International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Facial Recognition & Authentication in E-Learning Portal.

Akash Singh[1], Jay Nikhal[2], Rahul Khandekar[3], Supriya Gore[4], Prof. Deepa Athawle[5].

[12,3,4] *B.E. Students Department of Computer Engineering*
[5] *, Department of Computer Engineering, Bharat College of Engineering, Opp. Gajanan Maharaj Temple, Kanhor Road, Badlapur (West), Thane, Maharashtra - 421503*

Abstract - With the rapid growth of online education, ensuring secure and reliable authentication methods has become a critical concern. Traditional login mechanisms, such as passwords and PINs, are vulnerable to breaches, unauthorized access, and identity fraud. This paper explores the implementation of facial recognition technology as a secure and efficient authentication system for e-learning portals. Facial recognition leverages biometric features to verify users' identities, offering a seamless and user-friendly experience while enhancing security. The proposed system integrates artificial intelligence (AI) and machine learning (ML) algorithms to ensure accurate facial detection, minimize spoofing attempts, and adapt to variations in lighting, expressions, and facial features. Furthermore, this approach improves exam integrity by preventing impersonation and unauthorized access to online assessments. Despite its advantages, challenges such as privacy concerns, data security, and computational requirements must be addressed for widespread adoption. This paper discusses the benefits, limitations, and future scope of facial recognition in e-learning authentication, emphasizing its potential to revolutionize online education security.[3]

Key Words: Multi-Factor Authentication (MFA), Machine Learning Algorithms (Naïve Bayes, SVM, CNNs), Secure Login Mechanism, User Experience Optimization, Real-Time Authentication, Spoofing Attack Prevention, Encryption for Biometric Data Storage

1. INTRODUCTION

The rise of digital learning platforms has transformed the education sector, making knowledge accessible to a global audience. However, as e-learning grows, so do the challenges associated with user authentication, data security, and exam integrity. Traditional authentication methods, such as usernames and passwords, are prone to security breaches, unauthorized access, and identity fraud. To address these concerns, biometric authentication techniques, particularly facial recognition, have emerged as a promising solution for ensuring secure access to e-learning portals.

Facial recognition technology leverages artificial intelligence (AI) and deep learning algorithms to identify and verify users based on their unique facial features. This approach offers a more reliable and user-friendly authentication system, reducing the risk of credential theft and unauthorized usage. Additionally, it enhances the credibility of online assessments by preventing impersonation and exam fraud. The implementation of facial recognition in e-learning portals ensures a seamless and secure user experience, promoting trust in digital education systems.

Despite its advantages, facial recognition-based authentication comes with challenges, including privacy concerns, ethical considerations, and technical limitations such as lighting variations and spoofing attacks. Addressing these issues is essential for ensuring the widespread adoption of this technology in educational platforms. This paper explores the integration of facial recognition for e-learning authentication, discussing its benefits, challenges, and future implications in securing online education.

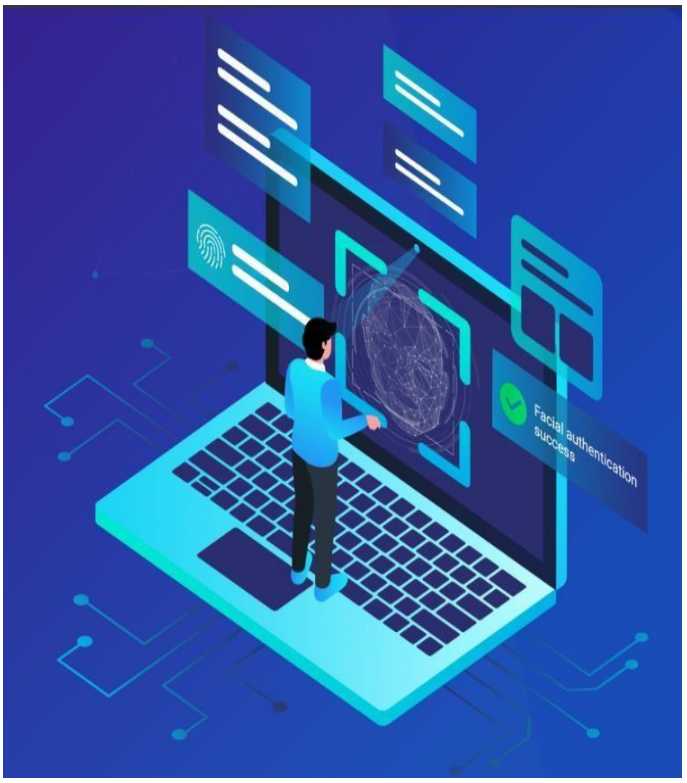

Fig 1. Facial Recognition & Authentication

1.1. Purpose

The integration of facial recognition and authentication in e-learning portals serves multiple purposes, addressing security concerns while enhancing user experience and operational efficiency. This technology provides a reliable and automated method for verifying user identity, ensuring only authorized individuals can access online learning platforms. The key purposes of implementing facial recognition in e-learning portals include:

1.1.1. Enhancing Security

Traditional authentication methods like passwords are vulnerable to hacking and credential theft. Facial recognition provides a more secure and tamper-proof way to verify user identity, preventing unauthorized access and impersonation in online learning environments.

1.1.2. Improving Productivity

Automated facial recognition eliminates the need for manual identity verification, saving time for both students and administrators. This allows institutions to focus more on educational content and less on administrative tasks.

1.1.3. Conserving Resources

Implementing facial recognition reduces the dependency on manual authentication methods, minimizing the need for additional security personnel and reducing operational costs. It also helps optimize digital infrastructure by streamlining authentication processes.

1.1.4. Enhancing User Experience

Facial recognition offers a seamless and hassle-free login process, eliminating the need for remembering complex passwords. This improves accessibility and convenience for students and educators, making e-learning more efficient and user-friendly.

1.1.5. Regulatory Compliance

Many educational institutions must adhere to strict data security and privacy regulations. A well-implemented facial recognition system can help ensure compliance with global standards such as GDPR and other data protection laws, reducing the risk of legal violations.

1.1.6. Reducing Legal Liabilities

By ensuring secure access and preventing fraudulent activities such as identity theft and exam impersonation, facial recognition technology helps institutions mitigate legal risks. It provides a reliable digital record of user authentication, which can serve as evidence in case of disputes.

1.2. Scope

Facial recognition and authentication technology have the potential to revolutionize e-learning platforms by offering secure, efficient, and personalized educational experiences. The scope of this technology extends across various domains, integrating advanced AI, multi-factor authentication, real-time monitoring, and emerging innovations to enhance security and user engagement.

1.2.1. Advanced AI & Deep Learning for Face Recognition

The implementation of deep learning models such as Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs), and transformers improves the accuracy of facial recognition. The integration of 3D facial recognition further enhances reliability by overcoming pose variations and lighting challenges. Additionally, emotion recognition capabilities enable real-time analysis of student engagement and concentration levels.

1.2.2. Multi-Factor Authentication (MFA) for Enhanced Security

To strengthen authentication, facial recognition can be combined with fingerprint scanning, voice recognition, or OTP-based verification. Liveness detection mechanisms prevent spoofing attacks using printed photos or videos. Furthermore, blockchain technology can be utilized to securely store authentication logs, ensuring data integrity and preventing tampering.

1.2.3. Real-Time Attendance & Proctoring System

Facial recognition enables automated attendance tracking in online classes, eliminating manual roll calls. AI-powered remote proctoring ensures exam integrity by detecting suspicious activities such as unauthorized screen movements and gaze deviations. Gaze tracking and head movement analysis further monitor student attentiveness during virtual lectures.

1.2.4. Personalized Learning & Adaptive Education

By analyzing facial expressions and engagement levels, AI-driven facial recognition systems can adapt educational content dynamically. This facilitates the creation of personalized study plans based on student behavior and attention levels. Additionally, real-time feedback systems empower educators to tailor their teaching strategies to enhance comprehension and retention.

1.2.5. Integration with Emerging Technologies

Facial recognition can be seamlessly integrated with Augmented Reality (AR) and Virtual Reality (VR) to provide immersive e-learning experiences. Edge AI computing allows local processing of facial recognition, reducing latency and addressing privacy concerns. Cloud-based facial recognition APIs enhance system scalability and ensure accessibility across global e-learning platforms.

1.2.6. Scalability & Cross-Platform Compatibility

The technology is designed to be adaptable across various platforms, including mobile applications, desktops, and smart classrooms. Multi-user authentication supports collaborative learning environments, ensuring seamless identity verification. Additionally, compatibility with wearable devices such as smart glasses enables hands-free authentication for enhanced accessibility.

1.2.7. Privacy, Ethical Considerations & Compliance

Strict adherence to data protection regulations such as GDPR ensures the secure handling of biometric data. A consent-based authentication framework allows students to opt in or out of facial recognition, promoting ethical use. Implementing decentralized facial recognition enhances privacy by encrypting biometric data, preventing unauthorized access.

1.2.8. Global Expansion & Multi-Language Support

Facial recognition systems can be tailored for global e-learning platforms by supporting multiple languages and regional preferences. AI models can be trained to recognize diverse facial features across ethnicities and age groups, ensuring inclusivity. Voice-assisted authentication further enhances accessibility for differently-abled students.

1.3. Aim

The implementation of facial recognition and authentication in e-learning portals aims to enhance security, improve user experience, and ensure the integrity of digital education. By integrating advanced technologies such as artificial intelligence (AI), deep learning, and multi-factor authentication, this system provides a seamless and secure learning environment. The key aims of this technology include:

1.3.1. Enhancing Security and Preventing Unauthorized Access

Implement a biometric authentication system to ensure only registered users can access e-learning platforms. Reduce risks associated with password-based authentication, such as credential theft and hacking. Utilize liveness detection to prevent spoofing attacks using photos or videos.

1.3.2. Improving Exam Integrity and Academic Credibility

Develop AI-powered remote proctoring to monitor online exams and prevent impersonation or cheating. Use facial recognition for real-time student verification during assessments. Implement gaze tracking and head movement analysis to ensure students remain focused during exams.

1.3.3. Automating Attendance Tracking and User Authentication

Replace traditional attendance methods with an automated facial recognition system for online and hybrid learning environments. Enable real-time attendance tracking without requiring manual input from educators. Support multi-user authentication to facilitate collaborative learning sessions.

1.3.4. Improving User Experience and Accessibility

Provide a seamless and password-free authentication system for a more user-friendly experience. Develop an adaptive learning system that customizes educational content based on students' engagement and focus levels. Ensure cross-platform compatibility with mobile apps, desktops, and wearable devices for convenient access.

1.3.5. Integrating Emerging Technologies for a Smarter E-learning System

Implement Augmented Reality (AR) and Virtual Reality (VR) for immersive learning experiences. Utilize Edge AI computing to process facial recognition locally, reducing latency and improving privacy. Enable cloud-based authentication to ensure scalability and accessibility for global users.

2. Literature Survey

2.1. Historical Background

2.1.1 Face Recognition for Authentication in E-Learning Systems (2022)

A study by Zhang, Li, and Chen (2022) investigated the implementation of facial recognition for authentication in e-learning systems. The research highlighted the limitations of password-based authentication, which is susceptible to security breaches. By integrating deep learning-based facial recognition, the study demonstrated a reduction in identity fraud and an enhancement in user experience. However, challenges such as variations in facial expressions, lighting conditions, and privacy concerns were identified as areas requiring further research.

2.1.2 Biometric-Based Authentication for Online Learning Platforms (2021)

Kumar, Patel, and Reddy (2021) explored the effectiveness of biometric authentication methods as alternatives to traditional login credentials. Their study evaluated multiple biometric techniques, including fingerprint scanning, retina scanning, and facial recognition. Among these, facial recognition emerged as the most efficient and user-friendly method. However, the research also emphasized ethical concerns regarding biometric data storage and user consent, underscoring the need for secure encryption methods.

2.1.3 AI-Based Face Recognition for Secure Online Examinations (2020)

A study by Singh, Sharma, and Mehta (2020) introduced an AI-driven face recognition system designed to enhance security in online examinations. The research demonstrated that real-time face tracking and liveness detection could significantly reduce impersonation and cheating incidents. The system's scalability was a major advantage, as it effectively handled large numbers of students. However, challenges in low-light

environments were noted, with recommendations to integrate infrared-based facial detection to improve accuracy.

2.1.4 Security Concerns in Face Recognition-Based Authentication (2019)

Williams, Brown, and Garcia (2019) conducted an extensive analysis of the security risks associated with facial recognition in e-learning authentication. Their study highlighted issues such as spoofing attacks, data breaches, and privacy concerns. To mitigate these threats, they recommended implementing multi-factor authentication (MFA), combining facial recognition with OTP verification. While acknowledging advancements in facial recognition technology, the research emphasized the necessity of ethical data handling and regulatory compliance.

2.2. Machine Learning Approaches in Facial Recognition

2.2.1 Naïve Bayes Classifier for Face Recognition

Naïve Bayes, a probabilistic machine learning model, has been applied to facial recognition tasks due to its ability to handle high-dimensional data. A study by Gupta et al. (2021) explored its effectiveness in classification-based facial recognition. The model performed well with properly preprocessed datasets but struggled with variations in facial expressions and lighting conditions. Feature selection and dimensionality reduction techniques were suggested to improve accuracy.

2.2.2 Support Vector Machines (SVM) for Facial Authentication

SVM has been widely used in facial recognition due to its strong generalization capabilities. A study by Lee and Kim (2020) demonstrated that SVM models trained on optimized feature sets achieved high accuracy in facial authentication. The research highlighted the benefits of kernel functions in handling non-linear facial data. However, computational efficiency remained a challenge, particularly in real-time applications.

2.2.3 Deep Learning-Based Face Recognition

Deep learning approaches, particularly Convolutional Neural Networks (CNNs) and Siamese Networks, have significantly improved facial recognition accuracy. CNN-based architectures, such as ResNet and VGG, have been extensively used for feature extraction and classification. Siamese Networks, which learn facial similarity rather than classification, have been instrumental in one-shot learning applications for facial authentication. The primary limitation of these models is their high computational cost, which necessitates the use of cloud-based processing or edge AI solutions for optimization.

2.3. Feature Engineering and Data Processing in Facial Recognition

2.3.1 Feature Extraction Techniques

Feature extraction is crucial for enhancing the accuracy of facial recognition models. Commonly used techniques include:

Histogram of Oriented Gradients (HOG): Effective for detecting facial structures by analyzing gradient patterns.

Local Binary Patterns (LBP): Used for texture analysis, improving performance in different lighting conditions.

Principal Component Analysis (PCA): Reduces dimensionality while retaining essential facial features.

2.3.2 Data Preprocessing for Improved Recognition Accuracy.

To improve the performance of facial recognition systems, various preprocessing techniques are employed:

Image Normalization: Adjusting brightness and contrast to ensure consistency across images.

Face Alignment: Correcting head tilt and pose variations using facial landmarks.

Data Augmentation: Applying transformations such as rotation, flipping, and cropping to enhance model robustness.

2.4. Liveness Detection for Anti-Spoofing

Liveness detection is a critical component in facial recognition systems to prevent spoofing attacks. Modern anti-spoofing techniques include:

Blink Detection: Ensures authentication is granted only to real users by analyzing eye movement.

Head Movement Tracking: Detects natural head motions to differentiate between live users and static images.

Infrared-Based Thermal Imaging: Enhances security by identifying heat patterns unique to living individuals.

3. SYSTEM ARCHITECTURE AND DESIGN

This diagram represents a Facial Recognition System workflow. It begins with capturing an input image, followed by pre-processing, feature extraction, and classification to determine if the face is known or unknown using a face database. A meta-recognition system monitors recognition accuracy and takes corrective actions like operator intervention, data fusion, or acquiring more data in case of failure. If successful, the process is completed; otherwise, it restarts for improved accuracy.

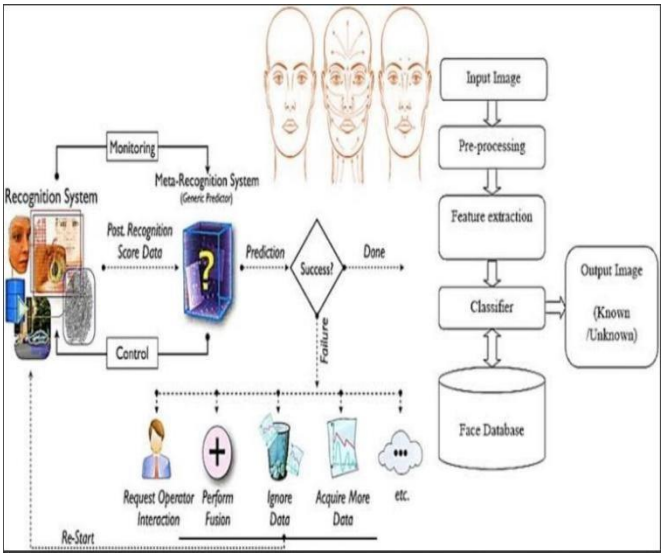

Fig 2: System Architecture & Design Diagram

3.1. Hardware requirement

1. Processor – A dual-core processor such as Intel i5 or AMD Ryzen 5 is required to efficiently handle real-time facial recognition computations and authentication processes.

2. RAM – A minimum of 4GB RAM is necessary, but 8GB is recommended for better performance and faster processing of facial recognition algorithms.

3. Storage – At least 100GB of free space is required to store face recognition data, logs, and related authentication records.

4. Camera – A built-in or external webcam with a minimum 720p resolution ensures clear facial image capture, which is crucial for accurate recognition.

5. Microphone – A built-in or external microphone is needed for additional biometric authentication methods, such as voice recognition or communication during online learning.

6. Network – A stable internet connection with at least 5 Mbps speed is required to ensure seamless real-time authentication and prevent delays in login or attendance tracking.

3.2. Software requirement

1. Operating System – The system requires a Linux-based server (e.g., Ubuntu, CentOS) or Windows Server for backend hosting. On the client-side, it supports Windows, macOS, or Linux (e.g., Ubuntu) for users accessing the platform.

2. Facial Recognition Libraries – Python-based libraries such as OpenCV, Dlib, and face_recognition are used for facial detection and recognition. TensorFlow or PyTorch support deep learning models to enhance accuracy and performance in real-time face authentication.

3. Backend Development – The platform is developed using Django, a Python-based web framework that ensures secure and scalable application development. MySQL is used for efficient database management, storing user credentials and authentication logs.

4. Frontend Development – The user interface is designed using HTML, CSS, and JavaScript for an interactive experience. Frameworks like Vue.js and Nuxt.js are used to enhance the responsiveness and dynamic behavior of the platform.

4. PROPOSED SYSTEM AND IMPLEMENTATION

The Facial Recognition and Authentication System for E-Learning enhances security by using AI-driven face recognition to verify users, prevent unauthorized access, and automate attendance tracking. It eliminates password-based authentication, reducing login hassles while ensuring secure exam participation. The system integrates deep learning algorithms for identity verification, liveness detection to prevent spoofing, and encryption for biometric data security. It is built with Python-based frameworks (Django, TensorFlow/ Py Torch) and supports multi-device compatibility. The backend handles secure data processing, while the frontend offers a user-friendly interface for seamless access. This solution ensures a scalable, efficient, and secure e-learning experience.

4.1. Project Implementation

The facial recognition authentication system is implemented using a combination of machine learning models, biometric authentication algorithms, and secure data handling techniques.

4.1.1. Face Recognition Model Development

Preprocessing: Captures and normalizes facial images for accurate recognition.
Feature Extraction: Uses deep learning techniques such as Convolutional Neural Networks (CNNs) to extract unique facial features.
Classifier: Employs Support Vector Machine (SVM) or Naïve Bayes classifiers to differentiate users.

4.1.2. System Architecture

Client-Side: The system captures facial images through webcams and sends data for processing.
Server-Side: The authentication engine verifies user identity and grants access.
Database: Stores encrypted biometric data securely.

4.1.3. Anti-Spoofing & Security Measures

Liveness Detection: Prevents photo or video-based spoofing by detecting live motion (blink detection, head movements).
Encryption & Secure Storage: Uses AES-256 encryption to protect biometric data.
Multi-Factor Authentication (MFA): Integrates face recognition with OTP-based verification for enhanced security.

4.1.4. System Deployment

Backend: Built using Django (Python framework) with MySQL for data management.
Frontend: Developed using HTML, CSS, JavaScript, and Vue.js for a seamless user experience.
AI Model Integration: TensorFlow or PyTorch is used for deep learning-based facial recognition.

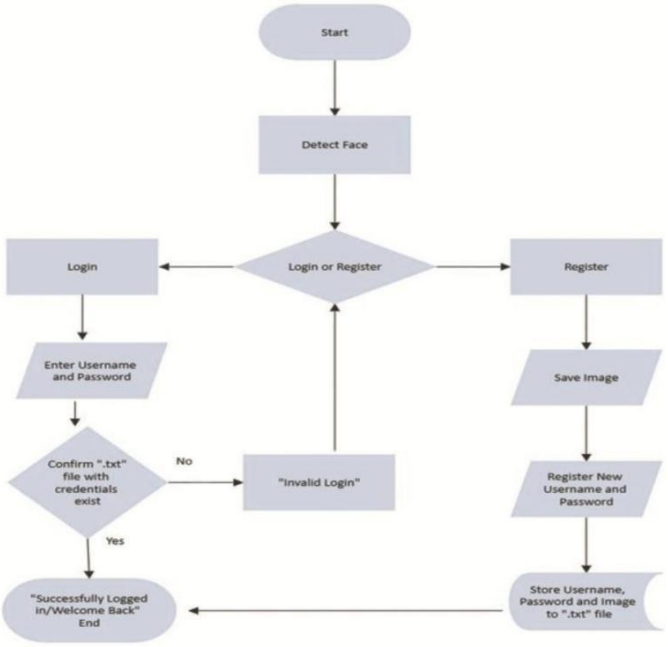

Fig 3: Work Flow Diagram

4.2. Portal Registration Page Overview

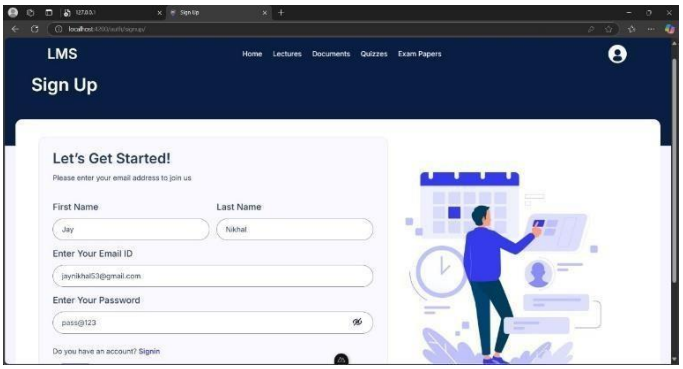

Fig 4: Portal Registration Page

The registration page of the Learning Management System (LMS) allows new users to create an account by providing basic details such as their first name, last name, email ID, and password. This step ensures secure access to the platform. Once the required details are entered, users can proceed to the next stage, where they register their facial data for authentication. This biometric-based registration enhances security, making the login process more seamless and preventing unauthorized access. The "Sign In" option is also available for returning users who have already created an account.

4.3. LMS Portal Facial Recognition Enrollment Page Overview

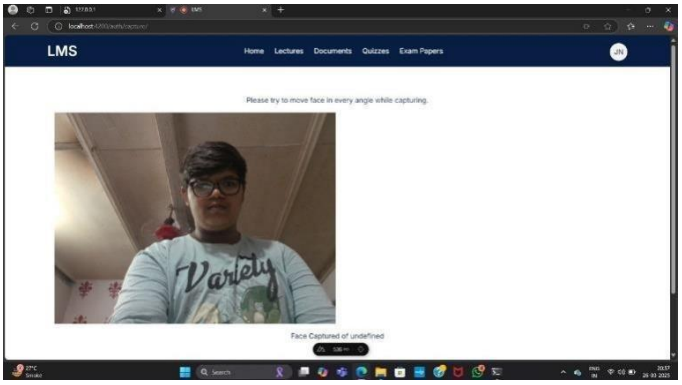

Fig 5: LMS Portal Facial Recognition Enrollment Page

The Facial Recognition Enrollment Page in the Learning Management System (LMS) is designed to register users' biometric data for enhanced security and seamless authentication. Once a user completes the registration process by providing personal details such as their name, email, and password, they are required to capture their facial data.

The page instructs users to move their faces in different angles to ensure a comprehensive scan, which helps improve recognition accuracy. The system processes and stores the captured face data, enabling secure login access without requiring manual credentials in future sessions. If the system fails to detect a face properly, users may need to adjust their position, lighting, or camera angle for successful enrollment.

This biometric authentication method strengthens security by preventing unauthorized access and ensuring that only registered individuals can log in to the LMS.

4.4. LMS Portal Facial Recognition Notification Page Overview

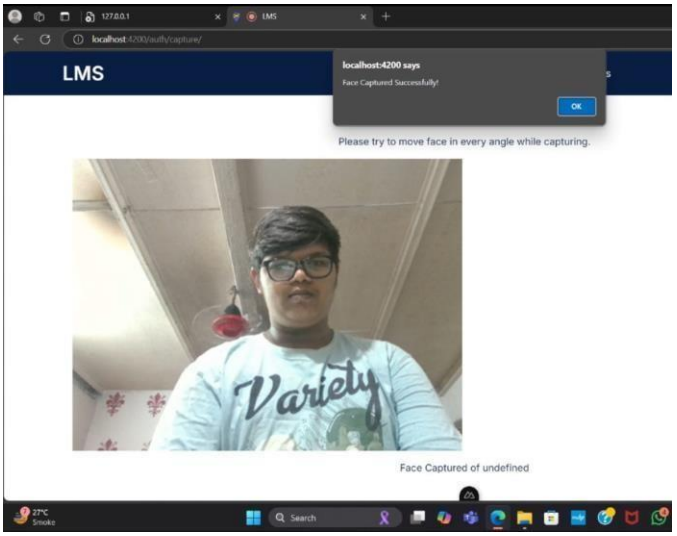

Fig 6: LMS Portal Facial Recognition Notification Page

The Facial Recognition Notification Page in the Learning Management System (LMS) confirms the successful capture of a user's face data during the enrollment process. Once the

system accurately registers a user's facial features, a pop-up notification appears, stating "Face Captured Successfully!"

This page plays a crucial role in ensuring that the facial recognition system has correctly recorded the user's biometric data. The confirmation message reassures users that their facial data has been stored and can be used for secure authentication in future logins.

By implementing facial recognition, the LMS enhances security, reduces the need for traditional login credentials, and provides a seamless and efficient authentication experience for users.

4.5. LMS Portal Sign-In Interface Overview

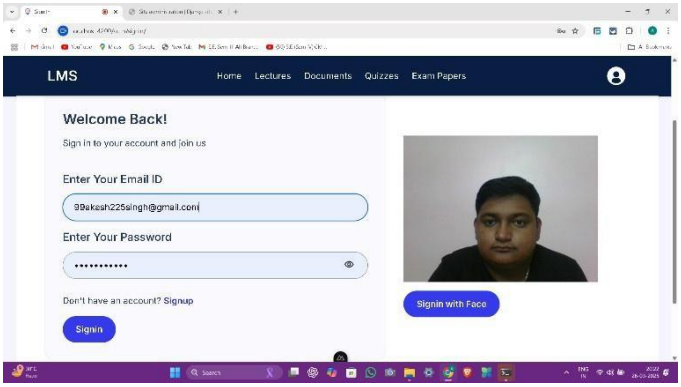

Fig 7: LMS Portal Sign-In Interface

The Sign-In Interface of the Learning Management System (LMS) provides users with multiple authentication options for a secure and seamless login experience. Users can either enter their email ID and password or opt for facial recognition-based login.

The traditional login method requires users to input their credentials, ensuring a familiar and secure authentication process. Alternatively, the "Sign in with Face" option allows users to authenticate using facial recognition, offering a faster and more convenient access method.

By integrating both password-based and biometric authentication, the LMS enhances security, accessibility, and user experience, catering to diverse user preferences.

4.6. LMS Portal Home Landing Page Overview

Fig 8: LMS Portal Home Landing Page

The Home Landing Page of the Learning Management System (LMS) serves as the central hub for students and educators, providing easy access to various academic resources. The interface is designed for seamless navigation, allowing users to explore key sections such as Lectures, Documents, Quizzes, Exam Papers, and Notices.

With a modern and intuitive design, the portal enhances the learning experience by ensuring that essential materials, assignments, and assessments are readily available. The homepage also features an engaging banner with a tagline, emphasizing the platform's goal of fostering smart learning for a smarter future.

5. CONCLUSIONS

The facial recognition system enhances authentication security by analyzing facial traits and generating secure credentials. These credentials are efficiently stored for easy access and management. To further strengthen security, integrating multi-factor authentication (MFA) with facial recognition can prevent unauthorized access. Additionally, using pre-trained deep learning models like Res Net or VGG can improve recognition accuracy. Implementing strong password policies, periodic password changes, and data encryption ensures enhanced system reliability and user privacy. These advancements collectively improve authentication security and system dependability in e-learning platforms.

6. ACKNOWLEDGMENT

We sincerely appreciate the support and encouragement of everyone who contributed to the successful completion of this project. We extend our heartfelt gratitude to **Prof. Deepa Athawale**, our project guide, for providing invaluable guidance, motivation, and constant support throughout this journey. Her insightful suggestions and willingness to assist at every stage greatly helped us refine our work.

We are also thankful to **Prof. Deepa Athawale**, our Project Coordinator, for her constructive feedback and practical insights that enhanced our project. Our sincere gratitude goes to **Prof. Radhika Nanda (HOD)**, Head of the Computer Engineering Department, for her motivation and valuable inputs.

Additionally, we extend our appreciation to **Prof. Dr. B.M. Shinde**, our honorable Principal, for his valuable suggestions to improve our project report. We also express our thanks to the entire teaching staff, our college, our families, and everyone who contributed, knowingly or unknowingly, to the successful completion of this project.

Lastly, I extend my sincere gratitude to everyone who played a role, directly or indirectly, in the successful completion of this project. The combined efforts, guidance, and encouragement of all those mentioned above have been instrumental in making this work possible.

7. REFERENCES

1. B. W. Mugalu, R. C. Wamala, J. Serugunda, and A. Katumba, "Face Recognition as a Method of Authentication in a Web-Based System," arXiv preprint arXiv:2103.15144, Mar. 2021.

2. A. K. Jain, S. Pankanti, and R. Bolle, "An Identity-Authentication System Using Fingerprints," Proceedings of the IEEE, vol. 85, no. 9, pp. 1365-1388, Sep. 1997.

3. A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004.

4. G. G. Medioni et al., "Identifying Non-Cooperative Subjects at a Distance Using Face Recognition," in Proceedings of the IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2007.

5. I. Masi, A. T. Trần, T. Hassner, J. T. Leksut, and G. Medioni, "Do We Really Need to Collect Millions of Faces for Effective Face Recognition?," in European Conference on Computer Vision (ECCV), 2016.

6. X. Ding, "Multilingual Character and Document Recognition: A New Frontier in OCR Research," Tsinghua University, [Online].

7. M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, "Authentication Schemes for Smart Mobile Devices: Threat Models, Countermeasures, and Open Research Issues," Telecommunication Systems, vol. 72, no. 3, pp. 627-642, Sep. 2019.

8. H. Khan, U. Hengartner, and D. Vogel, "Mimicry Attacks on Smartphone Keystroke Authentication," ACM Transactions on Privacy and Security, vol. 23, no. 1, pp. 1-37, Feb. 2020.

9. A. K. Jain, K. Nandakumar, and A. Nagar, "Fingerprint Template Protection: From Theory to Practice," in Security and Privacy in Biometrics, Springer, London, 2013, pp. 187-214.

10. A. Serwadda et al., "Toward Robotic Robbery on the Touch Screen," ACM Transactions on Information and System Security, vol. 18, no. 4, pp. 1-25, May 2016.

11. C. Shen, Y. Zhang, X. Guan, and R. A. Maxion, "Performance Analysis of Touch-Interaction Behavior for Active Smartphone Authentication," IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 498-513, Mar. 2016.

12. M. Shahzad, A. X. Liu, and A. Samuel, "Behavior Based Human Authentication on Touch Screen Devices Using Gestures and Signatures," IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2726-2741, Oct. 2017.