



SURVEY: CHEATING DETECTION IN ONLINE EXAMS

Rehab Kareem kadthim¹, and Zuhair Hussein Ali ²

¹⁻²Department of Computer Science, College of Education

Mustansiriyah University,

Iraq

ABSTRACT

The COVID-19 pandemic has compelled students and faculty at schools and institutions worldwide to switch to remote coaching. One of the most challenging aspects of online education is maintaining the academic integrity of student tests. Exams are now being administered. Without the presence of students and teachers in the exact location, students and teachers can learn online using e-learning platforms, which creates various difficulties such as exam integrity and safety. The COVID-19 pandemic has stretched university test processes to their limits. The deployment of e-assessments was hastened. Cheating attempts had been identified, and college students believe that most cheating attempts went undetected. Despite the recent increase in distance education, there has been little research on whether online exams make it easier for students to cheat. This study explores the topic of cheating in online education, focusing on cheating and plagiarism. Detection Methodologies It includes cheating strategies, cheating methods, Detecting methods, such as (Biometric techniques, Online Proctoring, lockdown browsers, challenges questions, and text originality checks). The impact of this paper is that it provides a concept for beginners to expertise and a foundation for reducing assessment dishonesty.

Keywords: Cheating Detection, E-Learning, Examination, Online Proctoring, Academic Dishonesty.

1. INTRODUCTION

During crucial situations such as natural catastrophes, conflicts, and pandemics like COVID 2019, e-learning has demonstrated potential effects. As a result, many methodologies and learning management software have been developed to offer and promote E-learning successfully during the last three decades. The use of E-learning is increasing all the time, which brings both opportunities and challenges in terms of online lecture delivery, material management, and adequately managing online assessments. In combination with dependable and high-speed internet infrastructure, different technological improvements enable E-learning to be a credible educational platform. [1]

Cheating in exams has been taking place seeing that appearance. However, there are growing concerns about using electronic devices in the present cheating technique in written exams. Attempts to benefit from a bonus aren't a new and present-day phenomenon or one that instructional institutions were unaware of, considering that tests and examinations were first hired. [2]

Cheating in summative re-evaluation is the aim uncertainty amongst university lecturers[3] because the new methods and technical possibilities are numerous, and there are only a few accredited means of monitoring. Prior research suggests various attempts to deal with dishonesty in higher education and assessment. While a few publications don't forget technical alternatives of cheating [4], some explore the transition from analogue to virtual and the new forms of cheating that come with it[5]. Others capture only reasons to cheat inside the instructional sense [6]without looking more carefully at virtual occasions. It is assumed that most cheating is undetected. Understanding the cheating defecation is step one toward preventing it. Suppose one knows why a pupil is dishonestly boosting their overall performance. In that case, one can intrude preventively by growing technical hurdles or selecting a most excellent character didactical approach. But it has no longer yet been investigated why college students cheat in summative assessment, exceptionally written online assessments[7].

The most common motivation for cheating among college students' is parental pressure, Fear of failure. Ambiguous educational goals, a desire for a higher grade, and a lack of time. easy the solution access online. [8] To reduce the spread of cheating, strict surveillance and the usage of video cameras were implemented [9]. Understanding the strategies students

employ to cheat during tests is of particular interest to educational authorities [10]. As a result, this research aims to look into the tactics that students use to cheat and the methods utilized to identify cheating.

2. CHEATING METHODS

Now section has highlighted technology methods of cheating, with technology that can hold more significant amounts of information.

2.1 Reflection- Screen Sharing. When taking an exam from a distance, applicants can use numerous displays to approach and answer a friend's test question simultaneously. Candidates have been known to cheat on tests by sharing their screens.

2.2 They are using Cutting-Edge Technology. Students will frequently find ways to cheat in an online exam with cameras. Companies that administer high-tech online exams like the CAT, MAT, and other competitive exams have lately been mentioned, with test-takers employing smaller, almost undetectable Bluetooth devices.

2.3 Cellular phones. Fraud using smartphones in invigilated online tests is on the rise. Candidates can use connected devices to save answers and to help fellow test-takers find answers from each other or outside sources.

2.4 Software for automatic coding. During school/university exams or recruitment programming tests, candidates can employ auto coding software to pass the exam. These applications are created by software that does not require the candidate to write any code.

2.5 Offers in Navigation During online exams. Students took advantage of their easy access to the internet and social media platforms to commit fraud. They tend to connect to unapproved websites during the test, paste questions into URLs, and grab the best solution they can.

2.6 Impersonation. Taking the test for someone else is well-known. When tests are given remotely online, however, the odds of a student attending the exam on behalf of others are very high. Many testers have used impersonators to derail so-called "high-integrity" tests for years.

2.7 External Devices are used. Fraudsters frequently employ hard drives, USBs, MicroSD, and other external smart devices in online tests since they are easy to conceal and difficult to detect. Students insert them before or after the test to make a replica of online tests that they may sell to other students' post-exam or distribute online

2.8 In the room are their relatives and friends. Helping a family member or acquaintance get near to individuals who come to the test is one of the most prevalent ways to cheat on multiple-choice tests or quizzes online. These aides have hidden behind the screen or away from the webcam. They either write or whisper the answer

Such students frequently cover their faces, disappear from the computer, glance around the room, or make suspicious movements.

2.9 Copying and pasting. As well as other keyboard shortcuts, Copying and pasting answers are some of the most popular forms of cheating on online tests. Students can frequently copy and paste answers from documents or notepads that have been prepared in a different window before the start of the test. These are easy techniques to deceive remote proctoring software that doesn't know what's happening on the screen. Because the IRIS Invigilation software records screen activity, the student would be detected cheating in this situation.

2.10 They are exiting the test deliberately. Students who consider cheating on online tests frequently try to outsmart the program by intentionally omitting themselves from the exam. They make excuses like a bad internet connection or a power outage to get out of the exam and turn off the camera recording so they can search for answers to exam questions quickly. After that, they log back in and continue with their evaluation. Some students flatly lie and claim that they cannot use the software at all, but they are only creating excuses to avoid being invigilated.

3. CHEATING DETECTION METHODS

The need and use for online or computer-based examinations appear to be increasing. In contrast, this type of examination gives students a more comprehensive range of opportunities, including cheating, than non-computerized examination methods. There are many different reasons to check for cheating and many ways to perform it. And many ways to deal with it. Given the balance at this level, new methods of abuse merit new ways to prevent or at least detect. And as universities move to online delivery. Faculty and administrators face the difficulty of discovering new approaches for appropriately assessing student learning online while maintaining academic honesty.

Figure 1 presents the Detection methods For cheating, which consists of biometric techniques, online proctoring, challenge questions, checks for text originality, lockdown browsers.

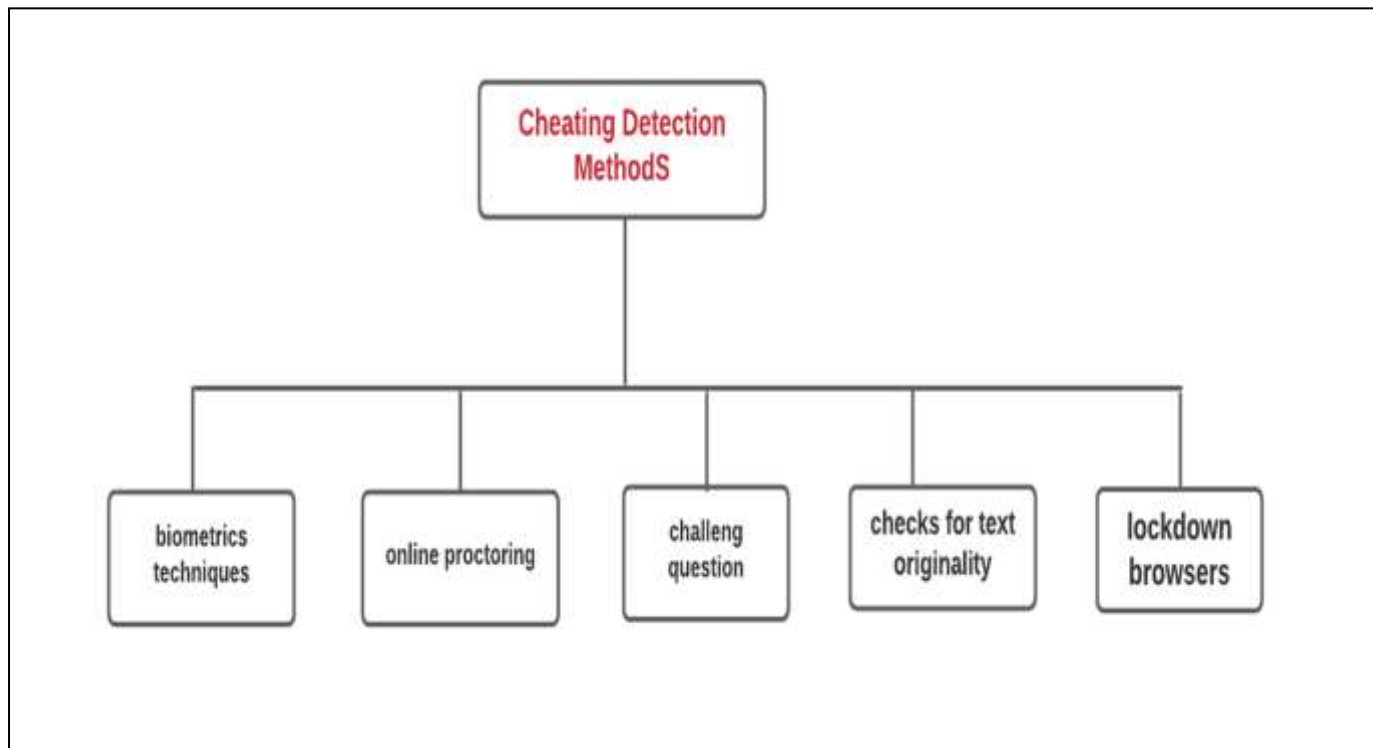


Figure (1): methods cheating detection

3.1 Biometric technique

Biometric authentication is one of the most common techniques. For verifying the identity of participants in online testing environments By comparing a recorded biometric sample with recent Biometrics taken to identify the student Biometric technologies can be categorized into two types They involve contact with a scanner (such as fingerprints) and those that do not, such as eyes Biometrics[11] typically use physiological characteristics such as fingers, eyes or behavioural characteristics such as signature, mouse movement or fundamental press dynamics The combination of two or more of the above features increases the accuracy of software recognition which is vital to ensure protection. Thus, biometric techniques are one of the effective ways that most researchers are studying to find more efficient solutions to prevent cheating in electronic examinations[12].

3.2 Online Proctoring

There are several methods for detecting cheating in online tests available. Online proctoring can take a variety of forms: -

3.2.1 Video summarization

Artificial intelligence is used to detect cheating activities that may occur during the exam using video abstraction software, commonly known as video abstraction. Throughout the exam, students are videotaped using their webcams. If a case of cheating is detected. The software will notify an observer that the video is available for future viewing. Observers' time (A set of images derived from the video source) or video clips can be created by video summarizing tools (video clips extracted from the video source). An intelligent application that includes a Monitoring system to detect suspicious student activity in the examination hall using a high-density camera is an example of this.[13]

3.2.2 Web Video Recording

When a student is videotaped throughout a test so that the teacher may watch it later, this is referred to as web video recording. Administrators and teachers may have more faith in this service because they can see the entire test rather than just the noted scenarios. They have access to the whole exam, not just the ones that have been highlighted. However, it is unlikely that you will review all of the tests individually. there may be confusing situations reported electronically with no option to investigate further and no method to mitigate risks if potentially suspicious behaviour happens[14]

3.2.3 Live Online Proctoring

This method employs the webcam and microphone of the student to allow a live observer to monitor students throughout an online exam. Individual observation sessions are available, and group observation sessions in which a single monitor supervises many pupils. Because it is the most similar to a personal test, many administrators may feel more comfortable employing this type of service. Cheating conduct can go undetected even with a direct observer supervising the student. Because the proctor does not have a consistent 360-degree view of the student, there are additional methods not to catch cheating in an online test. Students usually are asked to reveal their test environment to their observer at the start of the session. Nevertheless, cheating materials throughout the session are prohibited. [14]

3.3 challenges question

This is one of the most straightforward approaches for validating a test. This method is called a "knowledge-based authentication" method since it involves personal knowledge to validate the learner. Multiple-choice questions based on their backgrounds are being asked. Such as information about their previous home addresses, the name of their high school, or their mother's name. This exemplifies this strategy. Then, to acquire entry to the test, pupils must answer these questions, which may be random during the evaluation. These queries are usually based on data gathered from third parties using data mining technologies, or the student can enter them during the first login process before any exam. [15]

This straightforward procedure can be used to verify the test taker's identity. However, it cannot be utilized to keep track of Exam-related student behaviour. Furthermore, kids may circumvent the authentication process by sending answers to others to have someone else take the examination or by collaborating with others while taking the examination. As a result, this method should be used in conjunction with additional security testing methodologies.

3.4 checks for text originality

If the usage of tests necessitates a written response. Using software to check for text originality (such as "Turnitin") can assist in identifying material that has been plagiarized without due citation. Thus, submitted artworks are compared to other work maintained in the software's bank for this purpose. The advantages of this technique include the ability to compare submitted work to work that is open to the public (as defined by the software organization) to check for basic levels of overlap and compare submitted work to past assignments.

Although examining the text's validity can help reveal both with dedication. There are ethical concerns regarding the technique. Including copyright infringement of student work.[14]

3.5 lockdown browsers

Lockdown browsers prevent you from accessing additional electronic materials during tests by preventing college students from visiting external websites or running unapproved programs on the same device used to take the test. These programs take control of the entire laptop device.

Lockdown browsers, while likely advantageous, cannot ensure that outside data will not be accessible During an examination. Students may still have access to records by utilizing any other computer, a cell phone, class notes, and so on. College students can also get around the lockout browser application by disabling it. For these reasons, it is recommended that these applications be used with other examination security measures to prevent and detect fraudulent activity during exams. [14,16].

4. CONCLUSION

Academic staff should be concerned with academic dishonesty because of the following eight issues: equity, character development, the task of imparting knowledge, student morale, faculty morale, future student behaviour, reputation for learning, and public trust in higher education. In this paper, we reviewed the great importance of e-learning, as well as the concept of cheating in exams and some types of cheating practiced by students, which increase and vary in conjunction with the general of e-learning, in addition to the main ways in which researchers can expand to find solutions that will detect cheating. The idea is that we have reached the scientific importance in the proper investigation of the methods used in the detection, whether they are biometric, statistical, or direct control methods, and we intend to find solutions and methods for detecting fraud that is practical and easy to apply to achieve scientific sobriety and academic integrity. We hope to review them in our upcoming research.

ACKNOWLEDGMENT

The authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad – Iraq, for its support.

REFERENCE

- [1] A. W. Muzaffar, M. Tahir, M. W. Anwar, Q. Chaudry, S. R. Mir, and Y. Rasheed, "A systematic review of online exams solutions in e-learning: Techniques, tools, and global adoption," *IEEE Access*, vol. 9, pp. 32689–32712, 2021, DOI: 10.1109/ACCESS.2021.3060192.
- [2] K. Curran, G. Middleton, and C. Doherty, "Cheating in Exams with Technology," *Int. J. Cyber Ethics Educ.*, vol. 1, no. 2, pp. 54–62, 2011, DOI: 10.4018/ijcee.2011040105.
- [3] P. Dawson, "Five ways to hack and cheat with bring-your-own-device electronic examinations," *Br. J. Educ. Technol.*, vol. 47, no. 4, pp. 592–600, 2016, DOI: 10.1111/bjet.12246.
- [4] H. Mellar, R. Peytcheva-Forsyth, S. Kocdar, A. Karadeniz, and B. Yovkova, "Addressing cheating in e-assessment using student authentication and authorship checking systems: Teachers' perspectives," *Int. J. Educ. Integr.*, vol. 14, no. 1, 2018, doi: 10.1007/s40979-018-0025-x.
- [5] A. Chirumamilla, G. Sindre, and A. Nguyen-Duc, "Cheating in e-exams and paper exams: the perceptions of engineering students and teachers in Norway," *Assess. Eval. High. Educ.*, vol. 45, no. 7, pp. 940–957, 2020, DOI: 10.1080/02602938.2020.1719975.
- [6] H. Yu, P. L. Glanzer, B. R. Johnson, R. Sriram, and B. Moore, "Factors Why College Students Cheat : A Conceptual Model of Five Factors," vol. 41, no. 4, pp. 549–576, 2018.
- [7] A. Jantos, "Motives for Cheating in Summative E-Assessment in Higher Education - a Quantitative Analysis," *EDULEARN21 Proc.*, vol. 1, no. July, pp. 8766–8776, 2021, DOI: 10.21125/edulearn.2021.1764.
- [8] R. Bawarith, D. Abdullah, D. Anas, and P. Dr., "E-exam Cheating Detection System," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 4, pp. 176–181, 2017, DOI: 10.14569/ijacsa.2017.080425.
- [9] "Cheating in Academic Institutions : A Decade of," no. November 2014, pp. 37–41, 2010, DOI: 10.1207/S15327019EB1103.
- [10] D. A. Odongo, E. Agyemang, and J. B. Forkuor, "Innovative Approaches to Cheating : An Exploration of Examination Cheating Techniques among Tertiary Students," vol. 2021, pp. 12–16, 2021.
- [11] A. M. Duhaim, S. O. Al-Mamory, and M. S. Mahdi, "Cheating {Detection} in {Online} {Exams} {During} {Covid}-19 {Pandemic} {Using} {Data} {Mining} {Techniques}," 2021.
- [12] K. Rabuzin and M. Sajko, "E-learning : Biometrics as a Security Factor," vol. 00, no. C, 2006.
- [13] B. A. T. U. Truong and S. Venkatesh, "Video Abstraction : A Systematic Review and Classification," vol. 3, no. 1, pp. 1–37, 2007, DOI: 10.1145/1198302.1198305.
- [14] O. Holden, V. Kuhlmeier, and M. Norris, "Academic Integrity in Online Testing: A Research Review," 2020, DOI: 10.31234/osf.io/rjk7g.
- [15] J. M. Jr, A. Fitterer, E. Brazier, J. Leonard, A. Brown, and A. Texas, "Examining Online College Cyber Cheating Methods and Prevention Measures," vol. 11, no. 2, pp. 139–146, 2013.
- [16] N. P. Member, J. P. Member, and C. Martin, "The Virtual Invigilator : A Network-based Security System for Technology-enhanced Assessments," no. May 2014, 2008.