International Journal of Science, Engineering & Environmental

Technology (IJOSEET), 10(11): 71-79, 2023

ISSN0749-9650

www.repcomseet.org

A PROTOTYPE MULTI LEVEL AUTHENTICATION SYSTEM FOR MOBILE BASED EXAMINATION

Etudaiye Abdulmumuni Isah

Department, of Computer Science, Federal Polytechnic Ede, Osun State, Nigeria.

Author's Correspondence E-mail: mumeenbinissah@gmail.com

Abstract: In today's digital world, the demand for secure and reliable authentication systems for mobile-based examinations is ever-growing. Therefore, this paper proposes a prototype multi-level authentication system tailored specifically for mobile-based examinations, for the purpose of enhancing security and integrity while ensuring user convenience. The proposed system employs a combination of multiple authentication factors such as facial recognition, one-time passwords (OTPs) and Quick response codes to establish the identity of the test-taker. By leveraging these multi-level authentication mechanisms, the proposed system aims to mitigate the risks associated with unauthorized access, cheating, and impersonation during mobile-based examinations. The paper discusses the design principles, implementation details, and potential benefits of the proposed authentication system. Through this research, we endeavor to contribute to the advancement of secure and reliable authentication solutions suggested for the unique requirements of mobile-based Examinations.

Keywords: Authentication system, Facial recognition, Integrity, Mobile-based examinations, Multi-level authentication, One-time passwords (OTPs), Quick response code, Security.

1. Introduction

Computer-based examinations have surged in popularity due to the convenience and portability offered by mobile devices [4]. However, this trend also introduces new security challenges, particularly concerning examination malpractices. Cheating in computer-based examinations can manifest in various forms, including the use of unauthorized materials, sharing answers, or accessing the examination multiple times, thereby compromising the integrity of test results [10].

To address these challenges, multi-level authentication methods have been proposed. Regulatory bodies like the EU's Commission Implementing Regulation and NIST emphasize the importance of strong authentication processes involving multiple factors [4, 9]. Utilizing mobile devices for accessing examination resources can benefit from multi-level user identity verification, which enhances security [16].

Yet, the inherent risks of using mobile devices, such as the increased susceptibility to loss or theft, demand robust security measures [12]. Traditional authentication methods face challenges in the mobile environment, necessitating the adoption of mobile-specific security protocols [7].

Designing security protocols tailored to the mobile environment involves careful consideration of factors such as device characteristics and operating systems [9]. Combining different authentication factors, resistant to known attacks, further fortifies the authentication process [7].

Moreover, with the rise of online teaching and learning, online examinations have become indispensable. However, this shift brings forth concerns regarding examination security [4]. Authentication methods play a pivotal role in verifying user identities, with knowledge-based, token-based, and biometrics-based methods being commonly employed [6]. While passwords remain prevalent, biometric authentication offers enhanced security, albeit with its own set of challenges [7].

In light of these considerations, this work explores the intricacies of authentication in online examinations, delving into the challenges posed by mobile devices and the measures to mitigate associated risks.

2. Review of related works

In the work of [5], the authors proposed the use of Convolutional Neural Networks (CNN) to identify students accurately during online exams by monitoring their movements. However, CNN's limitations include the inability to analyze the orientation and position of students, as well as the requirement for a large amount of data to produce reliable results. It also did not conform to the EU, s Commission implementing regulation and the NIST identity guidelines [4 9]

In their recent work [13], the authors proposed a comprehensive authentication and examination process for online education systems. The system integrates various technologies and procedures to ensure the integrity and security of online examinations. Initially, students log in using their IP addresses, followed by the activation of an AI-based facial recognition system, along with a 360° AI view and noise detection system. The system then establishes an RDP (Remote Desktop Protocol) connection using SSH. Questions are shuffled and assigned to each internet protocol/ Identity (IP/ID), with specific time limits for answering each question. After collecting all answer scripts, plagiarism checks are performed, and scripts with plagiarism above seventy percent are flagged for potential collaboration. Marks are then forwarded to a block chain-based system for storage and verification. Scripts with plagiarism below seventy percent are sent for marking, and the marks are subsequently forwarded to the block chain system. This approach ensures the integrity of online examinations by detecting and preventing potential cheating behaviors. Overall, the work presents a robust solution to the challenges associated with conducting secure online examinations however the use of IP address poses a danger in spoofing while also introducing a lot of complexities due to the integration of block chain methods that requires more computing resources.

In their paper titled "A face detection method via ensemble of four versions of (You Only Look Once) YOLOs," presented at the 2022 International Conference on Machine Vision and Image Processing (MVIP), [7] propose an innovative approach to face detection using an ensemble of YOLO versions. The study introduces a real-time ensemble model that combines the results of YOLO v1 to v4 for improved face detection accuracy. Through rigorous experimentation using the WIDER FACE benchmark dataset, the authors demonstrate the efficacy of their ensemble method in significantly increasing the mean Average Precision (mAP) across images of varying difficulty levels. The results indicate substantial improvements in face detection performance, highlighting the potential of ensemble models in enhancing object detection tasks. Overall, [7] work contributes valuable insights to the field of computer vision and offers a promising approach for advancing face detection technology. This works provides fresh insight to the adoption of machine learning in the area of biometric authentication, it however not flexible for use in the context of mobile examinations.

The proposed system in [1] integrates palm print recognition with the traditional username-password combination for authentication. While this approach leverages an emerging biometric feature, palm print authentication, and ensures continuous surveillance through webcam supervision, it may not be practical for a mobile environment. Constant webcam monitoring could be cumbersome on mobile devices due to their limited resources and battery life. Additionally, palm print recognition might require specialized hardware or high-resolution cameras, which may not be readily available on all mobile devices.

In contrast, [11] suggests using keystroke patterns along with traditional username and password authentication, claiming low implementation costs and continuous surveillance without compromising privacy. However, this method may also face challenges in a mobile environment. Mobile keyboards vary widely in size and layout, making it difficult to accurately capture and analyze keystroke patterns across different devices. Moreover, mobile users often switch between multiple devices, which can lead to inconsistencies in typing patterns, reducing the accuracy and reliability of this authentication scheme. [3]

[2] Proposes a system for monitoring distance learning exams using IP addresses and timestamps. While this method does not require special hardware, its effectiveness is limited in a mobile environment. Mobile devices frequently change IP addresses as users move between networks, making it challenging to accurately track and authenticate users based solely on IP addresses [2]. Furthermore, mobile users can easily bypass IP-based authentication by using VPNs, undermining the security of the system.

A profile-based authentication framework combined with user ID and password is presented in [15]. Although this approach requires no special hardware and offers simple implementation, its efficacy in a mobile environment may be compromised. Mobile users often share devices or use multiple devices interchangeably, making it difficult to

maintain the uniqueness and secrecy of challenge questions. Moreover, mobile devices are susceptible to theft or loss, increasing the risk of unauthorized access to user profiles and compromising authentication security.

Another approach, based on yaw angle variation [14], utilizes webcam audio and video capture for authentication. While this method does not necessitate special hardware, its practicality in a mobile environment may be limited. Mobile devices vary in their camera quality and positioning, which can affect the accuracy and reliability of yaw angle variation analysis. Additionally, mobile users may encounter challenges in consistently positioning their devices for effective audio and video capture, potentially compromising the authentication process.

It's noteworthy that these authentication schemes do not fully comply with EU Commission implementing regulations and NIST guidelines on multifactor authentication, further highlighting the need for robust and adaptable authentication solutions, especially in mobile environments.

This research aims to facilitate the secure and efficient use of mobile devices for conducting examinations without compromising examination integrity. To achieve this goal, a prototype multi-factor authentication system suggested specifically for mobile-based examinations is designed and developed which will incorporate the use of facial recognition, QR Code, One Time Passwords(OTP) in addition to the traditional Username/Password and thus meets the European Union(EU) and National institute of Standards and Technology(NIST) requirements on authentication.

3. Design Methodology

The prototype beta version of the multi-factor authentication system for mobile examination integrates multiple distinct authentication factors: Username/Password, facial recognition, QR code scanning, and OTP verification. This comprehensive approach aims to bolster security measures while ensuring a seamless user experience.

3.1.1 Username/Password Authentication

In conjunction with the other proposed authentication factors, the system incorporates traditional username/password authentication as a foundational security measure. This aspect of the authentication process allows users to initiate the authentication procedure by inputting their unique credentials, consisting of their matriculation number and a corresponding Remita Retrieval Reference (RRR) number used during school fees payment.

3.1.1.1 Username/Password

Users commence the authentication process by providing their matriculation number, which serves as their username.

As an additional security measure, users are required to input a unique Remita Retrieval Reference (RRR) number, which functions as their password. The RRR number, generated by the Remita platform, serves as a secure identifier for users accessing the examination system.

3.1.2 Facial Recognition

Facial recognition plays a pivotal role in the authentication process. Feature Extraction is used to extract relevant features from the detected facial movements, such as head orientation and eye movements. These features provide valuable information about the students' engagement and potential cheating behaviors. Real-time images captured during the authentication process are meticulously compared against this pre-registered data using complex algorithms. Before comparison, the system will implement preprocessing techniques of feature extraction to enhance the accuracy of facial recognition. By incorporating facial recognition as an additional biometric authentication factor, the system will be able to significantly enhance security by verifying the user's identity based on unique physiological characteristics.

3.1.3 QR Code Scanning

The authentication process is initiated by the exam administrator or invigilator, who scans a unique QR code displayed on the student's mobile device using their own mobile device. This QR code serves as a cryptographic token, establishing a secure connection between the student's device and the authentication server. The secure connection facilitates the deployment of the OTP code necessary for completing the authentication process.

3.1.3 OTP Verification

Upon successful completion of the QR code scanning and facial recognition steps, students receive a one-time password (OTP) via app notification. The OTP serves as the final authentication factor, further fortifying the security of the authentication process. Students enter the OTP into the application to validate their identity and complete the verification process. Subsequently, they gain access to download the exam material and commence the examination.

3.2 The MobileExamAuth Framework.

To develop the proposed prototype multi-level authentication system for mobile examination in an android mobile environment, we develop the following conceptual model.

3.2.1 Interactions:

3.2.1.1 Authentication Initiation

User triggers authentication by entering username/password (UPA) and initiates facial recognition (FR).

3.2.1.2 QR Code Authentication

Examiner scans QR code (QRS) to establish a secure connection for OTP deployment (OTPV).

OTP Verification.

User receives OTP (OTPV) and enters it for final authentication.

3.2.2 Mathematical model.

The following represents the process of authentication

Username/Password Authentication (UPA)

UPA: AUPA= {u, p} 3.2.2.1

Where u represents the username (matriculation number) and p represent the password (RRR)

Facial Recognition (FR)

The facial recognition authentication is defined by

FR: AFR = {f1, f2, f3…fi} 3.2.2.2

Where fi represents the facial features captured and compared against pre-registered data.

QR Code Scanning (QRS)

QRS: AQRS = {qr} 3.2.2.3

Where qr represents the unique QR code scanned by the examiner

One-Time Password (OTP) Verification (OTPV)

OTPV: AOTPV = {otp} 3.2.2.4

Where otp represents the one-time password received by the student for verification.

To determine the authentication scheme for the multi-level authentication for mobile examination, we denote the authentication process as A, which encompasses the successful completion of all four authentication factors:

$A = UPA \cap FR \cap QRS \cap OTPV$ 3.2.2.4

Where:

UPA represents the Username/Password Authentication factor,

FR represents the Facial Recognition factor,

QRS represents the QR Code Scanning factor, and

OTPV represents the OTP Verification factor.

Thus all four factors must be successfully completed for the overall authentication process to succeed.

Figure 1 shows the schematic diagram of the proposed multi factor authentication system for mobile examination.

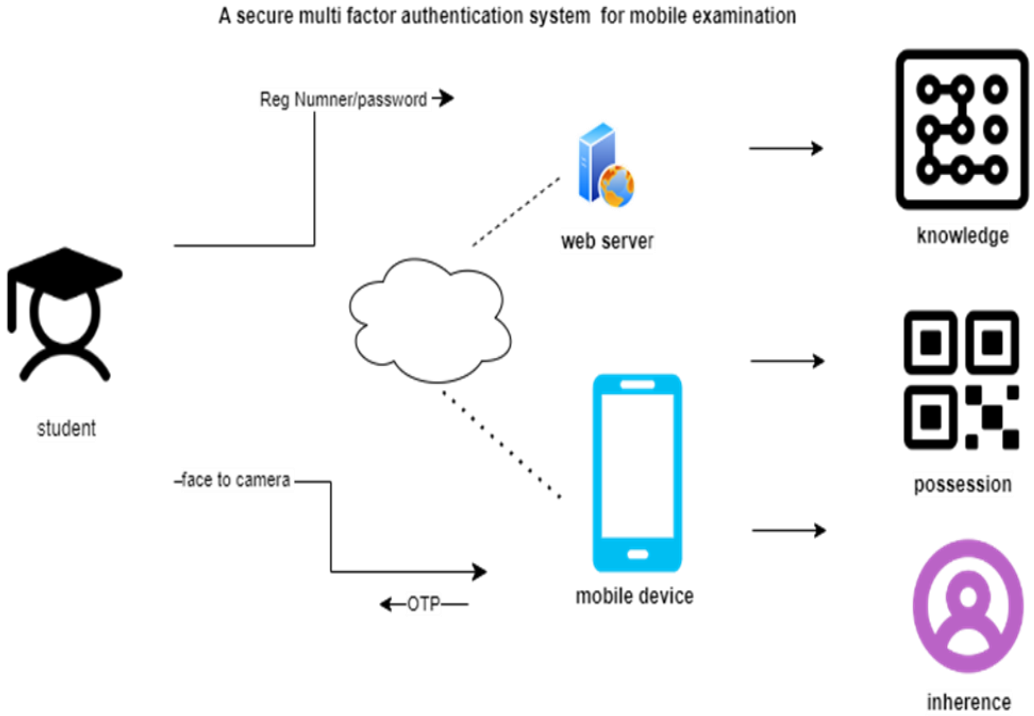

Fig 1. System Architecture for Multi-level authentication system for Mobile Examination

Figure 1 l depicts a conceptual representation of a secure multi- level authentication system for mobile examinations, showing the three main authentication factors: knowledge, possession, and inherence. Here's an explanation of each term and how they relate to authentication.

3.3.1 Knowledge

Knowledge refers to something that the user knows, such as a password, PIN, or security challenge response.

In the context of Multi-level authentication system for Mobile Examination, knowledge-based factors require students to demonstrate knowledge of their Matriculation number and Remita Retrieval reference (RRR) that is unique to them.

3.3.2 Possession

Possession refers to something that the user has, such as a physical token, smart card, or mobile device.

Possession-based factors involve users providing or presenting an object or device they possess to authenticate their identity.

In the context of the prototype Multi-level authentication system for Mobile Examination, possession based factors requires that the student gets their device scanned via QR code in their device.

Inherence:

Inherence refers to something that is unique to the user, typically based on biometric characteristics like fingerprints, facial features, or iris patterns.

Inherence-based factors rely on biometric data to authenticate users by verifying their unique physical traits.

In the context of the prototype Multi-level authentication system for Mobile Examination, inherence based factors requires that the student gets their facial image captured by the camera on their respective mobile device.

In this context, Multi-Factor Authentication (MFA): MFA combines two or more of these authentication factors to provide stronger security than using a single factor alone.

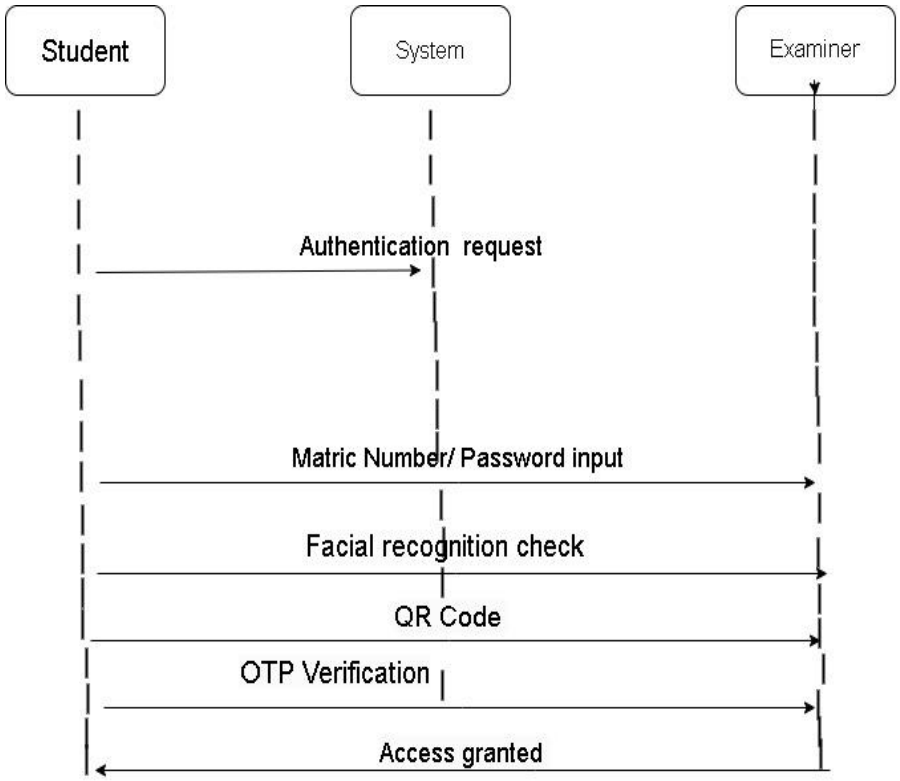

Fig2. Sequence diagram of the Proposed Multi level authentication system for Mobile Examination.

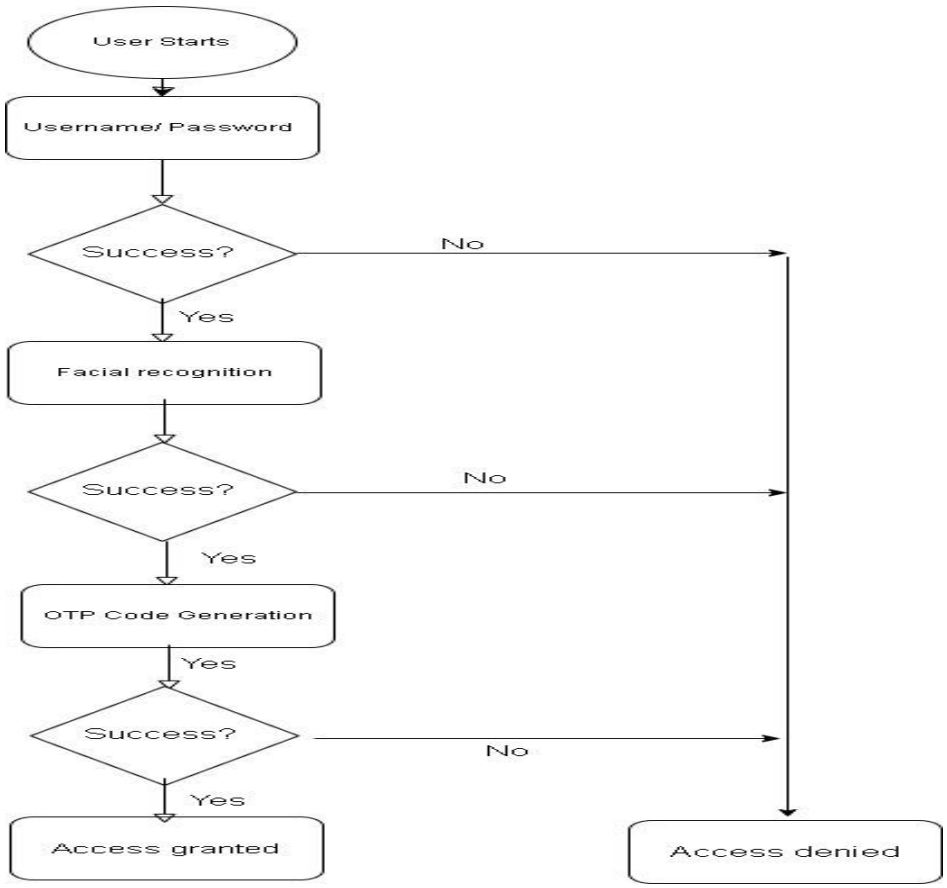

Fig 3. Activity diagram of the Multi-level authentication system for Mobile Examination

4.0 Implementation

The implementation phase of the multifactor authentication system for the mobile examination application is undergoing active development. We are currently focusing on refining the prototype and enhancing the system's functionality to meet the requirements of both students and examiners.

4.1 Key Features under Development:

4.1.1 Comprehensive Modules

We are designing and developing two distinct modules within the application, catering specifically to the needs of students and examiners at the Federal Polytechnic Ede, Osun State. This modular approach ensures that each user group has access to features tailored to their role, maximizing usability and effectiveness.

4.1.2 Username/Password Authentication

Users will initiate the authentication process by entering their username (matriculation number) and a password (Remita Retrieval Reference number). This traditional form of authentication provides an initial layer of security to verify the user's identity.

4.1.3 Facial Recognition Authentication

Upon login, users will undergo facial recognition authentication to securely verify their identity. Advanced facial recognition algorithms (feature extraction) are being implemented to accurately authenticate users based on their facial features.

4.1.4 QR Code Authentication

Following successful facial recognition, users will be prompted to scan a QR code to add an additional layer of authentication. This QR code authentication process establishes a secure connection between the user's device and the authentication server, enhancing overall security.

4.1.5 One-Time Password (OTP) Verification

After completing the QR code authentication, users will receive a one-time password (OTP) on their device via Firebase token. This OTP serves as an additional verification step, further strengthening the security of the authentication process.

4.1.6 Access to Examination Materials

Once authenticated, users can seamlessly download examination questions and access other relevant materials through the application’s interface. This ensures a smooth and efficient examination experience for all users.

4.1.7 Current Status:

We are actively developing and rigorously testing the application's functionalities. While the prototype version includes hardcoded login credentials, future iterations will incorporate user account creation capabilities to enhance flexibility and usability.

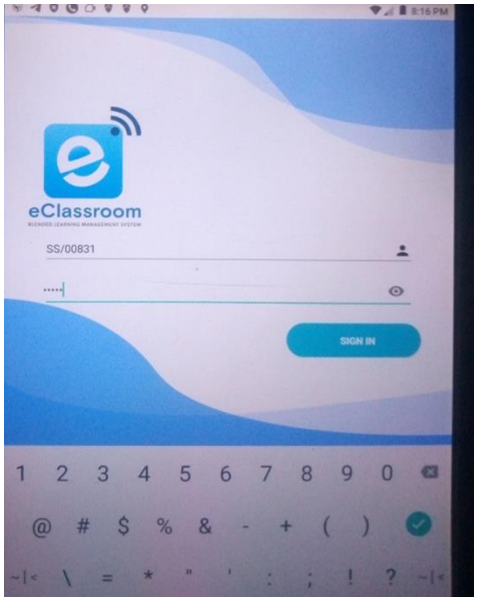

Fig 4.0 Prototype showing Examiners Login screen

5.0 Conclusion and Recommendations.

This study addressed the need for a robust multi-factor authentication system for mobile examinations. The method adopted involved integrating various authentication factors, including username/password, facial recognition, QR code scanning, and OTP verification, to enhance security and user experience.

Our findings so far demonstrated that the implementation of these authentication factors can effectively mitigate security threats such as unauthorized access and cheating during online examinations. The combination of biometric authentication with traditional username/password and OTP verification promises a comprehensive security framework that meets regulatory requirements.

Based on the preliminary results obtained, we recommend the widespread adoption of multi-factor authentication systems in mobile examination platforms to safeguard the integrity of online assessments. Future works will involve

further refining the authentication process, completing the software design, exploring additional biometric modalities, and enhancing user interface design to streamline the authentication experience.

References

1. Al-Saleem, S. M., & Ullah, H. (2014). Security considerations and recommendations in computer-based testing. Scientific World Journal, 1.

2. Bartłomiejczyk, M., Imed, E. F., & Kurkowski, M. (2019). Multifactor Authentication Protocol in a Mobile Environment. IEEE Access, 7, 157185-157199. https://doi.org/10.1109/ACCESS.2019.2948922

3. Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. Computer Networks, 170, 107118. https://doi.org/10.1016/j.comnet.2020.107118

4. COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502

5. Gao, Q. (2012). Using IP Addresses as Assisting Tools to Identify Collusions. International Journal of Business, Humanities, and Technology, 2(1).

6 Jiang, B., Li, X., Liu, S., Hao, C., Zhang, G., & Lin, Q. (2022). Experience of Online Learning from COVID-19: Preparing for the Future of Digital Transformation in Education. International Journal of Environmental Research and Public Health, 19(24), 16787. https://doi.org/10.3390/ijerph192416787

7. Khalili, S., & Shakiba, A. (2022). A face detection method via ensemble of four versions of YOLOs. In Iranian Conference on Machine Vision and Image Processing, MVIP. http://dx.doi.org/10.1109/MVIP53647.2022.9738779

8. Noorbehbahani, F., Mohammadi, A., & Aminazadeh, M. (2022). A systematic review of research on cheating in online exams from 2010 to 2021. Education and Information Technologies, 27. https://doi.org/10.1007/s10639-022-10927-7

9. National Institute of Standards. (n.d.). NIST SP 800-63-3. Retrieved from https://doi.org/10.6028/NIST.SP.800-63-3

10. Onyema, E. M. (2019). Opportunities and challenges of the use of mobile phone technology in teaching and learning in Nigeria—a review. International Journal of Research in Engineering and Innovation, 3(6), 352-358.

11. Ramu, T., & Arivoli, T. (2013). A framework of secure biometric-based online exam authentication: An alternative to traditional exam. International Journal of Scientific & Engineering Research, 4(11).

12. Reciprocity. (n.d.). How to Apply Cybersecurity Measures to Reduce Risk? Retrieved from https://reciprocity.com/blog/apply-cybersecurity-measures-to-reduce-risk/

13. Sattar, M. R. I. (2023). An advanced and secure framework for conducting online examination using blockchain method. Elsevier.

14. SwathiPrathish, Narayanan, S. A., & Bijlani, K. (2016). An Intelligent System for Online Exam Monitoring. In Information Science (ICIS), International Conference.

15. Ullah, A., Xiao, H., Lilley, M., & Barker, T. (2012). Using challenge questions for student authentication in online examination. International Journal for Informatics, 5(3).

16. Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. Computer Networks, 170, 107118. https://doi.org/10.1016/j.comnet.2020.107118