

Chapter 10

Plagiarism and Cybersecurity in the Digital Age: A Cross-Level Study of Academic Integrity in Higher Education

Dr. Richa Chaurasia, Assistant Professor & Head, Department of Education, Saheed Anurup Chandra Mahavidyalaya, University of Calcutta

Abstract

Plagiarism has evolved significantly in the digital age, transforming from traditional cut, copy and paste based misconduct to technologically facilitated academic dishonesty. Simultaneously, cybersecurity threats in higher education institutions have intensified and alarming, at the same time exposing vulnerabilities related to intellectual property theft, unauthorized data access, and digital manipulation of academic manuscripts and content. The present study examines the intersection of plagiarism and cybersecurity across and among undergraduate (UG), postgraduate (PG), doctoral (PhD), and faculty levels. A cross-sectional survey of 200 participants was conducted to assess awareness, attitudes, experiences and expectations related to plagiarism and institutional cybersecurity mechanisms. The findings reveal high dependence on digital sources, moderate awareness of plagiarism policies, and limited understanding of cybersecurity frameworks about protecting academic data. Results indicate a statistically significant relationship between usage of digital tool and unintentional plagiarism practices. The study concludes that plagiarism must be addressed prominently as an ethical issue and also as a cybersecurity concern requiring technological, institutional, and behavioural interventions.

Keywords: *Plagiarism, Cybersecurity, Academic Integrity, Digital Ethics, Intellectual Property, Ethical Issues.*

Introduction

Plagiarism is traditionally defined as the act of presenting another individual's intellectual work ideas, words, data, or creative expressions as one's own without proper acknowledgment. Historically, plagiarism was confined to manual reproduction of texts. However, the rapid expansion of internet accessibility, cloud storage systems, and artificial intelligence tools has fundamentally transformed its scale and complexity. Higher education institutions increasingly rely on digital platforms for teaching, submission of assignments, peer collaboration, and research dissemination. While these advancements have democratized knowledge, they have also created opportunities for academic misconduct. Digital plagiarism now includes copy-paste practices, paraphrasing software misuse, AI-generated text submission, and code replication.

At the same time, universities face escalating cybersecurity threats. Data breaches, ransomware attacks, unauthorized database access, and intellectual property theft threaten academic ecosystems. The intersection between plagiarism and cybersecurity emerges when research data, unpublished theses, or proprietary academic content are accessed or misused through digital vulnerabilities.

Plagiarism is no longer solely an ethical violation; it has become intertwined with digital security frameworks. Understanding this intersection is essential across UG, PG, and PhD levels, as well as among faculty who guide research integrity.²⁰⁹

This study aims to:

1. Examine the evolving nature of plagiarism in the digital environments.
2. Analyse cybersecurity and vulnerabilities that facilitate academic misconduct.
3. Assess awareness levels of students and faculty across UG, PG and PhD.
4. Provide recommendations based on evidence for strengthening academic integrity systems.

Review of Related Literature:

- Evolution of Plagiarism in Digital Contexts

1. Research indicates that internet proliferation has significantly increased plagiarism

rates among students. Digital accessibility reduces the perceived effort required to replicate academic material. Studies show that students often engage in unintentional plagiarism due to inadequate citation knowledge.²¹⁰

2. AI-based writing systems have further complicated detection mechanisms. Automated content generation tools blur the boundary between assistance and misconduct, challenging traditional definitions of originality.

- Cybersecurity in Higher Education

1. Universities hold large volumes of sensitive data such as unpublished research, patents, examination systems, and personal student records. According to cybersecurity frameworks proposed by the National Institute of Standards and Technology (NIST), US based standards agency that academic institutions often lack enterprise-level security infrastructure.¹⁹⁴

2. Research published by IEEE organisation professional association for technology emphasizes the growing trend of ransomware attacks targeting educational institutions.

²⁰⁹ Morthy, M.S.N. (2007) *Encyclopedia of Multimedia and Communication Technology (Vol-1)* Delhi: Arise Publishers and distributions

²¹⁰ Bretag, T. (2016). Challenges in addressing plagiarism in education. *Educational Integrity Journal*, 12(2), 45–59.

These attacks not only disrupt operations but also expose confidential academic material.²¹¹

- Detection Tools and Technological Safeguards

1. Plagiarism detection services such as Turnitin use similarity indexing and algorithmic comparison to detect content overlap.²¹² However, these systems primarily address textual similarity rather than cybersecurity vulnerabilities like unauthorized file access.²¹³

2. Studies suggest that integration of blockchain technology could secure academic authorship records and timestamp intellectual property.²¹⁴

Although plagiarism and cybersecurity have been individually studied by a large number of researchers but limited empirical research explores their intersection across academic levels. Therefore, the present study bridges that gap by combining theoretical analysis with survey-based evidence.

Theoretical background of Plagiarism and Cyber security

1. Deterrence Theory

Deterrence theory suggests individuals are less likely to commit misconduct when the perceived risk of detection and punishment is high. Plagiarism detection software acts as a deterrent mechanism. However, if the cybersecurity systems are weak there is a high opportunity of increase in misconduct.

2. Routine Activity Theory (Cyber Adaptation)

This theory posits that in digital academia crime occurs when three elements converge. They are: -

The blockchain and kudos: A distributed system for educational record.

Journal of Learning Analytics, 3(3), 1–7.

- Motivated offender i.e. student or researcher,
- Suitable target i.e. digital academic content

²¹¹ Morthy, M.S.N. (2007) *Encyclopedia of Multimedia and Communication Technology (Vol-1)* Delhi: Arise Publishers and distributions

²¹² Morthy, M.S.N. (2007) *Encyclopedia of Multimedia and Communication Technology (Vol-1)* Delhi: Arise Publishers and distributions

²¹³ National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity.

²¹⁴ Bandhopadhyaya, A.K. (2008). *International Encyclopedia of Audio Visual Media (Vol- 1)* Delhi: Anmol Publication Pvt Ltd

- Absence of capable guardian i.e. cybersecurity & plagiarism systems¹

The study concludes that weak digital guardianship increases risk of crime or misconduct.

3. Technology Acceptance Model (TAM)

TAM explains that perceived usefulness and ease of use influence adoption of detection software. Faculty acceptance significantly impacts institutional enforcement of plagiarism policies.

The study is based on following methodologies.

- i) Research Design- A quantitative cross-sectional survey was conducted.
- ii) Population – The population of the study will consist all the undergraduate students, post-graduate students, research scholars and faculty members of University of Calcutta and its affiliated colleges.²¹⁵
- iv) Sample - There are 100 participants as shown in detail in the table below which are selected from the population.²¹⁶

Sl. No.	Types of participants	No. of participants
1	Undergraduate	40
2	Post- graduates	25
3	Research Scholars	20
4	Faculty Members	15
Total no. of participants		100

iii) Sampling Method

Convenience sampling method within the university setting is employed here.

iv) Tool

²¹⁵ Ibid.

²¹⁶ National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity.

A self- made structured questionnaire containing short answer type, one word answer type, MCQ type and Yes or No type items constructed and administrated. The detailed structure of questions is given in the table below.

Sl. No.	Types of questions	No. of questions
1	Demographic questions	5
2	Likert-scale questions	15
3	Yes/No questions	5
Total no. of questions		25

v) Ethical Considerations

The study is conducted in an open environment where voluntary participation is encouraged and anonymity of the participants are maintained. However, the data collected strictly used for academic research only.

Data Analysis

The data collected are analysed through Descriptive statistics i.e. percentage analysis and Correlation analysis among the students, research scholars and faculty members based on three main points. They are - - Digital tool use

- Plagiarism awareness
- Cybersecurity awareness

Results of the Survey

- Demographic Distribution

Sl. No.	Category of participants	Percentage of participants
1	Undergraduate	40%
2	Post- graduates	25%
3	Research Scholars	20%
4	Faculty Members	15%
TOTAL		100%

Findings of the study-

The key findings of the study are mentioned as follows.

- A. Study of awareness of plagiarism policy: 78% of participants have keen awareness where 22% are partially aware.
- B. Study of awareness of Cybersecurity Policy: 46% of participants are aware where 54% are unaware.²¹⁷
- C. Use of online sources without proper citation: 72% of participants uses online sources without proper citation and 18% of participants frequently omits where 10% never use any.
- D. Use of AI tools: 64% of participants reported using AI assistance frequently among them undergraduate students have higher usage of 82%.²¹⁸
- E. Study of Confidence in Detection Tools: - 58% of participants have moderate confidence, 25% have high confidence and 17% low confidence.

Correlation Finding

A moderate positive correlation ($r = .52$) was observed between heavy digital tool usage and selfreported unintentional plagiarism.

Discussion

- The findings of the study suggest that while plagiarism awareness is relatively high among all whereas cybersecurity awareness remains significantly lower. This gap exposes institutions towards academic misconduct facilitated through digital systems.
- Undergraduate students show higher AI tool usage. Hence potentially increasing unintentional plagiarism risk among them.
- Faculty members show high confidence in detection systems that suggests institutional trust, yet awareness gaps among students weaken preventive impact too.

²¹⁷ Becta, (2004) British Educational Communications and Technology Agency. *A review of the Research literature on barriers to the uptake of ICT by teachers*

²¹⁸ Jain, M.E. and Agarwal, J.C. (2008) *Encyclopedia of Education (Vol-2)* Delhi: Anshan publishing house

- The moderate correlation between digital tool use and plagiarism indicates that technology, without structured guidance, increases vulnerability.²¹⁹

Recommendations

1. There must be mandatory cybersecurity and academic integrity training in all levels of higher educational institutes for both students and faculties.
2. The integration of plagiarism detection into Learning Management Systems.
3. Introduction of Blockchain timestamping of theses and study materials.
4. There must be Two-factor authentication for academic submissions.
5. National academic cybersecurity frameworks should be developed.
6. AI-detection algorithm should be upgraded.

Conclusion

Therefore, it can be concluded that plagiarism in the digital era extends beyond the ethical misconduct and misuse. Hence, intersects with institutional cybersecurity vulnerabilities. In spite of availability of numerous detection tools, awareness and technological safeguards remain uneven across all academic levels both among students and teachers. Therefore, institutions must adopt a holistic strategy by combining education, technology and policy enforcement to protect intellectual integrity and minimise misconduct.

Suggestion for further studies

The present study has been conducted on a sample of students and teachers in the city Kolkata. This study may be replicated on school students and teachers and students and teachers of urban and rural areas, students and teachers of English medium as well as Hindi medium at different levels of education with different Boards of education. Studies may also be conducted to find out interaction or comparison between students and teachers of different universities, colleges or streams.²²⁰

²¹⁹ Anandan,K. & William Dharma Rja, B. (2010). *Educational Technology*, New Delhi: A.P.H. Publishing Corporation

²²⁰ IEEE. (2020). Cybersecurity threats in higher education institutions. *IEEE Security Review*, 18(4), 22–30.