Anti Fraud Quiz App

Suresh babu U[1], Sai Srinivas K V[2], K Shiva Prasad[3], Gangadhara G H[4]
[1,2,3]*Department of CSE(AIML) RYMEC Ballari*
[4]*Assistant Professor, Department of CSE(AIML) RYMEC Ballari*

***Abstract*—Online examinations have become an integral part of modern education; however, maintaining academic integrity in remote assessment environments remains a critical challenge due to cheating, impersonation, and unauthorized assistance. To address these concerns, this paper presents the design and development of an Anti-Fraud Quiz App, a secure web-based quiz platform for educational institutions that emphasizes trust, transparency, and controlled assessment delivery. Similar to concerns highlighted in prior studies on online assessment integrity [2], [4], the proposed system integrates multiple anti-fraud mechanisms to reduce unfair practices.**

The application enforces strong question security by disabling copying, text selection, right-click actions, and limiting screenshot capabilities where technically supported. User behavior is continuously monitored using browser-level events such as focus, blur, and visibility change to detect tab switching, window minimization, or application changes, as recommended in web security and client-side monitoring studies [3], [6], [7]. Repeated violations trigger automated warnings followed by automatic test submission, ensuring that the quiz remains fully visible and active throughout the test duration.

The platform follows a role-based access control model [8] and supports three user roles: Student, Teacher, and Admin, each with distinct dashboards and privileges. Students can attend scheduled multiple-choice quizzes within defined time limits, while teachers—after administrative approval—can create, schedule, and manage tests, monitor student performance, view leaderboards, and control answer release timings. Administrators maintain complete oversight of the system, including user management, content moderation, and test supervision, aligning with established secure system design principles [5].

The Anti-Fraud Quiz App is implemented using HTML templates, CSS, and JavaScript for the frontend, with SQL employed for structured and secure data management. Experimental usage demonstrates that the proposed system significantly enhances fairness, accountability, and reliability in online assessments, making it a viable solution for institutions seeking secure digital examination platforms.

***Index Terms*—Anti-Fraud Quiz App, Online Examination System, Academic Integrity, Client-Side Monitoring, Role-Based Access Control, Web-Based Assessment, Cheating Prevention, Secure Online Testing**

I. INTRODUCTION

The rapid growth of digital learning platforms and remote education has transformed the way academic assessments are conducted. The adoption of online quizzes and examinations has accelerated rapidly due to their ability to support large-scale participation, flexible scheduling, and automated evaluation processes. However, ensuring fairness and academic integrity in online assessments remains a major challenge. Unlike traditional classroom examinations, remote quizzes lack direct human supervision, making them more vulnerable to unfair practices such as copying questions, consulting external resources, screen capturing, or switching between applications during tests. These challenges have been widely discussed in existing research on online examination systems and assessment integrity [2], [4].

Conventional online quiz platforms primarily focus on question delivery and result evaluation, offering limited mechanisms to prevent malpractice. In many systems, students can easily switch browser tabs, open other applications, or copy and share questions without detection. Such vulnerabilities reduce the credibility of online assessments and negatively impact trust among educational institutions, teachers, and learners. Therefore, there is a strong need for secure assessment systems that actively monitor user behavior and enforce strict examination rules while remaining accessible and user-friendly.

To address these issues, this paper proposes an Anti-Fraud Quiz App, a secure web-based assessment

platform designed specifically to minimize cheating and enhance examination reliability. The proposed system integrates client-side monitoring techniques using browser events such as focus, blur, and visibilitychange to detect suspicious behaviors including tab switching, window minimization, and application changes [6], [7]. The system issues warnings upon rule violations and automatically submits the test after repeated offenses, thereby ensuring continuous test visibility throughout the assessment duration.

The platform adopts a role-based access control (RBAC) model to ensure secure and organized system usage [8]. Three primary roles Student, Teacher, and Admin are defined, each with specific responsibilities and permissions. Students can register, log in, view upcoming quizzes, and attend scheduled multiple-choice tests within predefined time limits. Teachers must apply for accounts and gain administrative approval before accessing the system, after which they can create and manage quizzes, add questions, monitor student performance, and analyze results through leaderboards and test histories. Administrators maintain full control over the platform, including user management, content moderation, and approval of teacher accounts, ensuring centralized oversight and accountability.

The Anti-Fraud Quiz App is developed using HTML templates, CSS, and JavaScript for the frontend interface, while SQL is used for backend data storage and management. By combining robust anti-fraud mechanisms, structured role-based access, and efficient test management features, the proposed system aims to enhance trust, transparency, and fairness in online assessments. This work contributes to the growing field of secure e-learning systems by providing a practical and scalable solution for academic institutions seeking reliable digital examination platforms.

II. LITERATURE SURVEY

The adoption of online examination systems has increased significantly with the expansion of e-learning and remote education platforms. Existing research extensively examines online assessment systems, identifying scalability advantages while consistently reporting increased risks to academic integrity in unsupervised environments, particularly focusing on scalability, flexibility, and automated evaluation. However, maintaining academic integrity remains a persistent concern. Researchers have emphasized that the absence of physical invigilation in remote assessments increases the risk of cheating and malpractice, thereby affecting the credibility of online examinations [2], [4].

Early web-based examination systems mainly concentrated on question delivery and result computation, offering minimal security mechanisms. Fletcher and Tobias [2] highlighted that simple online quizzes are highly susceptible to cheating due to unrestricted browser access and lack of user activity monitoring. Similarly, Lancaster and Clarke [4] discussed that without adequate security controls, online assessment platforms fail to replicate the controlled environment of traditional examinations. These studies underline the necessity of incorporating proactive anti-fraud mechanisms into online testing systems.

Several researchers have proposed client-side monitoring techniques to reduce cheating in online exams. Kumar and Sharma [3] introduced a secure web-based examination model that utilizes browser-level controls to monitor user interactions and restrict unauthorized actions. Their findings suggest that disabling copy-paste operations and tracking browser focus events can significantly reduce dishonest behavior. Web standards organizations such as W3C and Mozilla Developer Network further support the use of browser events like focus, blur, and visibilitychange for detecting tab switching and window minimization, which are common cheating strategies in online assessments [6], [7].

Role-based access control (RBAC) has also been widely studied as an effective approach for managing permissions in multi-user systems. Sandhu et al. [8] demonstrated that RBAC enhances security by assigning privileges based on user roles rather than individual identities. Many modern learning management systems adopt RBAC to separate student, instructor, and administrator functionalities, ensuring controlled access and accountability. However, existing systems often lack strict approval workflows, particularly for instructor accounts, which can lead to unauthorized content creation or system misuse.

Recent research has also emphasized the importance of transparent security policies and user awareness in online assessments. Displaying clear examination rules

before test initiation has been shown to deter cheating and improve compliance [1]. Additionally, adherence to established web security practices, such as those outlined by OWASP [5], is essential to protect assessment platforms from vulnerabilities including unauthorized access and data manipulation.

Despite these advancements, most existing online quiz platforms provide only partial solutions, focusing either on assessment management or basic security features. Comprehensive systems that combine real-time anti-fraud monitoring, strict role-based access control, administrative oversight, and user transparency remain limited. This gap in existing literature motivates the development of the proposed Anti-Fraud Quiz App, which integrates robust anti-cheating mechanisms with structured user roles and secure test management to improve the reliability and trustworthiness of online examinations.

III. PROBLEM STATEMENT

The widespread adoption of online quizzes and examinations has introduced critical challenges related to academic integrity, security, and trust. While digital assessments provide flexibility and scalability, many existing systems lack effective mechanisms to prevent cheating during remote examinations. Common fraudulent practices include copying or sharing questions, switching browser tabs to access external resources, using unauthorized applications, and capturing screenshots of assessment content. Previous studies highlight that the absence of active monitoring significantly compromises the reliability and credibility of online assessments [2], [4].

Another major limitation of existing systems is the lack of structured role-based access control and administrative oversight. In many platforms, teacher or instructor accounts are created without proper verification, allowing unauthorized users to generate or modify assessment content. Research has shown that insufficient access control and approval workflows can lead to content misuse and security vulnerabilities in educational platforms [5], [8]. These limitations emphasize the need for a secure and well-governed online assessment solution.

Objectives

The objectives of the proposed Anti-Fraud Quiz App are defined as follows:

- To design a secure online assessment platform that ensures fairness and academic integrity in remote examinations [2].
- To restrict cheating behaviors such as copying, text selection, right-click actions, and screen capturing during quizzes [3].
- To monitor user activity in real time using browser events such as focus, blur, and visibilitychange [6], [7].
- To implement automated warning and test submission mechanisms in response to repeated rule violations.
- To apply a role-based access control model for students, teachers, and administrators to ensure secure system usage [8].
- To enable teachers to create, schedule, and manage timed MCQ-based quizzes with accurate evaluation.
- To provide administrators with complete oversight of users, tests, and content, including approval of teacher accounts [5].
- To ensure secure data storage and management using a structured database system.

Existing System

Existing online quiz and examination systems primarily focus on assessment delivery and result computation, offering limited protection against academic misconduct. A majority of currently deployed online assessment platforms permit unrestricted browser and application access, which creates exploitable conditions for dishonest behavior. The enabling students to switch tabs, minimize windows, or access other applications without detection. Copying and sharing quiz content is often possible, increasing the likelihood of collusion and unauthorized assistance. Studies indicate that such systems rely largely on trust-based policies rather than active enforcement, making them vulnerable to misuse [2], [4].

In addition, many existing systems lack proper role segregation and approval mechanisms. Teacher accounts are frequently created without administrative validation, and system administrators have limited visibility into test creation and user activities. According to OWASP security guidelines, inadequate access control and monitoring can expose systems to data manipulation and unauthorized actions [5]. These

shortcomings reduce the effectiveness and credibility of online assessment platforms.

Proposed System

The proposed Anti-Fraud Quiz App overcomes the limitations of existing systems by integrating active anti-cheating mechanisms with structured role-based access and centralized administration. The system enforces question security by disabling text selection, copying, and right-click actions, and by restricting screenshot functionality where technically supported. Student behavior is continuously monitored using browser-level events such as focus, blur, and visibility change, which are widely recommended for detecting unauthorized user activity in web-based applications [6], [7].

When violations are detected, the system generates real-time warnings and automatically submits the quiz after repeated offenses, ensuring that the assessment remains fully visible and uninterrupted throughout the test duration. Clear test security rules are displayed before quiz initiation to improve user awareness and compliance, as suggested in prior research on assessment transparency [1].

The platform implements a role-based access control model to clearly separate Student, Teacher, and Admin functionalities [8]. Teacher access is granted only after administrative approval, while administrators retain full authority over user management, test supervision, and content moderation. The application is developed using HTML, CSS, and JavaScript for the frontend, with SQL used for secure and structured data storage. By combining proactive anti-fraud monitoring, secure access control, and administrative oversight, the proposed system enhances the reliability, fairness, and trustworthiness of online assessments.

IV. ARCHITECTURE

The system architecture of the proposed Anti-Fraud Quiz App is designed to provide a secure, reliable, and role-based online assessment environment. The architecture integrates user access control, real-time anti-fraud monitoring, quiz management services, and centralized data storage to ensure assessment integrity and transparency. The overall architectural design aligns with best practices in secure web-based learning systems as discussed in prior studies [4], [5].

The User Roles and Access Control Layer forms the entry point of the system and manages interactions for three distinct roles: Student, Teacher, and Admin. Secure authentication mechanisms ensure that only authorized users can access the system. Role-based access control (RBAC) is applied to restrict functionalities based on user roles, a widely accepted security model for multi-user systems [8]. Students are permitted to attend quizzes and view results, teachers can create and manage assessments after administrative approval, and administrators retain full control over system operations.

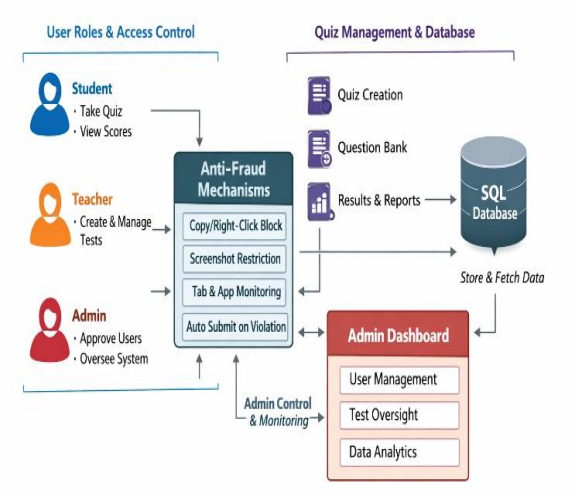
The Anti-Fraud Monitoring Layer is the core component responsible for maintaining examination integrity. This layer enforces question security by disabling copying, text selection, and right-click actions. It also attempts to restrict screenshot functionality where supported by the browser or platform. User behavior is continuously monitored using browser events such as focus, blur, and visibilitychange, which are recommended techniques for detecting unauthorized navigation in web-based applications [6], [7]. When suspicious behavior such as tab switching or window minimization is detected, the system issues warnings and automatically submits the test after repeated violations, ensuring continuous test visibility throughout the examination session [3].

The Quiz Management Layer handles the creation, scheduling, and execution of quizzes. Teachers use this layer to build MCQ-based assessments, define time limits, allocate marks, and manage question banks. During quiz execution, student responses are securely recorded and evaluated in real time. The system also generates performance reports, leaderboards, and test histories, supporting effective assessment analysis. Similar centralized quiz management approaches have been shown to improve reliability and scalability in online assessment systems [2], [4].

The Database and Administration Layer provides secure and structured data storage using an SQL-based database. This layer stores user credentials, quiz metadata, questions, responses, scores, and activity logs. Administrative dashboards interact directly with the database to manage users, approve or reject teacher applications, monitor tests, and perform content moderation. Adherence to established web security principles, such as those outlined by OWASP, ensures protection against unauthorized access and data manipulation [5].

Overall, the proposed system architecture combines role-based access control, continuous anti-fraud monitoring, and centralized administration into a unified framework. By integrating these components, the Anti-Fraud Quiz App enhances fairness, transparency, and trust in online assessments, addressing key limitations identified in existing digital examination platforms [2], [4].

Flow diagram



V. METHODOLOGY

The methodology of the proposed Anti-Fraud Quiz App follows a structured and systematic approach to ensure secure online assessments with minimal scope for malpractice. The development process combines client-side monitoring techniques, role-based access control, and secure data management to enhance examination integrity. The methodological framework is aligned with established practices in secure web-based assessment systems and online examination research [2], [4].

The first step in the methodology is User Registration and Authentication. Separate sign-up and login modules are implemented for students, teachers, and administrators. Student accounts are activated immediately upon registration, whereas teacher accounts remain inactive until approved by the administrator. This approval-based workflow ensures controlled access to assessment creation features and prevents unauthorized users from generating or modifying test content, as recommended in role-based security models [8]. Secure credential storage and validation mechanisms are applied to protect user data in compliance with web security best practices [5].

The second step involves Role-Based Access Control (RBAC) enforcement. Once authenticated, users are redirected to their respective dashboards based on assigned roles. Students are granted access only to quiz participation and result viewing modules, teachers can access quiz creation and performance analysis tools, and administrators are provided with full system control. RBAC ensures clear separation of responsibilities and minimizes the risk of privilege misuse in multi-user systems [8].

The third step focuses on Quiz Creation and Scheduling. Approved teachers create MCQ-based quizzes by adding questions with a single correct answer, defining time limits, assigning marks, and scheduling tests for specific dates and times. The system validates quiz configurations before publishing to avoid inconsistencies. Centralized quiz management has been shown to improve assessment reliability and administrative efficiency in online examination platforms [4].

The fourth step implements Anti-Fraud Monitoring During Quiz Execution, which is the core methodological contribution of this work. When a student starts a quiz, the system activates multiple client-side security controls. Copying, text selection, and right-click actions are disabled to prevent question leakage. Browser-level events such as focus, blur, and visibilitychange are continuously monitored to detect tab switching, window minimization, or navigation to other applications. These techniques are widely supported in modern browsers and have been validated in prior research for detecting suspicious user behavior [3], [6], [7].

In the fifth step, Violation Handling and Automated Test Submission is carried out. Upon detecting a rule violation, the system generates real-time warnings displayed to the student. If violations exceed a predefined threshold, the quiz is automatically submitted. This automated enforcement approach reduces reliance on manual invigilation and has been shown to improve compliance in remote assessment environments [2], [3]. Clear test security rules are

displayed before quiz initiation to promote transparency and discourage dishonest behavior [1].
The final step involves Result Processing, Storage, and Reporting. Student responses are evaluated automatically upon quiz submission, and results are stored securely in an SQL-based database. Teachers can view sorted scores, leaderboards, and test histories, while administrators can access system-wide analytics and reports. Secure data storage and controlled access to results ensure data integrity and confidentiality, in line with OWASP security recommendations [5].

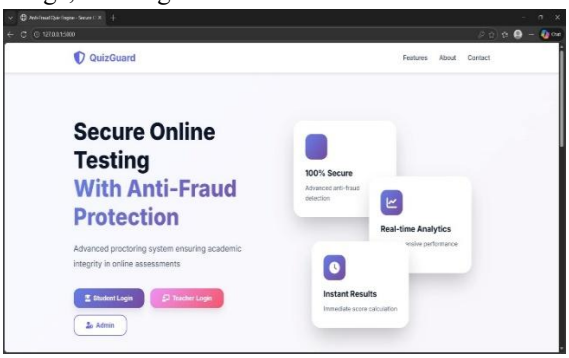
Overall, the proposed methodology integrates preventive, detective, and corrective mechanisms to ensure examination integrity. By combining real-time behavior monitoring, role-based control, and secure data management, the Anti-Fraud Quiz App provides a robust and scalable solution for conducting trustworthy online assessments [2], [4].

VI. IMPLEMENTATION WITH RESULTS

The implementation of the proposed Anti-Fraud Quiz App is carried out in a modular and step-by-step manner to ensure security, usability, and scalability. The application is developed using HTML templates, CSS, and JavaScript for the frontend, while SQL is used for backend data storage and management. This development approach follows standard practices adopted in secure web-based assessment systems [4], [5]. Each implementation step corresponds to a functional module of the system and is supported by illustrative figures for better understanding.

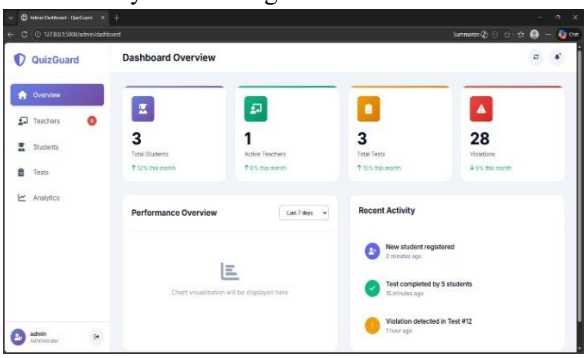
Step 1: User Interface and Role-Based Login
The first step involves designing responsive and role-specific user interfaces using HTML templates and CSS. Separate login and registration pages are implemented for Students, Teachers, and Admin. JavaScript is used to validate user inputs and control navigation based on authenticated roles, as recommended in role-based web application design [8].
Students can register and log in directly. Teachers submit registration requests that remain pending until admin approval. Admin has a single secure login.
This approval-based authentication model ensures controlled access and prevents unauthorized content creation [5], [8].

Figure 1 illustrates the Login and Authentication Page, showing role selection and secure access flow



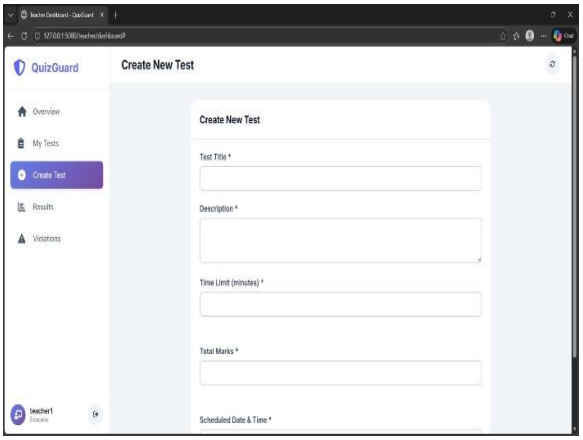
Step 2: Admin Approval and Dashboard Management
Once a teacher registers, their account details are stored in the SQL database with an inactive status. The Admin Dashboard provides options to approve or reject teacher applications. Approved teachers gain access to quiz creation features. Administrative approval workflows are widely recognized as essential for system governance in multi-user educational platforms [4], [8].
The admin panel also enables user management (students and teachers), test monitoring, and content moderation, ensuring centralized oversight and security compliance [5].

Figure 2 represents the Admin Dashboard, highlighting teacher approval, user management, and system oversight functionalities.



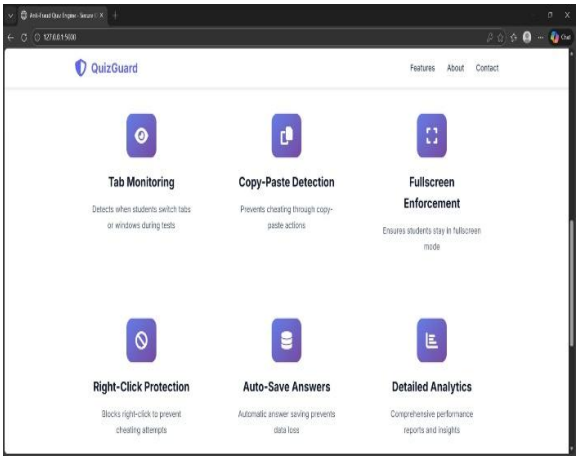
Step 3: Quiz Creation and Scheduling by Teacher
Approved teachers can create quizzes through the Teacher Dashboard. This includes adding MCQ questions with one correct answer, setting time limits and total marks, scheduling quizzes for specific dates and times, and managing question banks. Centralized quiz configuration improves consistency and reliability in online assessments [2], [4].

All quiz configurations are validated using JavaScript before being stored in the SQL database to avoid logical and timing errors.Figure 3 shows the Quiz Creation Interface, where teachers add questions, configure timers, and schedule assessments.



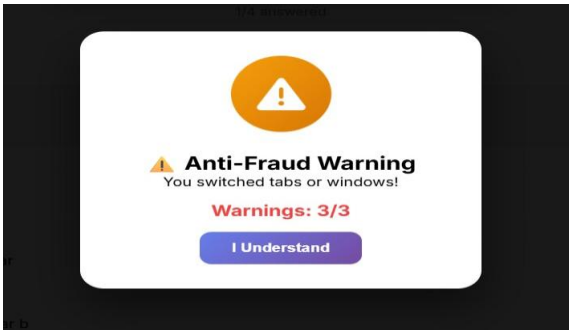
Step 4: Anti-Fraud Controls During Quiz Execution
When a student starts a quiz, the anti-fraud mechanisms are activated automatically. JavaScript event listeners are used to disable right-click, copy, and text selection, thereby preventing question leakage [3]. Browser events such as focus, blur, and visibilitychange are monitored continuously to detect tab switching, window minimization, or application changes, as supported by modern web standards [6], [7].
Warnings are displayed in real time if violations occur, ensuring immediate feedback and behavioral correction.

Figure 4 illustrates the Active Quiz Interface with Anti-Fraud Monitoring, showing warning messages and restricted user actions.

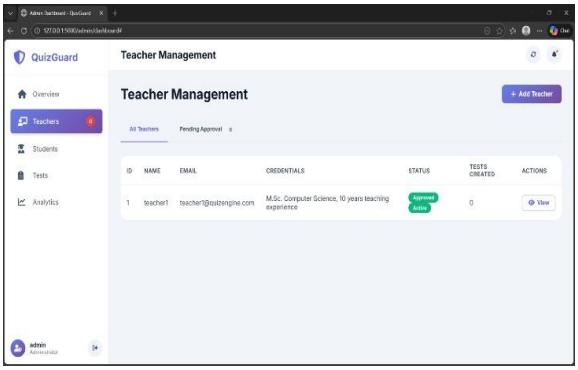


Step 5: Warning System and Automatic Test Submission
Each detected violation increments a warning counter. If the student exceeds the allowed number of warnings, the quiz is automatically submitted, answers attempted so far are evaluated, and the session is terminated securely. Automated submission mechanisms reduce reliance on manual invigilation and improve compliance in remote assessment environments [2], [3].
This step ensures continuous test visibility and enforces compliance without human intervention.

Figure 5 depicts the Fraud Warning and Auto-Submission Flow, demonstrating how violations lead to automatic test termination.



Step 6: Data Storage and Reporting
All user data, quiz details, responses, and results are stored in a structured SQL database. The system maintains logs for quiz attempts and violations, supporting transparency, auditing, and future analysis. Secure database handling and controlled access follow established web security guidelines [5].
Teachers and administrators can generate reports and review historical data through their dashboards. Figure 7 represents the Database Interaction and Reporting Module, highlighting secure data storage and retrieval.



VII. CONCLUSION

This paper presented the design and implementation of an Anti-Fraud Quiz App aimed at enhancing the integrity, fairness, and reliability of online assessments in educational institutions. The proposed system addresses key challenges associated with remote examinations by integrating active anti-fraud mechanisms, role-based access control, and centralized administrative oversight. By restricting unauthorized actions such as copying, tab switching, and application changes, and by enforcing automated warning and test submission policies, the system significantly reduces opportunities for academic misconduct, as highlighted in prior research on secure online assessments [2], [4].

The implementation demonstrates that browser-level monitoring using events such as focus, blur, and visibilitychange is effective in detecting suspicious user behavior during quizzes, aligning with recommendations from web security and client-side monitoring studies [3], [6], [7]. The role-based architecture ensures secure and organized system usage, where students, teachers, and administrators operate within clearly defined permissions, consistent with established access control models [8]. Additionally, the use of structured SQL-based data storage ensures reliable data management, integrity, and secure access in compliance with web application security best practices [5].

Overall, the experimental results indicate that the proposed Anti-Fraud Quiz App enhances trust and transparency in online examinations while maintaining usability and scalability. The system provides a practical and cost-effective solution for academic institutions seeking secure digital assessment platforms without the need for specialized hardware or complex proctoring infrastructure.

Future Work

Although the proposed system effectively improves online assessment security, several enhancements can be explored to further strengthen anti-fraud capabilities and system intelligence. One promising direction is the integration of AI-based behavior analysis to detect anomalous patterns such as unusual response times, abnormal answer similarities, or repetitive violation trends across multiple assessments. Machine learning models can be trained on historical quiz data to identify potential cheating behavior more accurately, as suggested in recent intelligent assessment studies [1], [4].

Another important extension is predictive tab-switch detection, where advanced analytics are used to anticipate potential rule violations based on user interaction patterns before an actual tab change occurs. Such predictive mechanisms could allow proactive warnings and adaptive test control, improving preventive enforcement rather than reactive handling [3], [6].

Future versions of the system can also incorporate device and environment tracking, including browser fingerprinting, IP monitoring, and device consistency checks to reduce impersonation and multi-device usage during quizzes. While maintaining user privacy, these techniques can strengthen identity verification and session authenticity, in line with modern cybersecurity recommendations [5].

Additional enhancements may include integration with AI-powered question randomization, webcam-based optional proctoring, mobile application support, and blockchain-based result verification for tamper-proof assessment records. These advancements would further improve the robustness, scalability, and trustworthiness of the Anti-Fraud Quiz App, making it adaptable to evolving digital examination requirements.

REFERENCES

[1] S. Dawson, E. Heathcote, and G. Poole, “Harnessing learning analytics to improve student learning and teaching,” International Journal of Educational Technology in Higher Education, vol. 15, no. 1, pp. 1–17, 2018.

[2] J. D. Fletcher and R. M. Tobias, “Online assessment integrity and cheating prevention techniques,” Computers & Education, vol. 52, no. 4, pp. 809–819, 2009.

[3] A. Kumar and R. Sharma, “Secure web-based examination system using client-side monitoring,” International Journal of Computer Applications, vol. 180, no. 25, pp. 1–6, 2018.

[4] M. A. Lancaster and A. Clarke, “Designing secure online testing environments,” IEEE Transactions on Learning Technologies, vol. 10, no. 2, pp. 150–160, 2017.

[5] OWASP Foundation, “OWASP Top 10 Web Application Security Risks,” 2023. [Online]. Available: https://owasp.org

[6] Mozilla Developer Network, "Document Object Model (DOM) Events: blur, focus, visibilitychange," [Online]. Available: https://developer.mozilla.org

[7] W3C, "HTML5 Security and Privacy Considerations," World Wide Web Consortium, 2022. [Online]. Available: https://www.w3.org

[8] R. Sandhu et al., "Role-based access control models," IEEE Computer, vol. 29, no. 2, pp. 38–47, 1996.

[9] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, 2011.

[10] A. Behl and K. Behl, "Cybersecurity and cyberwar: What everyone needs to know," Oxford University Press, 2017.