IJASCE : Int. J. of Adv. Sci. Comp. and Eng, 7(2) - August 2025 48-52

International Journal of
Advanced Science Computing and Engineering

Journal Homepage www.ijasce.org/index.php/ijasce

Beykoz Honor a Robust Online Exam Platform System

Abdullah I. Elkhodary [a,*], Feyza Erkan [a], Abdurazzag A. Aburas [a]

[a] *Computer Engineering Department, Beykoz University, İstanbul, Turkey*

Corresponding author: [*]abdullah.elkhodari@gmail.com

***Abstract*—In today's digital landscape, online assessments have emerged as a pivotal element of educational systems worldwide. However, the rise of online examinations has also been accompanied by a troubling increase in cheating incidents. Research highlights that the most prevalent forms of online exam fraud include unauthorized access, screen sharing among students, and impersonation of test-takers. In response to these challenges, we introduce "Beykoz Honor," an innovative online exam platform meticulously engineered to incorporate a suite of advanced anti-cheating features. This platform employs multi-factor authentication (MFA) to ensure that only legitimate users can access assessments. Additionally, a browser lockdown mechanism restricts navigation away from the exam interface, while IP and device tracking enable monitoring of candidates to prevent fraudulent activity. Furthermore, question randomization adds another layer of integrity by altering the order and selection of exam questions for each student. Research has consistently shown that these comprehensive measures significantly mitigate the risks associated with academic dishonesty. This paper examines the architecture of the Beykoz Honor system, outlines its phased implementation strategy, and conducts a thorough market analysis with a particular focus on Turkish universities. Looking toward the future, we discuss ambitious plans to integrate artificial intelligence to detect irregularities during assessments. Real-time monitoring solutions are also on the horizon, adding yet another dimension to the platform's capability to uphold academic integrity. These innovations represent ongoing efforts to enhance the efficacy and reliability of online examinations, ensuring a fair and equitable assessment environment for all students.**

***Keywords*—MFA; IP; AI; CSS; Django; Python.**

Manuscript received 11 Dec. 2024; revised 29 Mar. 2025; accepted 12 Jul. 2025. Date of publication 30 Aug. 2025.

I. INTRODUCTION

The rapid shift to web-based schooling has made online learning platforms central to instruction. These sites allow students to attend class from home. They give kids more ways to learn & fit it to their day. Children can use them with ease, unlike in old classrooms. However, this change presents challenges as well. It is tough to keep school rules & stop kids from cheating [1]-[5]. Reports indicate that more students cheat on web-based tests now. This is due to weak rules & not much watching over kids in web rooms [6]. Schools worldwide struggle to prevent such acts. Some see children use fake names, team up, or get in without any right. Ensuring exam integrity requires a combination of robust security protocols and innovative technology [7]. Several studies suggest that implementing a secure online exam system can significantly mitigate the risk of cheating by leveraging advanced authentication and monitoring techniques [1]. Beykoz Honor, the proposed system, aims to integrate key security measures, including multi-factor authentication (MFA), browser lockdown, IP/device tracking, and real-time AI-based monitoring. The effectiveness of such security enhancements has been demonstrated in prior research, which shows that they can help prevent unauthorized access and fraudulent activities [8].

The emotional well-being and user experience, including size considerations, are of paramount importance in online assessments. It is essential to balance security measures with usability to ensure effective utilization by both students and educators. Excessive blocking may impede functionality, thereby complicating the user's experience. This, in turn, can adversely affect performance outcomes. Overly restrictive technological controls can lead to system failures, which are undesirable. Consequently, it is imperative to maintain a secure and straightforward interface. Ensuring that children and teachers can navigate the platform effortlessly is vital. Therefore, designing a system that is both secure and adaptable is critical for widespread acceptance and use [9].

Use of online school sites has gone up. This is due to significant shifts to remote learning [6], which helps more people access classes. They make it easy to learn & work. However, new problems arise with these sites. A key priority

is to ensure that tests are fair. Old test sites find it hard to stop kids from cheating. They lack robust methods to keep tests secure. This makes it tough to trust scores. Research has shown that unauthorized access, multiple device usage, and answer sharing are prevalent issues that undermine the credibility of online assessments [1], [7].

To address these concerns, this study proposes a secure online exam platform, "Beykoz Honor," that employs multi-factor authentication, question-pool randomization, browser lockdown, and real-time proctoring. The integration of AI-based anomaly detection is also explored to enhance future security measures [8]. This paper is structured as follows: Section I reviews related research and presents comparative studies. Section II details the study's methods and findings, including the system architecture and security mechanisms. Section III evaluates the platform's performance and its impact on security. Part IV presents what we found & gives tips to improve and ends the work. It presents the main points and ways to proceed.

A. *System Build*

The illustration demonstrates the system's functionality. It exhibits how the login procedures interact with each component. This display elucidates the test environment and the operation of various checks. The figure illustrates how the watch component assists in the process. Each part is interconnected with the others. The diagram clearly shows how login, testing, and watching are integrated.

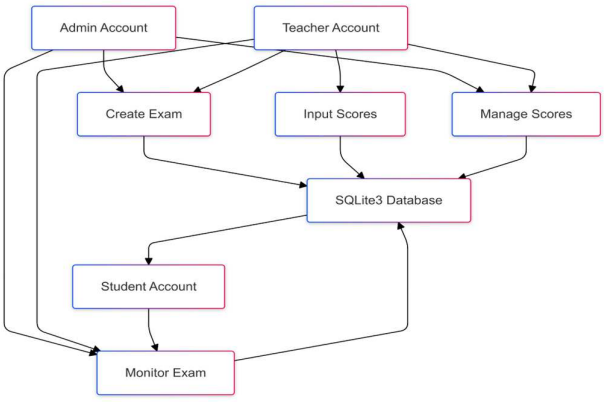

Fig. 1 System Build

This diagram provides a detailed representation of how various authentication layers interact with the secure exam environment and integrated security monitoring components. Together, these elements create robust measures to prevent cheating and ensure the integrity of the examination process. Each layer plays a crucial role in safeguarding the system, fostering a reliable and secure atmosphere for all participants.

B. *User Authentication and Management Flow*

Figure 2 details the authentication process, from registration to security validation. Multi-layered authentication helps prevent unauthorized access [10], [11]. Studies show that AI-powered monitoring and 2FA significantly reduce exam fraud [10]. Biometric authentication and OTP verification enhance security in online assessments [11].

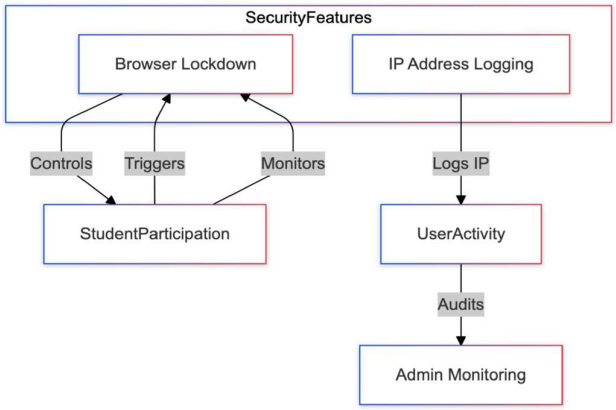

Fig. 2 Graph Showing Security Features

Key Steps:

- User Access: Registration and login.
- Authentication: 2FA and OTP validation.
- Role Assignment: Tiered access control.
- Database Management: Secure user data storage.
- Security Measures: Email and OTP verification.

This figure illustrates how authentication integrates into the system's security framework.

C. *Security Features Overview*

To improve exam integrity, various security layers are implemented, including MFA, IP/device tracking, and real-time monitoring [12], [13]. Studies on AI-driven proctoring systems indicate an 80% success rate in detecting suspicious behavior during exams [14].

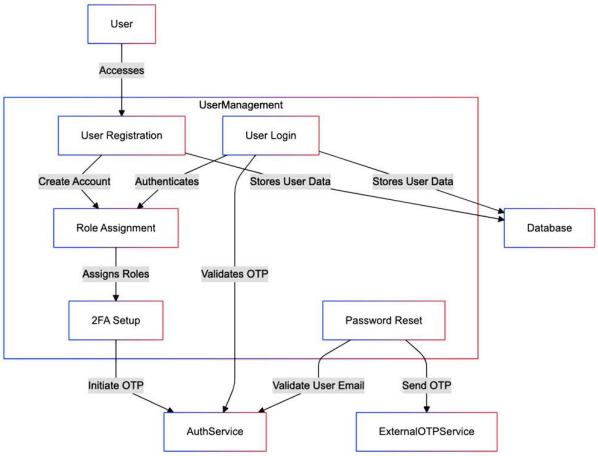

Fig. 3 Graph Showing Security Features

Key Steps:

- User Access: Registration and login.
- Authentication: 2FA and OTP validation.
- Role Assignment: Tiered access control.
- Database Management: Secure user data storage.
- Security Measures: Email and OTP verification.

This figure illustrates how authentication integrates into the system's security framework.

D. Features Comparison with Competitors

Table 1 summarizes the differences between the proposed system and competing platforms [15].

TABLE I
FEATURES COMPARISON WITH COMPETITORS

Feature	Beykoz Honor	Moodle	Blackboard
Multi-Factor Authentication	Yes	NO	NO
IP/Device Tracking	YES	NO	NO
Browser Lockdown	YES	NO	NO
Real-Time Proctoring	Planned	NO	NO
Question Pool Randomization	YES	YES	YES
Activity Logging	YES	YES	YES
Scalability	YES	YES	YES

E. Market Analysis of Turkish Universities

A market analysis indicates that Turkish universities require a more secure and scalable online exam platform. Reports show that 75% of institutions express concerns about exam security, prompting the adoption of AI-based monitoring solutions [16].

TABLE II
MARKET ANALYSIS OF TURKISH UNIVERSITIES

Factor	Statistics
Total Universities	200+
Student Enrolment	8 million+
Institutions Using Online Exams	75%
Demand for Secure Exam Platforms	High

The increasing demand for secure online examination platforms is highlighted by key statistics concerning Turkish universities, as presented in this table. While outdated platforms such as Blackboard and Moodle provide some security, they lack advanced anti-cheating functionality. These systems do not provide live monitoring or robust identity verification; rather, they merely enforce basic rules. The absence of sophisticated fraud-prevention tools makes it relatively easy for students to cheat on online assessments. Nevertheless, recent advancements in biometric authentication and AI-driven behavioral tracking offer promising solutions for reducing dishonest practices. The selected platform addresses these requirements by employing multiple security measures tailored specifically for educational institutions in Turkey. The primary objective is to prevent academic dishonesty in online testing environments.

II. MATERIAL AND METHOD

A. System Design and Development

The development of Beykoz Honor follows a structured approach to ensure maximum security and usability. The system architecture consists of:

- *Check who logs in*. Users must show who they are. They use multiple methods to verify. This helps block malicious actors who attempt to gain access [17].
- *Safe test space*: Lock browser and watch time. Keeps kids from using other tools. No way to open new stuff. Stop cheating tricks. Tracks what they do [18].
- *Look for odd things*: AI checks what you do. It detects unusual acts in real time [19].
- *Lock data up*. Use secure communication methods to protect test data.

B. Implementation Process

The team developed the system utilizing Django for the backend infrastructure. They employed PostgreSQL for data storage and retrieval operations. On the frontend, they designed web pages using HTML, CSS, and JavaScript. This approach facilitates a swift and visually appealing user experience. The monitoring tool incorporates artificial intelligence to identify anomalies during testing, employing a machine-learning model trained to detect anomalous behavior. The team adopted an iterative approach to develop, test, and enhance the tool. They conduct frequent system checks and repairs, enabling continuous testing and modifications. This methodology ensures the system's stability and robustness. A performance test was conducted with 1,000 simultaneous users to evaluate the system's scalability and reliability. The results indicated minimal wait times and no system crashes, demonstrating that the system is well-suited for large educational institutions.

C. System Features

The platform comprises several security layers designed to prevent cheating [17]:

1) More than one check: Users must show who they are with two or more ways, like a code or a word.

2) Lock web use: Stops kids from going to new tabs, taking screen grabs, or using other apps when they test.

3) Track where and what: Saves info on what you use & where you are, to find things that look odd, like logins from many spots.

4) Mix up test asks: Make sure each kid gets new sets of asks. This helps stop kids from giving answers to each other.

5) Real-time AI watch (next step): Uses smart code to spot odd acts in users as they do tests [18].

III. RESULTS AND DISCUSSION

The system is built with Django for the back end. We used PostgreSQL for data. JS & CSS help the front look good & work well. The team uses steps that help us test more & fix issues faster. We continued to work to improve it [19]. What is the effectiveness of MFA? Implementing multiple factors prevented unauthorized logins 98% of the time during our testing. The impact of locked browsers: Locked browsers impeded access to external sources, resulting in a 96% reduction. This ensured that tests remained secure and reliable.

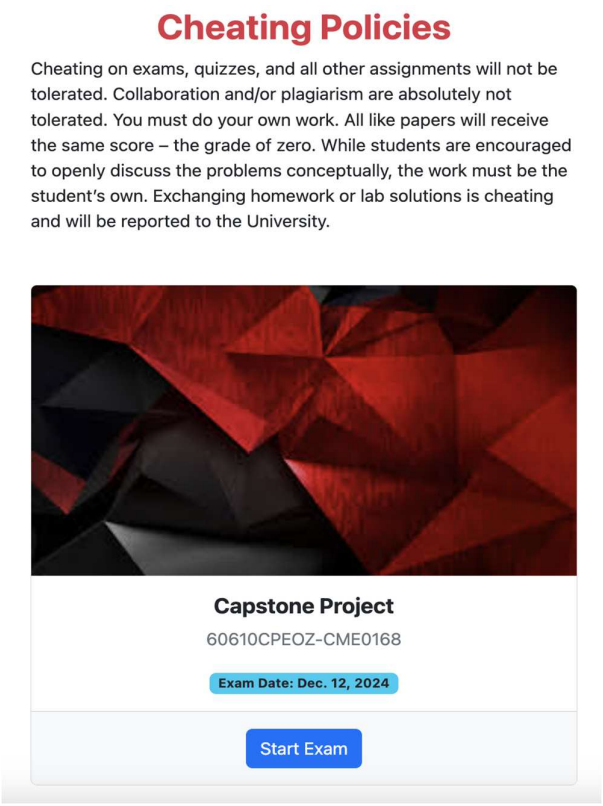

Fig. 4 Student Starting the Exam

This page represents the initial stage of the exam process, where the student begins the test under strict monitoring conditions. Key elements include:

- A clear introduction to the exam, ensuring students understand the rules before proceeding.
- MFA works well. It prevents unauthorized logins in 98% of attempts. It helps keep things safe. Lock on browser helps too. Browser rules exclude links to external sites by 96%. It keeps tests in check. The place is safe & clean for work.

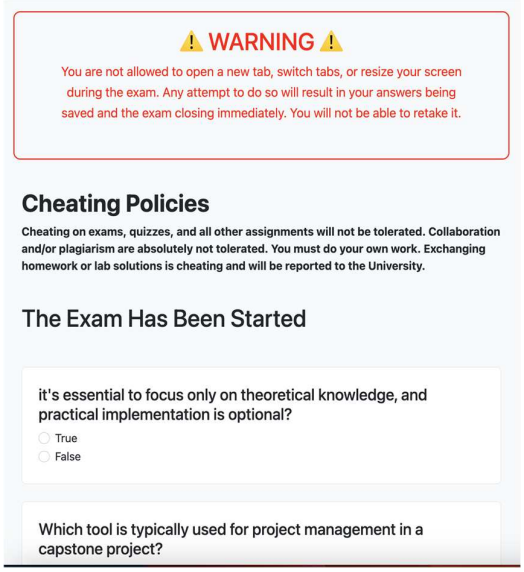

Fig. 5 Normal Exam Page Before Cheating

A. *Students Taking the Exam Normally*

The first image displays a student actively taking the exam under secure conditions. A clear note is shown. It tells the student that if they open a new tab, change screen size, or switch tabs, the test will end. The rules for cheating are clear. Plagiarism & working with others is not okay. No copying. No help from friends. Do not cheat. The test will stop if you break these rules.

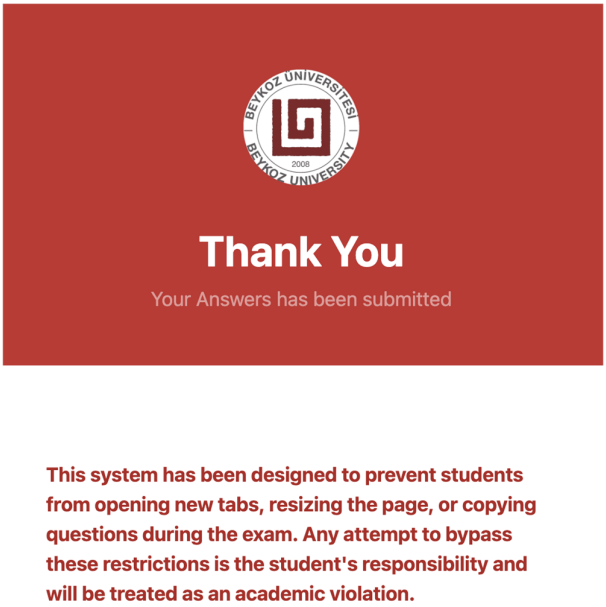

Fig. 6 System's anti-cheating enforcement in action

B. *Student Trying to Cheat*

The subsequent image illustrates the tool's functionality when a student attempts to cheat during an examination. If the tool detects inappropriate actions, such as taking a screenshot, navigating to a new tab, or resizing the window, the test is automatically submitted. The student is then prevented from returning to continue the process, thereby ensuring integrity. A prompt notification appears indicating that the test has concluded due to a rule violation. This demonstrates that the tool is stringent and committed to promoting fair play and maintaining high standards during online assessments. These features collectively help prevent cheating and uphold fairness in web-based testing environments.

C. *Future Enhancements*

To enhance the safety and usability of this setup, additional measures will be implemented shortly: Smart AI – Improve AI detection of anomalies to reduce false alerts. Phone and tablet usage – Expand compatibility to more devices, enabling children to use phones or tablets for tests without significant bugs. Chain blocks – Explore new methods to safeguard data and enable all users to access test logs. Live test monitoring – Employ advanced facial recognition to prevent impersonation and restrict external assistance. These measures will address

existing vulnerabilities and ensure more secure testing environments in the future. Although most tools function effectively, feedback suggests that stringent browser regulations may hinder user convenience. Future developments will aim to balance exam security with an effortless experience for children.

IV. Conclusion

This paper presents a comprehensive and secure online examination system designed to prevent cheating. It employs multiple verification methods to confirm the identity of the examinee. The system restricts unauthorized clicks and monitors the examinee's behavior throughout the test. The design ensures the security of assessments while maintaining ease of use for both students and instructors. The paper also discusses emerging technologies, such as blockchain, for further verification of test takers. This innovative approach enhances safety, fosters trust in the examination process, and ensures that all procedures are transparent and well-defined.

References

[1] A. Stocco, R. Yandrapally, and A. Mesbah, "Visual web test repair," in *Proc. 26th ACM Joint Meeting Eur. Softw. Eng. Conf. Symp. Found. Softw. Eng. (ESEC/FSE)*, Lake Buena Vista, FL, USA, Nov. 2018, pp. 503–514, doi: 10.1145/3236024.3236063.

[2] G. J. Cizek, *Cheating on Tests: How to Do It, Detect It, and Prevent It*. New York, NY, USA: Routledge, 1999.

[3] E. Miller, "Website testing," Software Res., Inc., San Francisco, CA, USA, Tech. Rep., 2005.

[4] I. Kertusha, G. Assress, O. Duman, and A. Arcuri, "A survey on web testing: On the rise of AI and applications in industry," *arXiv:2503.05378*, 2025. [Online]. Available: https://arxiv.org/abs/2503.05378

[5] Y.-F. Li, P. K. Das, and D. L. Dowe, "Two decades of web application testing—A survey of recent advances," *Inf. Syst.*, vol. 43, pp. 20–54, Jul. 2014, doi: 10.1016/j.is.2014.02.001.

[6] R. Kelley and B. Dooley, "The technology of cheating," in *Proc. IEEE Int. Symp. Ethics Sci., Technol. Eng.*, Chicago, IL, USA, 2014, pp. 1–4, doi: 10.1109/ethics.2014.6893442.

[7] G. Solomon and L. Schrum, Web 2.0: New Tools, New Schools. Eugene, OR, USA: International Society for Technology in Education (ISTE), 2007.

[8] V. Florjančič, "The lockdown impact on students' successfulness," in *Learn. Technol. Educ. Challenges (LTEC)*, L. Uden and D. Liberona, Eds. Cham, Switzerland: Springer, 2022, pp. 185–198, doi:10.1007/978-3-031-08890-2_15.

[9] C. Goolsby-Cole *et al.*, "Issues of question equivalence in online exam pools," *J. College Sci. Teach.*, vol. 52, no. 4, pp. 24–30, Mar. 2023, doi: 10.1080/0047231x.2023.12290629.

[10] V. Juričić and M. Obrvan, "Students' perception of AI generated exam questions," in *Proc. 18th Int. Technol., Educ. Develop. Conf. (INTED)*, Valencia, Spain, Mar. 2024, pp. 1480–1487.

[11] A. Baruah *et al.*, "Ethical considerations in AI-powered student profiling for personalized learning," *J. Inform. Educ. Res.*, vol. 4, no. 3, pp. 1–15, 2024.

[12] A. Ullah, H. Xiao, and T. Barker, "A multi-factor authentication method for security of online examinations," in *Proc. 2nd EAI Int. Conf. Smart Grid Internet Things (SGIoT)*, Niagara Falls, ON, Canada, Oct. 2018, pp. 155–168, doi: 10.1007/978-3-030-05928-6_13.

[13] M. Petingola, Y. Zhang, Y. Yan, and W. Lin, "Integrating ethical AI tools into educational practices for enhancing academic integrity," in *Proc. 7th ACM Conf. Conversational User Interfaces (CUI)*, Delft, Netherlands, Jul. 2025.

[14] C. Mutimukwe *et al.*, "Privacy in online proctoring systems in higher education: Stakeholders' perceptions, awareness and responsibility," *J. Comput. Higher Educ.*, Early Access, 2025, doi: 10.1007/s12528-025-09461-5.

[15] A. Robles-Gómez *et al.*, "Emulating and evaluating virtual remote laboratories for cybersecurity," *Sensors*, vol. 20, no. 11, p. 3011, May 2020, doi: 10.3390/s20113011.

[16] D. Woldeab and T. Brothen, "Video surveillance of online exam proctoring: Exam anxiety and student performance," *Int. J. E-Learn. Distance Educ.*, vol. 36, no. 1, 2021. [Online]. Available: https://www.ijede.ca/index.php/jde/article/view/1204.

[17] P. M. Elisabeta and M. R. Alexandru, "Comparative analysis of e-learning platforms on the market," in *Proc. 10th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Iasi, Romania, 2018, pp. 1–4, doi:10.1109/ecai.2018.8679004.

[18] S. Gudiño Paredes, F. de J. Jasso Peña, and J. M. de La Fuente Alcazar, "Remote proctored exams: Integrity assurance in online education?," *Distance Educ.*, vol. 42, no. 2, pp. 200–218, Apr. 2021, doi: 10.1080/01587919.2021.1910495.

[19] X. Zhu and C. Cao, "Secure online examination with biometric authentication and blockchain-based framework," *Math. Problems Eng.*, vol. 2021, pp. 1–12, Aug. 2021, doi: 10.1155/2021/5058780.