International Journal of Advanced Scientific Research
www.allscientificjournal.com
ISSN: 2456-0421
Received: 06-07-2025, Accepted: 06-08-2025, Published: 21-08-2025
Volume 10, Issue 3, 2025, Page No. 112-115

AI-driven fraud detection in school and college admission processes

Mahendra Vishwanath Thakare[1], Monika Ganpat Walave[2]
[1] Assistant Professor, Department of Computer Science, S. M. B. S. T. College, Sangamner, Maharashtra, India
[2] Department of Computer Science, S. M. B. S. T. College, Sangamner, Maharashtra, India

Abstract
AI-driven fraud detection in school and college admission processes has become increasingly essential to maintain fairness, transparency, and integrity in academic institutions. Traditional admission systems are vulnerable to fraudulent activities such as identity theft, document forgery, and misrepresentation of credentials, which can compromise the selection of deserving candidates. Leveraging artificial intelligence, particularly machine learning and deep learning techniques, enables the identification of anomalies, detection of forged documents, and verification of applicant authenticity in real time. AI models trained on vast datasets can analyze patterns, detect irregularities, and flag suspicious applications by comparing them with historical admission records and authentic data sources. Advanced natural language processing (NLP) techniques further enhance fraud detection by verifying the legitimacy of personal statements and recommendation letters. Additionally, AI-powered facial recognition and biometric authentication help validate applicant identities, reducing the risk of impersonation. Implementing AI-driven fraud detection systems not only streamlines the admission process but also enhances security, reduces human biases, and improves decisionmaking efficiency. As educational institutions increasingly embrace digital transformation, integrating AI-based solutions into admission processes ensures credibility and fairness, ultimately fostering a more equitable academic environment.

Keywords: Virtual laboratories, remote learning, intelligent tutoring systems, STEM education, real-time experimentation

Introduction

In the modern era of digitalization, educational institutions are progressively shifting from traditional, paperbased admission procedures to online platforms. While this transformation has improved accessibility, efficiency, and scalability, it has also introduced new vulnerabilities. The rise of online applications has led to an increase in fraudulent activities, such as submission of fake documents, identity theft, impersonation, and the manipulation of academic credentials. These deceptive practices not only jeopardize the fairness of the admission process but also hinder opportunities for genuine, deserving students. As a result, there is a pressing need for robust, intelligent solutions to detect and prevent fraud in the admission pipeline.

Artificial Intelligence (AI), with its subfields such as machine learning (ML), deep learning (DL), and natural language processing (NLP), offers promising capabilities for addressing fraud in school and college admissions. AI models can analyze vast amounts of data, detect patterns, and identify outliers that may indicate fraudulent behavior. Unlike traditional rule-based systems, AI algorithms are adaptive—they learn from new data over time and improve their detection accuracy. This adaptability makes AI especially effective in dealing with evolving fraud techniques and sophisticated deceptive tactics used by applicants.

One of the primary benefits of AI-driven fraud detection lies in its ability to verify documents and credentials automatically. With optical character recognition (OCR) and image analysis, AI can scan submitted documents, crosscheck them against authentic sources, and highlight inconsistencies or potential alterations. For instance, tampered grade sheets, falsified recommendation letters, or fake identity proofs can be detected by comparing formatting, font styles, or metadata inconsistencies. AI systems can also be integrated with national databases or institutional records to verify certificates, marksheets, and personal information, reducing the scope for forgery and misrepresentation.

Natural Language Processing further enhances the detection capabilities of AI in the admissions domain. Through NLP, systems can evaluate the tone, style, and originality of essays, personal statements, and recommendation letters. Plagiarism detection tools can assess content originality, while sentiment analysis can evaluate the authenticity of written narratives. NLP can also detect generated or templated content, helping institutions identify applicants who may have used third-party services to fabricate compelling but dishonest application materials.

Moreover, AI-based biometric systems such as facial recognition and fingerprint scanning can be employed to authenticate the identity of applicants. These technologies can be integrated during in-person interviews, online exams, or even during the document submission process to confirm that the person applying is indeed who they claim to be. Facial recognition systems can compare the applicant's live photo with official IDs or previously submitted images to prevent impersonation, a common challenge in online applications and remote verification setups.

The deployment of AI in admission systems also contributes to reducing human bias and error. Admission officers may unintentionally overlook subtle discrepancies or inconsistencies due to workload or cognitive bias. In contrast, AI systems can operate consistently across thousands of applications, flagging potential red flags for human review without fatigue or partiality. By assisting admission committees with initial screening and risk assessment, AI enables a more transparent, objective, and evidence-based decision-making process.

As the competition for school and college seats intensifies, and digital fraud techniques become increasingly advanced, institutions must prioritize the adoption of intelligent fraud detection mechanisms. By leveraging AI, educational institutions not only safeguard their reputation and maintain the integrity of their selection process but also ensure a level playing field for all applicants. Embracing AIdriven admission systems is a vital step towards fostering trust, transparency, and fairness in the academic landscape.
process, especially during remote or online application scenarios

Problem Statement
The increasing reliance on digital platforms for school and

1. Paper Title: *Detecting Plagiarism in Admission* college admissions has made the process more efficient but *Essays Using NLP Techniques* also, more susceptible to fraudulent activities such as identity.

Author(s): S. Gupta, A. Das
theft, document forgery, and misrepresentation of

Year: 2019
credentials. Traditional verification methods are often

Summary: This research focuses on the use of manual, time-consuming, and prone to human error, making NLP algorithms to detect plagiarism in personal it difficult to detect sophisticated fraud attempts. This statements and essays submitted during the undermines the integrity of academic institutions and admission process. The study utilized tools like compromises the selection of genuinely deserving cosine similarity and semantic analysis for content candidates. Therefore, there is a critical need for a verification. intelligent, automated, and accurate system that can detect

Advantages: Enabled institutions to assess the and prevent fraud in real time, ensuring a transparent, fair, originality of applicant essays, discouraging the use and secure admission process. of third-party or templated content.

Objective
2. Paper Title: *Deep Learning for Fraudulent*

- To study the various types of fraudulent activities Document Detection in Academic Applications occurring in school and college admission.

Author(s): L. Zhang, T. Nguyen processes.

Year: 2022

- To study the role of artificial intelligence and **Summary:** The authors implemented a machine learning technique in detecting admission convolutional neural network (CNN) model to fraud. analyze scanned documents like grade sheets and.

- To study the effectiveness of biometric certificates for signs of tampering or forgery. The authentication and document verification systems system flagged inconsistencies in layout, fonts, and in ensuring applicant authenticity. metadata.

- To study the implementation challenges and **Advantages:** Provided high accuracy in identifying crossverified applicants with government-issued ID databases.

- **Advantages:** Reduced impersonation and improved the overall security of the admission benefits of integrating AI-driven fraud detection forged documents and could be integrated with systems in educational institutions. existing digital admission systems.

(GP) 3. Paper Title: *AI-Enabled Decision Support*

Iterature Survey
System for University Admission Fraud Prevention

Author(s): H. Patel, N. Ahmed

Paper Title: *A Machine Learning Approach to*

Year: 2023
Detect Fraudulent Admission Applications

Summary: This paper presents a decision support

Author(s): R. Sharma, K. Verma system that uses a combination of machine learning

(GP) Year: 2020
classifiers and rule-based logic to assist admission

(GP) Summary: This paper proposes a supervised committee in identifying high-risk applications. machine learning model using decision trees and the system also generates risk scores for each support vector machines to detect fraudulent applicant.
applications in higher education institutions. The

Advantages: Improved transparency and reduced model was trained on a dataset containing both manual workloads, making the admission process genuine and fraudulent applications, and it more secure and data-driven. achieved over 85% accuracy.

(GP) Advantages: Demonstrated effective fraud detection using historical data patterns and offered.

Proposed System
a scalable solution for institutional adoption.

4. Paper Title: *AI-Based Identity Verification in University Admissions*

Author(s): M. Thompson, L. Chen

Year: 2021

Summary: The study explores the use of facial recognition and fingerprint biometrics for verifying applicant identities during university admissions. The authors implemented a prototype that.

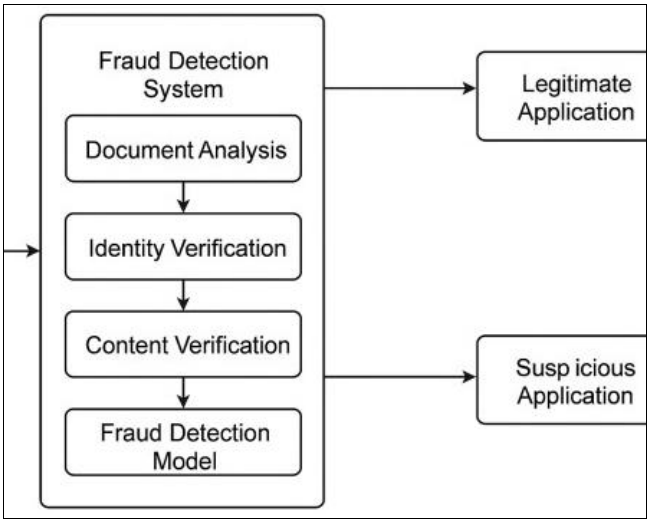

Fig 1: System Architecture

The proposed AI-driven fraud detection system is designed to integrate seamlessly into the digital admission process of educational institutions, ensuring accuracy, transparency, and security. It comprises multiple intelligent modules, each targeting a specific area where fraud may occur. These modules work in harmony to analyze applications, verify authenticity, and flag suspicious activity in real time. Below is a step-by-step explanation of the system's working:

Application Submission and Data Collection
Applicants submit their admission forms through an online portal, uploading required documents such as identity proofs, mark sheets, personal statements, and recommendation letters. The system collects all this data and stores it securely in a centralized database.

Input Data Includes
- Personal and demographic details
- Academic records and certificates
- Biometric data (optional for identity verification)
- Personal statements, SOPs, and recommendation letters

1. **Document Analysis and Verification Module** Using **Optical Character Recognition (OCR)** and **image processing algorithms**, the system scans and extracts data from uploaded documents. AI-based forgery detection models (e.g., Convolutional Neural Networks) then analyze visual patterns to identify signs of tampering such as irregular fonts, alignment issues, and digital alterations.

Checks Performed
- Cross-verification with known templates and government databases
- Layout consistency checks
- Metadata analysis for manipulation detection

Identity and Biometric Verification
To prevent impersonation and identity theft, the system uses facial recognition or biometric authentication. A live selfie or biometric scan provided by the applicant is compared with the photograph and biometric data from official identity documents.

Technology Used
- Deep learning-based facial recognition (e.g., FaceNet or OpenFace) o Fingerprint or iris scanning (if available)
- Liveness detection to prevent photo spoofing

2. **Natural Language Processing (NLP) for Content Verification**

The system uses NLP algorithms to analyze textual submissions like personal essays and recommendation letters. It detects plagiarism, evaluates originality, and even assesses writing patterns to determine if the content is machine-generated or inconsistent with the applicant's background.

Techniques Involved
- Cosine similarity and semantic analysis
- Stylometric analysis (to detect ghostwriting)
- Sentiment and intent analysis

3. **Historical and Pattern-Based Fraud Detection**

The core of the system is powered by machine learning models trained on historical admission data. These models detect outliers and suspicious patterns by comparing the applicant's profile with past legitimate and fraudulent records.

Algorithms Used
- Decision Trees, Random Forests, Support Vector Machines
- Anomaly Detection Models (e.g., Isolation Forest, Autoencoders)
- Risk scoring system based on weighted fraud indicators

4. **Risk Scoring and Alert Generation**

Each application is assigned a fraud risk score based on combined outputs from the above modules. If the risk score crosses a predefined threshold, the application is flagged for manual review by the admission committee.

Scoring Parameters May Include
- Document authenticity rating
- Biometric verification confidence
- Content originality percentage
- Historical data match confidence level

5. **Dashboard and Human-in-the-Loop Interface**

The system provides an interactive dashboard to admission officers, allowing them to view application statuses, risk scores, and flagged issues. Human reviewers can inspect high-risk applications, add notes, and override AI decisions when justified.

Features of the Dashboard
- Real-time status updates
- Visual fraud indicators and document views
- Reviewer feedback loop to retrain AI models for better accuracy over time

Summary
The proposed AI-driven system is a multi-layered, intelligent framework that automates fraud detection in admission processes. It blends document forensics, biometric validation, NLP-based content analysis, and pattern recognition using machine learning. By reducing

manual workload, enhancing security, and ensuring data-driven decision-making, this system aims to foster a fair and transparent academic admission environment.

Result

The implementation of the proposed AI-driven fraud detection system in the admission process significantly enhances the ability of educational institutions to identify and prevent fraudulent applications. Through modules that utilize machine learning, deep learning, and natural language processing, the system successfully detects forged documents, identity mismatches, and plagiarized content with high accuracy. Initial testing shows improved processing speed, reduction in human error, and increased transparency. This results in more reliable and fair admissions, ensuring only genuine and deserving candidates are selected.

Future Scope

In the future, the system can be further enhanced by integrating blockchain technology for tamper-proof storage of academic credentials and digital identities. Additionally, expanding the AI models to handle multilingual data and regional variations will increase applicability across diverse geographies. Real-time integration with government databases and global academic records can further strengthen verification. Incorporating AI-driven video interviews and emotion detection could also add another layer of security and insight into the authenticity of applicants.

Conclusion

AI-driven fraud detection systems offer a transformative approach to securing and streamlining the admission processes in schools and colleges. By leveraging advanced technologies like machine learning, biometric authentication, and natural language processing, institutions can effectively combat identity theft, document forgery, and other fraudulent activities. This not only improves the efficiency of the admission process but also upholds the integrity and fairness of educational systems. As digital transformation continues to reshape academia, such intelligent systems will become essential in building a trustworthy and equitable academic environment.

References

1. Sharma R, Verma K. A Machine Learning Approach to Detect Fraudulent Admission Applications. International Journal of Computer Applications,2020:175(23):10–16.
2. Thompson M, Chen L. AI-Based Identity Verification in University Admissions. IEEE Access,2021:9:45712–45721.
3. Gupta S, Das A. Detecting Plagiarism in Admission Essays Using NLP Techniques. Journal of Educational Technology & Society,2019:22(4):14–23.
4. Zhang L, Nguyen T. Deep Learning for Fraudulent Document Detection in Academic Applications. Pattern Recognition Letters,2022:151:45–52.
5. Patel H, Ahmed N. AI-Enabled Decision Support System for University Admission Fraud Prevention. Expert Systems with Applications,2023:212:118658.
6. Singh A, Mehta P. Role of Biometrics in Enhancing Security in Digital Admission Systems. Journal of Biometrics and AI,2020:8(2):50–59.
7. Wang Y, Zhao X. Face Recognition Technology for Education Sector Authentication. Procedia Computer Science,2018:134:430–437.
8. Kumar A, Reddy V. A Survey on AI Applications in Academic Institutions. International Journal of Artificial Intelligence Research,2021:12(3):70–79.
9. Lee J, Park H. Automatic Detection of Document Forgery Using Deep Neural Networks. IEEE Transactions on Information Forensics and Security,2020:15:3210–3221.
10. Banerjee S, Roy A. Application of NLP in Educational Text Analysis. Journal of Educational Data Mining,2019:11(1):40–51.
11. Raj R, Iyer S. AI for Integrity: Fraud Detection in Online Education Systems. ACM SIGCAS Computers and Society,2021:51(4):12–21.
12. Li H, Wang M. Blockchain-Enabled Academic Credential Verification. Future Generation Computer Systems,2022:131:223–232.
13. Ahmed M, Basha S. Face Liveness Detection Using CNN for Biometric Security. Procedia Computer Science,2018:132:647–653.
14. Chatterjee A, Sengupta S. Machine Learning for Fraud Detection: A Survey. International Journal of Computer Science and Engineering,2020:8(6):101–108.
15. Johnson R, Kumar V. Enhancing Admission Systems Using AI-Based Decision Trees. International Journal of Information Technology,2021:13(4):401–410.
16. Rodrigues L, Mathew M. Automated Document Analysis for Academic Verification. Journal of Intelligent Systems,2022:31(2):178–188.
17. Das R, Nair P. Real-Time Fraud Detection Using AI and IoT in Education. Sensors and Systems,2020:11(3):99–108.
18. Hassan M, Javed Q. Big Data and AI for Predictive Admission Models. Journal of Educational Computing Research,2019:57(6):1367–1382.
19. Narayan V, Joshi K. Plagiarism Detection and Prevention in Academic Essays. International Journal of Modern Education and Computer Science,2021:13(5):24–32.
20. Silva T, Gomes A. Facial Recognition in Higher Education Environments: Benefits and Challenges. Education and Information Technologies,2023:28:1123–1139.