A Multi-Layered AI-Driven E-Proctoring System Using Wearable EEG and Secure IoT Integration for Cheating Prevention and Cybersecurity in Online Exams

Qutaiba Ibrahim * and Hussein Mahmood

Posted Date: 12 November 2025

doi: 10.20944/preprints202511.0738.v1

Keywords: e-proctoring; remote exams; cheating detection; cybersecurity; IoT; wearable technology; artificial intelligence; EEG; moodle; safe exam browser

 doi:10.20944/preprints202511.0738.v1

Article

A Multi-Layered AI-Driven E-Proctoring System Using Wearable EEG and Secure IoT Integration for Cheating Prevention and Cybersecurity in Online Exams

Qutaiba I. Ali * and Hussein Mahmood

University of Mosul, Mosul/Iraq

* Correspondence: Qut1974@Gmail.com

Abstract

With the proliferation of remote education and online assessments, maintaining academic integrity while ensuring cybersecurity has become a critical challenge. This paper proposes a comprehensive and intelligent e-proctoring system that integrates Artificial Intelligence (AI), wearable EEG technology, and secure Internet of Things (IoT) components within the Moodle learning management environment. The system combines multiple security and proctoring techniques: webcam-based facial and environmental monitoring, EEG signal analysis via a Muse2 headband for real-time stress and identity detection, and a restricted examination environment enforced by the Safe Exam Browser (SEB). To ensure robust security, a layered defense model is employed, incorporating multi-factor biometric authentication, IPSec-based encryption, VPN tunneling, and entity verification through challenge-response protocols. Experimental evaluations validate the system's effectiveness in preventing and detecting cheating, while performance analyses confirm minimal network impact even under VPN-enforced encryption. The proposed solution demonstrates a scalable, secure, and intelligent approach to safeguarding academic integrity in digital education.

Keywords: e-proctoring; remote exams; cheating detection; cybersecurity; IoT; wearable technology; artificial intelligence; EEG; moodle; safe exam browser

1. Introduction

The rapid shift to online learning and assessments, accelerated by the COVID-19 pandemic, has underscored the critical need for robust e-proctoring systems [1–4]. Ensuring academic integrity in remote settings presents unique challenges, including preventing cheating and securing sensitive data from cybersecurity threats [5–7]. Traditional proctoring methods, reliant on physical presence, are inadequate for online environments. Consequently, research efforts have focused on developing innovative e-proctoring solutions that leverage advanced technologies to address these challenges [8–10].

Relevant research on e-proctoring systems can be categorized into three key themes: system design, cheating prevention and detection, and security risks.

1. **System Design:** Existing research on e-proctoring system design explores various approaches to monitor exam environments and enhance academic integrity. Atoum et al. [11] developed a multimedia analytics system using webcams and microphones to detect cheating behaviors through continuous analysis of key behavior cues, including gaze estimation and phone detection. Attallah and Ilagure [12] investigated the feasibility of integrating wearable devices, such as Google Glass and Muse headbands, into e-proctoring systems to improve monitoring capabilities. Sabbah [13] proposed two e-exam models, one with human proctors and another utilizing continuous bimodal biometric authentication (fingerprints and keystrokes) for increased automation and scalability. Hietanen [14] focused on the security and scalability of various e-exam approaches, proposing a threat model based on the STRIDE methodology and outlining mitigation strategies for potential

 doi:10.20944/preprints202511.0738.v1

threats. Muzaffar et al. [15] conducted a comprehensive review of 53 research papers, identifying key features, tools, and algorithms for developing e-exam systems, emphasizing the importance of considering infrastructure and cost factors in system selection.

2. **Cheating Prevention and Detection:** Researchers have proposed various methods to counter cheating in online exams. Karim and Shukur [16] conducted a systematic review of user authentication methods, highlighting the advantages of biometric-based methods in preventing impersonation. Dawson [17] examined cheating vulnerabilities in the Bring-Your-Own-Device (BYOD) scenario, identifying five hacking techniques and suggesting mitigation strategies. Bawarith [18] developed an e-exam management system incorporating fingerprint authentication and eye tracking to detect cheating behaviors during the exam session. Karabaliev et al. [19] compared the security features of Safe Exam Browser (SEB) and LockDown Browser (LDB), recommending SEB for its stricter restrictions and Moodle integration. Tiong and Lee [20] proposed using machine learning algorithms, including DNN, LSTM, and Dense LSTM, to detect cheating based on IP address analysis and behavioral patterns.

3. **Security Risks:** Addressing security risks is crucial for ensuring the reliability and integrity of e-proctoring systems. Foster [21] identified privacy and cheating as the primary security concerns in online exams, recommending strategies such as test file protection and controlled browser environments to prevent fraud. Bandara et al. [22] proposed countermeasures for specific security risks, including brute force attacks, ARP poisoning, and cross-site scripting (XSS). Frankl et al. [23] described a secure exam environment at AAU, employing a LAN network, restricted operating systems, firewalls, and SEB to prevent unauthorized access and cheating. Slusky [5] explored cybersecurity vulnerabilities in both hybrid and fully automated e-proctoring systems, evaluating various authentication methods, including biometrics and blockchain technology. The study recommended technical controls such as lockdown browsers, endpoint security, VPNs, and VMs to mitigate risks associated with remote proctoring.

In addition to the above, research on EEG signal analysis has shown its potential for both cheating detection and user authentication. Koelstra et al. [24] developed the DEAP dataset for analyzing human affective states using EEG signals, demonstrating the feasibility of using EEG for emotion recognition. Rakhmatulin [25] employed deep learning and machine learning algorithms to classify alcoholism based on EEG data, highlighting the potential of EEG analysis for biometric identification.

This review of existing research reveals a growing body of work focused on developing secure and effective e-proctoring solutions. However, existing systems often face challenges in balancing scalability, security, and user privacy. This paper presents a novel e-proctoring system that integrates IoT devices, wearable technology, and AI algorithms with the Moodle LMS to create a comprehensive and secure platform for online examinations. The system combines cheating prevention and detection mechanisms, employing a specially designed examination device, monitoring cameras, and a Muse2 headband for EEG signal analysis. A robust multi-layered security model provides protection against potential cyber-attacks, ensuring data confidentiality, integrity, and availability.

2. System Architecture

The proposed e-proctoring system, as illustrated in Figure 1, comprises two main units: the Examination Room and the Monitoring and Control Room, connected via the Internet.

 doi:10.20944/preprints202511.0738.v1

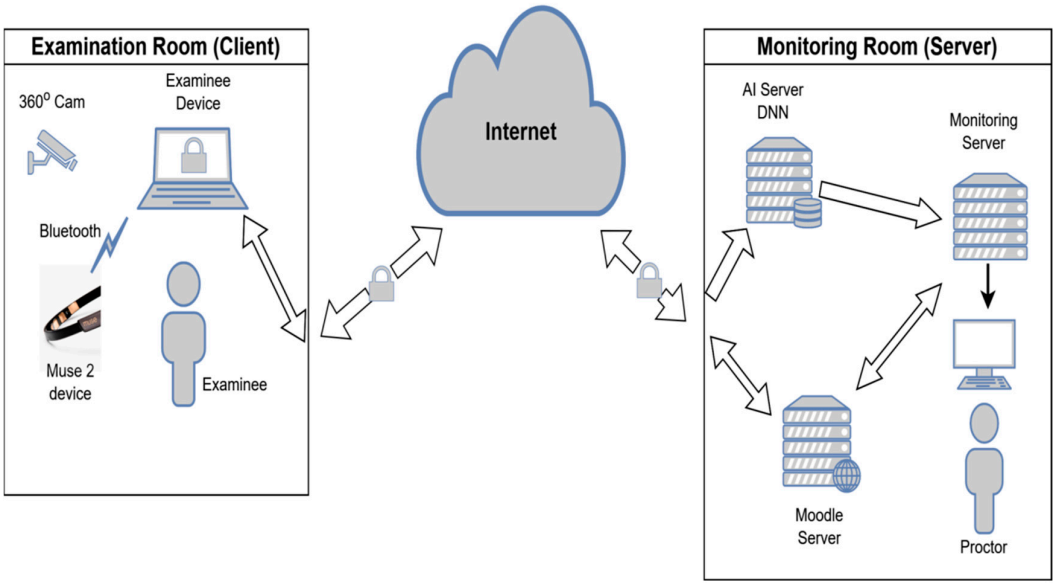


Figure 1. The proposed e-proctoring system.

2.1. Examination Room

The Examination Room environment includes the following components:

1. Monitoring Cameras: Two webcams are deployed for visual surveillance. The first webcam, integrated into the examination device, focuses on facial recognition and detecting suspicious head movements or facial expressions. The second webcam, a 360° camera, monitors the exam room environment to detect unauthorized individuals, devices, or resources. To conserve network bandwidth, video streams are transmitted randomly throughout the exam session and when the AI server flags suspicious activity.

2. Examination Device: A specially designed, locked, and restricted device (Figure 1) is provided solely for exam use. This device is configured during the registration phase with the SEB browser, which restricts access to internal device resources, external websites, unauthorized programs, and keyboard shortcuts, minimizing opportunities for cheating. The device remains active throughout the exam session to ensure continuous monitoring and prevent tampering.

Muse2 Headband: A wearable headband device records the examinee's EEG signal during the exam. This physiological data provides valuable insights into the examinee's cognitive state and is used for both user authentication and cheating detection.

2.2. Monitoring and Control Room

The Monitoring and Control Room houses the following servers:

1. AI Server: This server plays a crucial role in automating the proctoring process. It employs various AI techniques, including facial recognition, object detection, voice detection, and EEG signal analysis, to identify potential cheating attempts. The server continuously analyzes data from the monitoring cameras and the Muse2 headband, flagging suspicious activity for further review by human proctors.

2. LMS Server (Moodle): The Moodle platform serves as the LMS server, managing exam distribution, answer submission, and automated grading. Moodle's integration with the SEB browser provides an additional layer of security by restricting access to unauthorized resources during the exam session. Furthermore, the platform randomizes question sequences to minimize collusion among examinees.

3. Monitoring Server: This central server orchestrates the proctoring process, controlling communication between the AI server and the Moodle server. It grants access to exam questions upon

 doi:10.20944/preprints202511.0738.v1

successful user and device authentication, monitors the progress of each examinee, and alerts human proctors when suspicious activity is detected. The Monitoring Server serves as the central hub for controlling and overseeing the entire examination process.

3. System Operation

The proposed e-proctoring system follows a two-phase operational procedure:

3.1. Registration Phase

During the registration phase (Figure 2), the candidate creates an electronic profile by providing their name, photo, and biometric EEG data. The examination device is configured with the necessary SEB settings and passwords, and its unique device ID is recorded. The device is then locked and restricted, with instructions for the candidate to maintain its activation until the completion of the exam. This ensures that the device remains under continuous system control, minimizing the risk of tampering or unauthorized modifications.

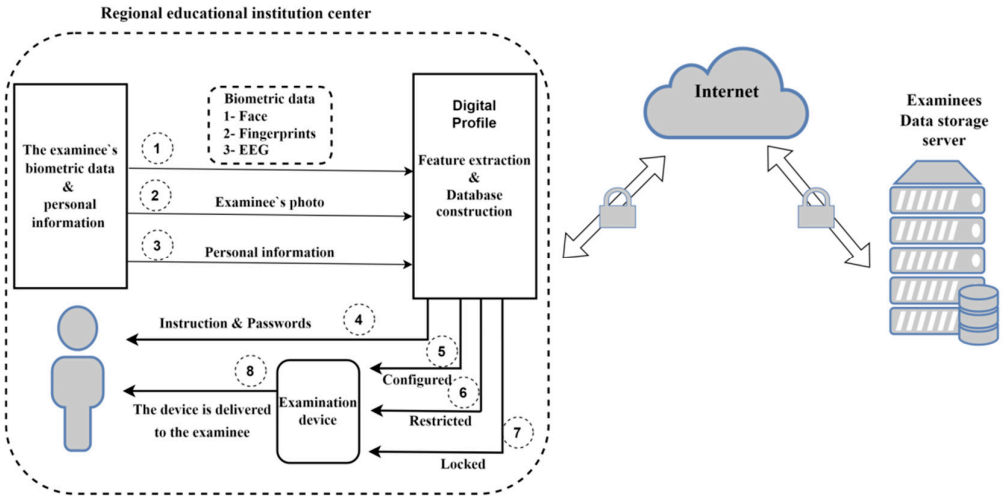


Figure 2. The registration phase.

3.2. Examination Session Phase

The examination session phase (Figure 3) involves the following steps:

1. Examinee Authentication and Instructions: Upon logging in, the examinee's EEG signal, camera data, and device information are transmitted to the AI server for authentication. The AI server verifies the user's identity based on the recorded EEG signal and facial recognition, ensuring that the registered individual is attempting the exam. Concurrently, the AI server authenticates the examination device using its unique ID and pre-configured SEB settings. After successful authentication, the Monitoring Server grants the examinee access to the exam questions.

2. Questions Answering: The examinee begins answering the exam questions. To further mitigate cheating, only one question is displayed at a time, and entity authentication is performed for each question request. The AI server continues to analyze the EEG signal for potential signs of cheating, while video streams are sent randomly and upon detection of suspicious activity.

3. Exam End Confirmation: To prevent accidental or premature termination, the exam is not officially concluded until the examinee confirms their intention to finish. Once confirmed, the answers are permanently stored and the exam session is closed.

 doi:10.20944/preprints202511.0738.v1

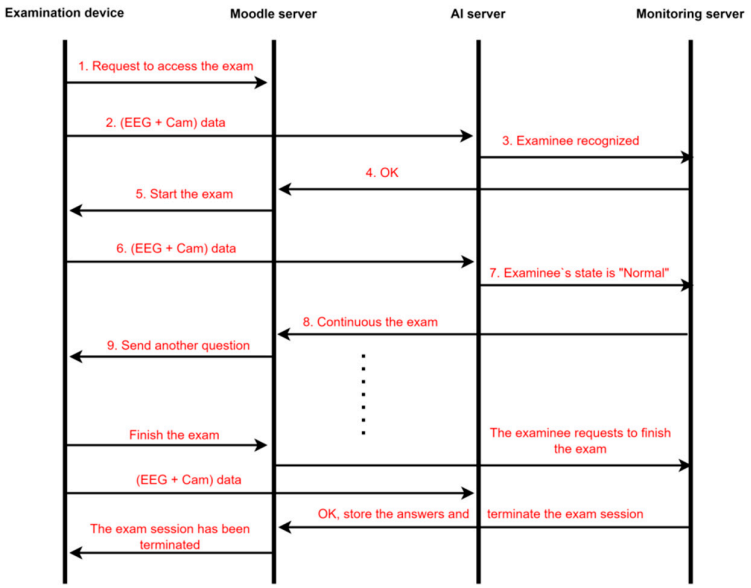


Figure 3. The examination session phase to the e-proctoring system.

4. Cheating Prevention and Detection Mechanisms

The proposed e-proctoring system employs a dual strategy to counter cheating:

4.1. Cheating Prevention

The integration of the SEB browser with the Moodle platform forms the cornerstone of the cheating prevention mechanism. SEB restricts the exam environment by limiting access to unauthorized resources, disabling keyboard shortcuts, and preventing the use of other applications during the exam session.

The effectiveness of SEB in mitigating cheating was tested by conducting exams with and without SEB activation. Table 1 summarizes the results of this experiment, showcasing the browser's ability to prevent access to unauthorized resources, block the execution of prohibited programs, and disable various cheating attempts.

Table 1. The response of cheating attempts in e-exams with SEB browser.

No.	Cheating attempt	Definition	Steps	Response with SEB	Countermeasure	Fail/ Success
1.	Unauthorized resources	Internal files and documents saved on the examinee`s device	The examinee tries to open files and documents to cheat	Unauthorized resources have been prevented	SEB uses the kiosk application which locks down the device	Failed
2.	Unauthorized programs	Like chatting programs, Some mathematics, and statistical programs	The examinee tries to open some programs to help solve the questions	Terminated by SEB browser	SEB uses the kiosk application which locks down the device	Failed
3.	Screen recording and Wireshark programs	Programs that record exam sessions to leak the questions,	The examinee tries to run screen recording software like Camtasia	Terminated by SEB browser	The administrator can add any program or software to	Failed

 doi:10.20944/preprints202511.0738.v1

		and network traffic analytical programs	to get a copy of the exam questions		the prohibited program`s list	
4.	Attempting the exam from unauthorized devices	The examinee can attempt the exam from any device he wants, which may be an uncontrolled device	The examinee pretends to attempt the exam from a controlled device but he uses another device	Not allowed	The administrator restricts the examine to use the controlled device with the legal configurations	Failed
5.	Ending the exam without confirming	The examinee can end the exam Incorrectly or unintentionally	The examinee ends the exam session and then he claims that he did not do that.	Password is needed to confirm ending the exam	The administrator restricts the examinee to enter the password	Failed
6.	Keyboard shortcuts & mouse right click	The examinee can use keyboard shortcuts and mouse right click to perform copy/ paste or other cheating tools	The use of these features can help the examinee to open some windows features like task manager	Not allowed	SEB uses the kiosk application which locks down the device	Failed
7.	Print screen	The examinee tries to print the exam screen to leak the questions to another person	This cheating attempt can help the examinee to get a copy of the questions	Not allowed	SEB uses the kiosk application which locks down the device	Failed
8.	Minimizing exam`s window	The examinee tries to minimize the window to open another app. or another web browser	This cheating attempt can help the examinee to open another app. or web browser	Not allowed	Setting the SEB browser on full- screen mode	Failed
9.	Virtual machine	Using a virtual machine to attempt the exam, so the examinee can open other web browsers and access unauthorized resources and programs	The examinee installs a V.Box and attempts the exam inside it, so he can cheat.	SEB Browser detects virtual machines	The administrator enables detecting virtual machine in the SEB configuration file	Failed
10.	Remote desktop	The examinee can attempt the exam from another device, so he can open other web browsers and access unauthorized resources	The examinee can follow some steps to enable this feature.	SEB Browser prevents remote desktop properties	The administrator enables detecting remote desktop in the SEB configuration file	Failed

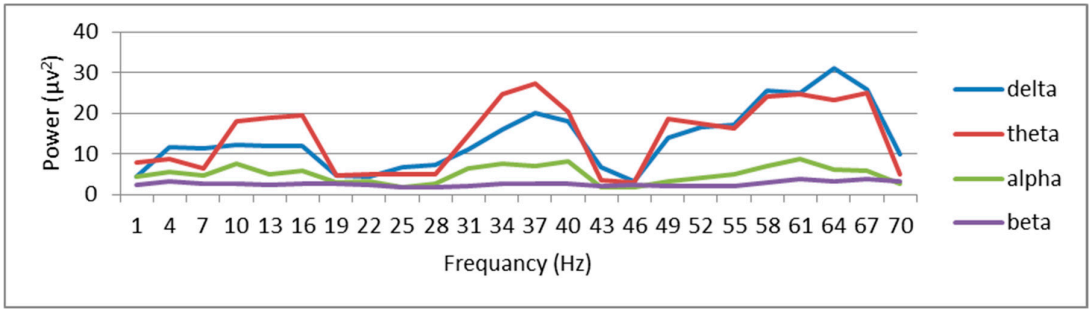
4.2. Cheating Detection

An innovative cheating detection method is implemented through the use of the Muse2 headband device. The device records the examinee's EEG signal during the exam, capturing physiological changes associated with stress. These changes can serve as indicators of potential

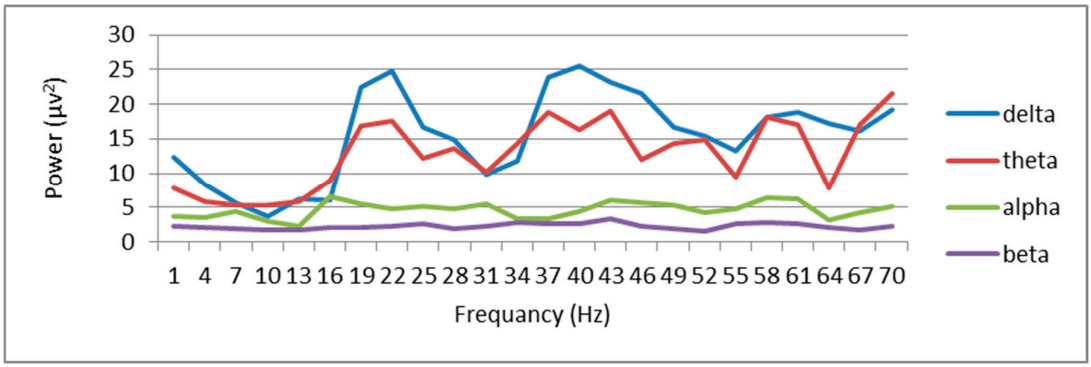
 doi:10.20944/preprints202511.0738.v1

cheating attempts, as examinees may experience heightened stress when engaging in unauthorized activities.

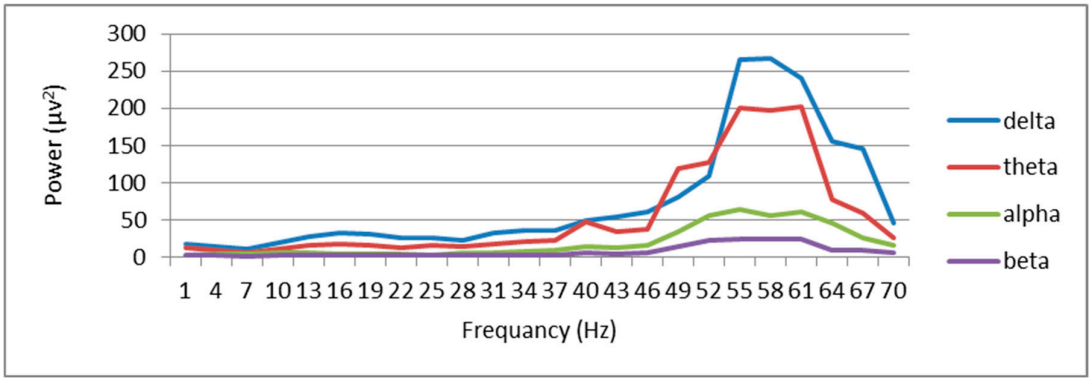
The recorded EEG data is analyzed using a Convolutional Neural Network (CNN) algorithm. The CNN model was trained on a dataset of EEG signals collected from 15 volunteers while they attempted an experimental electronic exam. The data included recordings under normal conditions and recordings during simulated cheating attempts, allowing the model to learn to differentiate between the two states. Figure 4 shows representative EEG signals for "Normal" and "Abnormal" states.



(a)



(b)



(c)

Figure 4. EEG signal for the "Normal" state (a) & (b), and the "Abnormal" state (c) for the same person.

 doi:10.20944/preprints202511.0738.v1

The trained CNN model classifies the examinee's state during the actual exam session as either "Normal" or "Abnormal." An "Abnormal" classification, indicating potential cheating due to elevated stress levels, triggers an alert to the Monitoring Server, prompting further review by human proctors.

The performance of the CNN model was evaluated using accuracy as the performance metric. Figure 5 displays the achieved accuracies for different EEG signal features, demonstrating the effectiveness of the approach. The system achieved an impressive accuracy of 97.37% for data with a 30-second duration (Table 2), indicating its high sensitivity in detecting abnormal EEG patterns associated with cheating.

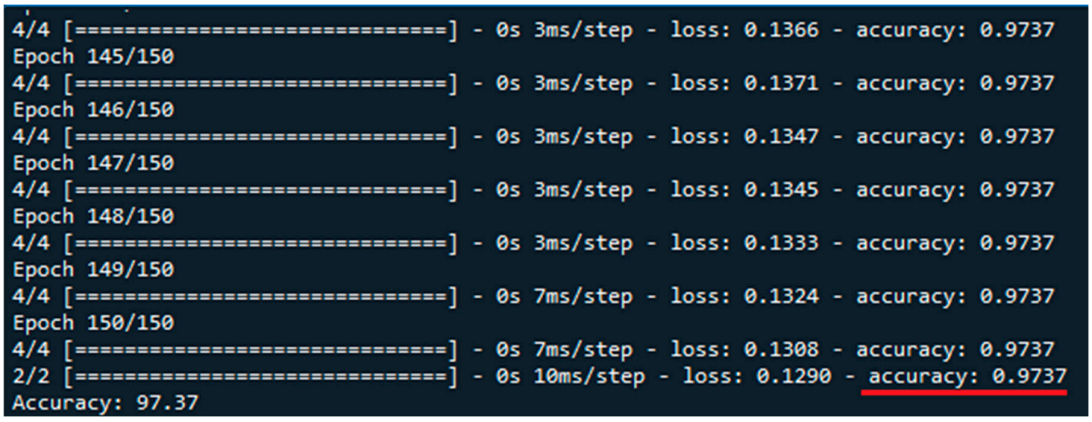


Figure 5. Achieved accuracy of the proposed system for data with 30s duration time.

Table 2. Obtained accuracy for each dataset of 30s duration time.

Power band	Accuracy %
Delta	73.68
Theta	63.16
Alpha	71.05
Beta	63.16
Gamma	57.89
Alpha-Beta	81.58
All bands	97.37

5. Cybersecurity Threat Mitigation

5.1. Threat Model

To effectively design a secure e-proctoring system, it is crucial to first identify and analyze potential cybersecurity threats. A threat model was developed to systematically assess vulnerabilities and potential attack vectors. Table 3 outlines the various components of the examination room and the associated breach methods.

Table 3. Security vulnerabilities for each component of the proposed system.

Component	Function	Breach method
The examinee	The individual that does the exam.	The attacker can impersonate the examinee ID.

 doi:10.20944/preprints202511.0738.v1

The examination device	Through it the exam will be done.	Disabling the device, changing its settings, Stealing the examinee's data, and Stopping its equipment such as the camera and microphone.
360o camera	Monitoring the exam environment of the examinee and the exam room remotely.	Disabling the device, Taking control of the camera and pointing it in a wrong direction.
Muse2 communication link	EEG data of the examinee are sent from the Muse2 device to the examination device through it.	Stopping sending EEG data of the examinee, inserting wrong EEG data.
Communication link to the Internet	All the examination data (the questions, the answers, the cam data, and the EEG data) between the examination device and the Internet are sent and received through it.	The attacker can steal the questions and/or the answers, change the questions and/ or the answers with the wrong ones, change the path of the data, steal the examinee's personal information, and other breaches.

The examination room components were further categorized based on their vulnerability to attacks, creating a hierarchical ordering as shown in Figure 6. This hierarchical model aids in prioritizing security measures and allocating resources to address the most critical vulnerabilities.

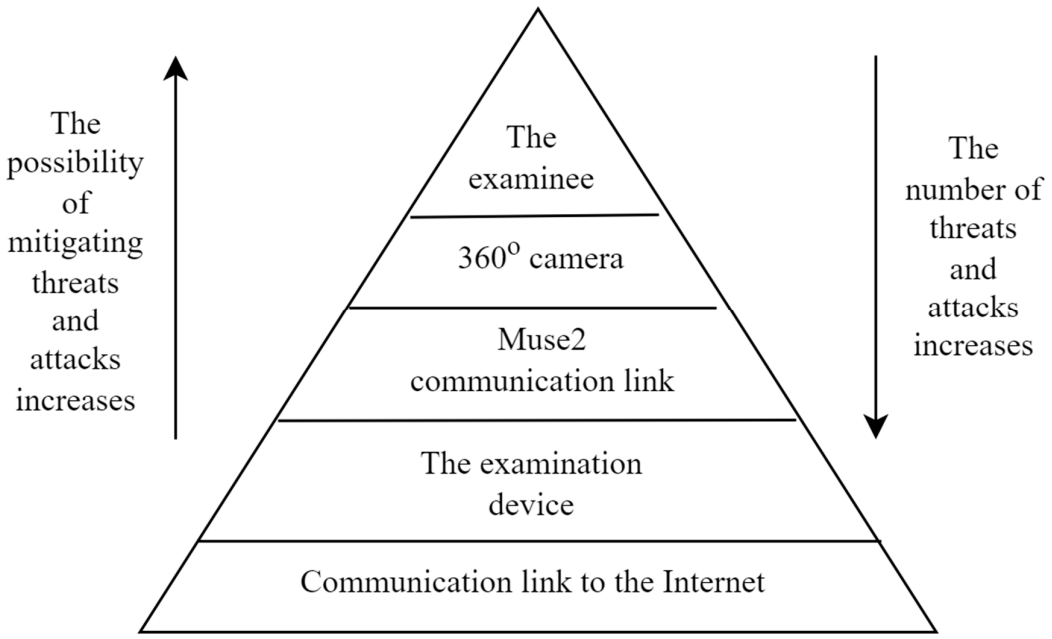


Figure 6. The hierarchical ordering of the examination room`s components of the proposed system.

Table 4 lists the potential cyber threats and attacks identified through the threat modeling process, providing a concise description of each attack type.

 doi:10.20944/preprints202511.0738.v1

Table 4. Potential threats and attacks to the proposed system.

Attack type	Description
1. Masquerading	The attacker uses a fake identity, to gain unauthorized access to the system to damage the system or do the exam instead of a real examinee.
2. Replay attack	The attacker simply sends a data element (e.g. a question) which was previously sent, in the hope of confusing the examinee.
3. Man-in-the-middle	The attacker positions himself in a conversation between the examinee and the server to steal the questions and/or the answers, modify them, or steal the personal information of the examinee.
4. Brute-force-attack	The attacker uses trial-and-error to guess login info, encryption keys, or find a hidden web page. One of the popular attacks is done by controlling the communication link and modifying packets maliciously.
5. Data injection	The attacker can run remote commands that can read or edit databases or update data on websites by injecting code into a program, query, or malware onto a machine.
6. Hacking attack	The attacker attempts to steal or modify data, and disable or breach the examination device to launch additional attacks.
7. Dos DDos	The attacker overburdens the system or the network by sending a deadly packet of requests that disrupt or delay the system's response.

Figure 7 visually depicts the potential attack points within the proposed e-proctoring system, highlighting the vulnerabilities of each component.

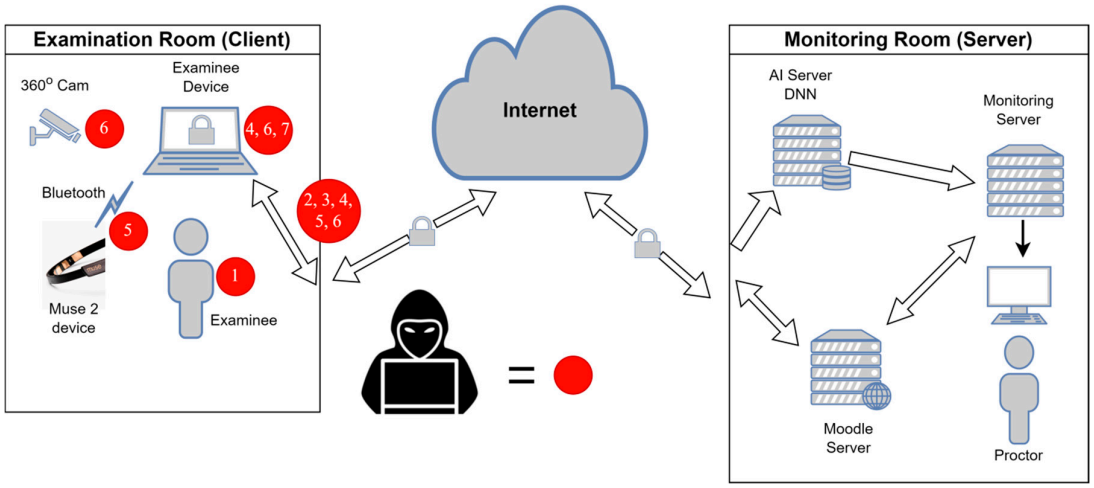


Figure 7. Possible cyber-attacks threaten the suggested examination room.

Table 5 maps the identified threats and attacks to the fundamental security principles of Confidentiality, Integrity, Availability, and Authenticity (CIAA). This mapping clarifies which security properties are most likely to be targeted by each attack type, guiding the selection of appropriate countermeasures.

 doi:10.20944/preprints202511.0738.v1

Table 5. The security property which is expected to be targeted by potential threats and attacks.

Attacks	Security property	Type
Masquerading	Authority, Integrity	Internal, External
Replay attack	Integrity	External
Man-in-the-middle	Confidentiality, Integrity	External
Brute-force-attack	Confidentiality, Integrity	External
Data injection	Integrity	Internal, External
Hacking attack	Confidentiality, Integrity	External
Dos DDos	Availability	External

5.2. Security Model

The proposed e-proctoring system incorporates a multi-layered security model to address the identified threats and vulnerabilities. The model comprises the following techniques [26–29]:

1. Two-way Entity Authentication: To ensure the legitimacy of both communicating parties, a two-way entity authentication mechanism is implemented. This mechanism uses a combination of the SEB's Browser Exam Key (BEK), the device's unique IPv6 address, and a challenge/response protocol (Figure 8). The BEK, generated by hashing SEB files and settings, serves as a unique identifier for the examination device. The IPv6 address ensures network-level identification, while the challenge/response protocol verifies the server's identity and protects against replay attacks. This multi-faceted authentication approach minimizes the risk of unauthorized access and impersonation attempts.

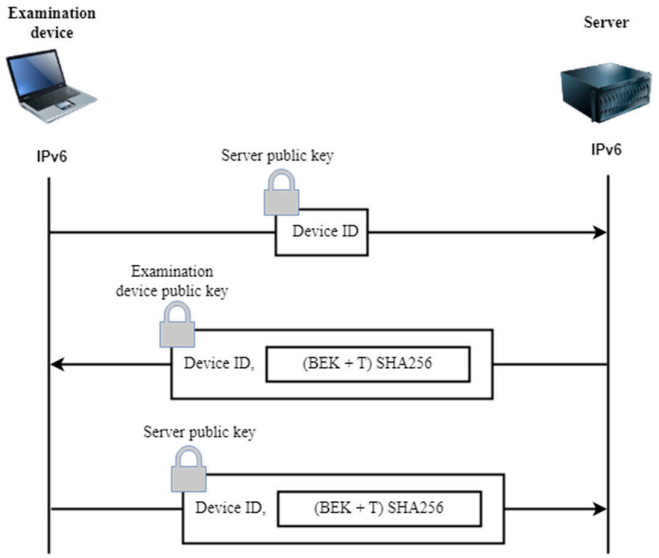


Figure 8. Entity Authentication procedure.

2. Data Encryption and Integrity: Confidentiality and integrity of transmitted data are paramount in a secure e-proctoring system. To protect data in transit, the system employs the IPSec protocol in ESP tunneling mode, providing end-to-end encryption and ensuring data integrity. Specifically, the system utilizes AES encryption, MD5 Hashed Message Authentication Codes (HMAC), and Diffie-Hellman Group 2 key exchange for robust protection against unauthorized access and data tampering.

 doi:10.20944/preprints202511.0738.v1

3. VPN and 4G/5G SIM Card: To further enhance security in unsecured communication channels, the examination device is equipped with a leased 4G/5G SIM card for Internet connectivity and utilizes a VPN tunnel. The dedicated SIM card eliminates the security risks associated with shared WiFi networks, while the VPN provides an additional layer of encryption and anonymizes the device's IP address, safeguarding against man-in-the-middle attacks and other network-based threats.

4. Packet Filtering Software: A signature-based Intrusion Detection System (IDS) is implemented to monitor network traffic in real-time, identifying and blocking malicious packets. The IDS utilizes a database of known attack signatures to detect intrusions and prevent unauthorized access to the system. This proactive approach strengthens network security and helps to mitigate Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

5. Multi-Factor Biometric User Authentication: To ensure continuous authentication throughout the exam session, the system employs multi-factor biometric authentication using both fingerprint and EEG data. Fingerprint authentication provides a robust and widely adopted method for identity verification, while EEG-based authentication leverages the uniqueness of an individual's brainwave patterns. Utilizing both modalities strengthens security and minimizes the risk of impersonation attempts.

Figure 9 provides a visual representation of the proposed security model, illustrating the integration of various security techniques to protect the e-proctoring system.

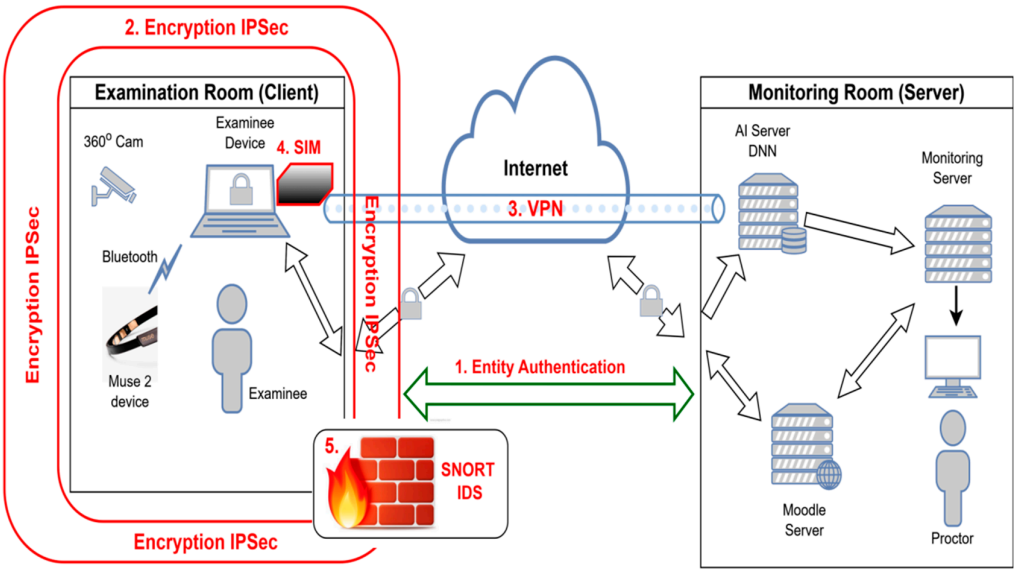


Figure 9. The general illustration of the suggested security model.

5.3. Security Model Evaluation

The proposed security model was rigorously evaluated by simulating various internal and external attack scenarios. Table 6 summarizes the assessment process, outlining the potential attack types, the vulnerable system components, and the corresponding countermeasures.

Table 6. Assessment of the suggested security model.

Attack type	The possible system part	Countermeasure method
Masquerading	The examinee, The examination device.	Biometric authentication, Entity authentication (IPv6, BEK, Private key, and Challenge/Response method).

 doi:10.20944/preprints202511.0738.v1

Replay attack	Communication link to the Internet.	Strong encryption method and sequence No. adopted by IPSec protocol.
Man-in-the-middle	Communication link to the Internet.	VPN and strong encryption method adopted by IPSec, 4G/5G SIM card.
Brute-force-attack	The examination device, Communication link to the Internet.	VPN and strong encryption method adopted by IPSec, 4G/5G SIM card.
Data injection	Communication link to the Internet, Muse2 communication link.	Ensuring message integrity by HMAC, VPN.
Hacking attack	The examination device, 360o camera.	Strong encryption method by IPSec, Packet-Filter firewall.
Denial of service (Dos), Distributed Denial of service (DDos)	The examination device.	Packet-Filter firewall.

The evaluation demonstrated the system's ability to effectively counter a wide range of security threats.

6. System Performance Analysis

A crucial aspect of any e-proctoring system is its impact on network performance. Excessive latency or reduced data rates can disrupt the exam experience for examinees and hinder the effectiveness of proctoring. To assess the performance of the proposed system, particularly the influence of the VPN connection, an electronic exam was conducted under two scenarios: without a VPN and with a VPN.

The exam consisted of multiple-choice questions, an essay question, and a mandatory file upload, simulating a realistic exam workload. Table 7 details the components and environment used for the performance analysis.

Table 7. The conducted exam components and environment.

Component	**Description**
Machine	Intel(R) Core(TM) i7-3632QM CPU @ 2.20GHz (with SSE4.2)
OS	64-bit Windows 10 (22H2), build 19045
Application	Dumpcap (Wireshark) 4.0.4 (v4.0.4-0-gea14d468d9ca)
Public IP address	85.31.41.130
VPN service software	Keep Solid VPN Unlimited
VPN server location	Hong Kong
Duration time of the exam	Nearby 350s

The network metrics analyzed included packet delay, packet lengths, data rate, and throughput. Figure 10 and Figure 11 illustrate the packet delays for the scenarios without and with a VPN connection, respectively. Table 8 and Table 9 present the distributions of packet lengths observed in

 doi:10.20944/preprints202511.0738.v1

each scenario. The data rates achieved in both scenarios are depicted in Figure 12 and Figure 13, while Figure 14 and Figure 15 show the throughput patterns. Table 10 summarizes the average values for each network metric in both scenarios.

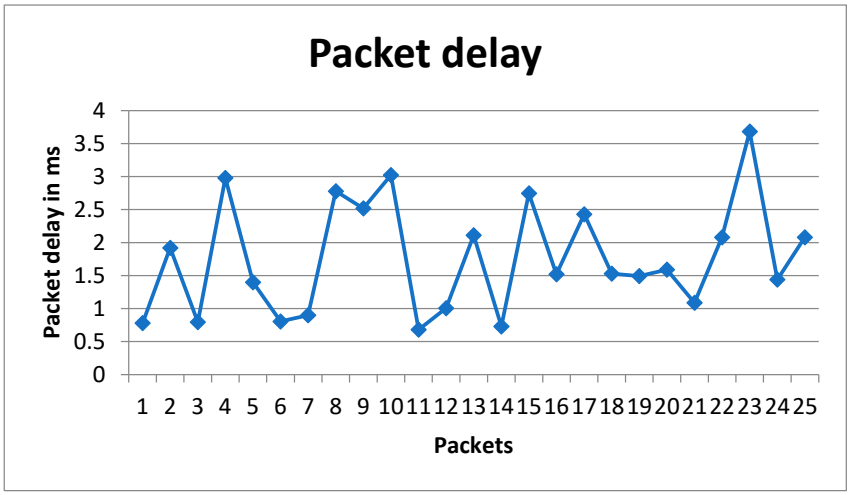


Figure 10. Packet delay without using VPN for some chosen packets.

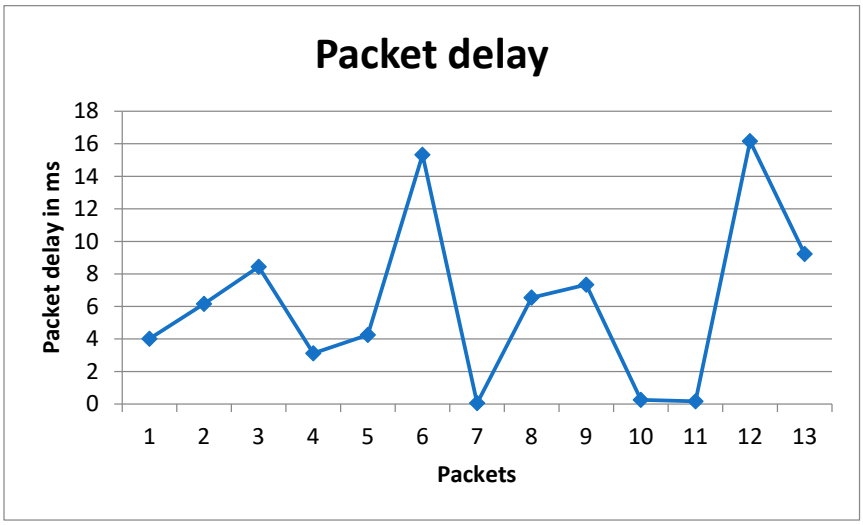


Figure 11. Packet delay with VPN for randomly chosen packets.

Table 8. Packet lengths sent during the exam session without VPN.

Average packet length	Count	Percent usage
75.59	46	2.60%
107.36	11	0.62%
207	1	0.06%
387.71	7	0.40%
944.8	10	0.57%
1291.97	1691	95.75%

 doi:10.20944/preprints202511.0738.v1

Table 9. Packet lengths sent during the exam session with VPN.

Average packet length	Count	Percent usage
58.15	2856	29.66%
152.48	464	4.82%
208.21	2486	25.82%
413.72	701	7.28%
892.86	282	2.93%
1403.63	2839	29.49%

Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
1,766	2.100 MiB	425	68.397 KiB	208.527481	138.0133	124.633 KiB

Figure 12. The obtained data rate without VPN.

IPv6 TCP · 1 UDP

Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
5,178	3.949 MiB	4,450	1.088 MiB	3.946086	331.8231	97.488 KiB

Figure 13. The obtained data rate with VPN.

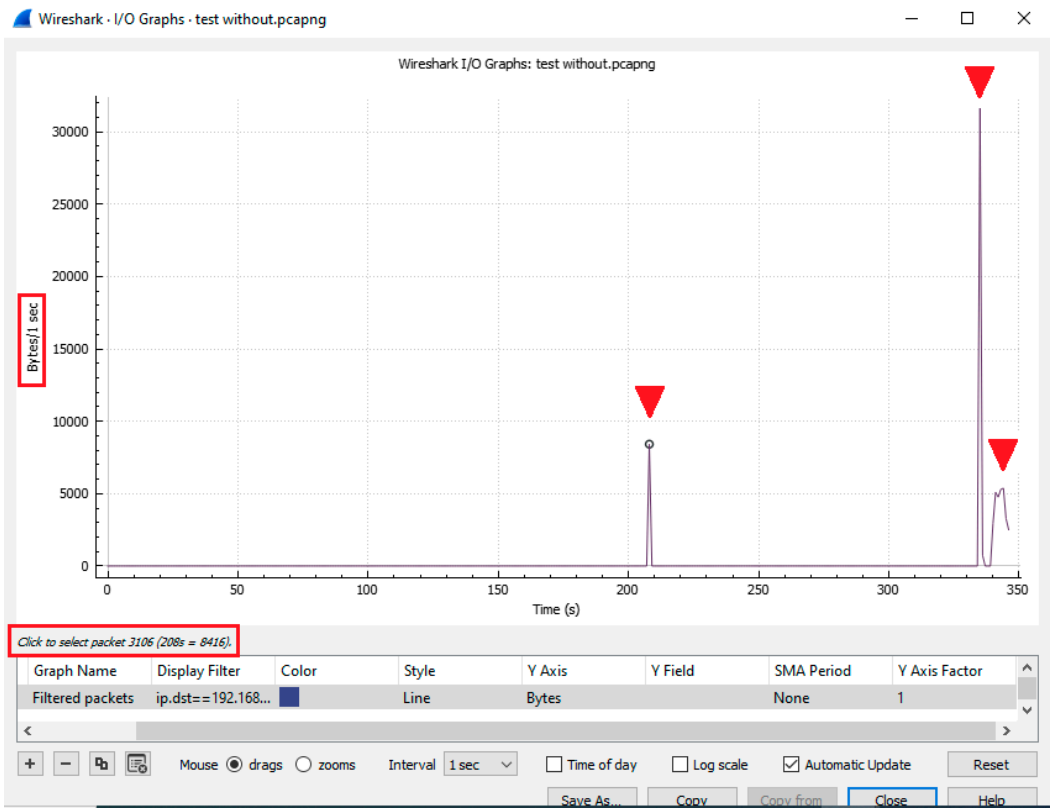


Figure 14. Throughput of captured exam session without VPN.

 doi:10.20944/preprints202511.0738.v1

Figure 15. Throughput of captured exam session with VPN.

Table 10. The obtained results of network metrics.

Network metric (average)	Scenario one without VPN		Scenario two with VPN	
Packet delay	2.15 ms		8 ms	
Packet lengths	76	2.60%	58	29.66%
	107	0.62%	152	4.82%
	207	0.06%	208	25.82%
	388	0.40%	414	7.28%
	945	0.57%	893	2.93%
	1292	95.75%	1404	29.49%
Data rate	Packets (A to B)	1766	Packets (A to B)	5178
	Bytes (A to B)	2.1 MB	Bytes (A to B)	3.949 MB
	Packets (B to A)	425	Packets (B to A)	4450
	Bytes	68.397 kB	Bytes	1.088 MB

 doi:10.20944/preprints202511.0738.v1

	(B to A)		(B to A)	
	Duration(s)	138.0133	Duration(s)	331.8231
	Bits/ second (A to B)	124.633 kB	Bits/ second (A to B)	97.488 kB
	Bits/ second (B to A)	3.964 kB	Bits/ second (B to A)	26.851 kB

The analysis revealed that the VPN connection, while adding minimal latency, did not significantly impact the overall network performance. The system maintained high data rates and throughput, even with the additional encryption and routing overhead introduced by the VPN. This demonstrates the feasibility of incorporating robust security measures without compromising the quality of the exam experience for examinees.

7. Proposed Pilot Study and Future Work

To evaluate the effectiveness, usability, and scalability of the proposed intelligent e-proctoring system, a pilot study is planned as a key step in future research. This pilot will serve to validate the system's core features—particularly its AI-driven cheating detection, wearable EEG-based biometric monitoring, and multi-layered cybersecurity framework—under semi-controlled conditions that simulate real-world online examinations. The results from this study will form the basis for refining the system before broader deployment.

7.1. Objectives of the Pilot Study

The proposed pilot study aims to achieve the following objectives:

1. Evaluate the usability and technical robustness of the complete e-proctoring system in a realistic exam setting.
2. Measure the reliability of EEG-based cheating detection, with specific focus on detecting abnormal stress patterns during exams.
3. Assess the impact of the system's security components, such as VPN, data encryption, and entity authentication, on overall network performance.
4. Collect qualitative feedback from users (students and instructors) regarding ease of use, perceived privacy, and acceptance of wearable technology.

7.2. Proposed Methodology

The study will involve approximately 20–30 volunteer students from the Computer Engineering Department in our University. Participants will be divided into two groups: a control group (standard exam session with no induced cheating) and an experimental group (with pre-defined simulated cheating scenarios such as attempting to use unauthorized resources or intentionally breaking focus).

Each student will be provided with a preconfigured exam device that includes:

- Safe Exam Browser (SEB) installed and locked to a specific Moodle exam session,
- Dual webcams for facial and environmental monitoring,
- A Muse2 EEG headband for real-time cognitive data acquisition,
- Enforced VPN connection over a 4G/5G SIM card.

During the session, the AI server will analyze video streams, facial recognition results, and EEG signals. The CNN model trained on labeled EEG data will attempt to classify brain states as either "Normal" or "Abnormal", the latter being a potential indicator of cheating behavior.

 doi:10.20944/preprints202511.0738.v1

The exam content will consist of 20 multiple-choice questions and a brief essay question, designed to complete within 30 minutes. SEB will restrict access to system resources, and continuous biometric and network activity logging will be enabled.

7.3. Expected Metrics and Analysis Plan

The following metrics will be collected and analyzed:

- True/False Positive Rates of cheating detection from the EEG classifier.
- Authentication delays, network packet delays, and throughput changes introduced by VPN and encryption layers.
- User feedback on usability and stress levels via post-exam surveys.
- System stability in terms of device crashes, connection losses, and response times under concurrent usage.

Data will be analyzed using standard statistical tools, and results will be compared across the control and experimental groups to evaluate model accuracy and system integrity.

7.4. Anticipated Challenges

The pilot study is expected to highlight several practical and technical challenges:

- EEG Signal Quality Variance: Differences in signal clarity due to improper Muse2 placement or user movement could affect the CNN model's accuracy.
- False Positives in Stress Detection: Elevated stress may not always indicate cheating. Future iterations of the model may require calibration to distinguish between stress caused by cheating vs. general exam anxiety.
- Privacy Concerns: Continuous biometric monitoring, especially EEG recording, may raise ethical questions that will need to be addressed through user consent, anonymization, and transparency.
- Network Constraints: Running the system on VPN and limited bandwidth may introduce latency, which needs to be minimized for scalability.

These challenges will guide future improvements to both hardware integration and AI model robustness.

7.5. Roadmap for Future Enhancements

Based on the findings of the pilot, the following enhancements are proposed for future development:

1. Personalized EEG Baselines: Introduce a pre-exam calibration stage to reduce false alerts by adapting the model to each user's normal EEG patterns.
2. Edge AI Implementation: Shift initial EEG processing and facial analysis to local (on-device) edge modules to reduce bandwidth consumption and improve real-time responsiveness.
3. Hybrid Behavioral Monitoring: Integrate additional behavior-based metrics (e.g., eye gaze, voice tone, keystroke rhythm) alongside EEG signals for multi-modal cheating detection.
4. Adaptive Security Policies: Develop a security orchestration layer that adjusts VPN and authentication levels dynamically based on threat levels and exam criticality.
5. Scalability and Institutional Integration: Conduct large-scale tests involving 100+ users and multiple institutions to validate scalability and promote system standardization.

7.6. Ethical Considerations and Compliance

As part of the future study, an ethical framework will be formalized to ensure compliance with privacy standards and institutional guidelines. This includes:

- Informed consent procedures for biometric data collection.
- Secure storage and anonymization of user data.
- Institutional review board (IRB) approval prior to deployment.

 doi:10.20944/preprints202511.0738.v1

Transparent communication with participants about what data is collected and how it is used will be central to gaining trust and ensuring ethical deployment.

The proposed pilot study will serve as a critical step in transitioning the e-proctoring system from a conceptual framework to a validated, deployable solution. It will allow the research team to evaluate system functionality under realistic conditions, identify improvement areas, and lay the groundwork for wider institutional adoption. Preliminary results and feedback from this study will significantly inform the system's future evolution, ensuring it balances effectiveness, user experience, and ethical integrity.

8. Conclusion

This paper has presented the design and proposed implementation of a secure, intelligent e-proctoring system that addresses the growing challenges of academic dishonesty and cybersecurity threats in online examinations. By integrating Artificial Intelligence (AI), Internet of Things (IoT) technologies, and wearable EEG-based biometric monitoring into a unified framework, the system aims to ensure academic integrity without compromising user experience or system performance.

The system introduces a multi-layered architecture that combines facial recognition, real-time environmental monitoring, EEG-based stress detection, and robust network security mechanisms—including VPN tunneling, IPSec encryption, and entity authentication protocols. Initial performance evaluations indicate that the system can support these features while maintaining acceptable levels of latency, throughput, and data integrity, even under encrypted network conditions.

The inclusion of EEG signals, captured using the Muse2 wearable headband, presents a novel approach to both examinee authentication and behavioral monitoring. The use of AI-driven classifiers, such as Convolutional Neural Networks (CNNs), demonstrates the feasibility of distinguishing between normal and suspicious cognitive states during exams. The layered security model further strengthens the platform by mitigating a broad spectrum of internal and external cyber threats, as identified through a comprehensive threat model.

Although the system has been conceptually validated and preliminary testing suggests high detection accuracy and system reliability, a more extensive pilot study is planned to rigorously assess its real-world applicability. This future work will focus on usability, signal reliability, ethical concerns, and scalability in institutional settings.

In summary, the proposed system offers a forward-looking solution to the persistent challenges faced by educational institutions in securing online assessments. By leveraging cutting-edge technologies in AI, biometric sensing, and cybersecurity, it contributes a holistic and practical framework for next-generation e-proctoring. Future enhancements and broader deployment can further refine the system, making it a viable candidate for widespread academic and professional examination environments.

References

1. K. Andersen, S. E. Thorsteinsson, H. Thorbergsson, and K. S. Gudmundsson, "Adapting engineering examinations from paper to online," in Proc. IEEE Global Engineering Education Conf. (EDUCON), Apr. 2020, pp. 1891–1895, doi: 10.1109/EDUCON45650.2020.9125273.
2. A. A. Alghamdi, M. A. Alanezi, and F. Khan, "Design and implementation of a computer aided intelligent examination system," Int. J. Emerging Technol. Learn. (iJET), vol. 15, no. 1, pp. 30–44, Jan. 2020, doi: 10.3991/ijet.v15i01.11102.
3. H. Li, M. Xu, Y. Wang, H. Wei, and H. Qu, "A visual analytics approach to facilitate the proctoring of online exams," arXiv preprint arXiv:2101.07990, Jan. 2021, doi: 10.1145/3411764.3445294.
4. S. L. Qaddoori and Q. I. Ali, "An efficient security model for industrial internet of things (IIoT) system based on machine learning principles," Al-Rafidain Eng. J. (AREJ), vol. 28, no. 1, 2023.

 doi:10.20944/preprints202511.0738.v1

5. L. Slusky, “Cybersecurity of online proctoring systems,” J. Int. Technol. Inf. Manage., vol. 29, no. 1, pp. 56–83, 2020.
6. N. Rjaibi, L. B. A. Rabai, A. B. Aissa, and M. Louadi, “Cyber security measurement in depth for e-learning systems,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no. 11, pp. 1–15, 2012.
7. Q. I. Ali and S. Lazim, “Design and implementation of an embedded intrusion detection system for wireless applications,” IET Inf. Secur., vol. 6, no. 3, pp. 171–182, 2012, doi: 10.1049/iet-ifs.2011.0152.
8. Q. I. Ali, “Securing solar energy-harvesting road-side unit using an embedded cooperative-hybrid intrusion detection system,” IET Inf. Secur., vol. 10, no. 6, pp. 386–402, 2016, doi: 10.1049/iet-ifs.2015.0180.
9. S. L. Qaddoori and Q. I. Ali, “An embedded and intelligent anomaly power consumption detection system based on smart metering,” IET Wirel. Sens. Syst., vol. 13, no. 2, pp. 75–90, 2023.
10. M. Ghizlane, B. Hicham, and F. H. Reda, “A new model of automatic and continuous online exam monitoring,” in Proc. Int. Conf. Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS), Dec. 2019, pp. 1–5, doi: 10.1109/SysCoBIoTS48768.2019.9028027.
11. Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, and X. Liu, “Automated online exam proctoring,” IEEE Trans. Multimedia, vol. 19, no. 7, pp. 1609–1624, Jul. 2017, doi: 10.1109/TMM.2017.2656064.
12. B. Attallah and Z. Ilagure, “Wearable technology: Facilitating or complexing education?,” Int. J. Inf. Educ. Technol., vol. 8, no. 6, pp. 433–436, 2018, doi: 10.18178/ijiet.2018.8.6.1077.
13. Y. W. S. Sabbah, “Proposed models for secure e-examination system,” Ph.D. dissertation, Faculty of Computers and Information, Cairo Univ., Cairo, Egypt, 2012.
14. J. Hietanen, “Security of electronic exams on students devices,” M.Sc. thesis, Aalto Univ., Espoo, Finland, 2021.
15. A. W. Muzaffar et al., “A systematic review of online exams solutions in e-learning: Techniques, tools and global adoption,” arXiv preprint arXiv:2010.07086, Feb. 2021. [Online]. Available: http://arxiv.org/abs/2010.07086
16. N. A. Karim and Z. Shukur, “Review of user authentication methods in online examination,” Asian J. Inf. Technol., vol. 14, no. 5, pp. 166–175, 2015.
17. P. Dawson, “Five ways to hack and cheat with bring-your-own-device electronic examinations,” Br. J. Educ. Technol., vol. 47, no. 4, pp. 592–600, Jul. 2016, doi: 10.1111/bjet.12246.
18. R. H. Bawarith, “Student cheating detection system in e-exams,” M.Sc. thesis, Faculty of Computing and Information Technology, King Abdulaziz Univ., Jeddah, Saudi Arabia, 2017.
19. M. Karabaliev et al., “Reliable and secure online exams during the COVID-19 pandemic,” in Proc. 15th Int. Conf. Virtual Learning, Univ. of Bucharest, Oct. 2020, pp. 326–331.
20. L. C. O. Tiong and H. J. Lee, “E-cheating prevention measures: Detection of cheating at online examinations using deep learning approach – A case study,” arXiv preprint arXiv:2101.09841, Jan. 2021. [Online]. Available: http://arxiv.org/abs/2101.09841
21. D. Foster, “Security issues in technology-based testing,” in Handbook of Test Security, New York, NY, USA: Routledge, 2011, ch. 3, doi: 10.4324/9780203664803.ch3.
22. I. Bandara, F. Ioras, and K. Maher, “Cyber security concerns in e-learning education,” in Proc. 7th Int. Conf. Education, Research and Innovation, Seville, Spain, Nov. 2014, pp. 728–734.
23. G. Frankl, P. Schartner, and D. Jost, “The Secure Exam Environment E-testing with students own devices,” in Tomorrows Learning: Involving Everyone, A. Tatnall and M. Webb, Eds., Cham, Switzerland: Springer, 2017, pp. 179–188, doi: 10.1007/978-3-319-74310-3_20.
24. S. Koelstra et al., “DEAP: A database for emotion analysis using physiological signals,” IEEE Trans. Affective Comput., vol. 3, no. 1, pp. 18–31, Jan. 2012, doi: 10.1109/T-AFFC.2011.15.

 doi:10.20944/preprints202511.0738.v1

25. I. Rakhmatulin, "Python (deep learning and machine learning) for EEG signal processing on the example of recognizing the disease of alcoholism," SSRN, 2020, doi: 10.2139/ssrn.3717324.
26. Q. I. Ali, "Enhanced power management scheme for embedded road side units," IET Comput. Digit. Tech., vol. 10, no. 4, pp. 174–185, 2016, doi: 10.1049/iet-cdt.2015.0123.
27. Q. I. Ali, "Green communication infrastructure for vehicular ad hoc network (VANET)," J. Elect. Eng., vol. 16, no. 2, pp. 10–10, 2016.
28. M. E. Merza, S. H. Hussein, and Q. I. Ali, "Identification scheme of false data injection attack based on deep learning algorithms for smart grids," Indones. J. Elect. Eng. Comput. Sci., vol. 30, no. 1, pp. 219–228, 2023, doi: 10.11591/ijeecs.v30.i1.pp219-228.
29. M. H. Alhabib and Q. I. Ali, "Internet of autonomous vehicles communication infrastructure: A short review," Diagnostic Pathology, vol. 24, no. 3, 2023, doi: 10.29354/diag/168310.