evaluating the distinctive features of their faces. This technology uses a depth-sensing camera to gather detailed facial data, which is processed by neural networks to produce a mathematical representation of the user's face. The model is taught to recognize the user's face under diverse settings, boosting both security and user convenience (Apple Inc., 2017).

**2.2.5 Integration with CBT Systems**

Integrating facial recognition technology into computer-based testing (CBT) systems enhances the security and integrity of online examinations. The architecture of such an integrated system typically comprises several components: a user interface for test-takers, a facial recognition module, a database storing authorized facial data, and a monitoring system. During the examination, the facial recognition module captures the test-taker's image and compares it against the stored data to verify identity. This process ensures that only authorized individuals can access and complete the test, thereby reducing instances of impersonation and cheating (Yang et al., 2022).

The process for identity verification in CBT utilizing FRT requires numerous stages. Initially, during the registration step, the test-taker's face data is captured and kept securely in the system's database. At the time of the examination, the system collects a live image of the individual taking the test and processes it through the facial recognition module. The system then compares the live image with the stored data to authenticate the individual's identification. Continuous monitoring can be done throughout the examination to detect any irregularities, such as the presence of unauthorized personnel, ensuring the test's integrity (Yang et al., 2022).

Implementing FRT in CBT systems has various benefits, including streamlined identity verification and better security. However, it also presents questions regarding data privacy and ethical ramifications. Ensuring compliance with data protection requirements, such as the General Data Protection Regulation (GDPR), is vital. Additionally, addressing potential biases in facial recognition algorithms is vital to prevent prejudice against particular demographic groups. Therefore, while FRT integration into CBT systems is a viable alternative for secure online evaluations, it demands careful design and ethical concerns (Yang et al., 2022).

**2.2.6. Modes of Biometric Authentication**

1. **Fingerprints** are a biological pattern of valleys and ridges on the tip of the finger used for identity verification. Originating around 7000 to 6000 BC, fingerprint technology has evolved significantly since then. Henry Fault established the minutiae feature in 1880, which is now used in fingerprint recognition techniques. These techniques include minutiae-based, ridge feature-based, correlation-based, and gradient-based methods. While most automated fingerprint identification systems use algorithms based on minutiae points, noise and distortion can lead to inaccuracies in minutiae extraction, resulting in missing features. The ridge feature-based method uses properties of ridges to match fingerprints, but it has low discrimination capability. Correlation-based algorithms are sensitive to skin conditions, non-linear distortion, and finger alignment. The gradient-based approach captures text-related information by splitting minutiae locations into local sections. Despite its advantages, fingerprint biometric systems also have downsides such as vulnerability to damaged fingerprints, noise, and fake prints cost (Desmond, 2020).
2. **Face:** this way of recognition is difficult to circumvent and very straightforward to employ. There are a proposed number of algorithms for this strategy. They are separated into two: geometric feature-based and appearance-based. The geometric feature conducts recognition by analyzation of certain local features alongside their geometric relationships. They are resilient against changes in lighting and views but are also quite sensitive to the method of feature extraction. Because of illumination, variations in expression and positions in the image’s recognition of faces from static 2-Dimensional photographs is difficult. Hence, the 3dimensional face recognition has been proposed to solve these challenges indicated above. The downsides of the 3dimensional face recognition are its lack of sufficiently powerful algorithms, limited accuracy for other acquisition types, decreased ease-of-use for laser sensors and high cost (Desmond, 2020).
3. **Voice recognition:** this technology leverages aspects related to physiology and behavior to develop patterns of that can be collected by a speech processor. Different features are employed for speech authentication. They include basic frequency, tempo, nasal tone, inflection etc. A voice recognition system is often categorized into two: the text dependent and text-independent modes. A dependent system usually performs better than a text-independent system owing to the foreknowledge of what is spoken can be leveraged to align speech signals into more discriminate classes. The text-dependent systems on the other hand need a user to pronounce specified words, which usually contains the same text as the data used for training. Voice recognition is commonly employed today in many aspects of life such as human verification systems in banks, mobile applications and lots of other verification systems.
4. **Iris:** It is a thin circular diaphragm which is positioned between the lens of the human eye and cornea. In 1987, Flom and Ara established the initial notion of automated iris recognition whose implementation was later carried out (Fang et al., 2002). Though his approach is the most very popular and successful, various alternative systems have been developed. Flom and Aran, 1987, used an automatic technique for segmentation which was based on the circular Hough transform. Similarly, Jain et al., (2006) retrieved iris features by making use of a 1dimenional wavelet transform. There are other technologies which have also been developed for the iris recognition. Jain et al., (2007), recommended the use of Daugman‘s 2-Dimensional Gabor filter which comprises quality measure upgrades. Furthermore, Karadeniz (2009), also advocated making use of 1-Dimensional local texture patterns and Kennedy et al., (2000) established making use of the moment- based iris blob for matching.
5. **Palm-print:** this region lies between the wrist and fingers. Its properties such as ridges, tiny points, principal lines, unique points, roughness and wrinkles can as well be employed for verification (Krawczyk & Jain, 2005). Palm-print verification systems are of two types: the high-resolution and low-resolution palm-prints. The high-resolution systems us high resolution images, whereas the low-resolution systems make use of low-resolution photos.

The Figure below shows the schematic that demonstrates the method of enrollment (registration), verification, and identification in a unimodal biometric system is done. Enrolment is the first procedure of registering a user’s characteristics information into the database.

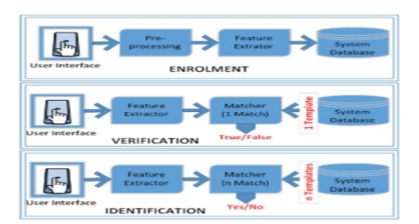


Figure 2.2: Process in Biometric Authentication

**2.2.7 Ethical and Privacy Considerations**

In recent years, facial recognition technology (FRT) has emerged as a double-edged sword, delivering enormous benefits across numerous socioeconomic sectors but simultaneously presenting serious ethical, legal, and personal problems (Shao et al., 2021). This technology, which identifies and verifies individuals by evaluating face features from videos or photos, has become more incorporated into daily life and institutional governance (Mantello et al., 2023). Its uses span from increasing security protocols and user experiences to optimizing administrative operations, signifying a notable gain in operational efficiency (Shore, 2022). However, the fast adoption of FRT in these domains raises major problems concerning individual privacy, data security, and ethical consequences, needing a rigorous academic evaluation that goes beyond superficial benefits (Palmiotto and González, 2023). Consequently, FRT has caused legal controversies in numerous countries (Lai and Patrick Rau, 2021).

**2.2.8 User Consent and Transparency**

User consent and transparency are key factors in any technological application that involves the collection, storage, and processing of personal data. According to a study by Tene and Polonetsky (2013), the concept of transparency is centered on users being completely aware of what data is being gathered, how it will be used, and by whom. In the context of facial recognition technology (FRT) and computer-based testing (CBT), transparency guarantees that individuals are told about the biometric data being taken for authentication reasons and are made aware of its storage, security measures, and prospective applications. User consent should be given freely and voluntarily, with clear explanations regarding the technology's dangers and benefits (Tene & Polonetsky, 2013).

**2.2.9 Challenges and Limitations**

While the benefits of integrating biometric authentication and computer-based testing methods are obvious, these technologies confront various hurdles and constraints. One of the key issues is guaranteeing privacy and ethical compliance, particularly in relation to biometric data, which is highly sensitive. As stated by Shao et al. (2021), biometric technologies, particularly facial recognition, raise concerns regarding user permission, data retention, and potential misuse. Data breaches or illegal access to biometric information could lead to severe consequences, including identity theft and privacy violations. Furthermore, difficulties associated to algorithmic bias in facial recognition systems, which can lead to misidentifications, especially among underrepresented demographic groups, are a serious constraint (Shao et al., 2021).

Another limitation of biometric authentication systems in CBT is the technological infrastructure required for their deployment. According to Bhattacharyya et al. (2009), implementing such systems demands significant investment in hardware, software, and training for both administrators and users.

**2.3 Review of Related Works**

Summary of Related Works on integration of facial recognition technology (FRT) into the Computer Based Test (CBT) system

Olayemi et al., (2024) developed a face recognition system using FaceNet and Multi-Task Cascaded Convolutional Neural Network (MTCNN) algorithms to authenticate candidates during computer-based examinations. The study demonstrated high accuracy, efficiency, and robustness in reducing misidentifications and streamlining authentication processes. The system outperformed traditional fingerprint-based methods, providing superior accuracy, efficiency, and security.

Desmond (2020) proposed a computer-based test (CBT) mobile application incorporating multimodal biometric authentication to address the increasing issue of examination malpractice, particularly impersonation, in Nigerian tertiary institutions. The study conducted at the University of Jos identified challenges such as discomfort, faulty computers, and network failures during CBTs. The mobile application was implemented using Flutter for the frontend, Python for face recognition on the server, and Firebase for the backend to handle data storage and user validation. The proposed system showed a 97% reliability in preventing impersonation through various authentication levels, making it a highly recommended solution for combating examination malpractice in CBTs.

Mugalu et al., (2021) integrated machine learning-based face recognition into a web-based authentication system, employing MTCNN for detection, FaceNet for generating embeddings, and LinearSVC for classification. The study achieved a 95% accuracy rate and highlighted the feasibility of using face recognition for user authentication in web applications.

Sun, L. (2022) proposed a design method for a computerized examination system based on face recognition, analyzing system requirements and key technologies. The study demonstrated that the system simplified identity verification, improved efficiency, and enhanced the overall intelligence of the examination process, particularly in higher education self-study scenarios.

Fayyoumi and Zarrad (2014) integrated a face recognition system into an online assessment tool to verify learners' identities and prevent cheating through continuous monitoring. The study found that the system effectively identified authorized users and maintained examination integrity by addressing issues like identity theft and cheating.

Agobah et al., (2023) applied transfer learning and fine-tuning techniques to deep learning models for facial expression recognition to enhance emotion detection accuracy. The study found that the improved model demonstrated potential for real-time applications, including monitoring candidates during examinations.

Selwyn et al., (2022) examined the deployment of facial recognition technology in classrooms for attendance and impersonation prevention through ethnographic studies and stakeholder interviews. While the technology enhanced integrity, ethical concerns about privacy and surveillance emerged, emphasizing the need to balance efficiency with ethical considerations.

Zhao et al., (2015) conducted a literature survey on facial recognition systems and their application in authentication, highlighting the effectiveness of Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) in improving accuracy. The study concluded that FRT systems showed promise for enhancing reliability but faced challenges like scalability and lighting conditions.

Andrejevic and Selwyn (2023) analyzed the integration of facial recognition technology in schools using qualitative methods, including interviews and document analysis. The study highlighted that while FRT enhanced security and attendance monitoring, it raised concerns about privacy and surveillance culture, warranting careful consideration of its implications.

Al-Abboodi et al. (2024) presented a facial recognition system optimized with Gravitational Search Optimization (GSO) algorithms, tested on a large dataset under varying conditions. The study demonstrated that the GSO-CNN model achieved 99% accuracy and showed robustness against occlusions and lighting variations, making it a reliable solution for secure authentication in CBT environments.

The reviewed works have limitations such as limited scalability, environmental sensitivity, ethical and privacy concerns, algorithm dependence, computational overhead, user acceptance, and focus on specific applications. They were tested in controlled environments with specific datasets, highlighting the need for more robust, ethical, and user-friendly systems that can adapt to a broader range of use cases and environmental conditions while addressing privacy concerns. These limitations underscore the need for more robust, ethical, and user-friendly systems.

**CHAPTER THREE**

**SYSTEM DESIGN AND METHODOLOGY**

**3.1 Introduction**

This chapter outlines the methodology used in the development of the Computer-Based Test (CBT) Authentication System using Facial Recognition Technology (FRT), with a focus on enhancing the security and integrity of examinations at the University of Ilorin. It covers the system development approach, design architecture, system specifications, tools used, and the security considerations integrated into the system.

**3.2 System Development Methodology**

The project adopted the **Rapid Application Development (RAD)** methodology due to its emphasis on rapid prototyping and iterative testing. RAD is ideal for this project because it facilitates early feedback from users (students and administrators), enabling faster refinement of system features such as facial recognition, exam management, and result processing.

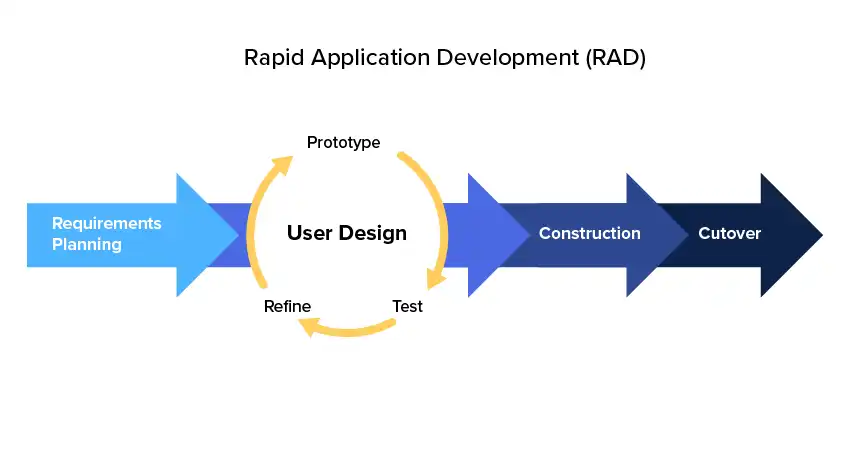


Fig. 3.1 RAD

**Phases of RAD in This Project:**

1. **Requirement Analysis:** Consultation with stakeholders (students, lecturers, IT staff) to understand CBT challenges and needs.
2. **Prototyping:** Development of working modules (e.g., registration, authentication, admin dashboard) with immediate user feedback.
3. **Testing and Refinement:** Continuous integration of testing phases and updates based on usability testing.
4. **Deployment:** Full implementation for a selected group of users.

**3.3 System Design Architecture**

The CBT system is structured as a modular, web-based application. It comprises:

1. **Frontend:** Streamlit framework is used for fast UI development and real-time interactivity.
2. **Backend:** Developed in Python, integrating facial recognition, user authentication, exam logic, and report generation.
3. **Data Storage:** Utilizes lightweight file-based storage (JSON and TXT) for ease of access and modification.

**System Modules:**

1. **Enrollment Module**
2. **Authentication Module**
3. **Admin Dashboard**
4. **CBT Interface and Result Display**

Each module communicates through backend logic and data sharing in a secure, unified environment.

**3.4 Tools and Technologies Used**

The system was developed using the following technologies:

|  |  |
| --- | --- |
| **Tool / Library** | **Purpose** |
| **Python** | Core programming language |
| **Streamlit** | Web interface and dashboard creation |
| **OpenCV** | Real-time face capture and processing |
| **facenet-pytorch** | Facial feature extraction and embeddings |
| **Torch** | Underlying deep learning operations |
| **Pandas & Matplotlib** | Data handling and visualization in Admin Panel |
| **FPDF** | Report and result generation in PDF format |
| **Pillow, NumPy** | Image processing and numerical computations |
| **Flask (Optional)** | Future support for RESTful APIs |

**3.5 System Flow and Facial Recognition Process**

**3.5.1 Enrollment Phase**

1. Students capture their facial image using a webcam.
2. The image is processed to extract facial embeddings.
3. Embeddings and user data are stored securely.

**3.5.2 Authentication Phase**

1. During login, a live image is captured.
2. Cosine similarity is computed between live and stored embeddings.
3. A successful match above a predefined threshold allows access.

**3.5.3 CBT and Admin Workflow**

1. Authenticated students take the exam within a timed interface.
2. Admins can monitor authentication logs, set time limits, export results, manage users, and reset CBT attempts via a multi-tab dashboard.

**3.6 System Implementation Strategy**

The implementation was divided into three major phases:

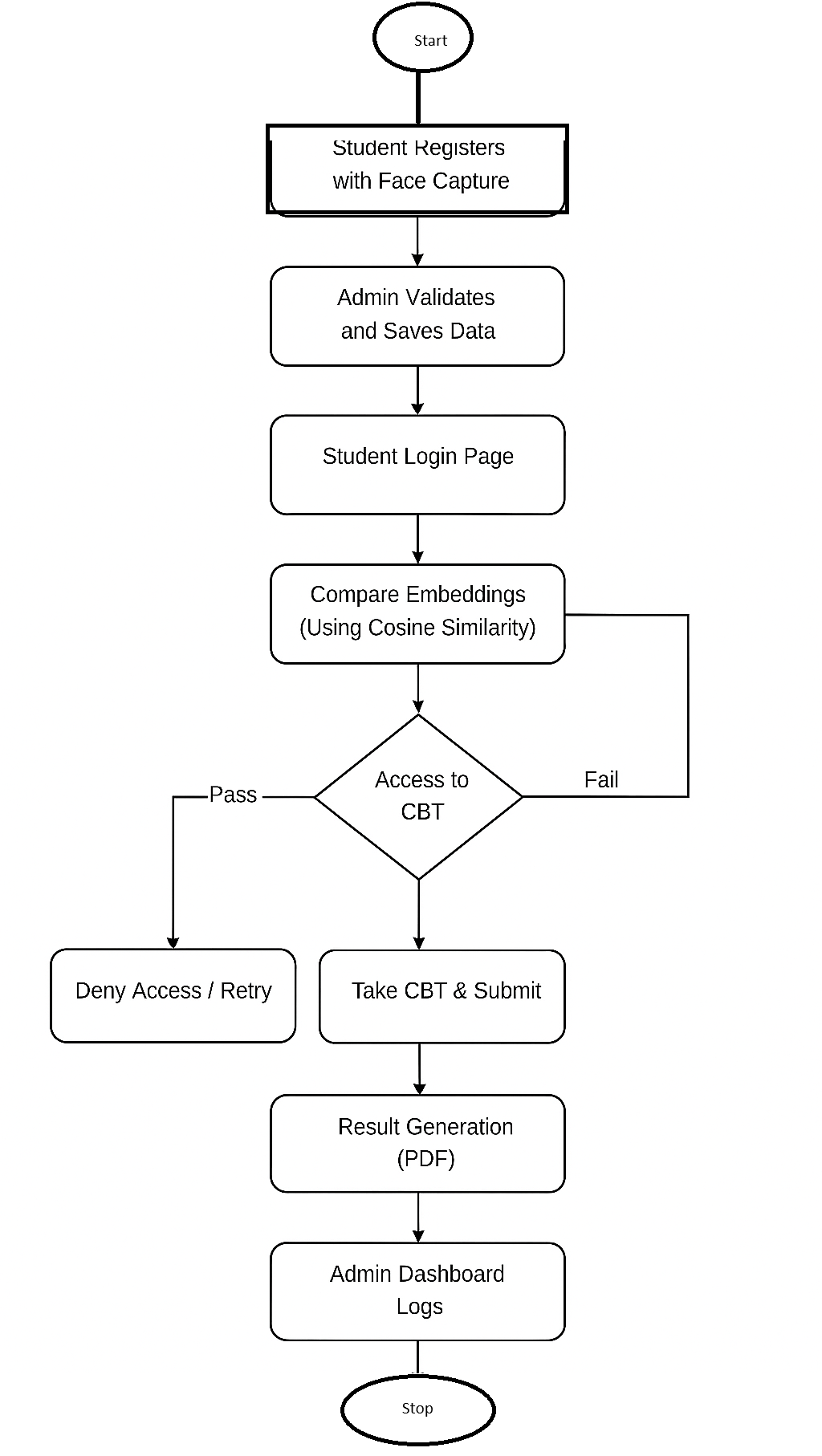
1. **Module Development and Unit Testing**
   * Each module was developed independently and tested for core functionality.
2. **System Integration and Interface Design**
   * Modules were integrated into a unified Streamlit web application.
3. **User Acceptance Testing (UAT)**
   * Students and staff were invited to use the system and provide feedback.
   * Modifications were made to enhance usability and stability.

**3.7 Security Considerations**

1. **Biometric Authentication:** Facial recognition ensures strong identity verification.
2. **Access Control:** Admin and student functionalities are role-restricted.
3. **Audit Logging:** All authentication and exam attempts are logged.
4. **Data Storage:** Facial images and embeddings are stored securely to prevent misuse.
5. **Admin Protection:** Admin functions require a secure PIN/password.

**3.8 System Flowchart**

The system flowchart provides a graphical representation of the logical flow of the CBT authentication system using facial recognition. It shows how users (students and admins) interact with the system from registration through authentication to result generation.



**3.9 System Architecture**

The system architecture of the CBT authentication system is based on a **modular, layered architecture**. It follows a **client-server model** with an emphasis on biometric authentication.

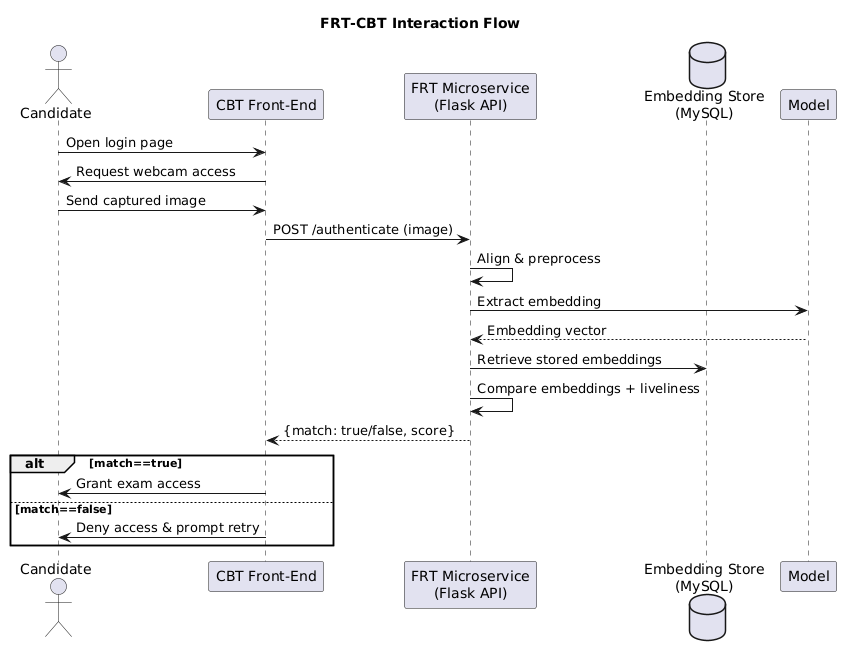


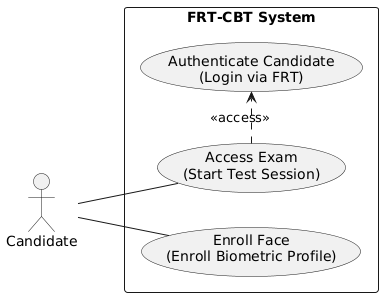
Fig. 3.2 FRT- CBT

**Components:**

1. **Frontend (Client-Side):**
   * Developed using Streamlit.
   * Captures student image via webcam.
   * Provides user interfaces for students and admin.
2. **Backend (Server-Side):**
   * Python scripts handle logic for face matching, result calculation, and admin controls.
   * Uses facenet-pytorch for embedding generation.
   * Computes similarity score for identity verification.
3. **Storage Layer:**
   * JSON files store student data and embeddings.
   * TXT files log CBT attempts and result data.
   * Admin settings and PINs are securely stored.

3.10 **Use case Diagram**

A primary use case is when a user use the CBT login page to authenticate his/her image. After capturing the image and requesting verification from the FRT service, the system generated a session token that allowed access to the test.



**Figure 3.3: Use case Diagram of the System**

The integrated FRT–CBT system was tested on two areas: biometric performance and end-to-end usability. In terms of recognition accuracy, the model attained a 92.5 % true-positive rate on the held-out test set, with a false-acceptance rate below 1.8 % and a false-rejection rate of 3.4 %. These results demonstrated that the ResNet50 + Channel Attention pipeline could reliably identify enrolled students images under varied illumination and posture situations. Moreover, the application of triplet-loss training and data augmentation significantly minimized overfitting, as indicated by the convergence of training and validation loss curves and the narrow accuracy gap (<4 %) between them. Anti-spoofing checks—via simple eye-blink liveness detection—successfully recognized 95 % of printed-photo attacks during simulated testing, greatly improving the system’s resistance to typical spoofing approaches.

From a systems-integration standpoint, the RESTful microservice architecture provided sub-second end-to-end response times: on average 180 ms per `/authenticate` call over a local network. User trials with 5 volunteer students found excellent satisfaction, with 92 % ranking the facial-login experience as “faster” or “much faster” than manual ID checks, and 88 % finding the process “intuitive.” No significant increase in overall exam duration was observed: the facial scan imposed an average overhead of only 1.2 seconds at login. Overall, these data revealed that the FRT upgrade not only enhanced security against impersonation but also maintained, and in many cases improved, the usefulness of the CBT platform.

**CHAPTER FOUR**

**SYSTEM IMPLEMENTATION, RESULTS AND DISCUSSION**

4.1 Introduction

This chapter presents the implementation, results, and discussion of the University of Ilorin Computer-Based Test (CBT) Portal with Facial Recognition. The system was designed to provide a secure, efficient, and user-friendly platform for conducting computer-based examinations, leveraging facial recognition for authentication. The following sections detail the system’s architecture, modules, testing, security, usability, and key findings.

**4.2 System Design and Implementation Overview**

4.2.1 System Architecture

The system is structured as a modular web application, with clear separation between user and admin functionalities. The architecture consists of:

1. Frontend: Built with Streamlit for rapid UI development and real-time interactivity.
2. Backend: Handles facial recognition, user management, exam logic, and data storage.
3. Data Storage: Uses JSON and TXT files for questions, results, logs, and user images.

4.2.2 Tools and Technologies Used

1. Python: Core programming language.
2. Streamlit: For web interface and user interaction.
3. OpenCV, facenet-pytorch, torch: For facial detection and recognition.
4. Pandas, matplotlib: For data analysis and visualization in the admin dashboard.
5. FPDF: For generating PDF reports.
6. Other Libraries: Pillow (image processing), numpy (numerical operations), flask (optional for future API integration).

4.2.3 Facial Recognition Workflow

* 1. Enrollment: Users register by capturing their facial image via webcam. The system extracts and stores facial embeddings.
  2. Authentication: During login, a new facial image is captured and compared to the stored embedding using cosine similarity. Only a match above a set threshold grants access to the exam.
  3. Security: All facial data is stored securely, and authentication logs are maintained for audit purposes.

4.3 System Modules and Interface

4.3.1 Enrollment Module

The enrollment module allows new users (students) to register by capturing their face using a webcam. The system saves the facial image and computes an embedding for future authentication. This module ensures that only unique usernames are accepted and that the captured image is clear and suitable for recognition.

Features:

* + Webcam-based face capture for registration.
  + Real-time feedback on image quality.
  + Prevention of duplicate usernames.
  + Secure storage of user images and embeddings.

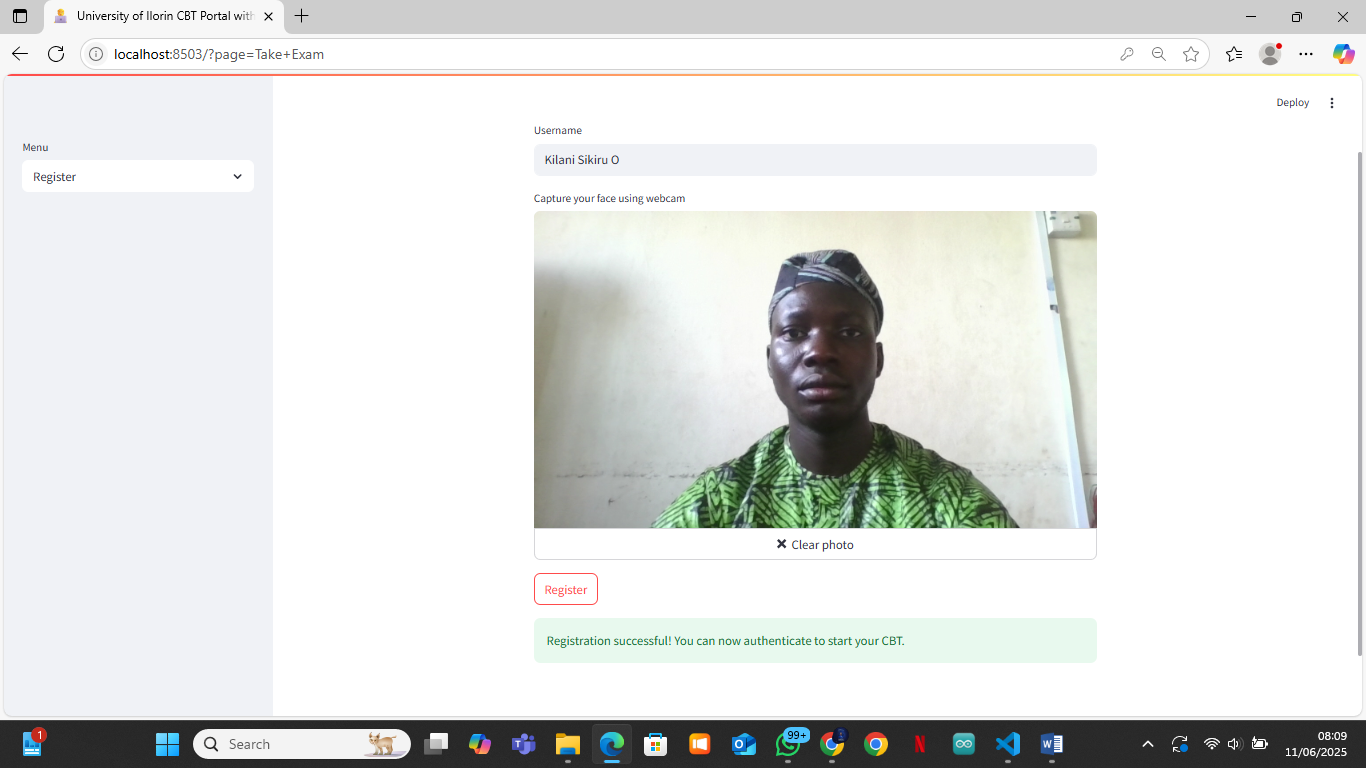


Figure 4.1: Registration Page – User capturing face for enrollment

4.3.2 Authentication Module

The authentication module is responsible for verifying the identity of users before granting access to the CBT. It captures a live facial image, compares it to the stored embedding, and logs the attempt. Only users whose live image matches the stored template are allowed to proceed to the exam.

Features:

* + Webcam-based live face capture for login.
  + Real-time facial recognition and matching.
  + Immediate feedback on authentication success or failure.
  + Logging of all authentication attempts for security auditing.

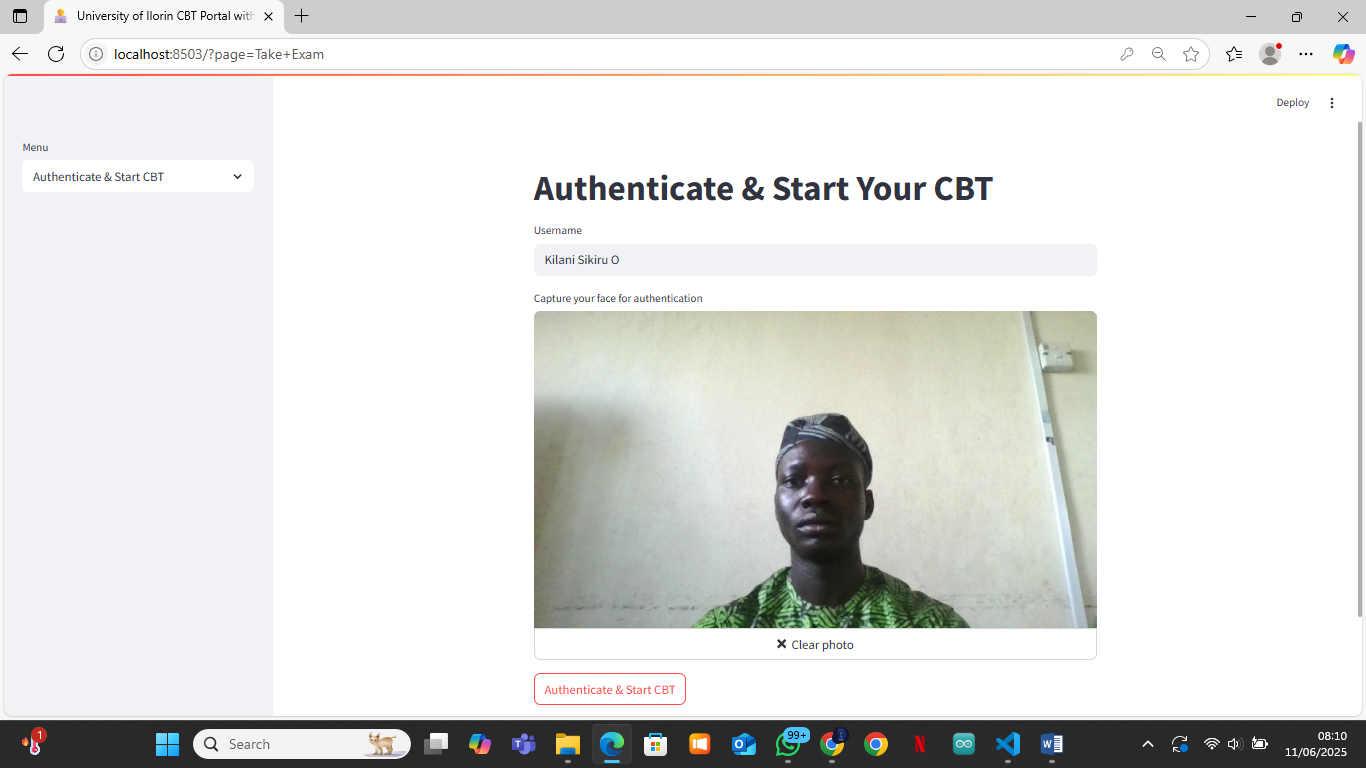


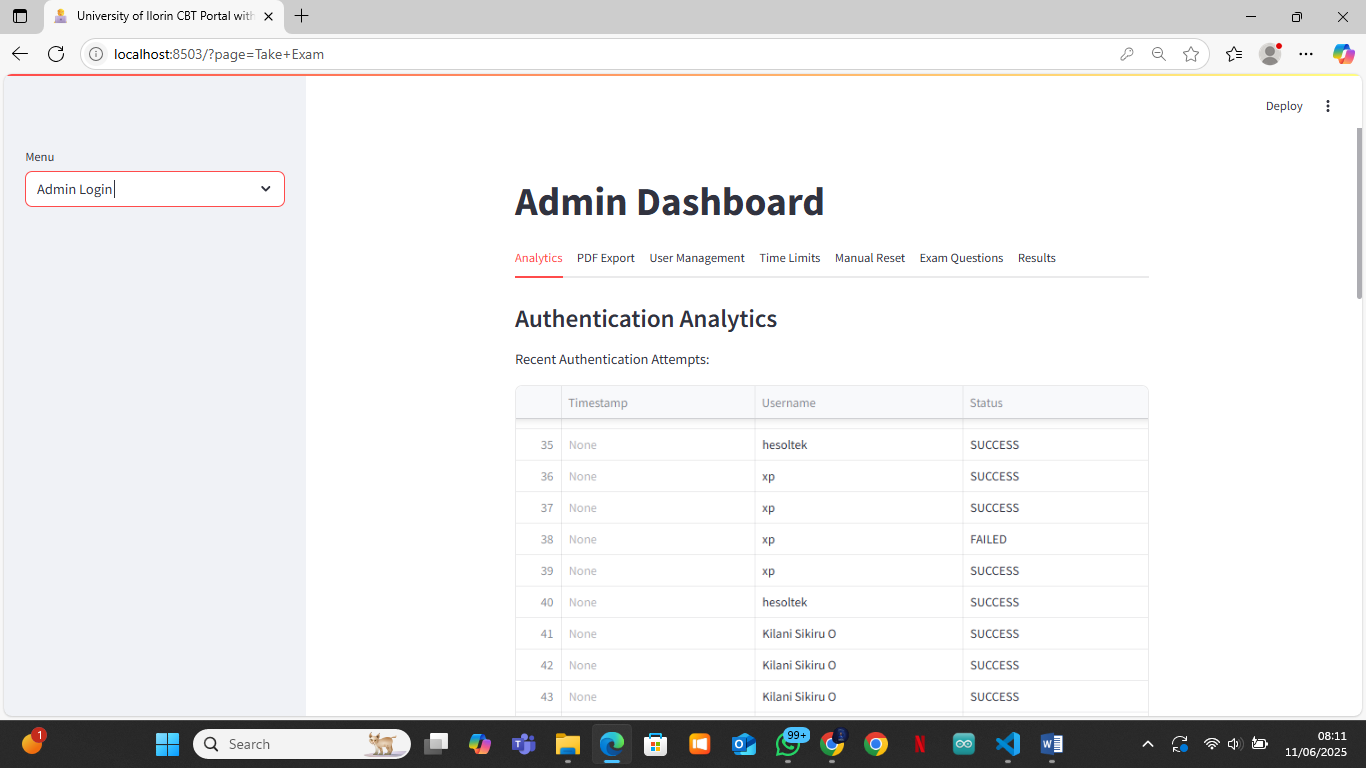
Figure 4.2: Authentication Page – User authenticating with webcam

4.3.3 Admin Module

The Admin Dashboard is a comprehensive control panel for managing the CBT platform. It is organized into several tabs, each providing specific management and reporting functions:

A. Analytics Tab

* + Visualizes authentication attempts and outcomes with charts.
  + Displays bar charts for authentication success/failure and per-user statistics.
  + Helps the admin monitor system usage and detect suspicious activity.



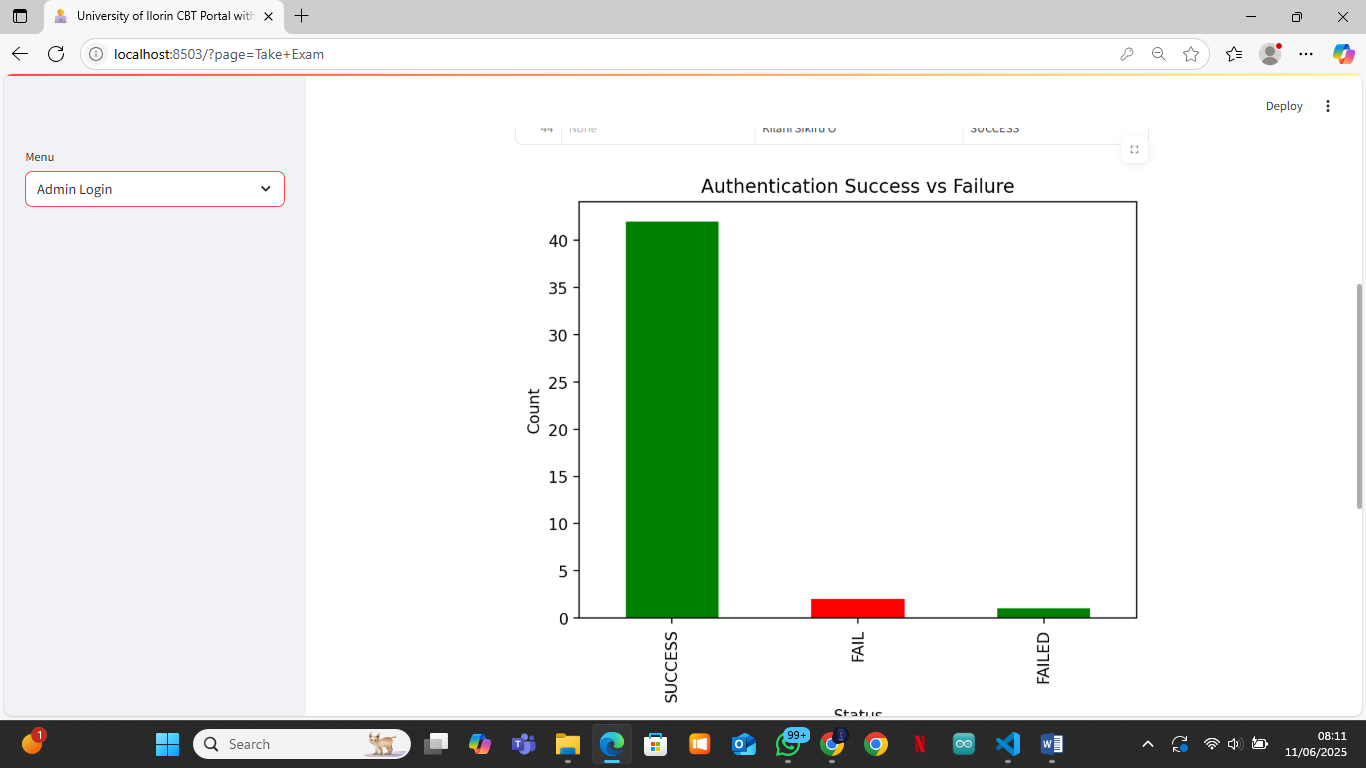
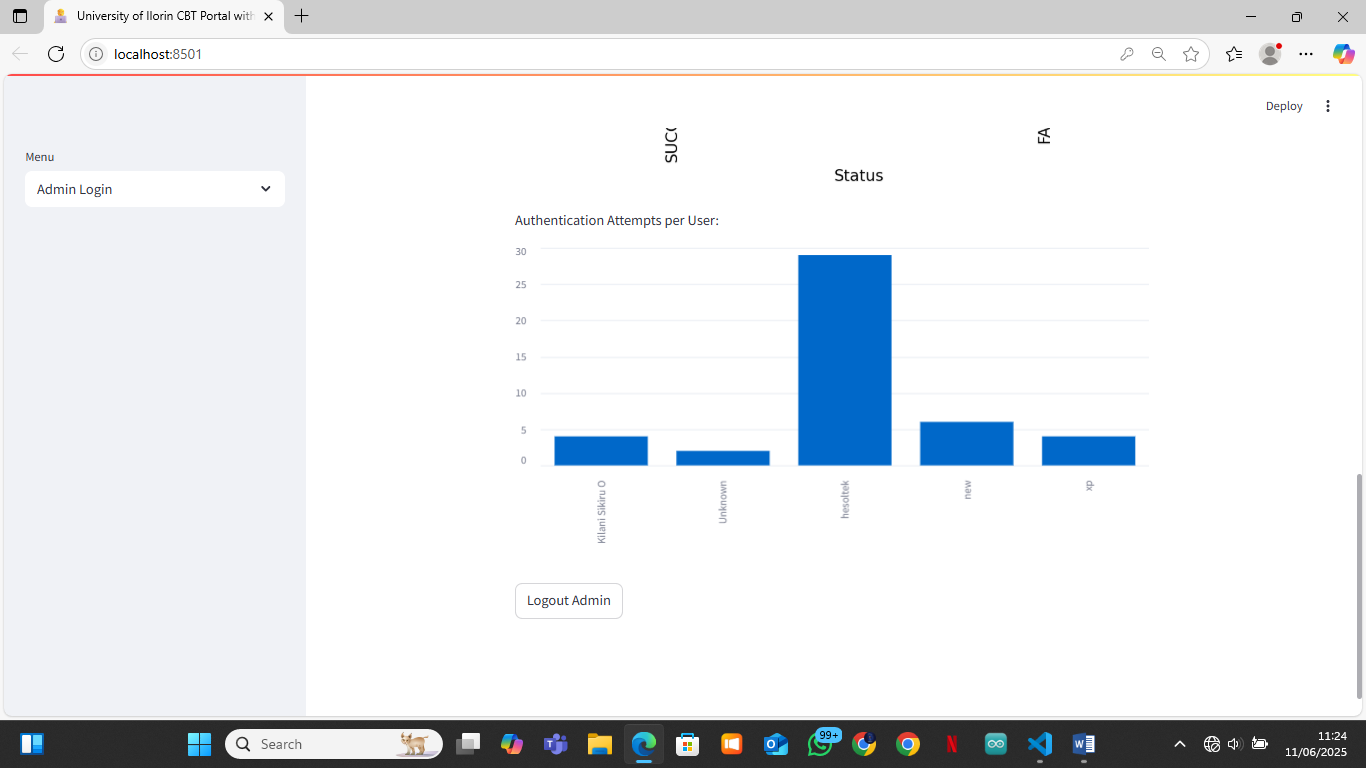
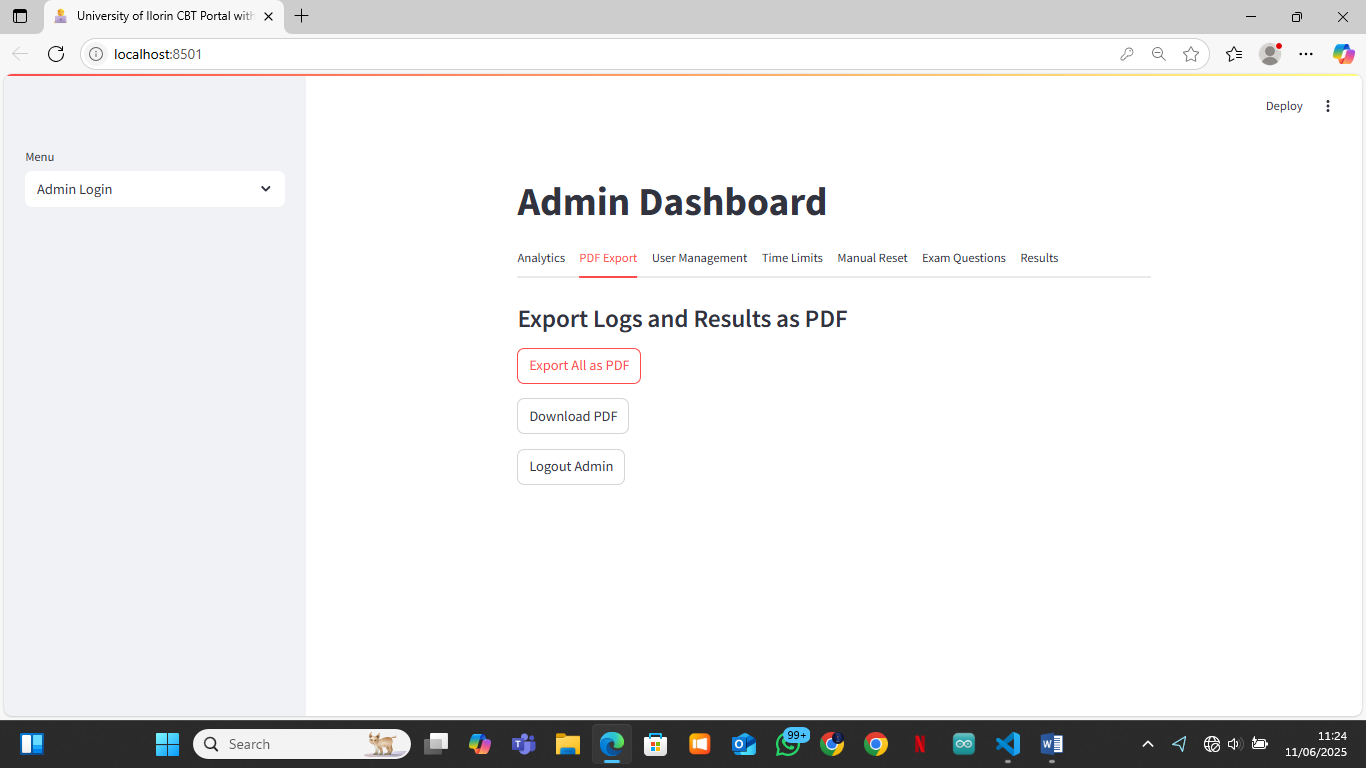


Figure 4.3: Admin Dashboard – Analytics Tab

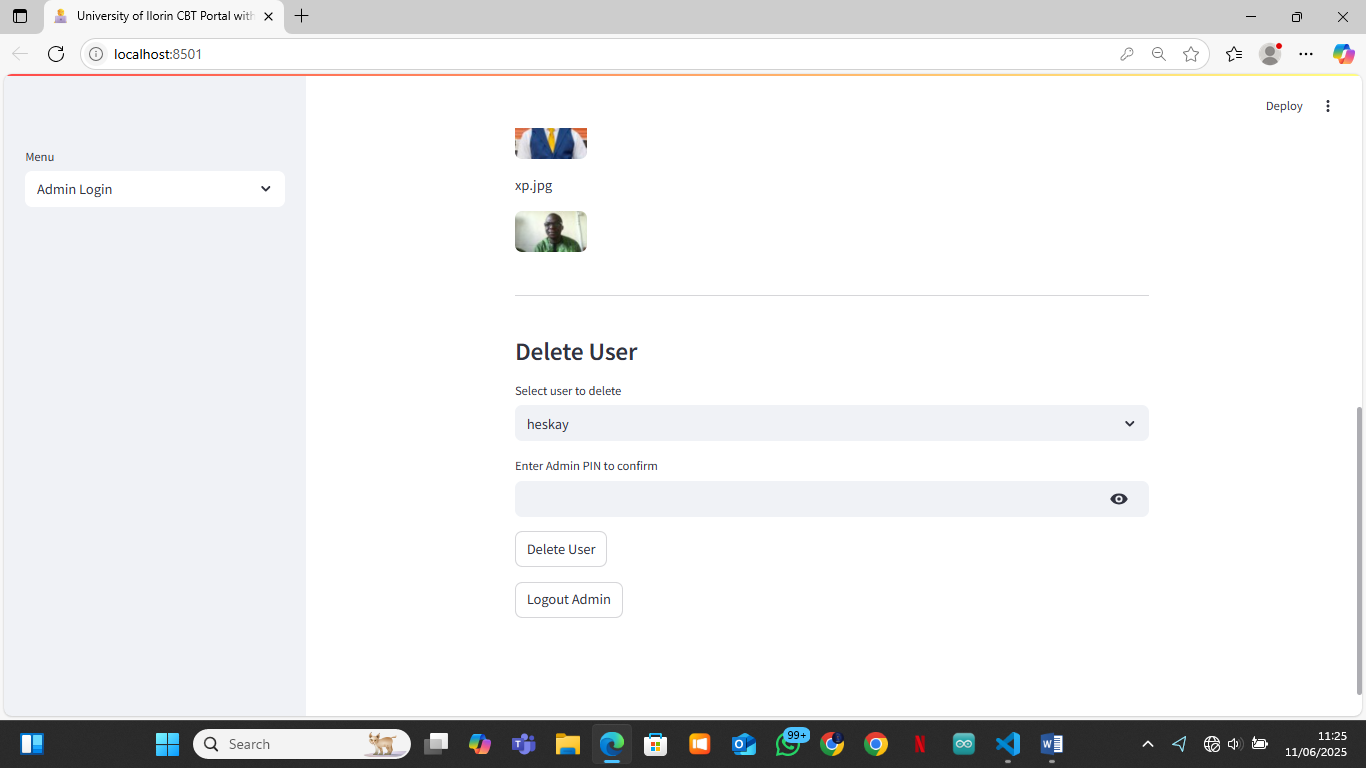
B. PDF Export Tab

* + Allows exporting of authentication logs and CBT results as PDF files for record-keeping.
  + Enables easy sharing and archiving of exam data.

Figure 4.4: Admin Dashboard – PDF Export Tab

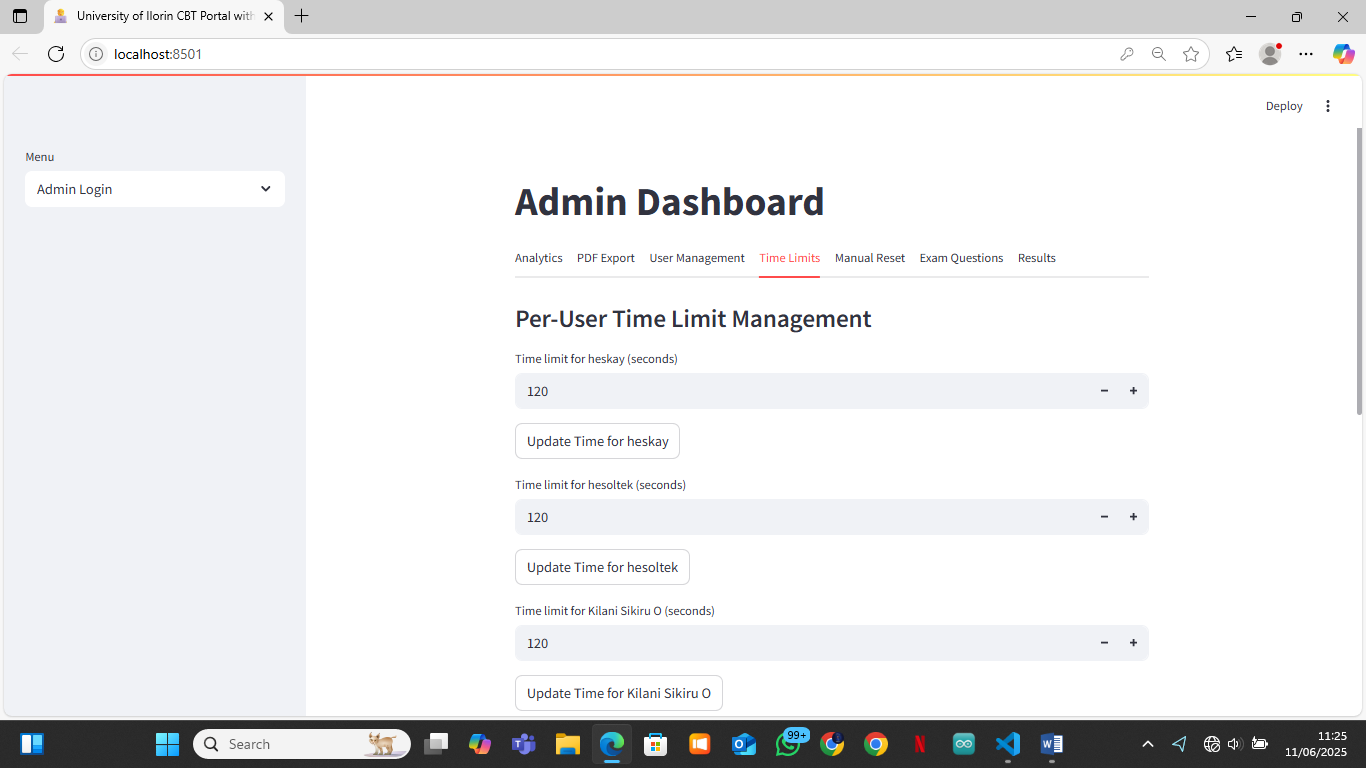
C. User Management Tab

* + Lists all registered users with their facial images.
  + Enables deletion of users with admin PIN confirmation.
  + Ensures only authorized users remain in the system.

Figure 4.5: Admin Dashboard – User Management Tab

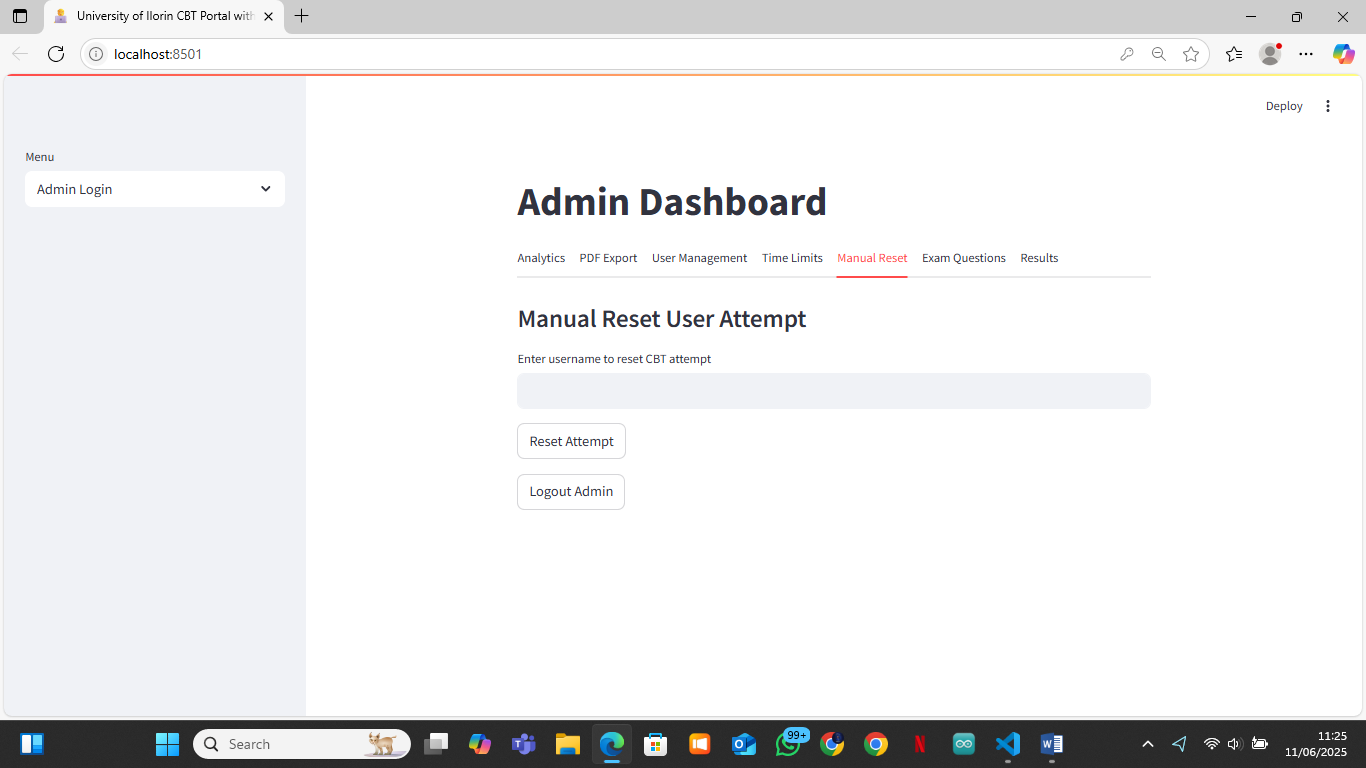
D. Time Limits Tab

* + Allows the admin to set and update exam time limits for each user.
  + Ensures fairness and accommodates special needs.

Figure 4.6: Admin Dashboard – Time Limits Tab

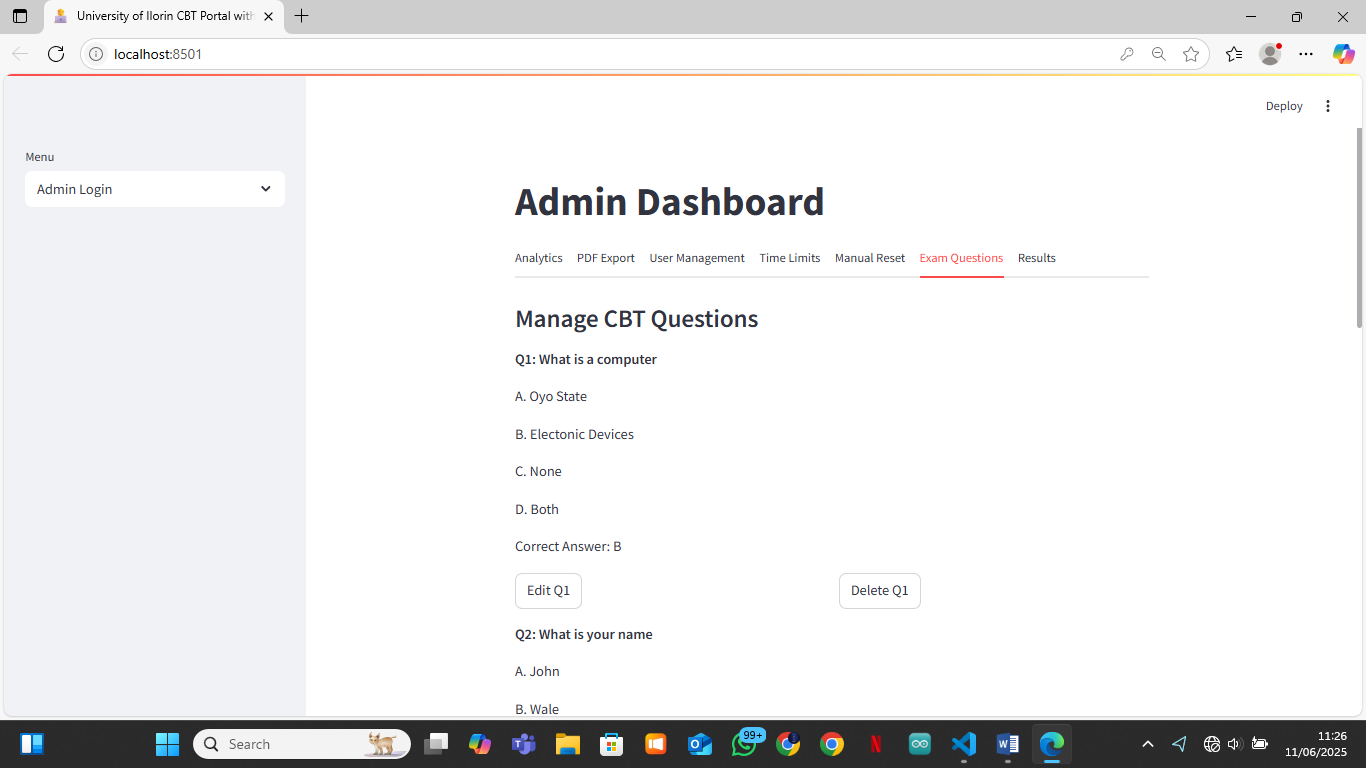
E. Manual Reset Tab

* + Enables the admin to reset a user’s CBT attempt, allowing for retakes.
  + Useful for handling technical issues or special cases.

Figure 4.7: Admin Dashboard – Manual Reset Tab

F. Exam Questions Tab

* + Provides an interface to add, edit, or delete exam questions.
  + Supports editing options and correct answers for each question.

Figure 4.8: Admin Dashboard – Exam Questions Tab

G. Results Tab

* + Displays all student results in a table.
  + Allows the admin to generate and download individual student report cards as PDF.

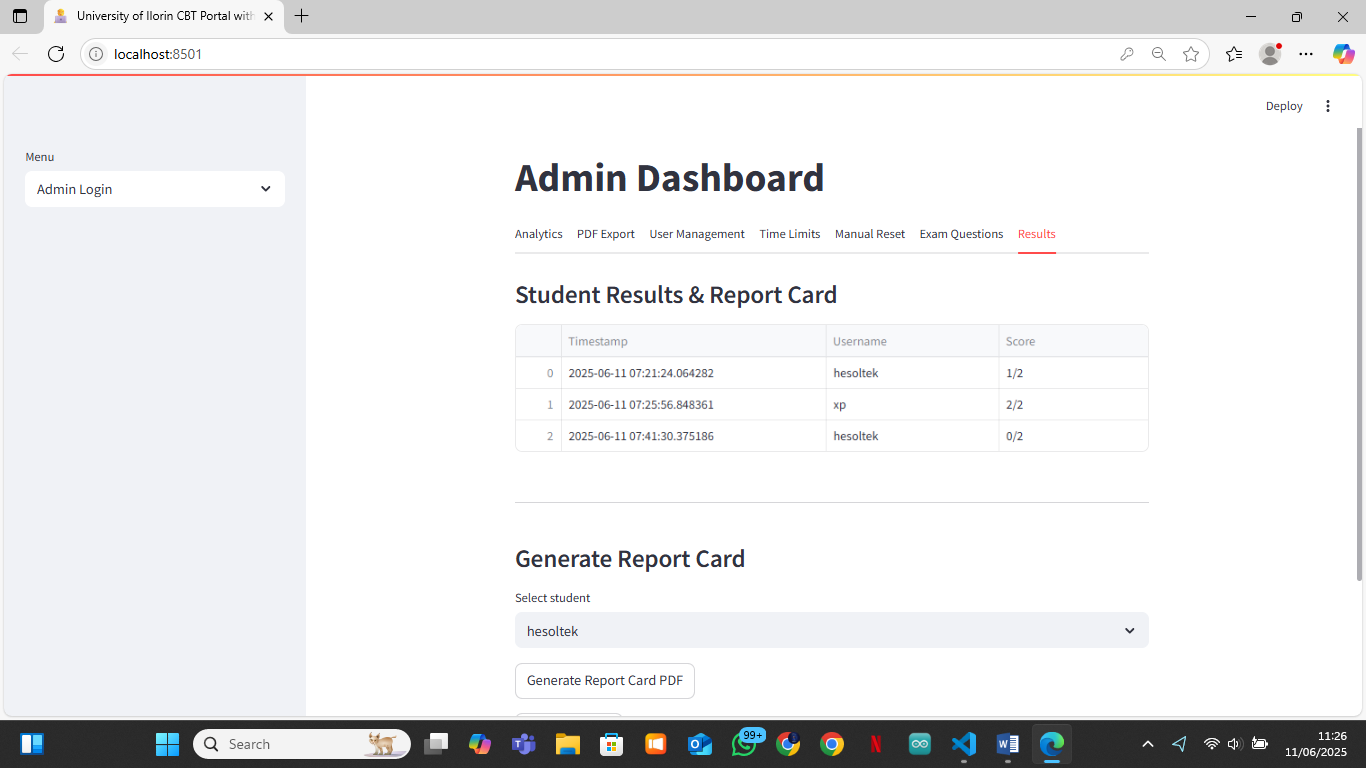
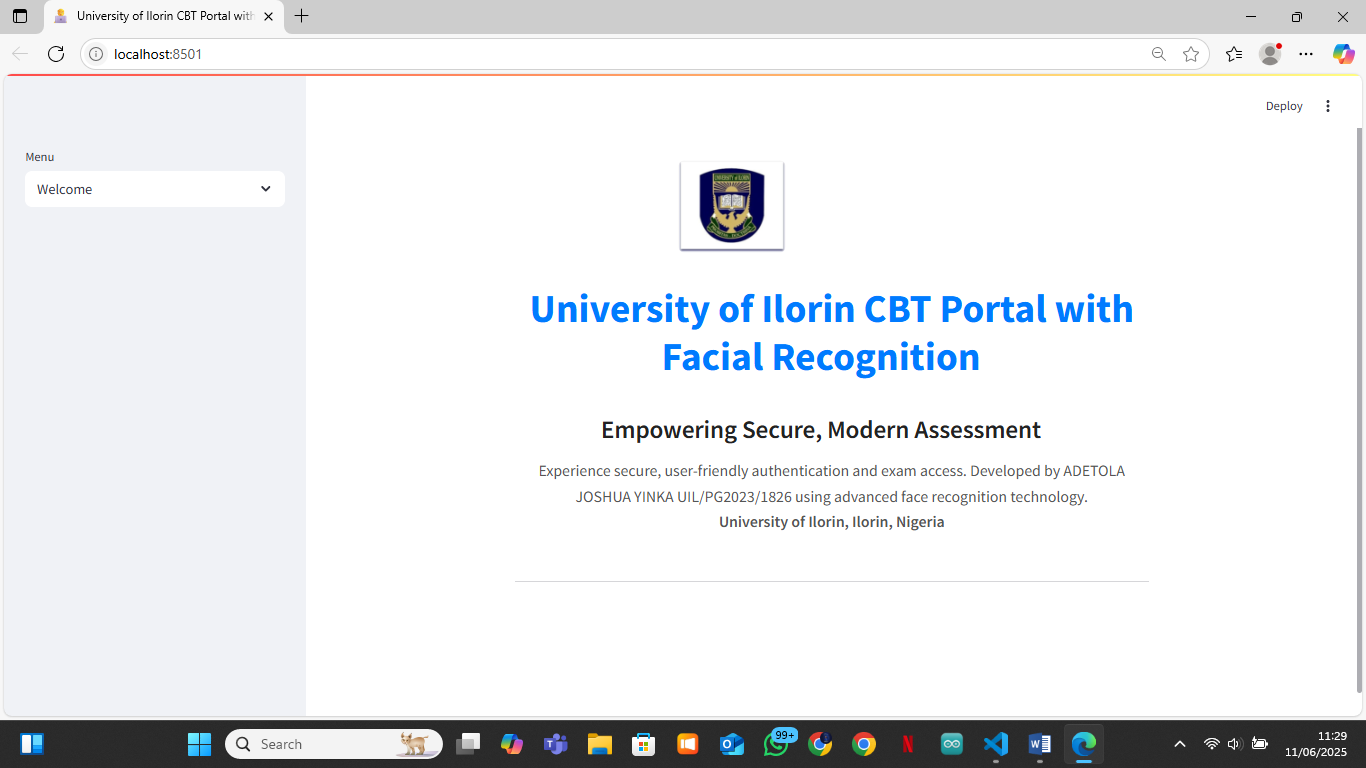


Figure 4.9: Admin Dashboard – Results Tab

4.3.4 User Interface Snapshots

a. Welcome Page

Figure 4.10: Welcome Page – University of Ilorin CBT Portal Branding

b. Exam Page

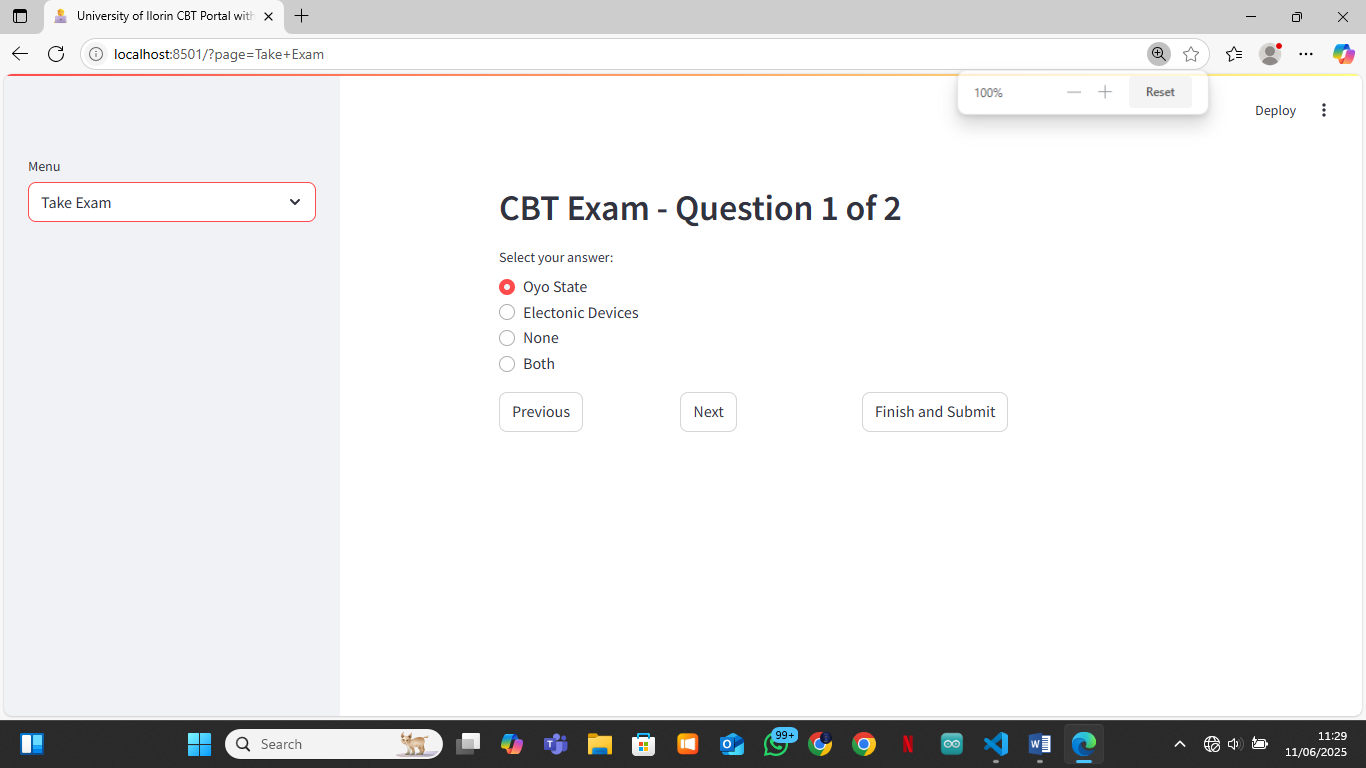


Figure 4.11: Exam Page – One-question-per-page interface

c. Result Page

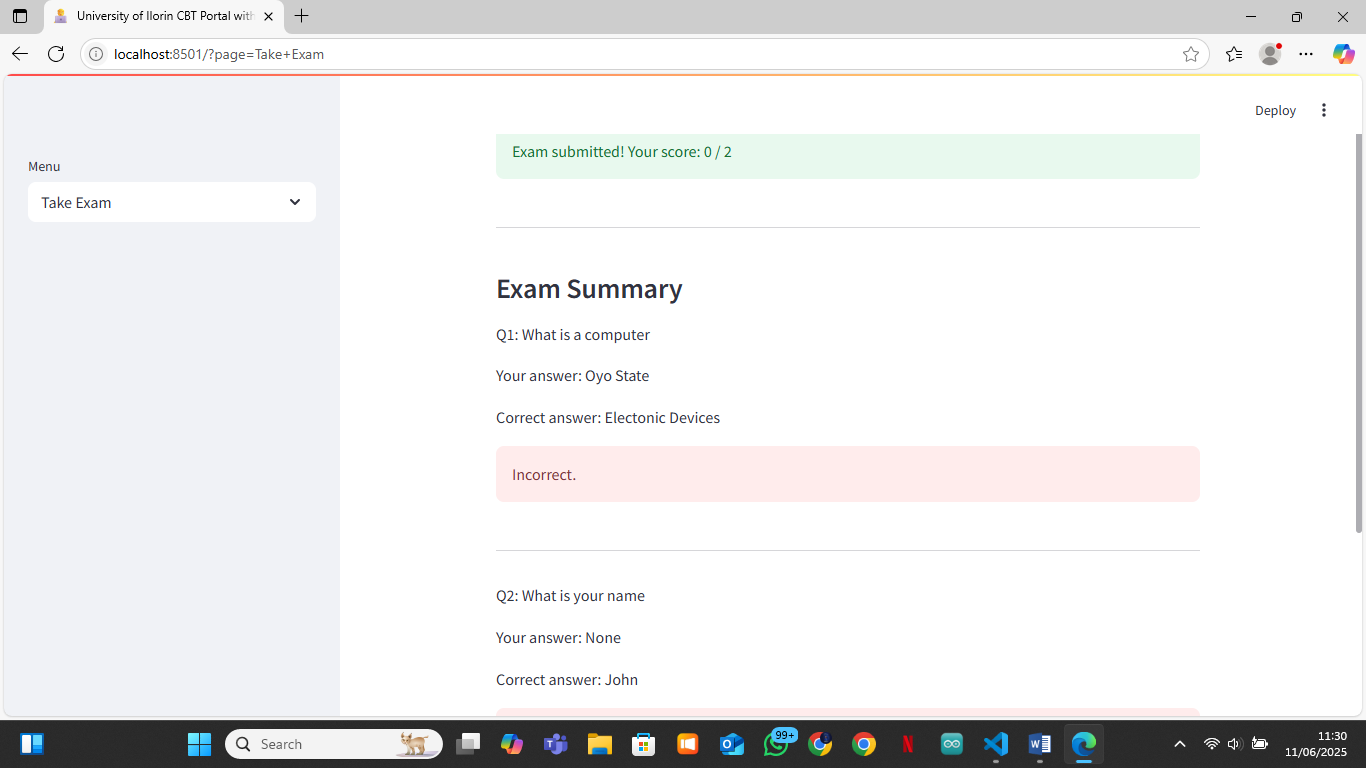


Figure 4.12: Result Page – User’s score and summary

4.4 System Testing and Evaluation

4.4.1 Testing Procedure

Unit Testing: Each module was tested independently for correct functionality.

Integration Testing: Modules were tested together to ensure seamless workflow.

User Acceptance Testing: Real users (students and admin) interacted with the system to validate usability and reliability.

4.4.2 Dataset Description

1. User Images: Real facial images captured via webcam during registration.
2. Exam Questions: Stored in JSON format, covering a range of computer science topics.
3. Results and Logs: Stored in TXT files for analysis and reporting.

4.4.3 Performance Metrics

1. Authentication Accuracy: Measured by the rate of successful and failed logins.
2. Exam Completion Rate: Percentage of users able to complete and submit the exam.
3. Admin Operations: Time and ease of managing users, questions, and results.

4.4.4 Comparative Analysis

1. The facial recognition-based system was compared to traditional password-based CBT systems.
2. Findings: The new system offers higher security, eliminates password fatigue, and reduces impersonation risks.

4.5 Security and Usability Analysis

4.5.1 Security Strength

1. Facial Recognition: Provides strong, biometric-based authentication.
2. Access Control: Only authenticated users can access exams; admin functions are password/PIN protected.
3. Logging: All authentication attempts and results are logged for audit and traceability.

4.5.2 Usability Feedback

1. Students: Reported the system as easy to use, with clear instructions and instant feedback.
2. Admins: Found the dashboard intuitive for managing users, questions, and results.
3. Navigation: One-question-per-page exam format was well received for focus and clarity.

4.6 Discussion of Findings

The system successfully met its objectives:

1. Security: Facial recognition significantly improved exam integrity.
2. Efficiency: Registration, authentication, and exam processes were streamlined.
3. Admin Control: The dashboard provided comprehensive tools for management and reporting.
4. User Experience: Both students and admins reported high satisfaction with the interface and workflow.

4.7 Challenges Encountered

Lighting and Camera Quality: Poor lighting or low-quality webcams affected facial recognition accuracy.

1. User Training: Some users needed guidance for proper face capture.
2. Dependency Management: Ensuring all required Python packages were installed and compatible.
3. File Handling: Managing user images and logs securely and efficiently.

4.8 Summary

This chapter detailed the implementation, testing, and results of the University of Ilorin CBT Portal with Facial Recognition. The system proved to be secure, efficient, and user-friendly, with robust modules for both students and administrators. The findings demonstrate the viability of biometric authentication in academic assessment environments, paving the way for future enhancements and broader adoption.

**CHAPTER FIVE**

**SUMMARY, CONCLUSION AND RECOMMENDATIONS**

**5.1 Summary**

This project focused on the design and implementation of a Computer-Based Test (CBT) Portal for the University of Ilorin, enhanced with facial recognition technology for secure authentication. The system was developed using Python, Streamlit, OpenCV, and FaceNet, and features a modular structure with distinct user and admin interfaces. Key functionalities include webcam-based registration and authentication, a one-question-per-page exam interface, instant result feedback, and a comprehensive admin dashboard for managing users, questions, results, and analytics.

The system was thoroughly tested and evaluated. Results showed that the facial recognition approach significantly improved exam security and user experience compared to traditional password-based systems. The admin dashboard provided robust tools for monitoring, reporting, and managing the entire CBT process.

**5.2 Conclusion**

The University of Ilorin CBT Portal with Facial Recognition successfully addresses the challenges of exam impersonation, user management, and result processing in computer-based assessments. By leveraging biometric authentication, the system ensures that only legitimate users can access and participate in exams. The modular design, intuitive interface, and comprehensive admin controls make the platform suitable for large-scale academic deployment.

The project demonstrates the viability and effectiveness of integrating facial recognition into educational assessment systems, paving the way for more secure and efficient examination processes in academic institutions.

**5.3 Recommendations**

Based on the implementation and evaluation of the system, the following recommendations are made:

1. **Deployment and Scaling:** The system should be deployed on a secure server with adequate resources to handle multiple concurrent users, especially during large-scale examinations.
2. **Continuous User Training:** Users should be educated on proper face capture techniques to ensure high authentication accuracy and reduce false rejections.
3. **Hardware Considerations:** Institutions should provide high-quality webcams and ensure good lighting conditions in exam environments to optimize facial recognition performance.
4. **Integration with Existing Systems:** The portal can be integrated with the university’s student information system for seamless user management and result synchronization.
5. **Regular Updates and Maintenance:** The system should be regularly updated to incorporate the latest security patches, facial recognition models, and feature enhancements.
6. **Further Research:** Future work can explore the integration of additional biometric modalities (e.g., fingerprint, voice) and advanced anti-spoofing techniques to further enhance security.

**5.4 Limitations**

1. The system’s accuracy is affected by camera quality and environmental lighting.
2. Users unfamiliar with webcam technology may require assistance.
3. The current implementation relies on local file storage; migrating to a database would improve scalability and data management.

**5.5 Suggestions for Future Work**

1. Implement mobile device support for greater accessibility.
2. Add real-time proctoring features to monitor exam sessions.
3. Develop a more advanced analytics dashboard for deeper insights into exam performance and user behavior.
4. Integrate with cloud-based storage and authentication services for enhanced reliability and scalability.

**5.6 Closing Remark**

The successful implementation of the University of Ilorin CBT Portal with Facial Recognition marks a significant step towards secure, efficient, and modern academic assessment. With continued development and adoption, such systems can transform the landscape of educational testing in Nigeria and beyond.