Jonathan Jobby, 2024, 12:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Elevating Exam Fairness: Advanced Proctoring and Monitoring in a Secure Offline Environment

Jonathan Jobby, Paul Thomas, Pranav Asokan, Professor Shyama R
Adi Shankara Institute of Engineering and Technology, Kalady, Kerala

Abstract- Offline Computer-Based Tests (CBTs) present unique challenges in ensuring test integrity and security within an offline framework. This paper presents the design and implementation of a novel Offline CBT Controller, a software solution aimed at enhancing the security of offline exams by seamlessly integrating various security measures. The system combines USB blocking, internet restrictions, and user activity monitoring to prevent malpractices during offline exams, thereby ensuring a secure testing environment. The project prioritizes user experience by providing a user-friendly interface for administrators to configure and manage security settings efficiently. The Offline CBT Controller is designed to address the specific security requirements of offline CBT environments, such as those found in practical computer lab exams. By implementing robust security measures, including USB blocking and internet restrictions, the system prevents unauthorized access to external resources during exams, thereby minimizing the risk of cheating. Additionally, user activity monitoring allows administrators to track and log system activities, providing a comprehensive activity history for auditing purposes. Key features of the Offline CBT Controller include its compatibility with various operating systems and its ability to seamlessly integrate with existing exam infrastructure. The system is developed using Java programming language, making it platform-independent and easy to deploy across different environments. Furthermore, the project emphasizes the importance of adherence to software development best practices to ensure the reliability and effectiveness of the solution.

Keywords- Offline Computer-Based Tests (CBTs), Test Integrity, Security measures, USB Blocking, Internet Restrictions, User Activity Monitoring, Software Solution, Exam Security, Java Programming, User-Friendly

I. INTRODUCTION

In the ever-evolving landscape of education, the paradigm shift towards computer-based testing has ushered in a new era of assessment methodologies. Amidst this transformation, the Offline Computer-Based Test Control System emerges as a pivotal innovation, poised to redefine the integrity and security of examinations conducted within offline frameworks. Traditional paper-based exams are gradually yielding to the advantages offered by computer-based testing, including increased efficiency, accuracy, and administrative ease. However, this transition brings forth a pressing concern regarding the safeguarding of examination integrity in a digitally-driven environment.

The Offline Computer-Based Test Control System addresses this concern by offering a robust and comprehensive framework designed to ensure the

security and authenticity of offline examinations. Particularly crucial in the context of practical computer lab exams, this system tackles the unique challenges posed by hands-on assessments, such as those administered by educational institutions. By streamlining the examination process and fortifying its credibility, the system not only enhances the efficiency of assessments but also instills confidence in the integrity of the results.

At its core, the project endeavors to achieve multiple objectives aimed at elevating test integrity and security within offline computer-based examinations. Central to its mission is the development of a seamlessly Interface, Platform-Independent, Best Practices, System Compatibility, Exam Infrastructure Integration. integrated system capable of managing the entire examination lifecycle, from test creation to result processing, within an offline environment. This entails the implementation of stringent encryption protocols, secure delivery mechanisms, and sophisticated authentication measures to verify the identity of test-takers and safeguard the integrity of test content.

Moreover, the project seeks to address the specific challenges inherent to practical computer lab exams, including the secure delivery of test materials, prevention of unauthorized access or tampering, and assurance of independent test-taker engagement. Through the integration of advanced features such as biometric authentication, lockdown browsers, and randomized question orders, the system aims to fortify the examination process against potential malpractices and ensure the credibility and reliability of offline computer-based assessments.

In conclusion, the Offline Computer-Based Test Control System represents a significant advancement in the domain of educational assessment, offering a comprehensive solution to the evolving challenges of examination security and integrity. As this project unfolds, it holds the promise of revolutionizing the offline examination experience, setting a new standard for secure and controlled testing environments in the digital age. With its multifaceted approach and innovative features, it is poised to become a cornerstone in the realm of educational assessment, paving the way for credible and reliable offline computer-based examinations.

II. TECHNOLOGIES USED

1. Internet and USB Restrictions

USB blocking and internet restrictions are pivotal features of the Offline Lab Exam Monitoring System, essential for maintaining the integrity and security of exam environments. USB blocking involves temporarily disabling USB ports on exam computers, achieved through tools like udev rules, to prevent students from connecting external storage devices or peripherals during exams, thus mitigating the risk of unauthorized data transfer. Similarly, internet restrictions, enforced via technologies like iptables or firewalls, ensure that students cannot access external resources or online materials during exams, preserving the fairness and validity of assessments. The technical implementation involves configuring the system to monitor and control USB ports and network connectivity, dynamically enabling or disabling restrictions based on predefined schedules or user permissions, and implementing robust logging mechanisms to track and audit system activities for compliance and security purposes.

Internet Restrictions

Internet restriction is a crucial component of the Offline Lab Exam Monitoring System, designed to uphold the integrity of exams by preventing access to external resources during testing sessions. This feature employs sophisticated firewall technologies, such as iptables or firewalld, to control network traffic and block access to unauthorized websites or online services. By configuring firewall rules, zadministrators can restrict outbound connections from exam computers, effectively isolating them from the internet while allowing essential local network communication to facilitate exam administration. Additionally, the implementation may involve the use of proxy servers or content filtering mechanisms to further refine access

controls and ensure compliance with exam regulations.

The technical implementation of internet restriction encompasses several key elements, including the configuration of firewall rulesets to specify which network traffic is permitted or denied based on predefined criteria such as IP addresses, port numbers, or protocol types. Furthermore, administrators may utilize dynamic firewall management tools or scripting languages like Bash to automate the deployment and maintenance of firewall rules, streamlining the management process and enhancing system scalability. Additionally, logging and monitoring mechanisms play a critical role in internet restriction, enabling administrators to track network activity, detect potential security breaches or policy violations, and generate comprehensive audit trails for post-exam analysis and compliance reporting.

In summary, internet restriction is a fundamental feature of the Offline Lab Exam Monitoring System, leveraging advanced firewall technologies and automation capabilities to create a controlled testing environment that safeguards exam integrity and prevents academic dishonesty. Through careful configuration and monitoring, administrators can enforce strict access controls, mitigate the risk of unauthorized online assistance, and uphold the credibility of offline exams, ensuring fair and equitable assessment practices.

USB Restrictions

USB restriction is a critical aspect of the Offline Lab Exam Monitoring System, serving to enhance exam security by preventing the use of external storage devices during testing sessions. This feature leverages advanced USB management techniques, such as USB device blacklisting or policy-based access control, to block unauthorized USB connections and mitigate the risk of cheating or data tampering. Through the implementation of kernel-level drivers or user-space utilities, administrators can enforce strict controls over USB ports on exam computers, ensuring that only approved devices, such as keyboards or mice, are permitted while blocking storage devices like USB drives or external hard disks.

The technical implementation of USB restriction involves several key components, including the development of custom device drivers or the utilization of existing kernel modules like usbguard or usbkill to monitor and control USB devices at the system level. Administrators may configure USB access policies using rule-based frameworks or scripting languages like Python, specifying criteria such as device IDs, vendor/product codes, or device classes to determine which USB devices are allowed or blocked. Furthermore, the system may incorporate real-time monitoring and alerting mechanisms to detect and respond to unauthorized USB connections, enabling administrators to promptly intervene and maintain exam integrity.

In summary, USB restriction is a crucial feature of the Offline Lab Exam Monitoring System, employing advanced USB management techniques and policy enforcement mechanisms to prevent the use of external storage devices and safeguard exam integrity. Through the implementation of kernel-level drivers, rule-based access controls, and real-time monitoring capabilities, administrators can effectively control USB port access, mitigate the risk of academic dishonesty, and ensure a fair and secure testing environment for all examinees.

2. Activity Monitoring

File Creation Isolation within the Offline Lab Exam Monitoring System is facilitated through the utilization of file system permissions and isolation mechanisms such as chroot and containerization. These technologies enable the system to restrict the creation of new files during exam sessions, thereby preventing students from introducing unauthorized materials or altering existing files. By implementing granular permissions and isolation controls at the file system level, administrators can ensure that exam-related data remains secure and isolated from external interference. Additionally, the system employs activity monitoring and logging technology to track user activities comprehensively throughout the exam process. Through the logging of user interactions, application usage, and system

events, administrators gain valuable insights into examinee behavior, allowing for real-time supervision and post-exam analysis to maintain exam integrity.

File Isolation

File creation isolation in the Offline Lab Exam Monitoring System is achieved through a combination of advanced file system permissions and isolation mechanisms. At its core, the system relies on the robust file system permissions provided by the underlying operating system, which allow administrators to control access to files and directories with fine granularity. By configuring permissions such as read, write, and execute at the user, group, and other levels, the system can restrict the ability of users, particularly exam takers, to create new files during exam sessions. Additionally, the system leverages isolation mechanisms such as chroot and containerization to further enhance file creation isolation. Chroot, a Unix-based utility, allows the system to change the apparent root directory for a process, effectively limiting its access to only a specific portion of the file system. This ensures that exam-related files are contained within a designated directory, preventing users from accessing or modifying files outside of this isolated environment. Similarly, containerization technologies like Docker provide lightweight, portable environments that encapsulate all dependencies and resources required for running applications, including file systems. By deploying exams within isolated containers, the system can maintain strict control over file creation and manipulation, safeguarding the integrity of the exam environment.

In addition to utilizing file system permissions and isolation mechanisms, the system employs various security measures to reinforce file creation isolation. For instance, it enforces the principle of least privilege, ensuring that exam takers only have the necessary permissions to perform exam-related tasks and nothing more. This minimizes the risk of unauthorized access or tampering with exam materials. Furthermore, the system employs auditing and logging mechanisms to track file creation activities in real-time. By logging relevant events such as file creation attempts, modifications, and deletions, administrators can monitor exam taker behavior closely and detect any unauthorized activities promptly. These audit logs serve as valuable forensic evidence in the event of security incidents or integrity breaches, enabling administrators to investigate and take appropriate actions as needed.

Overall, the technology used in file creation isolation represents a multi-layered approach to ensuring the security and integrity of exams conducted within the Offline Lab Exam Monitoring System. By combining file system permissions, isolation mechanisms like chroot and containerization, and additional security measures such as least privilege enforcement and auditing, the system establishes a robust framework for preventing unauthorized file creation and manipulation during exam sessions. This not only helps maintain the integrity of exams but also instills confidence in both exam takers and administrators regarding the fairness and reliability of the assessment process.

Logging

In the Offline Lab Exam Monitoring System, the technology employed for file creation isolation relies heavily on file system permissions and isolation mechanisms. These mechanisms grant administrators granular control over file access and modification rights, ensuring that only authorized actions can be performed within designated directories. File system permissions, a fundamental aspect of Unix-like operating systems, allow administrators to specify which users or groups have the authority to create, modify, or delete files. By configuring permissions appropriately, the system can restrict file creation during exam sessions to prevent unauthorized access or tampering. Additionally, isolation mechanisms such as chroot and containerization provide an additional layer of security by confining processes to a limited environment. Chroot, for instance, changes the apparent root directory for a process, effectively sandboxing it and limiting its access to specific files and directories. Similarly, containerization technologies like Docker enable

the creation of lightweight, isolated environments where file creation can be tightly controlled, further bolstering the security of the exam environment.

Activity monitoring and logging in the Offline Lab Exam Monitoring System are facilitated by specialized software components designed to capture and record user interactions, system events, and application usage. These monitoring tools continuously track and record various metrics, including keystrokes, mouse movements, application launches, and file accesses. The collected data is then stored in comprehensive activity logs, providing administrators with detailed insights into examinee behavior and system activity. To achieve this functionality, the system leverages a combination of system-level monitoring utilities and custom logging mechanisms. System-level utilities such as xprop and xdotool enable real-time monitoring of user interactions with graphical applications, capturing window properties and input events. Meanwhile, custom logging mechanisms implemented within the system's software architecture ensure the capture and storage of relevant activity data in a structured and accessible format.

In addition to monitoring user activities in real-time, the Offline Lab Exam Monitoring System employs advanced logging techniques to record and store activity data for post-exam analysis and audit purposes. These logs contain detailed information about user actions, system events, and security-related incidents, providing administrators with a comprehensive audit trail of exam sessions. The system utilizes secure logging protocols and encryption techniques to protect the integrity and confidentiality of log data, ensuring that sensitive information remains inaccessible to unauthorized parties. Furthermore, the system may incorporate features such as log rotation and archival to manage log files efficiently and prevent data loss due to storage constraints. By combining real-time monitoring capabilities with robust logging mechanisms, the system enables administrators to maintain exam integrity, detect anomalies, and investigate security breaches effectively.

III. RELATED WORKS

1. Tim Thomas et al.

The paper, "A Mandatory Access Control Mechanism for the Unix File System," presents a significant advancement in the domain of computer security by addressing the longstanding challenges associated with integrating Mandatory Access Control (MAC) mechanisms into the UNIX file system. The literature review reveals a gap in the existing solutions, emphasizing the need for a more efficient and seamless MAC design. Previous endeavors, such as Linus IV and Secure Xenix, are scrutinized, shedding light on their limitations and highlighting the complexity introduced by partitioned directories. The review underscores the absence of a comprehensive solution that eliminates the need for users to log in and out for utilizing upgraded directories, making a compelling case for the proposed innovative approach.

In exploring prior work, the paper critically assesses the drawbacks of existing MAC mechanisms and draws attention to the unique contribution of file name hiding in the proposed design. This feature allows users to interact with directories more flexibly, simplifying user experience while maintaining robust security protocols. By providing a comprehensive analysis of the existing literature, the paper establishes a foundation for its groundbreaking MAC design, positioning itself as a pioneering solution to enhance security measures in the UNIX file system.

2. Sebastian Neuner et al.

The paper "USBlock: Blocking USB-Based Keypress Injection Attacks" by Neuner et al. proposes a novel approach to detecting and defending against such attacks. The authors analyze the temporal characteristics of USB packet traffic to identify suspicious patterns indicative of malicious activity. They find that BadUSB-like attacks inject keypresses at a rate significantly faster than human typing speeds. USBlock utilizes this insight by monitoring the interarrival time between keypress events and triggering a two-step defense mechanism upon detection of a rapid

keypress sequence (RES). This mechanism disconnects the offending device and unloads its associated driver, effectively preventing the attack from succeeding.

USBlock offers several benefits over existing approaches. Its automatic operation eliminates the need for user intervention, making it more user-friendly. Additionally, its real-time RES detection ensures fast and effective defense against malicious activity. Finally, USBlock's design is extensible, allowing it to be adapted to detect and defend against new attacks by modifying the RES detection logic. This makes it a valuable tool for organizations seeking to protect themselves from the evolving threat landscape of USB-based attacks.

3. Jiwoong Won et al.

This paper proposes iFetcher, a user-level disk prefetching framework for Linux that reduces latency caused by disk access. It operates with low overhead by monitoring disk requests made by a target application at specific times. iFetcher collects information on read-related functions and file mapping operations using library preloading and periodically references the /proc/[pid]/maps file to gather file-mapping information. The analyzer identifies periods of burst reads and sparse reads based on the collected data and selects trigger events for prefetching. The prefetcher monitors file events using the inotify mechanism and prefetches data associated with the trigger events. Experiments show that iFetcher can improve application launch times by up to 41% and run-time loading times by up to 9%. iFetcher offers several advantages over existing prefetching schemes, including a low overhead, the ability to reduce both launch and run-time data loading times, and a user-level implementation that does not require kernel modifications. It also overcomes the limitations of existing kernel-level prefetchers by monitoring file operations instead of individual block reads and using the inotify mechanism to trigger prefetching, eliminating the need for continuous monitoring. Future work will focus on improving the accuracy of data collection, taking the correlation between prefetching triggers into account to predict the flow of an application and perform more accurate prefetching.

4. Mohan Vamsi A et al.

This paper tackles the challenge of maintaining academic integrity in e-learning environments. It proposes a comprehensive, automated proctoring system leveraging machine learning and multimedia analytics. Existing solutions range from labor-intensive human proctoring to software tools with limited detection capabilities. The paper identifies existing methods like face verification, active window detection, and gaze estimation as promising but prone to limitations. The proposed system combines several modules for enhanced proctoring. User verification ensures the test taker's identity, while number of person detection and object/phone detection prevent external assistance. Gaze detection identifies suspicious head movements, and audio processing tackles verbal communication. This system offers benefits like affordability, convenience, and effectiveness compared to existing solutions. It reduces administrative burden and automates cheat detection. Future work involves improving module accuracy, exploring new detection methods, and personalizing the system to individual users. Additionally, leveraging temporal-spatial features and optimizing system efficiency are considered. By combining various machine learning techniques, this system holds promise for secure and reliable online exam proctoring, ensuring academic integrity in e-learning.

This paper reviews existing online exam proctoring systems, highlighting their limitations and strengths. It then introduces a novel system that utilizes machine learning and multimedia analytics for comprehensive and automated proctoring. The system combines user verification, number of person detection, object/phone detection, gaze detection, and audio processing to effectively prevent cheating behaviors. This system offers several advantages over existing solutions, including affordability, convenience, and effectiveness, while reducing administrative burden.

5. Fatima Mahmood et al.
Academic dishonesty, particularly cheating in examinations, is a pervasive issue that undermines the integrity of educational institutions. Traditional invigilation methods, relying on human observation, are often limited in their effectiveness due to fatigue, scalability, and subjectivity. In recent years, advances in computer vision and artificial intelligence have paved the way for automated invigilation systems as a potential solution to this challenge.

Several studies have explored the use of deep learning techniques for automated exam proctoring, proposed a system utilizing a multi-task convolutional neural network (CNN) for face detection and recognition, achieving high accuracy in identifying students and their activities. Similarly, employed a Faster R-CNN model for real-time detection of suspicious behaviors based on head movements, demonstrating its effectiveness in large-scale examinations. However, these studies primarily focused on individual aspects of invigilation, such as face recognition or head pose estimation.

This research contributes to the existing body of literature by proposing a comprehensive automated invigilation system that integrates face detection, recognition, head movement analysis, and report generation. The proposed system leverages the combined strengths of MTCNN and Faster RCNN, achieving high accuracy in both individual student identification and activity monitoring. Furthermore, the system's ability to generate detailed activity reports provides valuable insights for educators and facilitates improved exam administration.

6. Tanzila Saba et al.
This paper proposes a novel deep learning-based approach for automatic exam proctoring. The proposed system employs a pre-trained L2-GraftNet model for image feature extraction and an atom search optimization (ASO) algorithm for feature selection. The extracted features are then fed to various classifiers, with the fine K-nearest neighbor (FKNN) classifier achieving the highest accuracy of 93.88%. The proposed system has the potential to improve academic integrity by automating exam proctoring and reducing the burden on invigilators.

This work builds upon existing research on student action modeling and exam deception detection. It introduces a new L2-GraftNet architecture that combines the strengths of AlexNet and SqueezeNet, demonstrating its effectiveness in extracting relevant features from exam images. The use of ASO for feature selection further enhances the system's performance by reducing the dimensionality of the features and improving classification accuracy. Additionally, the system's modular design allows for easy integration with existing exam management systems and its adaptability to different exam settings.

IV. PROPOSED SYSTEM

The proposed system, designed for publication in a paper, encompasses a comprehensive Offline Lab Exam Monitoring System tailored to address the unique challenges of maintaining exam integrity in offline computer-based testing environments. At its core, the system integrates a suite of security measures and monitoring functionalities to create a controlled and secure testing environment. One key aspect of the proposed system is its ability to enforce USB blocking and internet restrictions during exam sessions. Leveraging advanced firewall rules and USB port management techniques, the system effectively prevents the use of external devices and unauthorized internet access, mitigating the risk of cheating or information leakage.

Furthermore, the proposed system incorporates sophisticated user authentication mechanisms to ensure that only authorized individuals can access exam-related resources and functionalities. By implementing secure login mechanisms and role-based access controls, the system provides administrators with granular control over user permissions and privileges, safeguarding sensitive exam materials and data. Additionally, the system offers real-time monitoring of user activities,

tracking application usage, system interactions, and any deviations from normal behavior. This monitoring capability enables administrators to detect and respond to suspicious activities promptly, maintaining the integrity and security of exam sessions.

To enhance the user experience and streamline administrative tasks, the proposed system features a user-friendly interface for configuring security settings, managing exam sessions, and generating comprehensive activity reports. By prioritizing usability and accessibility, the system empowers administrators to efficiently oversee exam operations and ensure compliance with established security protocols. Overall, the proposed Offline Lab Exam Monitoring System represents a significant advancement in the field of educational assessment, providing educators and institutions with a robust solution for conducting secure and reliable offline computer-based exams.

Objective

The primary objective of this is to contribute to the field of educational assessment by introducing a novel Offline Lab Exam Monitoring System tailored to meet the specific challenges of conducting secure offline computer-based tests. Through comprehensive research and development, our aim is to address the growing need for effective solutions that ensure the integrity and reliability of exam processes in educational institutions. By disseminating our findings and insights through academic publication, we seek to share our innovative approach and contribute to the advancement of best practices in exam administration and security.

Moreover, this paper aims to provide a detailed overview of the proposed Offline Lab Exam Monitoring System, including its key features, underlying technologies, and implementation strategies. By presenting a thorough analysis of the system's design, functionality, and potential applications, we aim to offer valuable insights to researchers, educators, and practitioners interested in exploring similar solutions or integrating advanced security measures into their exam environments. Through rigorous evaluation and validation, we endeavor to demonstrate the efficacy and practicality of our system in safeguarding the integrity of offline computer-based tests, ultimately fostering trust and confidence in the assessment process.

V. METHODOLOGY

The methodology employed in this study encompasses a systematic approach to designing, developing, and evaluating the Offline Lab Exam Monitoring System. It involves several stages, including requirements gathering, system design, implementation, testing, and validation. Initially, extensive research is conducted to identify the specific needs and challenges associated with offline computer-based tests, informing the development of functional and technical requirements for the system. Subsequently, the system architecture is designed, taking into account factors such as security, usability, and scalability.

The implementation phase involves the utilization of relevant technologies and programming languages, such as Java, to build the system components and integrate key features such as USB blocking, internet restriction, and user activity monitoring. Rigorous testing and validation procedures are then employed to assess the system's performance, reliability, and security, ensuring that it meets the desired objectives and fulfills the requirements of educational institutions and exam administrators.

1. Internet and USB Restrictions Internet Restrictions

- Usb Restrictions

2. Activity Monitoring File Isolation

- Logging

VI. SYSTEM ARCHITECTURE

The system architecture of the Offline Lab Exam Monitoring System comprises two primary components: Internet and USB

Restrictions, and Activity Monitoring with File Isolation and Logging.

Internet and USB Restrictions
This component focuses on enforcing restrictions to ensure a secure testing environment. Internet Restrictions involve the implementation of firewall rules or other mechanisms to block internet access during exam sessions. This prevents students from accessing external resources, maintaining exam integrity. USB Restrictions entail temporarily disabling USB ports on exam computers to prevent the connection of external devices, minimizing the risk of unauthorized data transfer or device tampering during exams.

Activity Monitoring with File Isolation and Logging
This component is responsible for monitoring user activities during exam sessions and ensuring data integrity. Activity Monitoring tracks application usage, system interactions, and any suspicious behavior to generate comprehensive activity reports for examiners. File Isolation employs file system permissions and isolation mechanisms like chroot or containerization to isolate the creation of new files during exams, preventing students from altering or introducing external materials. Logging involves the generation and storage of detailed activity logs for each exam session, including information on user actions, system events, and security-related incidents, facilitating post-exam analysis and integrity verification.

Overall, the system architecture integrates these components to create a robust and comprehensive solution for offline lab exam monitoring, enhancing exam security and ensuring a controlled testing environment.

Functional Requirements
Functional requirements are essential specifications that outline the specific features and functionalities a system must possess to meet its objectives effectively. In the context of the Offline Lab Exam Monitoring System, these requirements encompass various aspects, including security measures, monitoring functionalities, and user interactions.

Key functional requirements include:

USB Blocking
Enable the system to temporarily disable USB ports on exam computers to prevent the connection of external devices, enhancing the security of the exam environment.

Internet Restrictions
Implement firewall rules or other mechanisms to block internet access during exam sessions, ensuring that students cannot access external resources and maintaining a controlled testing environment.

File Creation Isolation
Isolate the creation of new files during exam periods to prevent students from altering or introducing external materials during examinations.

Monitoring User Activities
Continuously monitor user activities during exams, tracking application usage, system interactions, and any suspicious behavior to generate comprehensive activity reports for examiners.

Activity Logging
Generate and store detailed activity logs for each exam session, including information on user actions, system events, and security-related incidents for post-exam analysis and integrity verification.

Comprehensive Reporting
Provide examiners with comprehensive reports summarizing user activities during each exam, including details on application usage, system interactions, and deviations from normal behavior.

Non-Functional Requirements
Performance
Ensure prompt response times and scalability to accommodate increasing exam session loads.

Security
Implement data encryption and strict access control measures to safeguard sensitive information.

Reliability
Maintain high availability and incorporate fault tolerance mechanisms to ensure uninterrupted operation.

Usability
Design an intuitive user interface and ensure accessibility for users with diverse abilities.

Compatibility
Ensure cross-platform and compatibility to accommodate various computing environments.

Scalability
Scale performance capabilities and database components to handle growing demands.

Maintainability
Design with modularity and provide comprehensive documentation for ease of maintenance and updates.

VII. CONCLUSION

In summary, the Offline Lab Exam Monitoring System presents a comprehensive solution tailored to the evolving needs of educational assessment in offline environments. By meticulously addressing both functional and non-functional requirements, the system stands as a beacon of integrity, ensuring the sanctity of examinations. Through stringent user authentication mechanisms and features like USB blocking and internet restrictions, the system fortifies the examination process against external influences, fostering a secure testing environment. Its ability to seamlessly integrate with monitoring tools and provide comprehensive reporting empowers administrators with the insights needed to uphold exam integrity effectively.

Moreover, the system's scalability, reliability, and usability underscore its adaptability to various educational settings, promising seamless operation across diverse computing environments. With a focus on modularity and comprehensive documentation, the system remains primed for future updates and maintenance, reinforcing its sustainability and long-term viability. As educational landscapes continue to evolve, the Offline Lab Exam Monitoring System stands as a testament to the indispensable role of technology in safeguarding the credibility and reliability of examinations conducted offline.

In conclusion, the Offline Lab Exam Monitoring System epitomizes a holistic approach to ensuring exam integrity, combining technological innovation with user-centric design principles. Its implementation heralds a new era of trust and reliability in offline assessments, setting a precedent for educational institutions worldwide. As the system continues to evolve and adapt to emerging challenges, its impact on educational assessment practices is poised to be profound and enduring, reinforcing the critical importance of integrity in the educational process.

Declaration

Ethical Approval and Consent to Participate
Ethical approval was not required for this study as it did not involve human participants. No human data was collected or analyzed during the development of the Offline Lab Exam Monitoring System.

Consent for Publication
Consent for publication is not applicable in this research. The manuscript does not include any identifiable information about human participants. This research did not involve human subjects, so informed consent for publication is not required. The manuscript focuses solely on the technical aspects of the Offline Lab Exam Monitoring System and excludes any identifiable human data.

Availability of Supporting Data
The data used to design the Offline Lab Exam Monitoring System is readily available. We can share the details of resources and code used upon reasonable request by contacting the corresponding author. This ensures transparency while protecting any proprietary information.

Competing Interests
The authors declare no competing interests.

Funding
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.(Not applicable)

Abbreviations

- **USB -** Universal serial Bus
- **CBTs -** Computer-Based Tests
- **UNIX -** UNiplexed Information Computing System
- **MAC -** Mandatory Access Control RES - Rapid Keypress Sequence
- **CNN -** Convolutional Neural Network
- **MTCNN-**Multi-Task Cascaded Convolutional Neural Networks
- **RCNN -** Region-based Convolutional Neural Network
- **ASO -** Atom Search Optimization FKNN - fine K-nearest neighbor

REFERENCES

1. A Mandatory Access Control Mechanism For The Unm" FILE SYSTEM Tim Thomas Motorola Inc., Microcomputer Division Champaign-Urbana Design Center 1101 E. University Avenue, Urbana, IL, 61801
2. USBlock: Blocking USB-Based Keypress Injection Attacks Sebastian Neuner, Artemios G. Voyiatzis, Spiros Fotopoulos, Collin Mulliner, Edgar R. Weippl
3. iFetcher: User-Level Prefetching Framework With File-System Event Monitoring for Linux Jiwoong Won1 , Oseok Kwon, Junhee Ryu, Dongeun Lee, And Kyungtae Kang, (Member, IEEE)
4. Remote Online Proctoring System. Mohan Vamsi A, Niteesh B, Sai Ashwin D,K Kajendran
5. Implementation of an Intelligent Exam Supervision System Using Deep Learning Algorithms Fatima Mahmood, Jehangir Arshad, Mohamed Tahar Ben Othman, Muhammad Faisal Hayat , Naeem Bhatti , Mujtaba Hussain Jaffery , Ateeq Ur Rehman and Habib Hamam
6. Categorizing the Students' Activities for Automated Exam Proctoring Using Proposed Deep L2-GraftNet CNN Network and ASO Based Feature Selection Approach TANZILA SABA, (Senior Member, IEEE), Amjad Rehman, (Senior Member, IEEE), NOR Shahida Mohd Jamail1 , Souad Larabi-Marie-Sainte, Mudassar Raza, (Senior Member, IEEE), and Muhammad Sharif, (Senior Member, IEEE)