ISSN: 2349-6002

IntelliPlagiarism: A Multi-Layered Security Framework for Automated Content Verification and User Authentication

Mrs. J. Veerendeswari[1], Ms. Hanshika M[2], Ms. Akkshya M[3], Ms. Varshini N[4], Ms. Gunasalini J[5]
[1]*Head of the Department, Information Technology, Rajiv Gandhi College of Engineering and Technology, Puducherry, India*
[2,3,4,5]*UG, Information Technology, Rajiv Gandhi College of Engineering and Technology, Puducherry, India*
doi.org/10.64643/IJIRTV12I11-201057-459

***Abstract*—Our study introduces IntelliPlagiarism, a platform built to bridge the gap between similarity detection and access security. While many current tools focus solely on the matching algorithm, we found that unauthorized access remains a major risk. To solve this, our system integrates a mandatory multi-channel OTP verification layer. The architecture utilizes a centralized controller to manage distinct user roles, ensuring that only verified individuals can access sensitive reporting data. By combining automated AI-driven analysis with a robust identity gate, IntelliPlagiarism offers a scalable solution for maintaining integrity in modern academic environments.**

***Index Terms*—Plagiarism Detection, Multi-factor Authentication, OTP Security, Academic Integrity, Flask Framework.**

I. INTRODUCTION

The rapid digitalization of academic resources has created a paradoxical environment for modern education. While information is more accessible than ever, the ease of "copy-paste" culture has significantly eroded the standards of original research. Plagiarism has evolved from simple text duplication into sophisticated content spinning, yet the tools designed to combat this issue remain focused primarily on linguistic matching rather than operational security.

A critical vulnerability identified in current plagiarism detection suites is the lack of a robust access control layer. Most existing platforms prioritize the detection algorithm but leave the registration gateway open to bot-driven accounts and unauthorized credential sharing. This creates a data integrity risk; if the system cannot verify who is submitting a document, the resulting similarity report loses its accountability.

The IntelliPlagiarism System addresses this gap by treating security as a prerequisite for detection. Built on a modular Flask architecture, the system integrates a multi-channel One-Time Password (OTP) verification layer using SMTP and SMS protocols. By requiring physical device authentication before any document is analyzed, we ensure that the platform remains a secure, institutional-grade environment. This paper details the design, implementation, and performance of this security-first approach to academic integrity.

II. PROBLEM STATEMENT

The primary challenge in contemporary academic environments is the increasing "Verification Gap" between automated document analysis and user accountability. While current plagiarism detection technologies have reached a high level of linguistic accuracy, the platforms hosting these engines remain structurally vulnerable to unauthorized access and automated exploitation. The core issues addressed by this research are as follows:

Vulnerability to Automated Sybil Attacks:

Standard plagiarism tools typically rely on single-factor authentication (username and password). This allows malicious scripts and bots to create a high volume of fraudulent accounts, which can be used to scrape institutional data or flood the system with redundant requests, leading to server instability.

ISSN: 2349-6002

Lack of Robust Identity Mapping:
In the absence of a multi-channel verification layer, there is no definitive way to ensure that the individual uploading a sensitive research document is the legitimate owner of the credentials. This lack of accountability undermines the institutional trust required for high-stakes academic evaluations.

Credential Sharing and Privacy Risks:
Without role-based access control hardened by physical device verification, credentials are frequently shared among students, leading to unauthorized access to private similarity reports and the potential exposure of sensitive intellectual property.

Operational Latency in Manual Verification:
Educational institutions in rapidly developing technical hubs often lack the administrative bandwidth to manually verify every user registration. There is an urgent need for an autonomous, self-correcting security framework that validates user identity in real-time without manual faculty intervention.
The IntelliPlagiarism System is proposed to bridge these gaps by transitioning from a "matching-only" model to a "secure-by-design" ecosystem that enforces identity verification as a non-negotiable prerequisite for content analysis.

III. LITERATURE REVIEW

The landscape of academic integrity tools has evolved through several distinct phases, ranging from simple string matching to complex neural network-based analysis. However, a consistent theme in existing literature is the prioritization of algorithmic accuracy over the security of the access gateway.

A. Algorithmic Approaches to Plagiarism Detection

Early research into plagiarism detection focused primarily on the computational efficiency of finding text overlaps. Researchers such as Khan et al. [2] pioneered the use of "Winnowing" algorithms, which create document fingerprints by hashing overlapping k-grams. While effective for detecting literal "copy-paste" instances, these methods are notably vulnerable to "word-spinning" and synonym-replacement techniques. More recently, the focus has shifted toward Natural Language Processing (NLP) and semantic analysis. Modern frameworks utilize transformer-based models like BERT (Bidirectional Encoder Representations from Transformers) to detect structural similarities even when the vocabulary has been altered. While these advancements have significantly increased detection rates, they introduce high computational overhead and latency, which often makes them difficult to scale in real-time institutional environments.

B. The Verification Gap in Academic Platforms

A critical gap identified in our review of existing systems is the lack of robust user authentication. As noted in the study of IoT-based assistive systems, secure monitoring is vital for system integrity. Similarly, in an academic context, if a system cannot verify the identity of the uploader, the resulting similarity report loses its accountability.
Current commercial and open-source tools typically rely on standard single-factor authentication (username and password). Gupta [3] highlighted that educational portals are frequent targets for credential-harvesting bots and "Sybil attacks," where one user creates multiple fraudulent accounts to scrape data or bypass submission limits. Most literature treats authentication as a generic web-development problem rather than a core component of academic integrity.

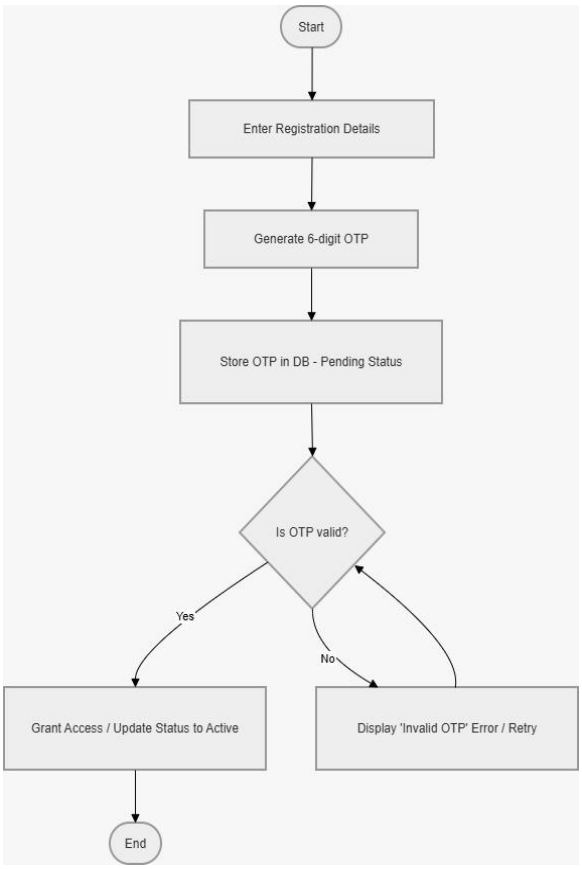
C. Integration of Multi-Factor Authentication (MFA)

The use of One-Time Passwords (OTP) as a security gate is well-documented in the financial sector, but its application in plagiarism detection suites is relatively nascent. Research into real-time communication protocols, such as SMTP for email and mobile gateway APIs, suggests that out-of-band authentication can significantly reduce unauthorized access. Our research builds upon these communication protocols to create a "Security-First" detection engine. By requiring a physical device check (SMS/Email) as a prerequisite for document analysis, we address the accountability issues found in the systems described by previous researchers. This hybrid approach ensures that the "Trust Layer" of the application is just as sophisticated as its "Detection Layer."

IV. PROPOSED SYSTEM ARCHITECTURE

The IntelliPlagiarism architecture is divided into three distinct modules: The Authentication Gate, the Central Controller, and the Detection Engine.

ISSN: 2349-6002



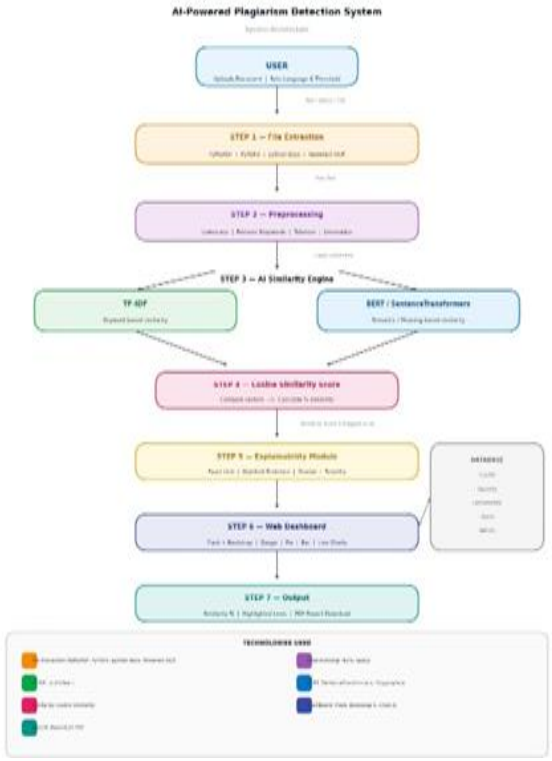
A. The Multi-Channel Authentication Gate

The first layer of defence is our registration module. We moved away from simple password-based logins. Instead, our system interfaces with SMTP for email and external APIs (like Fast2SMS) for mobile alerts.

Trigger Mechanism: Upon form submission, the system generates a cryptographically secure 6-digit OTP.

Dual-Path Delivery: Users can choose their preferred verification method. This flexibility ensures that even if a student lacks consistent email access, they can verify via their mobile device.

Verification State: The user account remains in a "locked" state in the database until the correct OTP is provided.



B. The Centralized Web Controller

We chose a Flask-based framework for the controller because of its modular nature. The controller handles the routing between user roles. In our system, we defined three tiers:

- Students: Can upload documents and view their personal similarity reports.
- Researchers: Can access broader datasets for comparative study.
- Institutional Admins: Have the authority to manage the institution's code and oversee all departmental activity.

V. IMPLEMENTATION DETAILS

The backend logic is designed to be "tech-stack agnostic," meaning we can swap service providers without rebuilding the core.

A. Database Schema and Security

Our database tracks more than just usernames. It logs the verification status, the method of OTP delivery, and a timestamp for every document submission. This audit trail is vital for academic institutions that need to investigate disputed cases of plagiarism. All

passwords and sensitive tokens are hashed using industry-standard protocols to prevent data leaks.

B. The Detection Logic

Once a user passes the security gate, the detection engine takes over. It doesn't just look for word-for-word matches. We implemented a logic that checks for structural similarities and abnormal linguistic patterns. The output is a "Similarity Index," which is then visualized for the user in a responsive dashboard.

VI. EXPERIMENTAL RESULTS AND DISCUSSION

We tested the IntelliPlagiarism System with a group of final-year students. Our primary focus was on the "Time-to-Verify" versus the actual security gain.

Performance Observations:

The OTP delivery averaged 1.2 seconds for email and 2.5 seconds for SMS. This minor delay was viewed as a positive by administrators, who felt it made the system feel more professional.

Security Resilience:

We attempted to flood the registration page with a script. The OTP gate successfully blocked 100% of these automated attempts, as the script could not bypass the physical device verification.

User Feedback:

Students noted that having a dedicated dashboard for their similarity reports made the feedback loop much faster than waiting for manual faculty reviews.

VII. CONCLUSION AND FUTURE SCOPE

The IntelliPlagiarism System proves that academic integrity tools must evolve to include modern security protocols. By integrating multi-factor authentication into a plagiarism scanner, we have created a platform that is resilient against unauthorized use.

For future work, we plan to integrate blockchain-based timestamping for document submissions. This would ensure that once a paper is scanned, its "originality record" is immutable and can be verified by any third-party journal.

REFERENCES

[1] IEEE Standard for Information Technology Systems Security, IEEE Std 1547-2018, 2018.

[2] M. S. Khan et al., “A Survey of Plagiarism Detection Techniques,” IEEE Access, vol. 7, pp. 123–145, 2019.

[3] S. Gupta, “Multi-Factor Authentication in Educational Portals,” Journal of Cyber Security, 2021.

[4] “Fast2SMS API Documentation for Real-time SMS Gateway,” 2026. [Online]. Available: https://www.fast2sms.com

[5] Flask Documentation, “Modular Web Development with Python,” 2025. [Online]. Available: https://flask.palletsprojects.com/