Minor Project Synopsis Report

Behavioral Academic Integrity Checker

Project Category: University Based

Projexa Team id- 26E1173

Submitted in partial fulfilment of the requirement of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE and ENGINEERING (Section -E)

to

K.R Mangalam University

By

Virat-25010101356

Krishang-2501010277

Jasleen-2501010291

Aprajita-2501010313

Daksh-2501010293

Under the supervision of **Ms. Megha Sharma**

Department of Computer Science and EngineeringSchool of

Engineering and Technology K.R Mangalam

University, Gurugram- 122001, IndiaJanuary2026

INDEX

ABSTRACT

Academic integrity represents a cornerstone of higher education, ensuring that assessment outcomes genuinely reflect student competence and learning. However, traditional plagiarism detection systems focus predominantly on textual similarities, failing to identify behavioural anomalies that may indicate academic misconduct. This project proposes a Behavioural Academic Integrity Checker designed to analyse student submission patterns, typing behaviours, and temporal characteristics during assignment completion.

The system employs machine learning algorithms to establish baseline behavioural profiles for individual students and detect deviations that warrant further investigation. By integrating keystroke dynamics, timestamp analysis, and submission pattern recognition, the proposed solution provides a complementary layer of integrity verification beyond conventional content-matching tools. The system maintains ethical considerations by implementing human-in-the-loop validation, ensuring that automated flags serve as indicators rather than conclusive evidence of misconduct.

This research addresses the growing sophistication of academic dishonesty methods, particularly in remote and online learning environments, whilst respecting student privacy and maintaining fairness in academic assessment processes.

INTRODUCTION

 Digital learning platforms and remote assessments have significantly transformed academic evaluation.

 These technologies improve accessibility but introduce new challenges in maintaining academic integrity.

 Traditional tools like proctoring systems and plagiarism checkers have limitations.

 Existing systems mainly detect textual similarity and fail to identify non-plagiarism-based misconduct.

 Advanced academic dishonesty methods such as contract cheating often bypass content-based checks.

 Behavioural biometrics (typing patterns, submission timing, work progression) can indicate genuine authorship.

 An intelligent system analysing these behavioural factors can enhance integrity verification.

 The proposed Behavioural Academic Integrity Checker complements existing tools.

 It builds individual behavioural profiles using legitimate coursework.

 The system flags anomalous behaviour for review without excessive surveillance or privacy intrusion.

MOTIVATION

Limitations of Existing Systems

Contemporary plagiarism detection tools demonstrate significant efficacy in identifying textual duplication but remain inadequate in detecting behaviourally-based academic misconduct. Contract cheating, unauthorised collaboration, and externally completed assignments frequently evade detection through conventional content-matching algorithms.

Evolution of Academic Dishonesty

The commercialisation of assignment completion services and the availability of sophisticated paraphrasing tools have rendered traditional integrity measures increasingly ineffective. Students can now obtain externally completed work that exhibits no textual similarity to existing sources, necessitating alternative detection methodologies.

Remote Learning Challenges

The accelerated adoption of online education has created environments where physical proctoring is impractical or impossible. Behavioural analysis provides a scalable, non-intrusive alternative that maintains assessment integrity without requiring continuous surveillance or excessive resource allocation.

Ethical Integrity Verification

This project prioritises ethical implementation by incorporating human validation processes, transparent operation, and privacy-preserving methodologies. The system serves as a decision-support tool rather than an automated adjudication system, respecting due process in academic misconduct investigations.

LITERATURE REVIEW

 Behavioural biometrics are widely recognised as reliable authentication mechanisms in security systems.

 Keystroke dynamics reveal individual-specific typing patterns, including rhythm, key pressure, and inter-key timing.

 Studies by **Monrose and Rubin** demonstrated that keystroke patterns are distinctive enough to function as biometric identifiers, with low false acceptance rates.

 In educational settings, researchers have analysed temporal patterns to detect anomalous submission behaviour.

 Northcutt et al. used learning management system timestamp data to identify irregular assignment completion patterns.

 Their research found that sudden deviations from normal work habits often correlate with higher instances of academic misconduct.

 Bawarith et al. used supervised learning models to classify submission behaviour, achieving higher accuracy than traditional methods.

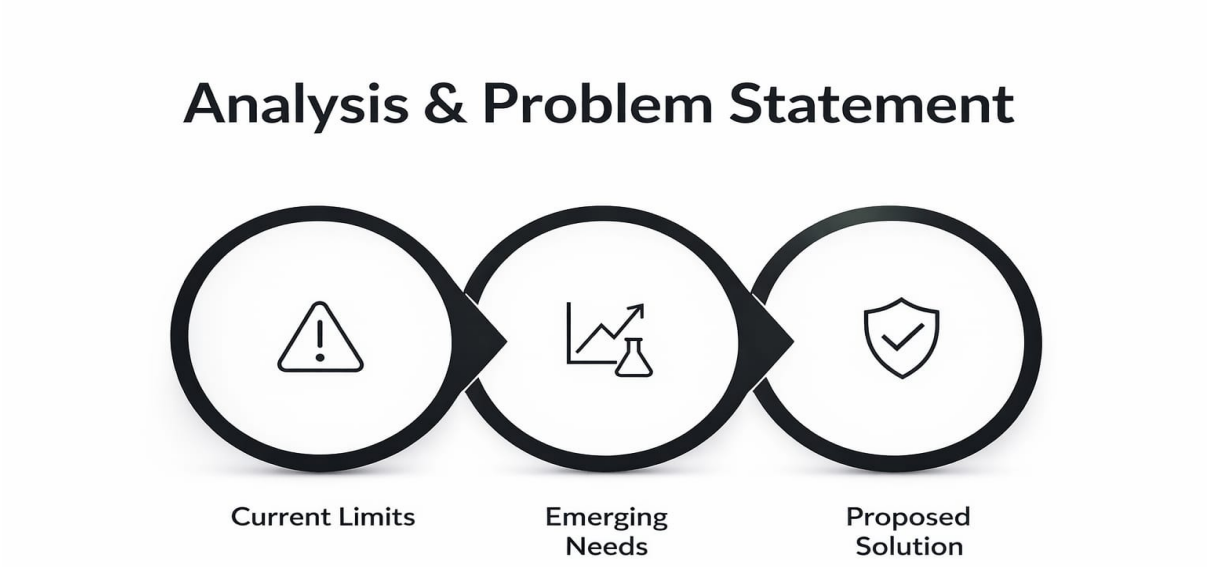
 Existing machine learning approaches face challenges such as large training data requirements and potential algorithmic bias.

 Ethical concerns are a key focus in automated integrity systems research.

 Lancaster and Clarke emphasise that automated tools should support investigation, not replace human judgement.

 This approach supports educational values by encouraging formative intervention rather than purely punitive action.

GAP ANALYSIS



Existing academic integrity systems address content-level plagiarism effectively but exhibit critical gaps in behavioral anomaly detection, creating vulnerabilities that sophisticated misconduct methods exploit.

Identified Gaps in Current Systems

Behavioural Analysis Absence

Conventional systems lack mechanisms to analyse submission behaviours, typing patterns, or temporal characteristics that indicate authorship authenticity.

Profile-Based Detection

Current tools do not establish individual student baselines, preventing identification of submission patterns inconsistent with historical behaviour.

Holistic Assessment

Existing solutions operate in isolation from learning management systems, missing contextual information valuable for integrity verification.

PROBLEM STATEMENT

Academic institutions are increasingly facing challenges in maintaining academic integrity due to the widespread availability of online resources, AI-assisted writing tools, and unauthorized collaboration among students. Traditional plagiarism detection systems primarily rely on text similarity comparison or final content analysis, which provides limited insight into how an assignment was actually produced. As a result, these systems may generate false positives, fail to detect sophisticated misconduct, and offer little contextual evidence for faculty during evaluation.

There is a growing need for an approach that goes beyond surface-level content analysis and instead examines the behavioural patterns exhibited during the assignment creation process. Indicators such as typing rhythm, editing frequency, paste actions, writing duration, and sudden content insertion can provide valuable insight into whether an assignment was developed gradually by the student or inserted through external sources.

The key challenge is to design a system that can identify such behavioural anomalies while maintaining ethical standards, protecting student privacy, and avoiding automated or unjust accusations. Universities require tools that assist educators with additional evidence rather than replacing human judgment.

This project addresses the above challenge by proposing the development of a behavioural academic integrity checker that analyses the assignment creation process and generates explainable integrity risk indicators to support informed academic decision-making.

OBJECTIVES

1) Behavioural Profile Development
Develop algorithms to establish individual student behavioural baselines through analysis of legitimate coursework submissions

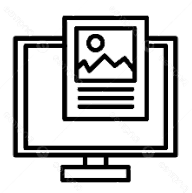
2) Anomaly Detection Implementation
Implement machine learning models to identify statistically significant deviations from established behavioural patterns

3) Ethical Framework Integration
Design human-in-the-loop validation processes ensuring automated flags require academic review before action

4) System Integration
Create seamless integration with existing learning management systems and assignment submission platforms

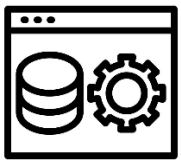
Tools/Technologies Used

Frontend



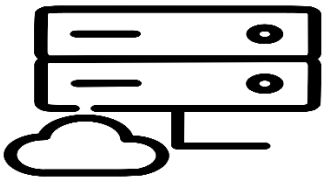
- HTML
- CSS
- JavaScript
- Browser event listeners

Backend



- Python
- Fast API
- Pydantic

Data Handling



- JSON-based payloads
- In-memory event processing

Architecture

- Client-Server model
- Restful API design

METHODOLOGY

Data Collection Phase

Gather keystroke dynamics, submission timestamps, editing patterns, and work progression data from consenting students during legitimate assignments. Establish ethical data handling protocols and obtain institutional review board approval.

Profile Generation

Employ statistical analysis and machine learning algorithms to create individualised behavioural profiles. Identify characteristic patterns in typing speed, pause distribution, revision frequency, and temporal work habits unique to each student.

Anomaly Detection

Implement supervised and unsupervised learning models to identify submissions exhibiting significant deviations from established profiles. Calculate confidence scores and flag submissions exceeding predetermined thresholds for academic review.

Human Validation

Route flagged submissions to academic staff for contextual evaluation. Provide educators with comparative visualizations and statistical evidence whilst maintaining final determination authority with human reviewers.

The methodology incorporates continuous model refinement through feedback loops, enabling the system to improve detection accuracy whilst minimising false positive rates. Privacy preservation remains paramount throughout implementation, with anonymised data processing and secure storage protocols protecting student information.

Conclusion

This project addresses critical gaps in academic integrity verification by introducing behavioural analysis methodologies that complement existing content-matching systems. Through ethical implementation emphasising human oversight and privacy preservation, the proposed solution enhances institutional capacity to maintain assessment credibility whilst respecting student rights. The Behavioural Academic Integrity Checker represents a forward-looking approach to academic integrity that acknowledges the evolving nature of educational dishonesty whilst prioritising fairness and due process in misconduct investigations.

REFERENCES

1. *Securing Cyberspace: International and Asian Perspectives | Manohar Parrikar Institute for Defense Studies and Analyses*. (n.d.). Retrieved July 21, 2023, from https://www.idsa.in/book/securing-cyberspace_csamuel-sharma
2. Sivan, R., & Zukarnain, Z. A. (2021). Security and Privacy in Cloud-Based E-Health System. *Symmetry*, *13*(5), Article 5. https://doi.org/10.3390/sym13050742
3. Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and Privacy in theMedical Internet of Things: A Review. *Security and Communication Networks*, *2018*, e5978636. https://doi.org/10.1155/2018/5978636