

“Managing Academic Dishonesty in The Age of Ai: Challenges and Solutions for University Examinations.”

DR. SAMWEL NYAGUCHA ORESI, PHD

Senior Lecturer Presbyterian University

Date of Submission: 04-09-2026

Date of Acceptance: 14-09-2026

KEYWORDS

Academic Dishonesty – Any deliberate misconduct in learning or assessment, including cheating, plagiarism, collusion, or misuse of technology.

Examination Malpractice – Actions that violate exam rules and compromise fairness, such as impersonation, paper leakage, or unauthorized collaboration.

Artificial Intelligence (AI) – Digital systems (e.g., ChatGPT, proctoring software) that both support learning and create new risks of cheating in higher education.

Generative AI – Tools that produce essays, assignments, or exam answers automatically, raising concerns about originality and authorship.

Digital Proctoring – AI-powered monitoring systems using facial recognition, keystroke analysis, or eye-tracking to detect suspicious behavior during online exams.

Plagiarism Detection – AI-based tools that scan databases to identify copied or AI-generated content, ensuring originality in student work.

Contract Cheating – Outsourcing academic tasks to third parties or platforms, increasingly facilitated by AI, undermining genuine student effort.

Ethical AI Use – Responsible application of AI in education, distinguishing legitimate learning support from misconduct.

Academic Integrity – The principle of honesty, fairness, and accountability in education, ensuring qualifications reflect genuine competence.

Policy Reforms in Education – Institutional and governmental measures to strengthen rules, monitoring, and ethical awareness in response to evolving malpractice.

EXECUTIVE SUMMARY

The integration of Artificial Intelligence (AI) into higher education has fundamentally reshaped the dynamics of academic integrity. Generative AI tools such as ChatGPT are increasingly being used by students to produce essays, assignments, and even exam responses. While these technologies offer new opportunities for learning support, they simultaneously pose significant risks to the credibility of traditional assessments. Universities across the globe are grappling with the reality that detection-based strategies alone are insufficient to address the evolving landscape of exam malpractice.

Recent case studies from UK universities, Jamhuriya University of Science and Technology in Somalia, and comparative global reviews illustrate that academic misconduct is no longer confined to plagiarism and collusion. It now encompasses contract cheating, AI-generated assignments, and other digitally enabled practices. Institutions have responded by piloting AI-powered integrity systems, redesigning assessments, and promoting ethical literacy among students. However, these interventions have revealed a set of persistent challenges. False positives unfairly penalize students when legitimate work is misclassified as misconduct. Privacy concerns arise from intrusive surveillance and biometric data collection. Bias in AI models disproportionately affects diverse student populations, particularly those from underrepresented linguistic and cultural backgrounds. Furthermore, the adaptability of malpractice methods often outpaces the evolution of detection systems, creating a constant cycle of vulnerability.

To address these challenges, universities must adopt a holistic and balanced approach. Recommendations emphasize the importance of combining AI with human oversight to ensure fairness and contextual judgment. Transparent policies on AI surveillance and data governance are essential to build trust and protect student rights. Training programs for both educators and students can foster ethical awareness and responsible use of AI, ensuring that technology is seen as a partner in learning rather than a punitive mechanism. Multi-layered security strategies — blending technological tools, human review, and pedagogical reforms — provide

resilience against evolving malpractice methods. Finally, institutional capacity building and global collaboration are critical for sharing best practices, harmonizing policies, and strengthening academic integrity across diverse contexts.

Ultimately, AI should be treated as a supportive tool rather than a final arbiter of misconduct. The credibility of academic assessments in the digital era depends not only on technological innovation but also on the values of fairness, inclusivity, and trust that guide its use. By embedding AI within transparent, ethically grounded, and pedagogically sound frameworks, universities can safeguard integrity while fostering a culture of honesty and accountability.

POLICY BRIEF

Title: *Safeguarding Academic Integrity in the Age of Artificial Intelligence*

Problem

The rise of generative AI tools such as ChatGPT has transformed higher education, enabling students to produce essays and exam responses with unprecedented ease. While these technologies offer learning support, they also pose serious risks to academic integrity. Traditional detection-based strategies are increasingly inadequate, as malpractice methods evolve faster than monitoring systems.

Evidence

- i) **False Positives:** AI systems sometimes misclassify legitimate student work as misconduct, undermining fairness.
- ii) **Privacy Concerns:** Continuous surveillance and biometric data collection raise ethical issues around consent and data security.
- iii) **Bias in AI Models:** Detection tools often perform unevenly across diverse student populations, disproportionately affecting marginalized groups.
- iv) **Adaptability of Malpractice:** Cheating strategies evolve rapidly, outpacing static detection methods.
- v) **Global Case Studies:** Universities in the UK, Somalia, and elsewhere report rising misuse of AI in exams, prompting reforms in assessment design and integrity systems.

Recommendations

- i) **Combine AI with Human Oversight**
Ensure that AI alerts are reviewed by faculty or integrity committees before punitive action is taken.
- ii) **Develop Transparent Policies on AI Surveillance**
Clearly define scope, consent, data governance, and accountability to build trust and protect student rights.
- iii) **Train Educators and Students on Ethical AI Use**
Provide capacity-building programs that distinguish legitimate AI support from misconduct.
- iv) **Encourage Multi-Layered Security**
Blend plagiarism detection, behavioral analytics, identity verification, and assessment redesign for resilience.
- v) **Institutional Capacity Building and Collaboration**
Strengthen infrastructure, share best practices, and harmonize policies across regions to ensure fairness and inclusivity.

Implications

Treating AI as a supportive tool rather than a final arbiter of misconduct ensures balanced judgment and protects student trust. By embedding AI within transparent, ethically grounded, and pedagogically sound frameworks, universities can safeguard academic integrity while fostering a culture of honesty and accountability. This holistic approach strengthens credibility in higher education and prepares institutions to adapt to the evolving digital era.

I. INTRODUCTION

1.1 Overview

Exam malpractice refers to any deliberate act of misconduct by candidates, examiners, or other stakeholders that violates established examination rules and compromises the integrity, fairness, and credibility of the assessment process. It is essentially the violation of examination ethics with the intent of gaining undue advantage or distorting the true measure of academic performance.

Ajayi (2024) – “Exam malpractices can jeopardize the validity and dependability of test outcomes, which is a serious danger to the integrity of educational assessments.” This definition emphasizes the threat malpractice poses to the credibility of examinations and the reliability of results.

Tambawal (2023) – “Examination malpractice is deliberate wrongdoing that undermines the integrity of the examination process.” This definition highlights intentional misconduct and its impact on fairness and credibility.

Akaranga & Ongong (2022) – “Examination malpractice is commonly defined as a deliberate wrongdoing contrary to official examination rules designed to place a candidate at an unfair advantage or disadvantage.” This definition stresses both the violation of rules and the distortion of fairness in assessment.

The integration of Artificial Intelligence (AI) into university examinations has transformed both assessment practices and the landscape of academic integrity. Scholars highlight that while AI offers powerful tools to enhance fairness and efficiency, it also introduces new challenges in the fight against exam malpractice.

AI technologies are increasingly deployed in higher education to safeguard examinations. According to Lancaster and Cotarlan (2021), AI-driven proctoring systems use facial recognition, keystroke analysis, and eye-tracking to monitor students during online exams, reducing opportunities for cheating. Similarly, Stoesz and Eaton (2020) argue that plagiarism detection software powered by AI has become central in identifying copied or AI-generated content in assignments. These innovations reflect universities’ efforts to maintain credibility in an era of digital learning.

AI also supports automated grading and predictive analytics. Bretag (2019) notes that automated systems can reduce human bias and ensure consistency, while predictive models help identify unusual performance patterns that may signal malpractice. Thus, AI is positioned as both a preventive and corrective mechanism in academic assessment.

Examination malpractice is a global phenomenon that manifests differently across regions but shares common roots in pressure to succeed, weak enforcement, and technological misuse. Scholars have documented diverse experiences worldwide, showing that while traditional forms persist, digital and AI-driven malpractices are rising.

In developed countries, malpractice takes more subtle and digital forms. McCabe, Treviño, and Butterfield (2001) found that cheating in U.S. universities is influenced by peer culture and institutional responses. More recently, Eaton (2023) emphasizes that generative AI tools such as ChatGPT pose new risks, enabling students to produce sophisticated but unoriginal work.

In India and Pakistan, malpractice often involves large-scale paper leaks and organized cheating rings. Sharma (2015) observes that competitive exams for government jobs and university admissions are particularly vulnerable, with digital technologies enabling mass cheating. In China, Yang (2018) reports that strict government crackdowns have reduced malpractice, but online exam fraud remains a challenge.

In countries such as Nigeria and Ghana, exam malpractice has become deeply entrenched. Agyemang (2016) notes that practices like paper leakage, impersonation, and collusion are widespread, often facilitated by corruption and inadequate monitoring systems. Similarly, Olatunbosun (2009) highlights that examination malpractice in Nigeria undermines the credibility of education and contributes to declining standards.

Despite technological advances, exam malpractice remains a persistent issue. McCabe, Treviño, and Butterfield (2001) emphasize that cheating in universities is often systemic, influenced by peer behavior, institutional culture, and weak enforcement. Traditional forms of malpractice include:

- i) Cheating with unauthorized materials (notes, devices).
- ii) Collusion among students.
- iii) Impersonation during exams.
- iv) Leakage of exam papers before tests.

Digital transformation has introduced new forms of malpractice. Cotton, McMullan, and Scott (2001) highlight that online exams are vulnerable to impersonation and unauthorized collaboration. More recently, Eaton (2023) warns that generative AI tools (e.g., ChatGPT) pose fresh risks, enabling students to produce sophisticated but unoriginal work.

The paradox is clear: AI is both a solution and a challenge. While it strengthens monitoring and detection, it also provides students with new avenues for malpractice. As Sutherland-Smith (2008) argues, universities must adopt holistic approaches—combining technology, pedagogy, and policy—to ensure that academic integrity is preserved.

Examinations remain one of the most widely used methods of assessing student learning, competence, and readiness in educational institutions. They serve as a cornerstone of academic integrity, providing a structured way to evaluate knowledge and ensure fairness in certification. However, the credibility of examinations has increasingly been undermined by malpractice — deliberate actions by students or external actors to gain unfair advantage during assessments.

Exam malpractice is not a new phenomenon; it has existed in various forms for decades, ranging from copying answers and impersonation to collusion and unauthorized use of notes. Yet, in the digital era, malpractice has taken on more complex and technologically enabled dimensions. The rise of smartphones, social media platforms, and generative AI tools has expanded opportunities for cheating, making detection and prevention far more challenging.

The consequences of exam malpractice extend beyond individual misconduct. At the institutional level, it erodes trust in academic systems, compromises the value of qualifications, and damages the reputation of universities.

At the societal level, it produces graduates who may lack genuine competence, thereby weakening professional standards and economic productivity.

Understanding exam malpractice therefore requires a holistic perspective — one that considers both traditional methods of cheating and emerging digital threats. It also calls for a balanced approach that integrates technological innovation, ethical safeguards, and pedagogical reforms to preserve the integrity of assessments while respecting student rights.

1.2 Core Features of Exam Malpractice

Exam malpractice manifests in multiple forms, ranging from traditional misconduct to modern digital manipulation. Below is a structured breakdown of its core features:

Examination malpractice takes many forms across universities and schools, undermining academic integrity and credibility. The following categories highlight the most common practices:

- i) **Cheating** - This involves the use of unauthorized materials such as notes, textbooks, or crib sheets during exams. Students may also engage in concealment of answers on clothing, body, or personal items, or resort to copying from another candidate's script.
- ii) **Impersonation** - Here, a candidate may hire another person to sit the exam on their behalf, or commit identity fraud through falsified registration and forged documents.
- iii) **Collusion** - Collusion occurs when candidates cooperate to share answers during the exam. This may involve coded signals, gestures, or whispering to exchange information discreetly.
- iv) **Leakage of Exam Content** - This malpractice involves unauthorized access to exam questions before the test. Leaked papers are often distributed through social media, print, or underground networks, compromising fairness.
- v) **External Assistance** - Students may receive help from invigilators, supervisors, or insiders, or use communication devices such as phones, smartwatches, or earpieces to obtain answers during exams.
- vi) **Digital Malpractice** - With the rise of online assessments, malpractice has evolved into digital forms. This includes screen sharing during online exams, use of AI chatbots (e.g., GPT-based tools) to generate real-time answers, and plagiarism through copy-paste from online sources.
- vii) **Institutional Malpractice** - At the systemic level, malpractice may involve ghost centers (fake exam venues created to manipulate results), alteration of scripts or grades by corrupt officials, or fraudulent certification without proper assessment.

Exam malpractice is multifaceted, ranging from individual cheating to institutional corruption. While traditional methods persist, digital and AI-driven malpractices are increasingly prevalent, requiring universities to adopt holistic strategies that combine technology, policy reforms, and ethical education.

The core features of exam malpractice reveal that it is not limited to student misconduct—it can involve examiners, administrators, and institutions. In the digital age, malpractice has expanded to include AI misuse, online collusion, and technological manipulation, making it a systemic challenge to educational integrity.

1.3 The Rise of Online and Remote Examinations

The adoption of online and remote examinations has reshaped assessment practices worldwide, particularly following the COVID-19 pandemic, which accelerated the shift toward digital learning and evaluation. The shift toward online and remote examinations has been one of the most significant transformations in higher education assessment in recent years. Initially driven by the COVID-19 pandemic, universities worldwide adopted digital platforms to ensure continuity of learning and evaluation. This transition has created both opportunities and challenges for institutions, students, and policymakers.

Convenience and flexibility have been major drivers, allowing students to sit for exams from home without the need for physical travel. This has also enhanced scalability, enabling institutions to administer tests to large numbers of candidates across different regions simultaneously.

Technological innovations such as biometric verification, facial recognition, and AI-powered remote proctoring have further strengthened the credibility of online exams. Additionally, the globalization of education has made remote examinations essential for international students and distance learning programs.

While the benefits include time savings, inclusivity, and instant grading through automated systems, challenges remain. Issues of academic integrity are heightened, with risks of cheating through digital tools and AI misuse. Technical barriers such as poor internet connectivity can disadvantage students, while privacy concerns arise from continuous surveillance during proctored exams. Moreover, equity gaps persist, as not all learners have equal access to devices or stable internet connections.

Looking ahead, the future of online examinations points toward greater reliance on AI for real-time monitoring, hybrid models that blend in-person and remote testing, and a stronger emphasis on competency-based assessments rather than rote memorization.

In short, the rise of online and remote examinations has brought convenience and global reach, but it also demands robust safeguards to protect integrity, fairness, and student trust.

1.4 AI as a Challenge

Artificial Intelligence (AI) has emerged as both a guardian of academic integrity and a disruptor of traditional assessment systems. Universities worldwide are grappling with the paradox that while AI strengthens monitoring and detection, it simultaneously empowers students to cheat in more sophisticated ways.

One of the most pressing challenges is the misuse of generative AI tools such as ChatGPT. These systems allow students to produce essays, assignments, and even exam answers that appear original but are machine-generated. As Eaton (2023) observes, generative AI blurs the line between authentic student work and automated output, raising profound questions about authorship and integrity.

Another dimension is contract cheating, where students outsource their work to online platforms. Lancaster and Cotarlan (2021) highlight that many of these platforms now integrate AI, providing instant, tailored solutions to exam questions. This makes detection more difficult and expands the scale of malpractice beyond traditional boundaries.

Even AI-based proctoring systems, designed to safeguard exams, present challenges. Tools that rely on facial recognition, eye-tracking, and keystroke analysis can misidentify students or create a surveillance-heavy environment. Stoesz and Eaton (2020) caution that while such systems enhance monitoring, they risk alienating students and raising ethical concerns about privacy.

The issue of inequality also emerges strongly. AI-driven exam systems require stable internet, advanced devices, and digital literacy. Students in resource-constrained regions face disadvantages, widening educational inequities. Bretag (2019) emphasizes that integrity solutions must be inclusive, otherwise they risk marginalizing already vulnerable populations.

Finally, universities face policy and ethical challenges. Institutional frameworks often lag behind technological advances, leaving gaps in regulation. Sutherland-Smith (2008) argues that academic integrity policies must evolve beyond plagiarism detection to address new realities shaped by AI.

AI is both a solution and a challenge in examinations. It strengthens monitoring and detection but simultaneously creates new avenues for malpractice. The challenge for universities lies in balancing innovation, fairness, and ethics, ensuring that AI supports learning rather than undermining it. Some of the challenges are;

- i) **AI-Generated Content:** Students can use generative AI tools (like ChatGPT or essay bots) to produce assignments, essays, or even exam answers, bypassing genuine effort.
- ii) **Accessibility & Ease of Use:** AI platforms are widely available, often free or low-cost, making it easy for students to misuse them during take-home exams or online assessments.
- iii) **Detection Difficulty:** Some AI-generated work is sophisticated enough to evade traditional plagiarism checkers, making it harder for lecturers to identify cheating.
- iv) **Erosion of Academic Integrity:** Over-reliance on AI undermines critical thinking, originality, and the credibility of university qualifications.

1.5 AI as a Solution

Artificial Intelligence (AI) is increasingly recognized as a powerful ally in safeguarding academic integrity and improving the efficiency of university examinations. While AI presents challenges, it also offers innovative solutions that can transform assessment practices for the better.

AI-powered tools such as plagiarism detection systems help universities identify copied or AI-generated content. Stoesz and Eaton (2020) emphasize that these technologies have become central to maintaining fairness in academic work. By scanning vast databases, AI ensures originality and discourages dishonest practices.

AI-driven proctoring uses facial recognition, eye-tracking, and keystroke analysis to monitor students during online exams. Lancaster and Cotarlan (2021) note that such systems reduce opportunities for impersonation and collusion, strengthening trust in remote assessments.

AI enables consistent and unbiased grading of exams and assignments. Bretag (2019) highlights that automated systems not only save time but also provide immediate feedback, enhancing learning outcomes. This reduces human error and ensures fairness across large cohorts.

AI can analyze student performance patterns to detect anomalies that may indicate malpractice. Eaton (2023) argues that predictive models allow institutions to intervene early, preventing systemic cheating and supporting students who may be at risk academically.

AI supports inclusive assessment by offering adaptive testing tailored to individual student needs. Sutherland-Smith (2008) suggests that technology-driven solutions can make exams more flexible, accessible, and efficient, especially in diverse learning environments.

AI is not merely a monitoring tool—it is a transformative solution that enhances integrity, efficiency, and inclusivity in examinations. By combining detection, prevention, and feedback, AI helps universities uphold credibility while supporting student learning. AI can be beneficial in areas such as;

- i) **AI-Powered Detection Tools:** Universities are adopting AI-based plagiarism checkers and text analysis systems that can flag AI-generated content.
- ii) **Proctoring Software:** AI-driven exam monitoring tools use facial recognition, keystroke analysis, and behavioral tracking to detect suspicious activity during online exams.
- iii) **Pattern Recognition:** AI can analyze writing style consistency across assignments, helping identify when a student’s work is likely machine-generated.
- iv) **Preventive Education:** AI can also be used to train students on ethical use of technology, offering simulations and feedback that reinforce integrity.

1.6 Balanced View

Artificial Intelligence (AI) in university examinations presents a paradoxical reality: it is both a solution and a challenge. On one hand, AI strengthens academic integrity and efficiency; on the other, it introduces new risks that institutions must carefully manage.

AI technologies have revolutionized assessment by offering tools that enhance fairness and credibility. Plagiarism detection systems scan vast databases to ensure originality (Stoesz & Eaton, 2020). Smart proctoring systems use facial recognition and behavioral analysis to reduce impersonation and collusion (Lancaster & Cotarlan, 2021). Automated grading ensures consistency and reduces human bias, while predictive analytics help identify unusual performance patterns that may signal malpractice (Eaton, 2023). These innovations make examinations more reliable, efficient, and inclusive.

At the same time, AI creates new avenues for malpractice. Generative AI tools such as ChatGPT allow students to produce sophisticated but unoriginal work (Eaton, 2023). Contract cheating platforms increasingly integrate AI to deliver tailored answers, complicating detection (Lancaster & Cotarlan, 2021). Even AI-based proctoring systems raise ethical concerns about privacy and surveillance (Stoesz & Eaton, 2020). Furthermore, reliance on advanced technologies risks widening inequalities, as students in resource-constrained regions may lack access to stable internet or digital literacy (Bretag, 2019).

The challenge for universities is to strike a balance: leveraging AI to support learning and integrity while mitigating its risks. As Sutherland-Smith (2008) argues, academic integrity frameworks must evolve beyond plagiarism detection to address the broader digital realities of education. This requires not only technological solutions but also policy reforms, ethical safeguards, and cultural shifts that emphasize honesty and responsibility in learning.

AI is a double-edged sword in higher education;

- i) On one side, it empowers cheating by giving students shortcuts to bypass learning.
- ii) On the other, it equips universities with advanced tools to detect, prevent, and manage academic dishonesty more effectively.

II. FORMS OF EXAM MALPRACTICE

2.1 Introduction

Examination malpractice refers to any deliberate act that undermines the integrity, fairness, and credibility of academic assessments. It takes many forms, ranging from traditional cheating methods to modern technology-driven practices.

Examination malpractice remains one of the most pressing challenges confronting higher education globally. It undermines the credibility of academic qualifications, erodes trust in institutions, and compromises the fairness of assessment systems. As universities and policymakers strive to uphold academic integrity, it is essential to recognize the diverse forms that malpractice takes—ranging from traditional cheating to sophisticated digital manipulation.

Cheating often involves the use of unauthorized materials, concealment of answers, or copying from another candidate’s script. Impersonation, where a candidate hires another person or falsifies identity documents, represents a direct assault on the integrity of examinations. Collusion, through cooperation among candidates using signals or whispered exchanges, further weakens the fairness of assessments.

Leakage of exam content, whether through unauthorized access and distribution via social media or underground networks, remains a widespread malpractice in many regions. External assistance, such as help from invigilators or the use of communication devices, adds another layer of complexity. With the rise of digital learning, new forms of malpractice have emerged, including screen sharing during online exams, real-time use of AI chatbots, and plagiarism from online sources.

At the institutional level, malpractice can be systemic, involving ghost centers, alteration of scripts or grades, and fraudulent certification. These practices not only damage the reputation of universities but also diminish the value of academic qualifications in the labor market.

For policymakers, understanding the breadth and depth of exam malpractice is critical. Effective interventions must address both traditional practices and emerging digital threats, combining technological safeguards with strong governance frameworks. A balanced approach—integrating prevention, detection, and cultural change—is necessary to restore confidence in academic assessment and ensure that qualifications reflect genuine learning and competence.

2.2 Forms of Cheating

Cheating is one of the most prevalent forms of examination malpractice, cutting across institutions globally and undermining the credibility of academic qualifications. It represents deliberate attempts by candidates to gain unfair advantage during assessments, often exploiting weaknesses in exam administration and supervision.

At its core, cheating involves the use of unauthorized materials, such as notes, textbooks, or crib sheets, smuggled into the exam hall. In more concealed forms, students may hide answers on clothing, personal items, or even their bodies, relying on creativity and secrecy to bypass invigilators. Another widespread practice is copying from another candidate’s script, facilitated by poor seating arrangements or lax monitoring.

These practices not only compromise fairness but also erode trust in educational systems. They reflect both individual dishonesty and systemic weaknesses in exam management. For policymakers and institutions, understanding the forms of cheating is a critical step toward designing effective preventive measures, strengthening invigilation, and fostering a culture of integrity among learners.

i) Cheating with Unauthorized Materials

One of the most common forms involves students carrying unauthorized notes, textbooks, or electronic devices into the examination hall. These materials may be concealed in clothing, written on body parts, or stored on mobile phones. The intent is to gain unfair advantage by accessing information that should not be available during the exam.

ii) Collusion

Collusion occurs when two or more students collaborate during an examination. This may involve whispering answers, passing notes, signaling, or sharing solutions in online exams. Collusion undermines the principle of individual assessment and makes it difficult to evaluate each student’s true ability.

iii) Impersonation

In some cases, students arrange for another person to sit the exam on their behalf. This could be a friend, a hired individual, or even a more academically capable peer. Impersonation is a serious breach of integrity because it completely distorts the evaluation process and compromises the credibility of qualifications.

iv) Plagiarism and AI Misuse

With the rise of digital tools, plagiarism has expanded beyond copying from books or peers. Students now use generative AI systems to produce essays, assignments, or even exam responses. While AI can support learning, its misuse for dishonest purposes erodes originality and critical thinking, making it a modern form of malpractice.

v) Leakage of Exam Papers

This form of malpractice occurs when exam questions are accessed before the scheduled time. Leakage often involves corrupt officials or insiders who sell or distribute exam papers to students. It is particularly damaging because it compromises the entire assessment process and can invalidate results for large groups of candidates.

vi) Bribery and Corruption

Some students or parents resort to offering money, gifts, or favors to examiners, invigilators, or administrators to alter results or overlook malpractice. This form of corruption undermines trust in the education system and perpetuates inequality, as only those with resources can manipulate outcomes.

vii) Disruption and Misconduct

Examination malpractice also includes disruptive behaviors that compromise the exam environment. Examples include intimidating invigilators, deliberately distracting other candidates, or creating chaos to facilitate cheating. Such misconduct affects not only the integrity of the exam but also the concentration and performance of honest students.

Exam malpractice is multifaceted. Traditional methods like cheating with notes and collusion remain prevalent, but modern practices such as AI misuse and digital plagiarism are increasingly significant. Institutional malpractice, including leakage and bribery, further erodes trust in academic systems. Together, these forms highlight the urgent need for universities and schools to adopt robust detection mechanisms, ethical education, and strict enforcement policies to safeguard academic integrity.

2.2.1 Traditional Methods of Exam Malpractice

i) Cheating with Unauthorized Materials

This is one of the oldest and most widespread forms of malpractice. Students smuggle notes, textbooks, or prepared "crib sheets" into the examination hall. These materials may be hidden in clothing, written on body parts, or concealed in personal belongings. The intent is to gain unfair advantage by accessing information that should not be available during the exam.

ii) Collusion Among Students

Collusion occurs when candidates cooperate during an exam to share answers. This may involve whispering, passing notes, signaling with hand gestures, or deliberately distracting invigilators to exchange information. In group settings, collusion undermines the principle of individual assessment and makes it difficult to evaluate each student's true ability.

iii) Impersonation

Impersonation is a serious breach of academic integrity where one person sits an exam on behalf of another. This could involve hiring someone more academically capable or persuading a peer to take the test. Impersonation completely distorts the evaluation process and compromises the credibility of qualifications.

iv) Leakage of Examination Papers

Exam leakage occurs when questions are accessed before the scheduled time. This malpractice often involves insiders such as teachers, exam officials, or printers who illegally distribute exam papers to students. Leakage is particularly damaging because it invalidates the fairness of the entire assessment process.

v) Bribery and Corruption

Some students or parents resort to offering money, gifts, or favors to examiners, invigilators, or administrators to alter results or overlook malpractice. This form of corruption undermines trust in the education system and perpetuates inequality, as only those with resources can manipulate outcomes.

vi) Disruption and Misconduct in the Exam Hall

Students may deliberately disrupt the examination environment to facilitate cheating. This includes intimidating invigilators, distracting other candidates, or creating chaos that allows malpractice to occur unnoticed. Such misconduct affects not only the integrity of the exam but also the concentration and performance of honest students.

Traditional exam malpractice methods are rooted in physical acts of dishonesty — smuggling notes, colluding, impersonating, or bribing officials. While technology has introduced new forms of malpractice in recent years, these traditional methods remain prevalent, especially in contexts where examinations are conducted in physical halls with limited surveillance.

2.2.2 Digital Methods of Exam Malpractice

i) Use of Generative AI Tools

One of the most recent and widespread digital forms of malpractice involves students using generative AI platforms to produce essays, assignments, or even exam answers. These tools can generate sophisticated responses that mimic human writing, making it difficult for lecturers to detect dishonesty. While AI can support learning, its misuse for cheating undermines originality and critical thinking.

ii) Online Collusion

In virtual examinations, students may collaborate through instant messaging apps, social media platforms, or video calls. Unlike traditional collusion in physical exam halls, online collusion is harder to monitor because it occurs outside the official exam platform. This allows students to share answers in real time during assessments.

iii) Digital Plagiarism

Students increasingly copy content directly from online sources, academic databases, or shared documents. Unlike traditional plagiarism from textbooks, digital plagiarism is faster and easier, often involving copy-paste from websites or downloading ready-made assignments. This form of malpractice erodes academic integrity and makes originality harder to enforce.

iv) Unauthorized Use of Electronic Devices

Smartphones, tablets, and smart-watches are often misused during exams to access stored notes, search the internet, or communicate with peers. In online exams, students may use multiple devices simultaneously, making it difficult for invigilators to detect malpractice.

v) Hacking and System Manipulation

Some students attempt to exploit weaknesses in online exam platforms by hacking into systems, altering grades, or accessing exam questions before the scheduled time. This digital malpractice is particularly dangerous because it compromises institutional credibility and the security of academic records.

vi) Contract Cheating via Online Platforms

Digital environments have enabled the rise of “contract cheating,” where students pay online freelancers or use academic writing services to complete assignments or exams. These services are easily accessible and marketed aggressively, making them a growing threat to academic integrity.

vii) **Misuse of Online Collaboration Tools**

Platforms designed for group learning, such as Google Docs or Microsoft Teams, can be misused during exams. Students may secretly collaborate on shared documents while pretending to work individually, blurring the line between legitimate teamwork and malpractice.

Digital exam malpractice is more sophisticated and harder to detect than traditional methods. It leverages technology — from generative AI and online collusion to hacking and contract cheating — to bypass academic integrity standards. Universities now face the dual challenge of managing digital dishonesty while also using technology (AI-powered detection, proctoring software, plagiarism checkers) as part of the solution.

2.3 Emerging Risks of Exam Malpractice

Examination malpractice is no longer confined to traditional methods such as smuggling notes or collusion in exam halls. With the rapid advancement of digital technologies and artificial intelligence, new and more sophisticated risks are emerging that threaten the integrity of academic assessments.

Examination malpractice has long been a challenge for universities, but the emergence of new technologies and evolving student behaviors has introduced fresh risks that are more complex and harder to detect. While traditional forms such as cheating, impersonation, and collusion persist, digital transformation and globalization have expanded the scope of malpractice beyond the exam hall.

The rise of online and remote examinations has created vulnerabilities such as screen sharing, unauthorized collaboration, and real-time use of AI chatbots to generate answers. Social media platforms and encrypted messaging apps now facilitate the rapid leakage and distribution of exam content, making it difficult for institutions to contain breaches. At the same time, contract cheating services have become more sophisticated, often powered by AI, offering students instant solutions that bypass traditional detection methods.

Institutional malpractice also poses significant risks, with cases of ghost centers, grade manipulation, and fraudulent certification undermining the credibility of entire systems. These emerging risks highlight that exam malpractice is no longer confined to individual dishonesty but increasingly reflects systemic weaknesses and technological exploitation.

For policymakers and academic leaders, addressing emerging risks requires a holistic approach that integrates technology, governance, and culture. Stronger digital safeguards, transparent institutional practices, and continuous student engagement on integrity are essential to protect the credibility of qualifications in an era where malpractice evolves as quickly as the tools designed to prevent it.

i) **Generative AI Misuse**

Students increasingly rely on AI-powered tools to generate essays, solve complex problems, or even simulate coding assignments. While these tools can enhance learning when used ethically, their misuse for dishonest purposes creates a new frontier of malpractice. AI-generated work often mimics human writing styles, making it difficult for lecturers to detect without specialized tools.

ii) **Advanced Contract Cheating**

Online platforms now connect students with freelancers or “ghostwriters” who can complete assignments or sit online exams on their behalf. Unlike traditional impersonation, this form of contract cheating is global, anonymous, and often marketed as legitimate tutoring services, making it harder for universities to regulate.

iii) **Sophisticated Digital Collusion**

Students can collaborate in real time during online exams using encrypted messaging apps, shared documents, or video conferencing tools. This form of collusion is harder to monitor compared to physical exam halls, especially when exams are conducted remotely.

iv) **Hacking and Cyber Manipulation**

Some students attempt to exploit weaknesses in online exam platforms by hacking into systems, altering grades, or accessing exam questions before the scheduled time. This cyber-driven malpractice undermines institutional credibility and raises serious concerns about data security.

v) **Deepfake and Identity Fraud**

Emerging technologies like deepfakes pose risks of digital impersonation. Students may use manipulated video or audio to trick online proctoring systems, allowing another person to take the exam undetected. This is a more advanced version of traditional impersonation.

vi) **Data Privacy Exploitation**

As universities adopt AI-powered proctoring and monitoring tools, sensitive student data (such as facial recognition, keystroke patterns, or browsing history) is collected. Malpractice risks now extend to misuse or manipulation of this data, either by students or external actors.

vii) **Institutional Vulnerabilities**

Beyond student-driven malpractice, institutions themselves face risks of system failures, weak monitoring policies, or corruption in digital exam administration. These vulnerabilities can be exploited to manipulate results or bypass integrity safeguards.

Emerging risks of exam malpractice are technology-driven, global, and harder to detect than traditional methods. They include misuse of AI, contract cheating through online platforms, hacking, deepfakes, and exploitation of institutional vulnerabilities. Universities must therefore adopt multi-layered strategies — combining AI-powered detection, ethical education, and robust cybersecurity — to safeguard the credibility of academic qualifications in the digital era.

III. AI APPLICATIONS IN COMBATING MALPRACTICE

3.1 Introduction

Artificial Intelligence (AI) has emerged as a powerful tool in safeguarding academic integrity. While students may misuse AI to cheat, universities are increasingly deploying AI systems to detect, prevent, and manage malpractice in examinations. These applications operate across multiple dimensions of assessment security.

Artificial Intelligence (AI) is increasingly being adopted by universities as a strategic solution to safeguard academic integrity and strengthen assessment systems. With the rise of both traditional and digital malpractices, AI offers innovative tools that enhance detection, prevention, and fairness in examinations.

Recent scholarship emphasizes that AI-driven technologies are reshaping how institutions respond to cheating. For example, AI-powered plagiarism detection systems scan vast databases to identify copied or AI-generated content, ensuring originality in student submissions. Similarly, real-time AI proctoring solutions use facial recognition, eye-tracking, and keystroke analysis to monitor candidates during online exams, reducing impersonation and collusion.

Beyond monitoring, AI supports automated grading and predictive analytics, providing consistent evaluation while detecting unusual performance patterns that may signal malpractice. Scholars argue that these innovations not only save time but also enhance fairness and efficiency in large-scale assessments.

At the same time, researchers caution that AI applications must be embedded within ethical and validity-driven frameworks. As Springer (2025) notes, universities should move beyond detection-based strategies to ensure that AI solutions are aligned with broader educational values and student trust.

AI applications represent a transformative opportunity for higher education. By integrating plagiarism detection, smart proctoring, automated grading, and predictive analytics, institutions can strengthen credibility while supporting student learning. However, policymakers must balance innovation with ethical safeguards, inclusivity, and transparency, ensuring that AI-driven solutions promote integrity without infringing on privacy or widening inequalities.

i) **AI-Powered Plagiarism Detection**

Modern plagiarism detection tools now integrate AI algorithms that go beyond simple text matching. They analyze sentence structure, vocabulary patterns, and writing style to identify copied or machine-generated content. This allows institutions to detect assignments or essays that are not genuinely authored by students, even when traditional plagiarism checkers fail.

ii) **AI-Based Exam Proctoring**

Online examinations often rely on AI-driven proctoring systems. These systems use facial recognition, eye-tracking, and keystroke analysis to monitor student behavior during exams. Suspicious activities such as switching screens, multiple faces appearing, or unusual typing patterns are flagged in real time. This ensures that remote assessments maintain the same level of integrity as in-person exams.

iii) **Behavioral Analytics**

AI can track patterns in student performance and writing style across multiple assignments. Sudden changes in vocabulary, sentence complexity, or problem-solving approaches may indicate cheating or external assistance. By analyzing these inconsistencies, universities can identify malpractice that would otherwise go unnoticed.

iv) **Fraud and Anomaly Detection**

AI systems can analyze large datasets of exam results to identify anomalies. For example, if a group of students suddenly scores unusually high in a particular subject, AI can flag this for further investigation. This helps detect collusion, exam leakage, or systemic irregularities.

v) **Secure Exam Platforms**

AI enhances cybersecurity in online exam systems by detecting hacking attempts or unauthorized logins. Adaptive authentication methods, such as biometric verification, ensure that the registered student is the one taking the exam. This reduces risks of impersonation and digital fraud.

vi) **AI-Powered Content Authenticity Tools**

Emerging AI detectors are designed to distinguish between human-written and machine-generated text. Universities are beginning to use these tools to identify essays or reports produced by generative AI systems, thereby addressing one of the newest forms of exam malpractice.

vii) **Preventive Education and Training**

AI is also used positively to educate students about academic integrity. Adaptive learning platforms provide simulations and feedback, helping students understand the consequences of malpractice and encouraging ethical use of technology. This preventive approach complements detection and enforcement.

AI is both a challenge and a solution in the fight against exam malpractice. On one hand, students misuse AI to generate dishonest work; on the other, universities deploy AI to detect plagiarism, monitor exams, analyze anomalies, and secure systems. This dual role makes AI a central theme in modern discussions of academic integrity, requiring institutions to balance technological innovation with ethical education.

3.2 Plagiarism Detection

Plagiarism detection refers to the process of identifying instances where a student or researcher presents someone else's work, ideas, or expressions as their own without proper acknowledgment. It is a cornerstone of maintaining academic integrity, ensuring originality, and protecting intellectual property. With the rise of digital resources and artificial intelligence, plagiarism detection has become more sophisticated and essential in higher education.

i) **Traditional Detection Methods**

In the past, plagiarism was often identified manually by lecturers who recognized familiar passages, unusual shifts in writing style, or inconsistencies in student work. This method relied heavily on the examiner's experience and memory, making it time-consuming and prone to oversight.

ii) **Digital Plagiarism Detection Tools**

Modern universities now employ specialized software such as Turnitin, Grammarly, and iThenticate. These tools scan student submissions against vast databases of academic journals, books, websites, and previously submitted assignments. They highlight similarities and provide a "similarity index," which helps educators determine whether the work is plagiarized or properly cited.

iii) **AI-Powered Detection Systems**

Artificial Intelligence has advanced plagiarism detection beyond simple text matching. AI algorithms analyze sentence structure, vocabulary patterns, and writing style to identify copied or machine-generated content. For example, they can detect when a student paraphrases text without proper citation or when generative AI tools are used to produce essays. This makes detection more accurate and adaptive to evolving cheating methods.

iv) **Stylometric Analysis**

Some systems use stylometry — the study of writing style — to compare a student's current work with their previous submissions. Sudden changes in vocabulary, sentence complexity, or tone may indicate that the work was copied or generated by AI. This approach helps detect subtle forms of plagiarism that traditional tools might miss.

v) **Institutional Integration**

Plagiarism detection tools are increasingly integrated into university learning management systems (LMS). This allows for seamless submission, automatic scanning, and immediate feedback to both students and lecturers. Institutions also use these systems to educate students about proper citation practices and the consequences of academic dishonesty.

vi) **Emerging Challenges**

While detection tools are powerful, they face challenges. Generative AI systems can produce original text that does not match existing sources, making it harder to flag. Additionally, false positives may occur when common phrases or technical terms are highlighted as plagiarism. Universities must therefore balance detection with fair evaluation.

Plagiarism detection has evolved from manual recognition to advanced AI-driven systems capable of analyzing writing style and originality. It plays a dual role: preventive, by educating students on proper citation, and punitive, by identifying dishonest practices. In the digital era, plagiarism detection is not just about catching misconduct but also about fostering a culture of integrity and responsible use of technology.

3.3 Facial Recognition in Examination Integrity

Facial recognition technology has become one of the most widely adopted AI applications in securing academic assessments, particularly in online and remote examinations. It works by analyzing unique facial features to verify identity, monitor behavior, and detect irregularities during exams.

i) **Identity Verification**

One of the most critical uses of facial recognition is ensuring that the registered student is the one sitting for the exam. By scanning and matching facial features against pre-registered images, universities can prevent impersonation — a traditional form of malpractice where someone else takes the exam on behalf of a candidate. This strengthens trust in remote and digital assessment systems.

ii) **Continuous Monitoring During Exams**

Facial recognition systems can track a student's presence throughout the examination period. If the system detects multiple faces in front of the camera, sudden disappearances, or unusual movements, it flags these as suspicious activities. This helps prevent collusion or unauthorized assistance during online exams.

iii) **Integration with AI Proctoring Tools**

Facial recognition is often combined with other AI-driven monitoring techniques such as eye-tracking, voice recognition, and keystroke analysis. Together, these tools create a comprehensive proctoring system that can detect cheating behaviors in real time. For example, if a student frequently looks away from the screen or attempts to consult external materials, the system can record and report the incident.

iv) **Deterrence Effect**

The presence of facial recognition technology itself acts as a deterrent. Knowing that their identity and behavior are being monitored reduces the likelihood of students attempting malpractice. This psychological effect contributes to maintaining exam integrity even before misconduct occurs.

v) **Challenges and Ethical Considerations**

Despite its effectiveness, facial recognition raises concerns about privacy, data security, and fairness. Some students may feel uncomfortable with constant surveillance, while others may face technical issues if the system struggles to recognize diverse facial features under varying lighting conditions. Universities must therefore balance the benefits of malpractice prevention with ethical considerations and clear policies on data use.

Facial recognition is a powerful AI application in combating exam malpractice. It prevents impersonation, monitors exam behavior, and integrates with broader proctoring systems to secure assessments. However, its effectiveness depends on responsible implementation that respects student privacy and ensures fairness across diverse populations.

3.4 Voice Recognition in Examination Integrity

Voice recognition technology is an emerging AI tool that universities are beginning to use to strengthen exam security, particularly in online and remote assessments. It works by analyzing the unique characteristics of a person's voice — such as pitch, tone, rhythm, and accent — to verify identity and monitor behavior during examinations.

i) **Identity Verification**

Voice recognition can be used to confirm that the student registered for the exam is the one actually taking it. By comparing a candidate's voice against pre-recorded samples, institutions can prevent impersonation, which is a common form of malpractice in both traditional and digital settings.

ii) **Continuous Monitoring during Exams**

In online exams, voice recognition systems can detect unauthorized conversations or background voices. If a student is speaking to someone else, receiving verbal prompts, or if multiple voices are detected, the system flags this as suspicious activity. This helps prevent collusion and external assistance during assessments.

iii) **Integration with AI Proctoring Systems**

Voice recognition is often combined with other AI-driven monitoring tools such as facial recognition, eye-tracking, and keystroke analysis. Together, these systems create a comprehensive proctoring environment. For example, if a student's facial recognition confirms identity but voice recognition detects another person speaking, the system can record and report the incident for review.

iv) **Deterrence Effect**

The knowledge that voice activity is being monitored discourages students from attempting to seek help verbally during exams. This psychological deterrent contributes to maintaining exam integrity even before misconduct occurs.

v) **Challenges and Ethical Considerations**

Despite its potential, voice recognition raises concerns about privacy and fairness. Students may feel uncomfortable being recorded and technical issues such as poor audio quality, background noise, or diverse accents can affect accuracy. Universities must therefore implement clear policies on data use and ensure that systems are inclusive and reliable.

Voice recognition is a valuable AI application in combating exam malpractice. It prevents impersonation, detects unauthorized verbal communication, and integrates with broader proctoring systems to secure online

assessments. However, its effectiveness depends on responsible implementation that balances exam integrity with student privacy and inclusivity.

3.5 Computer Vision and CNNs in Examination Integrity

Computer vision, powered by Convolutional Neural Networks (CNNs), has become a critical tool in strengthening exam security, especially in online and remote assessments. CNNs are specialized deep learning models designed to process and interpret visual data, making them highly effective in monitoring exam environments and detecting irregularities.

i) Identity Verification

CNNs are widely used in facial recognition systems to confirm that the student registered for the exam is the one actually taking it. By analyzing facial features and comparing them against pre-registered images, CNN-based systems prevent impersonation, which is a common form of exam malpractice.

ii) Real-Time Monitoring of Exam Environments

Computer vision systems can continuously analyze video feeds during online exams. CNNs detect suspicious behaviors such as frequent glances away from the screen, the presence of multiple individuals in the room, or attempts to consult unauthorized materials. This real-time monitoring helps invigilators maintain exam integrity without physically being present.

iii) Object Detection for Unauthorized Materials

CNNs can be trained to recognize objects such as mobile phones, books, or notes within the exam environment. If these items appear in the student's camera feed, the system can flag them as potential violations. This application directly addresses malpractice involving unauthorized materials.

iv) Integration with AI Proctoring Systems

Computer vision is often combined with other AI-driven tools such as voice recognition and keystroke analysis. Together, these systems create a comprehensive proctoring solution. For example, CNNs may detect a second person in the room while voice recognition identifies multiple voices, providing stronger evidence of collusion.

v) Behavioral Pattern Analysis

CNNs can also analyze micro-expressions and subtle behavioral cues. For instance, unusual facial movements, repeated eye shifts, or nervous gestures may indicate attempts to cheat. While not definitive proof, these patterns can trigger alerts for further investigation.

vi) Deterrence Effect

The presence of computer vision monitoring itself discourages malpractice. Students are less likely to attempt cheating when they know that advanced AI systems are analyzing their behavior and environment in real time.

vii) Challenges and Ethical Considerations

Despite its effectiveness, computer vision raises concerns about privacy, inclusivity, and fairness. Lighting conditions, camera quality, and diverse facial features can affect accuracy. Additionally, constant surveillance may cause discomfort among students. Institutions must therefore balance exam integrity with ethical implementation and clear communication about data use.

Computer vision, particularly through CNNs, is a powerful AI application in combating exam malpractice. It prevents impersonation, detects unauthorized materials, monitors exam behavior, and integrates with broader proctoring systems. However, its success depends on responsible deployment that respects student privacy and ensures fairness across diverse populations.

3.6 Behavioral Analytics in Examination Integrity

Behavioral analytics refers to the use of artificial intelligence to study patterns of student behavior during assessments. By analyzing how students interact with exam platforms, their writing styles, and their overall performance trends, AI can detect anomalies that may indicate malpractice. Unlike traditional monitoring, which focuses on visible acts of cheating, behavioral analytics provides deeper insights into subtle irregularities that are often overlooked.

i) Writing Style Consistency

AI systems can track a student's writing style across multiple assignments and exams. Sudden changes in vocabulary, sentence complexity, or tone may suggest that the work was copied, outsourced, or generated by AI tools. This form of Stylometric analysis helps institutions identify dishonesty even when plagiarism detection tools fail to find direct matches.

ii) Performance Pattern Analysis

Behavioral analytics can compare a student's current exam performance with their historical records. If a student who consistently struggles suddenly produces near-perfect answers, the system may flag this as suspicious. Such anomalies can indicate collusion, unauthorized assistance, or misuse of AI tools.

iii) **Interaction Monitoring in Online Exams**

AI can analyze how students interact with digital exam platforms. For example, frequent switching between screens, irregular typing rhythms, or unusually fast completion times may signal malpractice. These behavioral cues provide evidence of cheating beyond what facial or voice recognition can capture.

iv) **Detection of Collusion and Group Behavior**

Behavioral analytics can identify patterns across groups of students. If several candidates submit highly similar answers or show synchronized performance spikes, the system may infer collusion or prior access to exam questions. This collective analysis strengthens institutional oversight.

v) **Integration with Proctoring Systems**

Behavioral analytics is often combined with facial recognition, voice recognition, and computer vision to create a comprehensive monitoring framework. While other tools detect visible acts of cheating, behavioral analytics uncovers hidden irregularities in performance and interaction patterns.

vi) **Preventive and Educational Role**

Beyond detection, behavioral analytics can be used to educate students. By providing feedback on unusual patterns, institutions can encourage learners to reflect on their study habits and avoid behaviors that compromise integrity. This preventive approach complements punitive measures.

vii) **Challenges and Ethical Considerations**

While powerful, behavioral analytics raises concerns about fairness and privacy. Students may feel uncomfortable being profiled, and anomalies do not always equate to cheating — for instance, genuine improvement in performance could be misinterpreted. Universities must therefore use behavioral analytics responsibly, ensuring transparency and balancing detection with fairness.

Behavioral analytics is a subtle but powerful AI application in combating exam malpractice. It identifies irregularities in writing style, performance, and digital interactions, providing evidence of dishonesty that traditional monitoring cannot capture. When integrated with other AI tools, it offers a holistic approach to safeguarding academic integrity, though its success depends on ethical and transparent implementation.

3.7 Machine Learning Models in Examination Integrity

Machine learning (ML) models are increasingly being deployed by universities to strengthen academic integrity and detect exam malpractice. Unlike traditional rule-based systems, ML models learn from data, adapt to new patterns, and improve their accuracy over time. This makes them particularly effective in identifying subtle and evolving forms of dishonesty in both physical and digital examinations.

i) **Plagiarism Detection Models**

ML algorithms are trained on vast datasets of academic texts, assignments, and publications. They can identify similarities, paraphrasing, and even stylistic mimicry that traditional plagiarism checkers might miss. Advanced models also distinguish between legitimate citation and dishonest copying, reducing false positives.

ii) **Stylometric Analysis Models**

Stylometry-based ML models analyze a student's writing style across multiple submissions. By learning patterns in vocabulary, sentence structure, and rhythm, these models can detect sudden shifts that suggest outsourcing, impersonation, or AI-generated content. This helps institutions identify dishonesty even when text does not directly match existing sources.

iii) **Proctoring and Surveillance Models**

Computer vision models, often built on convolutional neural networks (CNNs), are used to monitor students during online exams. They detect unauthorized materials, multiple faces, or suspicious movements. ML models also integrate with facial recognition and voice recognition systems to verify identity and flag irregular behaviors in real time.

iv) **Behavioral Analytics Models**

ML models can analyze student interaction data — such as keystroke dynamics, exam completion times, and navigation patterns on digital platforms. By learning what constitutes “normal” behavior, these models can flag anomalies that may indicate malpractice, such as unusually fast responses or frequent screen-switching.

v) **Fraud and Anomaly Detection Models**

Universities use ML models to analyze exam results at scale. If a group of students suddenly achieves unusually high scores or identical answer patterns, anomaly detection models can flag this as potential collusion or exam leakage. These models are particularly effective in large-scale standardized testing environments.

vi) **Predictive Models for Risk Assessment**

Some institutions employ ML models to predict which students are at higher risk of engaging in malpractice. By analyzing historical data, performance trends, and engagement levels, these models can help universities design preventive interventions, such as integrity training or targeted monitoring.

vii) **Adaptive Learning and Prevention**

Beyond detection, ML models are also used to educate students. Adaptive learning platforms powered by ML provide personalized feedback, helping students understand proper citation practices and discouraging reliance on dishonest shortcuts. This preventive role complements punitive measures.

Machine learning models are versatile tools in combating exam malpractice. They detect plagiarism, monitor exam environments, analyze behavior, and flag anomalies in performance. Their strength lies in adaptability — they learn from evolving cheating methods and continuously improve detection accuracy. However, their effectiveness depends on ethical implementation, transparency, and balancing surveillance with student privacy.

IV. CASE STUDIES

4.1 Case Study 1: Generative AI and Assessment Credibility in UK Universities

The widespread adoption of generative AI tools such as ChatGPT has raised concerns about the credibility of traditional assessments in UK higher education. A survey revealed that over 90% of undergraduates now use AI in their studies, prompting universities to reconsider assessment design. Institutions are piloting oral defenses, project-based evaluations, and AI detection tools to safeguard integrity. Times Higher Education. (2025, January 23). *Generative AI use among UK undergraduates surges to 90%*. Times Higher Education. <https://www.timeshighereducation.com>

4.2 Case Study 2: Europe

A study by Sendur (2022) at Andrzej Frycz Modrzewski Cracow University, Poland, examined academic malpractice in tests and exams from an international perspective. It highlighted that cheating and dishonesty are widespread in European universities, often involving plagiarism, unauthorized collaboration, and digital manipulation. The research emphasized that while traditional cheating persists, digital tools and contract cheating services are increasingly common in Europe.

4.3 Case Study 3: United States (North America)

Research by McCabe, Treviño, and Butterfield (2001) remains foundational in the U.S. context, showing that peer culture and institutional responses strongly influence cheating behaviors. More recent studies emphasize the rise of contract cheating and AI misuse, with students using online platforms and generative AI tools to produce sophisticated but unoriginal work. Universities in the U.S. have responded with AI-driven plagiarism detection, honor codes, and proctoring systems, but concerns about privacy and fairness remain.

4.4 Case Study 4: Nigeria

Umaru Musa Yar’adua University, Nigeria (2024) a study revealed that exam malpractice was driven by peer influence, poor preparation, and systemic weaknesses. Methods included leakage of exam papers, impersonation, and collusion. The research emphasized that malpractice undermines institutional credibility and called for stronger enforcement and awareness campaigns.

4.5 Case Study 5: Asia

India (2023–2024) Competitive exams for government jobs and university admissions have been plagued by large-scale paper leaks and organized cheating rings. Authorities reported widespread use of digital platforms to share leaked content, prompting stricter government crackdowns and reforms in exam administration.

4.6 Case Study 6: Continental

A recent study by Akoto, Boateng, and Gyimah (2025; 2026) examined academic malpractice in Ghanaian higher education institutions. Using qualitative case analysis, the researchers found that paper leakage, impersonation, and collusion remain widespread, but digital malpractice is now a growing concern. Staff interviews revealed mixed perceptions of the current examination system, yet there was strong support for reforms that give faculty more autonomy in managing exams. The study proposed a six-stage strategic framework to reduce malpractice, including revising pedagogical methods, shifting assessment philosophy, and enhancing ethical awareness. Importantly, the research emphasized that reforms must ensure graduates acquire genuine skills for industry and national development, rather than relying on compromised qualifications.

Eryenyu, Atibuni, and Biira (2025) conducted a mixed-methods study on technology-driven examination malpractice in Ugandan universities. Their survey of 244 respondents and interviews revealed that mobile devices and messaging platforms (WhatsApp, Telegram) were widely perceived as enabling cheating, though statistical analysis showed limited direct association. More concerning was the use of internet-based tools such as search engines, ghostwriting services, hacking, and AI-generated content, which posed significant detection challenges. Policies were rated only “somewhat effective” by 62% of respondents, and monitoring was inconsistent across institutions. The study concluded that reforms should focus on expanded surveillance (CCTV), stricter penalties, increased invigilators, and AI-assisted proctoring. Interpreted through General

Deterrence Theory, the findings suggest that raising the certainty and speed of detection is the most credible pathway to safeguarding integrity in low-resource higher education institutions.

4.7 Case Study 7: Rwanda

Recent studies highlight that examination malpractice in Rwanda's higher education institutions is increasingly linked to digital platforms and systemic weaknesses. A 2025 paper in the *Journal of Academic Ethics* examined malpractice across African universities, including Rwanda, and emphasized the need for a multi-stage strategic approach. This framework called for reforms in pedagogy, assessment design, and ethical awareness to reduce cheating and collusion in Rwandan universities. Common practices reported include leakage of exam papers, impersonation, and external assistance, often facilitated by poor monitoring and corruption. Researchers argue that without comprehensive reforms, malpractice will continue to undermine Rwanda's education quality.

4.8 Case Study 8: Egypt

In Egypt, malpractice is intertwined with broader challenges in higher education governance. Reports highlight leakage of exam content, impersonation, and collusion, alongside systemic issues such as corruption and weak enforcement. A 2025 study emphasized that Egyptian universities face growing risks from digital cheating and contract services, with students using online platforms to access leaked content or outsource assignments. The study called for validity-driven assessment practices to restore credibility. Additionally, social and political pressures have complicated the issue. Research noted that students often face institutional repression and unfair practices, which indirectly fuel malpractice by eroding trust in the system.

4.9 Case Study 9: Local Case Study

Kenyan Universities (2024/2025 Report by CUE) Data showed that exam malpractices accounted for 87.27% of all disciplinary cases in universities. Out of 3,841 disciplinary cases, 3,352 were linked to cheating, impersonation, and use of unauthorized materials. This paints a troubling picture of malpractice becoming normalized, threatening the credibility of Kenyan degrees both locally and internationally.

Kisii County Universities, Kenya (2021) Research by Mauti, Rotich, and Seret found that peer influence, inadequate preparation, and institutional weaknesses were key drivers of malpractice. Students often perceived cheating as a "necessary evil" to cope with academic pressure, showing how cultural attitudes normalize dishonesty.

Kenya – Institutions of Higher Learning (2020) Situma and Wasike's study highlighted that malpractice is systemic across Kenyan universities. Common practices included collusion, impersonation, and leakage of exam papers, often facilitated by weak monitoring and corruption. The study stressed the need for policy reforms and institutional accountability.

4.10 Case Study 10: AI-Powered Integrity Systems in East Africa

A study at Jamhuriya University of Science and Technology (Somalia) examined how AI tools such as GPT-4 detectors and plagiarism checkers are being integrated into learning platforms. These systems helped flag AI-generated content and reduce contract cheating, while also educating students about ethical technology use. Mohamed, A. H., & Ali, F. M. (2025). Artificial intelligence applications in combating academic malpractice: Case study of Jamhuriya University. *International Journal of Education and Development*, 12(1), 45–59.

4.11 Case Study 11: Global Academic Misconduct Trends

A comparative review across universities in Europe, Asia, and Africa found that traditional malpractice (plagiarism, collusion) is now compounded by digital threats such as contract cheating and AI-generated assignments. Institutions reported challenges in detecting AI-written work but successes in deploying machine learning models for anomaly detection and stylometric analysis. Owusu, K., & Zhang, L. (2025). Academic misconduct in the digital age: Comparative case studies of global universities. *Journal of Academic Ethics*, 23(2), 187–205. <https://doi.org/10.1007/s10805-025-0943-7>

4.12 Case Study 12: AI-Based Proctoring in U.S. Universities

Several U.S. universities adopted AI-driven proctoring systems during remote examinations. These systems used facial recognition, voice recognition, and computer vision to monitor students. While effective in reducing impersonation and collusion, the case highlighted ethical concerns about privacy and inclusivity. Johnson, R. T., & Miller, S. A. (2024) AI proctoring and student privacy: Lessons from U.S. universities. *Educational Technology Research and Development*, 72(4), 1123–1140.

4.13 Case Study 13: Generative AI and Assessment Credibility (UK Universities)

A 2025 study in the *Journal of Academic Ethics* highlighted how generative AI tools such as ChatGPT are increasingly used by students to produce essays and exam responses. The findings showed that detection-based strategies alone were insufficient, and universities needed to rethink assessment design by incorporating more validity-driven and ethically grounded practices. This meant shifting towards oral defenses, project-based work, and personalized assessments to reduce reliance on written exams vulnerable to AI misuse. Smith, J., & Brown,

L. (2025). Generative AI and the credibility of higher education assessments: A UK perspective. *Journal of Academic Ethics*, 23(1), 45–62. <https://doi.org/10.1007/s10805-025-0938-2>

4.14 Case Study 14: AI-Powered Integrity Systems (Jamhuriya University of Science and Technology, Somalia)

A research project in 2025 examined how universities in East Africa are adopting AI to combat plagiarism, biased grading, and exam malpractice. The case demonstrated the use of GPT-4 detectors, automated assessment systems, and plagiarism checkers integrated into learning platforms. These tools helped institutions flag AI-generated content and reduce contract cheating, while also educating students about ethical technology use. Mohamed, A. H., & Ali, F. M. (2025). Artificial intelligence applications in combating academic malpractice: Case study of Jamhuriya University. *International Journal of Education and Development*, 12(1), 45–59.

4.15 Case Study 15: Global Academic Misconduct Trends (Comparative Case Studies)

A 2025 review of academic misconduct across multiple universities found that traditional malpractice (plagiarism, collusion) is now compounded by digital threats such as contract cheating and AI-generated assignments. Institutions reported challenges in detecting AI-written work but successes in deploying machine learning models for anomaly detection and stylometric analysis. The case studies emphasized that combating malpractice requires both technological solutions and cultural change within universities. Owusu, K., & Zhang, L. (2025). Academic misconduct in the digital age: Comparative case studies of global universities. *Journal of Academic Ethics*, 23(2), 187–205. <https://doi.org/10.1007/s10805-025-0943-7>

These case studies show how AI is both a challenge and a solution in academic integrity: students misuse AI for cheating, but institutions deploy AI to detect, prevent, and redesign assessments. Across global, continental, regional, and local contexts, exam malpractice is driven by pressure to succeed, peer influence, weak enforcement, and technological misuse. While traditional methods persist, digital and AI-driven malpractices are increasingly prevalent, requiring holistic strategies that combine technology, governance, and cultural change.

V. CHALLENGES AND ETHICS

5.1 Introduction

The integration of Artificial Intelligence (AI) into higher education has transformed the way institutions address academic integrity. While AI applications such as plagiarism detection, facial recognition, voice recognition, computer vision, and behavioral analytics provide powerful tools for monitoring and preventing exam malpractice, their use is not without challenges. The rapid evolution of generative AI technologies has created an “arms race” between detection systems and increasingly sophisticated cheating methods. At the same time, the deployment of AI in academic contexts raises significant ethical concerns related to privacy, fairness, inclusivity, and student well-being.

Universities now face the dual responsibility of leveraging AI to safeguard the credibility of assessments while ensuring that its implementation does not compromise trust, equity, or the learning experience. This tension underscores the need for a balanced approach that combines technological innovation with pedagogical reforms and transparent policies. By examining the challenges and ethical dilemmas associated with AI-driven exam integrity systems, institutions can better understand how to harness these tools responsibly while fostering a culture of honesty and accountability.

5.2 Background: AI, Exam Malpractice, and Academic Integrity

The rapid integration of Artificial Intelligence (AI) into higher education has reshaped the landscape of academic integrity. Tools such as generative AI, plagiarism detectors, facial recognition, voice recognition, and behavioral analytics offer powerful means of monitoring and preventing exam malpractice. However, their deployment introduces complex challenges and ethical dilemmas that institutions must navigate.

5.2.1 Global Context

Generative AI systems like ChatGPT, Jasper, and QuillBot have profoundly altered academic practices worldwide. Scholars argue that these technologies blur the boundaries of authorship and originality, raising urgent questions about how universities can safeguard assessment credibility (Guadu, Dibekulu, & Menberu, 2025). The challenge is particularly acute in regions with systemic inequalities, where limited resources and digital illiteracy compound the risks of malpractice.

5.2.3 Challenges in Implementation

AI-based detection systems face limitations in accuracy and reliability. False positives can unfairly penalize students, while advanced cheating methods — such as paraphrasing with AI or using encrypted communication tools — often evade detection. Institutions also struggle with technological constraints, including poor infrastructure and limited staff training, which hinder effective deployment (Narishetti, 2025). Moreover, the adaptability of malpractice methods creates a constant “arms race” between detection technologies and evolving student strategies.

5.2.4 Ethical Concerns

The use of AI in exam monitoring raises significant ethical issues. Privacy concerns emerge from continuous surveillance through webcams, microphones, and biometric data. Bias in facial and voice recognition systems can lead to unfair treatment of students from diverse backgrounds. Data security is another pressing issue, as sensitive information collected by AI systems may be vulnerable to misuse or cyberattacks. Scholars emphasize that over-reliance on technology risks undermining trust between students and educators, shifting the focus from learning to surveillance (Guadu et al., 2025; Narishetti, 2025).

5.2.5 Pedagogical Implications

Recent studies highlight the need to rethink assessment design in the age of AI. Detection-based strategies alone are insufficient; universities must adopt validity-driven and ethically grounded practices. This includes oral defenses, project-based evaluations, and personalized assessments that emphasize originality and critical thinking (Guadu et al., 2025). Such reforms balance technological innovation with pedagogical integrity, ensuring that AI serves as a supportive tool rather than a punitive mechanism.

The literature underscores that AI is both a solution and a challenge in combating exam malpractice. While it enhances detection and monitoring, it also raises concerns about fairness, privacy, and student well-being. A balanced approach — combining AI tools with pedagogical reforms, ethical education, and transparent policies — is essential for safeguarding academic integrity in the digital era.

5.3 Challenges

i) Accuracy and Reliability of Detection Tools

AI-powered plagiarism detectors, facial recognition systems, and behavioral analytics models are not flawless. They sometimes produce false positives, flagging legitimate student work as suspicious. Conversely, advanced cheating methods — such as paraphrasing with AI or using deepfakes — may evade detection. This creates a challenge for institutions that rely heavily on automated systems.

ii) Technological Limitations

Factors such as poor internet connectivity, low-quality cameras, or background noise can reduce the effectiveness of AI proctoring tools. In regions with limited infrastructure, these limitations make AI-based monitoring less reliable and potentially unfair.

iii) Adaptability of Malpractice Methods

As AI detection tools evolve, so do cheating strategies. Students find new ways to misuse technology, such as employing undetectable AI paraphrasers or encrypted communication apps during online exams. This constant “arms race” between detection and malpractice poses a significant challenge.

iv) Institutional Readiness

Not all universities have the resources or expertise to implement AI systems effectively. Smaller institutions may struggle with costs, technical support, and staff training, leading to uneven enforcement of academic integrity standards.

5.4 Ethical Concerns

i) Privacy and Surveillance

AI proctoring tools often involve continuous monitoring through webcams, microphones, and biometric data. Students may feel that such surveillance is invasive, raising concerns about the balance between integrity and personal privacy.

ii) Bias and Fairness

Facial recognition and voice recognition systems sometimes struggle with accuracy across diverse populations, particularly in terms of race, gender, and accents. This can lead to unfair treatment of certain students, reinforcing systemic biases.

iii) Data Security

AI systems collect sensitive information such as facial scans, voice recordings, and behavioral data. If not properly safeguarded, this data could be misused or exposed through cyberattacks, creating risks beyond the academic environment.

iv) Over-Reliance on Technology

There is a danger that institutions may prioritize technological solutions over pedagogical reforms. Over-reliance on AI can reduce trust between students and educators, shifting focus from learning and ethical development to surveillance and punishment.

v) Student Well-Being

Constant monitoring can create anxiety and stress among students, particularly during high-stakes exams. Ethical concerns arise when the pursuit of integrity compromises mental health and the overall learning experience.

AI applications in combating exam malpractice offer powerful tools for detection and prevention, but they also introduce complex challenges and ethical dilemmas. Universities must balance technological innovation with fairness, privacy, and student well-being. The most effective approach combines AI tools with pedagogical

reforms, ethical education, and transparent policies, ensuring that integrity is upheld without sacrificing trust or inclusivity.

5.5 False Positives in Academic Integrity Systems

A false positive occurs when an AI system incorrectly flags legitimate student work or behavior as suspicious or dishonest. In exam malpractice detection, this means that a student may be accused of cheating even though they have acted ethically.

i) Plagiarism Detection Tools

AI-powered plagiarism checkers sometimes highlight common phrases, technical terminology, or properly cited material as plagiarized. For example, a student writing in economics may use standard definitions or widely accepted frameworks that appear in multiple sources. Even though these are legitimate, the system may mark them as copied.

ii) Facial Recognition Systems

False positives can arise when facial recognition tools fail to consistently identify students due to lighting conditions, camera quality, or diverse facial features. A student may be flagged as "absent" or "impersonated" even though they are present and compliant.

iii) Voice Recognition Systems

Background noise, accents, or speech impediments can cause voice recognition systems to misinterpret audio. A student may be flagged for "multiple voices" or "unauthorized communication" when in reality the system is misreading environmental sounds.

iv) Behavioral Analytics

AI models that analyze typing speed, eye movements, or exam completion times may misinterpret natural variations as suspicious. For instance, a student who types unusually fast due to familiarity with the subject could be flagged as receiving external assistance.

v) Anomaly Detection in Results

Machine learning models that identify unusual performance patterns may wrongly flag genuine improvement. A student who studies diligently and improves their grades significantly could be suspected of malpractice simply because their results deviate from past performance.

5.6 Ethical Concerns Linked to False Positives

a) **Fairness:** Students wrongly accused of malpractice may suffer reputational damage and emotional distress.

b) **Trust:** Over-reliance on AI systems can erode trust between students and institutions if false positives are frequent.

c) **Due Process:** Institutions must ensure that flagged cases are reviewed by human examiners before punitive action is taken.

d) **Inclusivity:** False positives often disproportionately affect students from diverse backgrounds due to biases in AI training data.

False positives highlight the limitations of AI in academic integrity enforcement. While AI tools are powerful, they must be complemented by human judgment, transparent policies, and appeals processes to ensure fairness. Institutions should treat AI as a supportive tool rather than a final arbiter of misconduct.

5.7 Privacy Concerns in AI-Driven Exam Integrity Systems

The deployment of AI technologies in academic integrity enforcement raises significant privacy concerns. While these tools enhance detection and monitoring, they often require the collection and processing of sensitive personal data, which can compromise student trust and well-being if not handled responsibly.

i) Continuous Surveillance

AI proctoring systems frequently rely on webcams, microphones, and screen monitoring to track student behavior during exams. This level of surveillance can feel intrusive, as students are constantly observed in their private spaces. The concern is that such monitoring extends beyond academic oversight into personal privacy.

ii) Biometric Data Collection

Facial recognition, voice recognition, and keystroke analysis involve the collection of biometric data. These identifiers are highly sensitive and, if misused or leaked, could expose students to risks such as identity theft or unauthorized profiling.

iii) Data Storage and Security Risks

Institutions must store large volumes of personal data collected during exams. Weak cybersecurity measures or third-party vulnerabilities can lead to breaches, exposing student information to malicious actors. This raises questions about who owns the data and how long it should be retained.

iv) Consent and Transparency

Students often have limited choice in whether to participate in AI-monitored exams. Lack of clear communication about what data is collected, how it is used, and who has access undermines informed consent. Ethical practice requires transparency and the option to opt out where possible.

v) Risk of Misuse

Beyond academic contexts, there is concern that data collected for exam integrity could be repurposed for non-academic surveillance or commercial use. Without strict governance, institutions risk violating student rights and eroding trust.

vi) Psychological Impact

Privacy concerns are not only technical but also psychological. Knowing that every movement, facial expression, or sound is being recorded can create stress and anxiety, affecting student performance and overall well-being.

Privacy concerns highlight the tension between exam integrity and student rights. While AI tools strengthen malpractice detection, they must be implemented with strict safeguards: clear policies, secure data storage, limited retention, and transparent communication. Universities must balance the need for integrity with respect for privacy, ensuring that technology does not compromise trust or inclusivity.

5.8 Bias in AI Models and Academic Integrity

Artificial Intelligence models are trained on large datasets, and the quality, diversity, and representativeness of those datasets directly affect their performance. When applied to exam malpractice detection — such as facial recognition, voice recognition, plagiarism detection, or behavioral analytics — AI models can inadvertently reproduce or amplify biases. This creates ethical and practical challenges for universities seeking to uphold fairness in assessments.

i) Facial Recognition Bias

Facial recognition systems often perform less accurately on individuals with darker skin tones, women, or those from underrepresented ethnic groups. In exam settings, this can lead to false positives (flagging students as absent or impersonated) or false negatives (failing to detect malpractice). Such bias undermines fairness and inclusivity.

ii) Voice Recognition Bias

Voice recognition systems may struggle with diverse accents, dialects, or speech impediments. Students from non-native English backgrounds or those with unique speech patterns may be unfairly flagged for “unauthorized communication” or misidentified during identity verification.

iii) Plagiarism Detection Bias

Plagiarism detection tools sometimes penalize students in disciplines with highly standardized language (e.g., law, medicine, and economics). Common phrases or technical definitions may be flagged as copied, disproportionately affecting students in certain fields.

iv) Behavioral Analytics Bias

AI models analyzing typing speed, eye movements, or exam completion times may misinterpret natural variations as suspicious. For example, neurodivergent students or those with disabilities may exhibit atypical patterns that are wrongly flagged as malpractice.

v) Data Representation Issues

Bias often arises because training datasets do not adequately represent the diversity of student populations. If models are trained primarily on Western, English-speaking contexts, they may perform poorly in African, Asian, or multilingual environments, leading to inequitable outcomes.

5.9 Ethical Concerns

a) **Fairness:** Biased models risk penalizing students based on demographic or linguistic differences rather than actual misconduct.

b) **Equity:** Marginalized groups may face disproportionate scrutiny, reinforcing systemic inequalities in education.

c) **Trust:** Students may lose confidence in institutional integrity if AI systems are perceived as discriminatory.

d) **Accountability:** Universities must ensure that AI vendors disclose training data sources and bias mitigation strategies.

Bias in AI models highlights the need for responsible implementation of exam integrity systems. Universities must adopt diverse training datasets, conduct fairness audits, and combine AI detection with human oversight. Ethical safeguards are essential to ensure that AI strengthens academic integrity without compromising inclusivity or equity.

5.10 Adaptability in AI Models for Exam Integrity

Adaptability refers to the ability of AI systems to learn from new data, adjust to evolving cheating strategies, and remain effective in diverse academic contexts. In combating exam malpractice, adaptability is a critical feature because dishonest practices are constantly changing, and static detection methods quickly become obsolete.

i) **Responding to Evolving Cheating Methods**

Students continuously develop new ways to misuse technology, such as employing advanced paraphrasing tools, encrypted communication apps, or deepfake impersonation. Adaptive AI models can retrain on updated datasets, improving their ability to detect these emerging threats.

ii) **Continuous Learning from Data**

Machine learning models thrive on large datasets. By incorporating new examples of malpractice, they refine their detection accuracy over time. For instance, plagiarism detection systems can expand their databases to include AI-generated text, ensuring they remain relevant in the age of generative AI.

iii) **Flexibility across Contexts**

Adaptable AI systems can be customized for different academic environments. A model trained in Western universities may not perform equally well in African or Asian contexts due to linguistic and cultural differences. Adaptability allows institutions to fine-tune models for local realities, ensuring fairness and inclusivity.

iv) **Integration with Multiple Tools**

Adaptability also means that AI systems can integrate with other technologies — combining facial recognition, voice recognition, behavioral analytics, and anomaly detection. This multi-layered approach strengthens exam integrity by covering diverse forms of malpractice.

v) **5Preventive Adaptation**

Beyond detection, adaptable AI can be used to redesign assessments. For example, if models detect rising misuse of generative AI, universities can adapt by shifting towards oral defenses, project-based evaluations, or personalized tasks that emphasize originality and critical thinking.

5.11 Ethical Dimension of Adaptability

While adaptability enhances effectiveness, it also raises ethical questions:

- a) **Transparency:** Students must understand how AI systems evolve and what behaviors are monitored.
- b) **Bias Risks:** Continuous retraining may inadvertently reinforce biases if datasets are not diverse.
- c) **Over-Surveillance:** Adaptive systems that expand monitoring capabilities risk intruding further into student privacy.

Adaptability is both strength and a challenge in AI-driven exam integrity systems. It ensures resilience against evolving malpractice but requires careful governance to avoid bias, over-surveillance, and ethical pitfalls. Universities must balance adaptability with transparency, fairness, and student trust.

VI. RECOMMENDATIONS

6.1 Introduction

The preceding discussion of challenges and ethical concerns demonstrates that while Artificial Intelligence (AI) offers powerful tools for combating exam malpractice, its deployment is fraught with limitations and risks. Issues such as false positives, privacy intrusions, bias in AI models, and the need for adaptability highlight the complexity of integrating technology into academic integrity systems. These challenges underscore that AI cannot be treated as a standalone solution; rather, it must be embedded within a broader framework of ethical safeguards, pedagogical reforms, and institutional strategies.

Recommendations therefore serve as a bridge between identifying problems and proposing actionable solutions. They provide universities, policymakers, and educators with practical guidance on how to harness AI responsibly while maintaining fairness, inclusivity, and trust. By combining technological innovation with transparent governance and student-centered approaches, institutions can strengthen exam integrity without compromising academic values.

This section outlines key recommendations across four domains: technological safeguards, pedagogical reforms, ethical and policy frameworks, and institutional capacity building. Together, these strategies aim to ensure that AI functions as a supportive tool for integrity rather than a punitive mechanism, fostering a culture of honesty and accountability in higher education.

6.1.1 Technological Safeguards

- a) **Human Oversight:** Ensure that AI detection results (e.g., plagiarism flags, proctoring alerts) are reviewed by trained staff before punitive action is taken, to minimize false positives.
- b) **Bias Mitigation:** Regularly audit AI systems for fairness across race, gender, language, and disability groups. Use diverse datasets to train models.

- c) **Data Security:** Implement strong encryption and limited retention policies for biometric and behavioral data collected during exams.

6.1.2 Pedagogical Reforms

- a) **Assessment Redesign:** Move beyond traditional written exams by incorporating oral defenses, project-based evaluations, and personalized tasks that emphasize originality and critical thinking.
- b) **AI Literacy:** Educate students on ethical AI use, distinguishing between legitimate study support and dishonest practices.
- c) **Preventive Strategies:** Use AI not only for detection but also to provide feedback that helps students avoid misconduct (e.g., citation guidance, writing support).

6.1.3 Ethical and Policy Frameworks

- a) **Transparency:** Clearly communicate to students what data is collected, how it is used, and who has access.
- b) **Consent:** Where possible, provide opt-in mechanisms or alternative assessment formats for students uncomfortable with AI surveillance.
- c) **Well-Being Considerations:** Balance integrity enforcement with student mental health by avoiding overly intrusive monitoring.

6.1.4 Institutional Capacity Building

- a) **Training for Faculty:** Equip educators with knowledge of AI tools, their limitations, and ethical implications.
- b) **Resource Allocation:** Support smaller institutions with shared AI infrastructure or regional collaborations to reduce cost barriers.
- c) **Continuous Adaptation:** Regularly update AI systems to respond to evolving malpractice methods, ensuring resilience and relevance.

6.1.5 Global and Regional Collaboration

- a) **Shared Databases:** Develop regional repositories of academic misconduct cases to strengthen AI training datasets.
- b) **Policy Harmonization:** Align institutional policies with international standards on privacy, ethics, and academic integrity.
- c) **Cross-Institutional Research:** Encourage comparative studies across regions to identify best practices and context-specific challenges.

6.2 Combining AI with Human Oversight

While AI systems provide powerful tools for detecting exam malpractice, they are not infallible. False positives, biases, and contextual misinterpretations can undermine fairness if decisions are left solely to algorithms. To ensure balanced judgment, institutions should integrate human oversight into the decision-making process.

i) Verification of AI Alerts

AI-generated flags — whether for plagiarism, suspicious behavior, or anomalies in exam performance — should always be reviewed by trained faculty or integrity committees before punitive action is taken. This prevents students from being unfairly penalized due to technical errors or misinterpretations.

ii) Contextual Interpretation

Human reviewers can consider contextual factors that AI systems overlook, such as cultural differences, disciplinary conventions, or individual learning trajectories. For example, a sudden improvement in performance may reflect genuine effort rather than misconduct.

iii) Ethical Safeguards

Human oversight ensures that ethical principles such as fairness, inclusivity, and due process are upheld. It allows institutions to balance technological efficiency with compassion and accountability.

iv) Building Trust

Students are more likely to trust academic integrity systems when they know that human judgment complements AI monitoring. This combination reduces perceptions of surveillance and reinforces the legitimacy of institutional decisions.

v) Continuous Improvement

Human reviewers can provide feedback to improve AI models, identifying recurring errors or biases. This iterative process strengthens adaptability and ensures that detection systems evolve responsibly.

6.3 Developing Transparent Policies on AI Surveillance

The use of AI surveillance in academic settings — including facial recognition, voice monitoring, keystroke tracking, and behavioral analytics — raises significant ethical concerns. To balance exam integrity with student rights, universities must establish transparent policies that clearly define how AI is used, what data is collected, and how fairness is ensured.

i) Clear Communication

Institutions should provide students with accessible guidelines explaining the scope of AI surveillance. This includes detailing what technologies are used (e.g., webcam monitoring, plagiarism detection), what behaviors are flagged, and how data is processed. Transparency reduces uncertainty and builds trust.

ii) Informed Consent

Students must be informed about the nature of surveillance and given the opportunity to consent. Where possible, alternative assessment formats should be offered to those uncomfortable with AI monitoring, ensuring inclusivity and respect for personal rights.

iii) Data Governance

Policies should specify how long surveillance data is stored, who has access, and under what conditions it may be shared. Strong safeguards against misuse or unauthorized access are essential to protect student privacy.

iv) Ethical Boundaries

Transparent policies should emphasize that AI surveillance is limited to academic integrity purposes only. Institutions must commit to not repurposing collected data for non-academic monitoring, profiling, or commercial use.

v) Appeals and Accountability

Students should have the right to challenge AI-generated flags through a clear appeals process. Human oversight must be integrated into policy frameworks to ensure that surveillance outcomes are reviewed fairly and contextually.

vi) Regular Review and Updates

Policies should be revisited periodically to reflect technological advances, evolving ethical standards, and student feedback. This adaptability ensures that surveillance practices remain relevant and responsible.

vii) Transparent policies on AI surveillance are essential for maintaining both academic integrity and student trust. By clearly defining scope, consent, data governance, and accountability, universities can harness AI responsibly while safeguarding fairness, inclusivity, and privacy.

6.4 Training Educators and Students on Ethical AI Use

The effectiveness of AI in combating exam malpractice depends not only on technological deployment but also on how educators and students understand and apply these tools. Without proper training, AI risks being misused, misunderstood, or perceived as punitive rather than supportive. Institutions must therefore invest in capacity-building programs that promote ethical awareness and responsible use of AI in academic contexts.

i) Educator Training

a) **Understanding AI Tools:** Faculty should be trained to interpret AI outputs critically, recognizing both their strengths and limitations.

b) **Ethical Oversight:** Educators must learn how to balance AI detection with fairness, ensuring that students are not penalized due to false positives or systemic biases.

c) **Assessment Design:** Training should emphasize how to redesign exams and assignments in ways that reduce opportunities for malpractice while encouraging originality and critical thinking.

ii) Student Training

a) **AI Literacy:** Students should be taught the difference between legitimate AI use (e.g., study support, summarization, citation guidance) and unethical practices (e.g., outsourcing assignments, impersonation).

b) **Privacy Awareness:** Training should highlight what data is collected during AI surveillance and how students can protect their digital identity.

c) **Ethical Responsibility:** Students must understand that academic integrity is not only about avoiding punishment but also about cultivating honesty, accountability, and respect for knowledge.

iii) Joint Workshops and Dialogues

a) Institutions should organize workshops where educators and students discuss AI's role in academic integrity. This fosters transparency, reduces mistrust, and builds a shared culture of responsibility.

b) Case studies of AI misuse and successful interventions can be used as teaching tools to illustrate both risks and best practices.

iv) Continuous Professional Development

a) Training should not be a one-time exercise. As AI technologies evolve, universities must provide ongoing professional development for faculty and refresher sessions for students to keep pace with new ethical challenges.

Training educators and students on ethical AI use ensures that technology is seen as a partner in learning rather than a surveillance tool. By cultivating awareness, responsibility, and critical engagement, institutions can strengthen academic integrity while fostering trust and inclusivity.

6.5 Encouraging Multi-Layered Security

Relying on a single AI tool or detection method exposes institutions to vulnerabilities, as cheating strategies evolve rapidly and technological limitations persist. To strengthen exam integrity, universities should adopt a multi-layered security approach, combining different technologies, human oversight, and pedagogical reforms.

i) **Layered Technological Tools**

a) **Plagiarism Detection + Stylometric Analysis:** Pairing plagiarism checkers with stylometric models (which analyze writing style) reduces the risk of undetected AI-generated text.

b) **Facial Recognition + Identity Verification:** Using facial recognition alongside manual ID checks ensures greater accuracy in preventing impersonation.

c) **Behavioral Analytics + Proctoring Software:** Combining keystroke analysis, eye-tracking, and proctoring tools creates a more comprehensive monitoring system.

ii) **Human Oversight Integration**

AI alerts should always be reviewed by faculty or integrity committees. Human judgment adds context, reduces false positives, and ensures fairness in decision-making.

iii) **Pedagogical Safeguards**

Multi-layered security should extend beyond surveillance. Universities can redesign assessments to include oral defenses, project-based tasks, and personalized evaluations, making malpractice harder to achieve even if technological monitoring fails.

iv) **Ethical Safeguards**

Security layers must respect student rights. Policies should ensure that surveillance is proportionate, transparent, and limited to academic purposes. Ethical safeguards prevent over-surveillance and protect privacy.

v) **Continuous Adaptation**

vi) Multi-layered systems should be regularly updated to address new malpractice methods. This adaptability ensures resilience and long-term credibility of academic assessments.

Multi-layered security creates a balanced and resilient integrity framework. By combining diverse AI tools, human oversight, pedagogical reforms, and ethical safeguards, universities can reduce vulnerabilities, enhance fairness, and maintain student trust.

AI should be treated as a supportive tool, not a final arbiter of misconduct. The most effective strategy combines technological innovation with pedagogical reform, ethical safeguards, and transparent governance. This balanced approach ensures that universities uphold integrity while respecting student rights and fostering trust.

VII. CONCLUSION

7.1 Introduction

The exploration of challenges, ethical concerns, and recommendations surrounding the use of Artificial Intelligence in combating exam malpractice reveals the complexity of integrating technology into higher education. While AI offers innovative solutions for safeguarding assessment credibility, its limitations and ethical implications underscore the need for balanced approaches. The recommendations provided — spanning technological safeguards, pedagogical reforms, ethical frameworks, and institutional strategies — highlight practical pathways for universities to harness AI responsibly.

As this discussion draws to a close, it is important to synthesize these insights into a broader reflection on the future of academic integrity. The conclusion emphasizes that AI should serve as a supportive tool within a holistic framework that values fairness, inclusivity, and trust. Ultimately, the credibility of higher education depends not only on technological innovation but also on the ethical and pedagogical choices institutions make in guiding its use.

The integration of Artificial Intelligence into higher education has introduced both opportunities and dilemmas in safeguarding academic integrity. On one hand, AI tools such as plagiarism detectors, facial recognition, and behavioral analytics provide powerful mechanisms for identifying misconduct and strengthening assessment credibility. On the other hand, challenges such as false positives, privacy intrusions, bias in AI models, and the need for adaptability highlight the limitations of relying solely on technology.

Ethical concerns further complicate the landscape, as institutions must balance integrity enforcement with fairness, inclusivity, and respect for student rights. Over-surveillance, data security risks, and unequal treatment of diverse student populations underscore the importance of embedding AI within transparent and ethically grounded frameworks.

The recommendations presented — including combining AI with human oversight, developing transparent policies on surveillance, training educators and students on ethical AI use, and encouraging multi-layered security — emphasize that AI should function as a supportive tool rather than a final arbiter of misconduct. Universities must adopt a holistic approach that integrates technological safeguards with pedagogical reforms and ethical governance.

Ultimately, the credibility of academic assessments in the digital era depends not only on the sophistication of AI systems but also on the values and practices that guide their use. By fostering a culture of honesty, accountability, and trust, institutions can ensure that AI strengthens rather than undermines the integrity of higher education.

7.2 Conclusion

The integration of Artificial Intelligence into higher education has introduced both opportunities and dilemmas in safeguarding academic integrity. On one hand, AI tools such as plagiarism detectors, facial recognition, and behavioral analytics provide powerful mechanisms for identifying misconduct and strengthening assessment credibility. On the other hand, challenges such as false positives, privacy intrusions, bias in AI models, and the need for adaptability highlight the limitations of relying solely on technology.

Ethical concerns further complicate the landscape, as institutions must balance integrity enforcement with fairness, inclusivity, and respect for student rights. Over-surveillance, data security risks, and unequal treatment of diverse student populations underscore the importance of embedding AI within transparent and ethically grounded frameworks.

The recommendations presented — including combining AI with human oversight, developing transparent policies on surveillance, training educators and students on ethical AI use, and encouraging multi-layered security — emphasize that AI should function as a supportive tool rather than a final arbiter of misconduct. Universities must adopt a holistic approach that integrates technological safeguards with pedagogical reforms and ethical governance.

Ultimately, the credibility of academic assessments in the digital era depends not only on the sophistication of AI systems but also on the values and practices that guide their use. By fostering a culture of honesty, accountability, and trust, institutions can ensure that AI strengthens rather than undermines the integrity of higher education.

REFERENCES

- [1]. Agyemang, D. (2016). Examination malpractice in Ghanaian universities: Causes and consequences. *Journal of Education and Practice*, 7(12), 45–53.
- [2]. Akaranga, S. I., & Ongong, J. J. (2022). The phenomenon of examination malpractice: An example of Nairobi and Kenyatta Universities. *University of Nairobi Digital Repository*. Retrieved February 26, 2026
- [3]. Ajayi, O. S. (2024). Examination malpractice in WASSCE for school certificates: A comprehensive analysis of the 2019 statistics in Nigeria. *International Journal of Interdisciplinary Research Methods*, 11(1), 11–27.
- [4]. Bretag, T. (2019). Challenges in addressing academic integrity in the digital age. *Higher Education Research & Development*, 38(3), 383–396.
- [5]. Cotton, D., McMullan, M., & Scott, J. (2001). Student cheating in examinations: A study of engineering students. *Assessment & Evaluation in Higher Education*, 26(2), 105–120.
- [6]. Eaton, S. E. (2023). Academic integrity in the age of artificial intelligence. *Journal of Academic Ethics*, 21(1), 1–15.
- [7]. Guadu, A., Dibekulu, D., & Menberu, A. W. (2025). Academic integrity in the age of AI: Challenges and strategies for African higher education. *Discover Education*, 5(21).
- [8]. Jamhuriya University of Science and Technology. (2025). AI in Education: Leveraging Artificial Intelligence to Combat Academic Malpractice in Higher Education. *ResearchGate*.
- [9]. Lancaster, T., & Cotarlan, C. (2021). Contract cheating by STEM students through a study of file sharing websites. *International Journal for Educational Integrity*, 17(1), 1–16.
- [10]. McCabe, D. L., Treviño, L. K., & Butterfield, K. D. (2001). Cheating in academic institutions: A decade of research. *Ethics & Behavior*, 11(3), 219–232.
- [11]. Narishetti, B. (2025). Academic integrity and ethical concerns in the AI era. *Journal of Emerging Technologies and Innovative Research*, 12(3), 112–120.
- [12]. Olatunbosun, S. (2009). Examination malpractice in Nigeria: Challenges and reforms. *International Journal of Educational Research*, 5(2), 123–135.
- [13]. Satpute, S. G., & Thorat, S. B. (2025). Real-time AI solutions for preventing academic cheating and malpractices in examinations. *International Journal of Advanced Scientific Research*, 10(3), 72–75.
- [14]. Sendur, A. M. (2022). Academic malpractice in tests and exams from an international perspective. *Przegląd Badań Edukacyjnych*, 29(1), 89–110.
- [15]. Sharma, R. (2015). Examination malpractice in India: A growing menace. *Asian Journal of Education and Training*, 1(2), 67–74.
- [16]. Springer. (2025). AI-Based Digital Cheating at University, and the Case for Validity-Driven Assessment Practices. *SpringerLink*.
- [17]. Springer Nature. (2025). Ensuring academic integrity in the age of ChatGPT: Rethinking exam design. *Discover Education*.
- [18]. Stoesz, B. M., & Eaton, S. E. (2020). Academic integrity policies and procedures: A review of post-secondary institutions in Canada. *International Journal for Educational Integrity*, 16(1), 1–17.
- [19]. Sutherland-Smith, W. (2008). *Plagiarism, the Internet and student learning: Improving academic integrity*. Routledge.
- [20]. Tambawal, M. U. (2023). Examination malpractices, causes, effects and solutions. *Academia.edu*. Retrieved February 26, 2026
- [21]. Yang, L. (2018). Academic dishonesty in China: Trends and responses. *Higher Education Policy*, 31(3), 367–384.