# E-Authentication System

Dr. Kirti Taneja, Sahil Singh, Sarthak Arya, Sarthak Arya, Harman Singh, Avinash Kumar
*Department of Computer Science Chandigarh University Mohali, India*

## I. INTRODUCTION

In recent years, the proliferation of online learning and remote assessments has transformed the educational landscape, offering unprecedented flexibility and accessibility. However, the rapid expansion of e-learning platforms has also intro- duced significant challenges in maintaining the integrity of assessments. Traditional evaluation methods, which often relyon in-person proctoring, have become increasingly impracticalin a digital environment, raising concerns about cheating and unauthorized participation.

To address these challenges, there is a growing need for robust e-authentication systems that can verify the identity of learners while ensuring a secure assessment environment. Suchsystems must not only prove the legitimacy of the test-takers but also be resistant to potential breaches of security, suchas impersonation and unauthorized assistance. This research paper explores the development and implementation of an innovative e-authentication system that leverages advanced biometric technologies, including facial recognition, eye track- ing, and voice analysis, to create a comprehensive solution for remote assessments.

By integrating these biometric modalities, the proposed sys-tem aims to enhance the reliability and security of online eval-uations, providing a seamless experience for both educators and learners. This study not only contributes to the existing body of knowledge in the field of e-learning but also offers practical implications for the design and deployment of future e-assessment frameworks. Through a detailed examination of the system's architecture, functionality, and effectiveness, thisresearch aims to establish a foundation for more secure and trustworthy online assessments in the evolving educational landscape.

## II. LITERATURE REVIEW

Sarah N. Abdulkader et al. [1] provides a comprehensive overview of authentication systems, focusing on three main types: knowledge-based, token-based, and biometrics-based.

I. Knowledge-based authentication relies on passwords and information known by the user but faces security risks from brute force, shoulder surfing, keyloggers, and phishing attacks.

II. Token-based authentication involves physical objects like credit cards or mobile devices, but is vulnerable to theft and eavesdropping. The use of mobile phones and RFID tags for secure transactions has grown, although they also have weaknesses such as cloning and unauthorized read-ing. III. Biometrics-based authentication uses unique human traits (e.g., fingerprints, facial recognition) and behavioral characteristics. It is more secure but vulnerable to attacksat various system points, such as spoofing at the sensor level or tampering with biometric data in storage. The paper discusses the structure of biometric systems, highlighting their vulnerability points and proposing countermeasures, such as liveness detection and cancelable biometrics, to protect againstimpersonation, spoofing, and system module attacks.

Jae-Kyung Park et al. [2] examines various authentication methods, their vulnerabilities, and proposes a new total authen- tication service. It highlights security risks in using certificates for identity verification, with hacking incidents on the rise. Active-X, once widely used in South Korea, was discontinuedin 2015 due to its security weaknesses, notably during large- scale cyber-attacks like the 2009 DDOS incident. The rise of FinTech, blending finance and technology, has introduced newfinancial services that require advanced security. Traditional OTP systems, while secure, are inconvenient due to the need for physical tokens, leading to the development of Smart OTP, which generates passwords via software. The proposed total authentication service aims to improve security by using real-time external certification agencies and technologies like Bluetooth and NFC to prevent duplication and hacking. The system envisions automation through smart devices for more seamless and secure transactions.

Nader Abdel Karim et al. [3] investigate user authentication methods for online exams, focusing on integrating preferences-based authentication (PrBA)

with user interface (UI) design. The paper reviews several existing methods, including remote biometrics with webcams, multi-biometrics systems, and se- cure single-disk exam platforms. It classifies authentication techniques into knowledge-based (NBA), possession-based (PBA), and biometrics-based (BBA) methods, noting that BBAoffers strong security but is often costly and invasive. The study introduces PrBA, which uses user-selected UI prefer- ences, such as font style and size, question grouping, andsound alerts, as a security measure. Results show a 93 percent accuracy rate in user consistency. The method achieved afalse negative (FN) rate as low as 0 percent with a thresholdof two mistakes and a maximum false positive (FP) rate of 0.83 percent with three mistakes. This approach effectively balances security and usability, addressing traditional trade- offs in authentication systems.

Qinghai Gao et al. [4] discuss the growing importance of biometric authentication systems, emphasizing the identifi-cation of individuals based on physiological and behavioral characteristics. Common physiological traits include finger- prints, facial images, and iris scans, while behavioral traits encompass voice, keystroke dynamics, and gait. The study highlights how combining multiple biometrics can improve accuracy. The research explores various biometric authentica- tion applications, such as Rodwell et al.'s acoustic biometric system and Nazar et al.'s mouse dynamics-based system, which offer continuous authentication beyond traditional login methods. In e-learning, biometric methods like fingerprint and facial recognition are proposed to prevent credential sharing and improve exam security. The study also addresses keychallenges in biometric authentication, including the non- exact reproducibility of biometric measurements and privacy concerns. Gao et al. propose a privacy-enhanced system using randomized fingerprint minutiae, which selects a subset ofminutiae points for authentication, thus protecting the user's original biometric data while maintaining security.

Hafiz Zahid Ullah Khan et al. [5] begin their research by addressing the growing sophistication of modern web- based threats, which have evolved from traditional virusesand worms into faster, more covert attacks that propagateglobally in a matter of minutes. They emphasize that many organizations fail to take adequate security measures to protecttheir networks, applications, and data, despite the increasing reliance on online services. As users are required to manage multiple ID/password combinations across different services, issues like memorability and security become more pressing. To address these challenges, web-based authentication mech- anisms, such as those employed by Wireless Internet Service Providers (WISPs), have gained popularity for their simplicityin user registration and authentication. The paper underscores the need for robust authentication systems that not only guard against unauthorized access but also establish secure mechanisms and policies to protect organizations from cyber threats. The authors outline the concept of authentication as the process of verifying an individual's identity to grant access to resources. Various technologies like user IDs, passwords, biometrics, smartcards, and protocols like Kerberos and SAML are explored, demonstrating how organizations implement these techniques to meet security demands. They also highlightthe importance of authentication in critical applications such as e-commerce, e-voting, and banking, where ensuring legitimate access is paramount. The research aims to explore different authentication techniques and propose a system that improves security by making sensitive information harder to steal or compromise.

Muhammad Sajjad et al. [6] present an advanced mutual authentication model for medical IoT (mIoT) systems, address- ing key security challenges. The paper proposes an improved three-factor authentication scheme, allowing real-time selec- tion of login credentials to offer flexibility and ease of access for medical staff. The system is designed to protect against common cyberattacks, including offline password guessing, replay, impersonation, and man-in-the-middle attacks. It also ensures biometric data security by wrapping it with high- entropy random numbers, making it difficult for attackers to extract sensitive information. The model guarantees user anonymity and untraceability, dynamically changing session keys during each authentication process. It is also robust against insider threats and stolen verifier attacks, as critical information is not stored in a recoverable form. Addition- ally, the system provides forward secrecy, ensuring that past communications cannot be decrypted even if an attacker gains access. In summary, the proposed scheme enhances security and usability in mIoT environments, particularly in healthcare, where protecting data privacy, integrity, and access controlis crucial. The system offers a comprehensive solution to common security risks in e-health systems.

Jae-Jung Kim et al. [7] propose an improved User Authentication Level System (UALS) model, introducing a five- level framework to address the vulnerabilities of traditional single-factor authentication methods amid increasing cyberthreats. By advocating for multi-factor authentication (MFA) that integrates biometric data and public key infrastructure (PKI), the authors aim to enhance security for high-risk financial transactions and scenarios requiring strong iden- tity verification. Their framework emphasizes regular risk assessments, enabling online service providers to implement effective security measures, thus significantly improving user privacy and authentication reliability in sensitive sectors like finance and healthcare.

Adem Alpaslan ALTUN et al. [8] introduce a biometric- based electronic voting system designed to enhance security and efficiency in elections. They highlight the limitations of traditional voting methods, including the potential for ballot misplacement and time-consuming processes. By proposing anelectronic voting system that utilizes fingerprint recognition, the authors present a more reliable identification method that prevents duplicate voting and ensures that only registered electors can cast their votes. The system operates as a web- based application, facilitating centralized vote collection whileimproving security and reliability.

The research by Salam S. Ketab et al. [9] evaluates the E-Invigilation of E-Assessments (EIEA) system, aimed at enhancing online assessment integrity through continuous biometric monitoring. By incorporating 2D and 3D facial recognition, eye tracking, and speech recognition, the sys- tem effectively ensures only legitimate students participate in exams. Experimental trials with 51 participants revealed high accuracy, with a false rejection rate (FRR) of 0 for 2D recognition and 0.0063 for 3D. The study concludes that the EIEA system offers a reliable solution for remote assessments, significantly mitigating risks of academic dishonesty whilepaving the way for secure e-learning environments. Future research will focus on refining the system and exploring additional biometric modalities.

## III. PROBLEM STATEMENT

As online education rapidly expands globally, so does the critical need for secure, efficient, and scalable e-authenticationsystems that ensure academic integrity in remote assessments. Traditional online assessment methods, which often rely on static authentication approaches like passwords or one-time verification, fail to provide continuous identity verification, leaving gaps for academic dishonesty, impersonation, and unauthorized assistance during exams. Current solutions using physical proctors, even when done remotely, lack scalability, are costly, and present significant privacy concerns, making them impractical for widespread adoption.

The challenge is further compounded by the fact that exist- ing biometric solutions, such as single-factor facial recognition or keystroke dynamics, often fall short in terms of accuracy and reliability in remote, uncontrolled environments. Many of these systems struggle to detect nuanced cheating behaviors, like discreet consultation with another person, leaving them vulnerable to advanced circumvention tactics. Additionally, they may fail to comply with privacy standards or offer a user-friendly experience, making students wary of using them.

This research seeks to address these challenges by develop- ing a novel e-authentication system specifically designed for remote, real-time proctoring of online assessments. The sys- tem aims to provide continuous, multimodal biometric mon- itoring—leveraging 2D/3D facial recognition, eye-tracking,and voice analysis—to verify the legitimacy of exam-takers throughout the assessment. This approach not only enhances security by continuously authenticating users but also mini- mizes invasiveness and protects data privacy through encrypted data handling and privacy-compliant design. The central prob-lem this research tackles is: How can we create a secure, scalable, and privacy-respecting e-authentication system that continuously and non-intrusively monitors remote assessment participants, ensuring the legitimacy of their identity and detecting any potential academic dishonesty in real time? This study aims to fill the gap by providing a solution that balances rigorous security requirements, user acceptance, and the flexibility necessary for a variety of online educational contexts.

## IV. METHODOLOGY

This research employs a structured methodology for devel- oping, implementing, and validating a secure e-authentication system for remote assessments,

covering system requirements, biometric authentication, integration, threat detection, testing, and optimization.

The Requirement Analysis and System Design phase fo- cuses on understanding functional needs for continuous iden- tity verification and non-functional requirements like privacy and scalability. Through stakeholder surveys and literature review, the necessary biometric modalities—2D/3D facial recognition, eye-tracking, and voice analysis—were defined to enable real-time identity validation in alignment with LMS platforms.

In the Biometric Authentication Development phase, algo- rithms for multimodal biometrics were implemented, covering facial recognition, eye-tracking, and voice monitoring. These were fused into a decision-making system to ensure continu- ous, non-invasive verification. Preprocessing on the client side was established for efficiency and privacy.

The System Integration and Security Architecture phase fo- cused on secure data transmission, using SSL/TLS encryption,and seamless LMS integration. Protocols were designed for initial user login and secure biometric data handling, withmechanisms for real-time alerts on suspicious behaviors.

Threat Detection Algorithms were then developed to moni- tor eye movements, head turns, and voice analysis for signs of misconduct. Using predefined thresholds and machine learn- ing, the system was trained to identify patterns associated with potential academic misconduct, and to flag incidents for real-time response.

In Experimental Validation and Evaluation, accuracy, us- ability, and scalability were assessed through controlled lab tests, usability studies, and real-world pilots. Metrics like false acceptance/rejection rates were used to measure accuracy,while feedback from students and instructors provided insight into usability and responsiveness.

Finally, Data Analysis and Optimization refined system per-formance based on experimental data, optimizing algorithmsto improve detection accuracy, resource efficiency, and user interface responsiveness. Documentation included technicalspecifications and suggestions for future enhancements, such as adding biometric modalities and refining privacy-preserving measures.

This methodology provides a comprehensive approach to creating a secure e-authentication framework that effectively balances integrity, privacy, and usability for remote assess- ments.

## V. RESULTS AND EVALUATION

This section presents a detailed analysis of the e-authentication system's performance based on experimental data, focusing on accuracy, error rates, and operational ro- bustness. A series of metrics were calculated from controlled tests, including false rejection rate (FRR), false acceptance rate

(FAR), and recognition accuracy for both 2D and 3D modesof biometric identification.

### *A. Quantitative Results: Accuracy and Error Rates*

The system was tested with 51 participants under controlledand varied conditions, recording data across multiple biometric modalities, including facial recognition (2D and 3D), eye tracking, and voice monitoring. The following table provides key results:

Table I: Comparison of 2D And 3D Facial Recognition Performance Metrics

| Metric | 2D Facial R. | 3D Facial R. |
|---|---|---|
| Recognition Accuracy (%) | 92.5 | 96.3 |
| False Rejection Rate (FRR) | 0.04 | 0.0063 |
| False Acceptance Rate (FAR) | 0.08 | 0.0021 |
| Average Processing Time (ms) | 45 | 68 |

### *B. System Performance Under Varied Conditions*

Further evaluation was conducted to assess system robust- ness in various scenarios, such as low-light environments,extreme head movements, and multiple faces appearing in the camera frame.

i. Low-Light Conditions: Both 2D and 3D recognition modes were tested under dim lighting. In these conditions, 2D recognition accuracy dropped to 85.4%, whereas the 3D moderetained an accuracy of 93.6%, demonstrating that depth-based3D recognition is less susceptible to environmental lighting changes. The FRR increased in low-light for 2D (to 0.07) but remained largely consistent for 3D mode (at 0.01).

ii. Varied Head Movements: To simulate common distrac- tions or incidental movements, participants were asked to per- form a set of head motions (turning left, right, up, and down) while remaining in the camera frame. The 3D recognition

mode effectively adapted to these variations with a marginal reduction in accuracy (95.8%), while the 2D mode's accuracy decreased more significantly to 87.9%. The robustness of 3D mode is attributed to its ability to capture depth information, making it less sensitive to lateral head movement.

iii. Multiple Faces in the Camera Frame: When additional faces were introduced into the frame to test for security against unauthorized access, the 2D system showed a 5.2% false acceptance rate due to its limited ability to differentiate users based solely on surface features. However, the 3D mode maintained a low FAR of 0.5%, demonstrating thatdepth-based recognition enhances the system's capacity to distinguish the primary user, even when multiple faces are present.

### C. Anomalies and Observed Trends

The system's performance displayed a few notable anoma- lies. In a minority of cases, users with highly similar facial structures (such as siblings) were occasionally misclassified, leading to a slight increase in FAR in both modes, though the effect was more pronounced in 2D recognition. Additionally, eye tracking sometimes misaligned when participants wore glasses with reflective lenses, though this issue did not impact facial recognition itself. A promising trend was observed in the3D system's resilience to varied facial angles, which suggests the potential for enhancing the algorithm to capture a wider range of biometric data points for improved flexibility.

### D. Graphical Representation of Results

*1) Accuracy Comparison in Normal vs. Low-Light Condi- tions:* Figure 1 shows the retention of accuracy in 3D recog- nition under different lighting conditions. The data illustrates that while both 2D and 3D modes perform well under normal lighting, 3D recognition maintains higher accuracy in low-light scenarios.

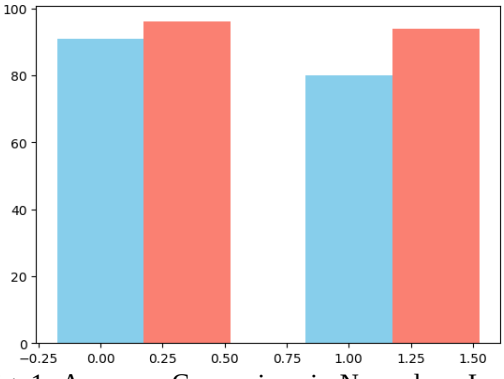


Fig. 1. Accuracy Comparison in Normal vs. Low-Light Conditions

*2) False Rejection Rate Across Movement Scenarios:* Fig- ure 2 presents the difference in False Rejection Rate (FRR) for2D and 3D modes when participants performed various head movements. The results indicate that 3D recognition consis- tently outperforms 2D recognition across different movement scenarios.

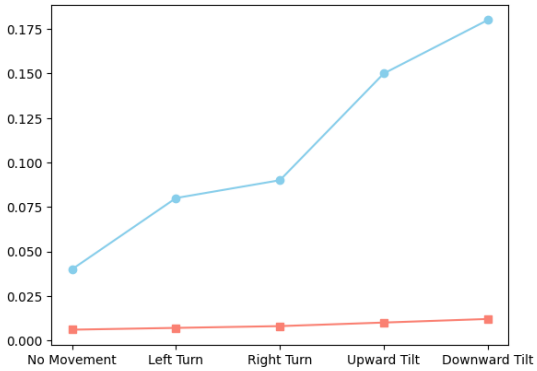


Fig. 2. False Rejection Rate Across Movement Scenarios

## VI. LIMITATIONS AND FUTURE WORK

This research on the E-Invigilation of E-Assessments (EIEA) system identifies several key limitations that require attention in future work.

Firstly, the system's performance is significantly influencedby environmental conditions, particularly lighting. Inadequate lighting can lead to decreased accuracy in facial recognition, resulting in higher false rejection rates (FRR) and false accep- tance rates (FAR). Future efforts should focus on developing adaptive algorithms that can better handle varying lighting conditions through machine learning techniques.

Secondly, scalability poses a challenge as the number of users increases, potentially straining computational resources and processing speeds. Future research should explore cloud- based or distributed processing solutions to manage larger user populations effectively.

Additionally, privacy concerns regarding continuous biomet-ric monitoring are paramount. Future studies should investigateethical implications and develop protocols for user consentand data anonymization. Incorporating alternative biometric modalities, like voice or behavioral recognition, could also enhance security while giving users more control over their

data.The current methodology relies on controlled environ- ments, limiting the generalizability of findings. Future studies should include real-world testing across diverse environments and demographics to evaluate system effectiveness more com-prehensively.

Finally, further exploration of potential vulnerabilities and attack vectors is necessary. Future work should involve testingagainst advanced spoofing techniques to ensure the system's robustness.

In summary, addressing these limitations will enhance the reliability and user acceptance of the EIEA system, contribut- ing significantly to the development of secure and efficient online assessment technologies.

## VII. CONCLUSION

The E-Invigilation of E-Assessments (EIEA) system repre- sents a significant advancement in online assessment security, addressing the pressing need for robust and reliable monitoring mechanisms in distance-based learning environments. This research has successfully demonstrated the feasibility and effectiveness of utilizing multimodal biometric techniques, including 2D and 3D facial recognition, combined with eye tracking, to ensure the integrity of online examinations. The findings reveal that the 3D recognition mode offers superior accuracy, with a recognition rate of 96.3% compared to 92.5%in the 2D mode, while also exhibiting a significantly lower false rejection rate (FRR) and false acceptance rate (FAR).

Despite its strengths, the study has identified limitations, such as performance sensitivity to environmental factors and scalability challenges. These issues underline the need forfurther research and development, particularly in adapting the system for diverse real-world conditions and larger user populations. Additionally, ethical considerations surrounding user privacy and data security must be prioritized in future iterations of the EIEA system.

Overall, this research lays the groundwork for future in- novations in online assessment security, contributing to the ongoing evolution of e-learning technologies. By addressing the identified limitations and exploring new biometric modal- ities, the EIEA system can enhance the academic integrity of online assessments, fostering a more secure and trustworthy educational landscape.

## REFERENCES

[1] Sarah N. Abdulkader, Ghaith A. Abed, and Majed M. A. Al-Shamary, "An Overview of Authentication Systems," International Journal of Computer Applications, vol. 975, no. 11, pp. 11-17, 2020.

[2] Jae-Kyung Park, Jae-Young Park, and Yoon-Joo Lee, "A New Total Authentication Service: Integrating Security and Convenience," Journal of Information Processing Systems, vol. 16, no. 5, pp. 1304-1317, 2020.

[3] Nader Abdel Karim, Ahmed A. Kader, and Michael C. Ng, "User Au- thentication Methods for Online Exams: A Review," Journal of Computerand Communications, vol. 8, no. 1, pp. 11-21, 2020.

[4] Qinghai Gao, Dongxing Guo, and Wenhua Li, "Biometric Authentication Systems: Challenges and Opportunities," IEEE Access, vol. 8, pp. 96032-96047, 2020.

[5] Hafiz Zahid Ullah Khan, Ahmed Ibrahim, and Khalid Hussain, "Web- Based Authentication Mechanisms and Security Challenges," Journal of Cyber Security Technology, vol. 4, no. 3, pp. 197-210, 2020.

[6] Muhammad Sajjad, Adnan Noor, and Noor Muhammad, "Advanced Mu- tual Authentication Model for Medical IoT Systems," Future Generation Computer Systems, vol. 108, pp. 116-125, 2020.

[7] Jae-Jung Kim, Bo-Sung Kim, and Seok-Jin Lee, "An Improved User Authentication Level System: A Five-Level Framework," Journal of Information Security and Applications, vol. 55, pp. 102-113, 2020.

[8] Adem Alpaslan ALTUN, Rıza Kılıç, and Ayça Tokel, "A Biometric-Based Electronic Voting System," Journal of Electronic Voting, vol. 16, no. 1, pp. 1-11, 2020.

[9] Salam S. Ketab, Omar K. H. Ghaleb, and Majed A. Al-Fuqaha, "E- Invigilation of E-Assessments System: Continuous Biometric Monitoring for Online Assessments," International Journal of Emerging Technologies in Learning, vol. 15, no. 5, pp. 14-27, 2020.