



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 14, Issue 3, March 2026



Smart Job Posting Classifier: Real vs Fake

Mrs. P. Kavya¹, Koppadi Rajeevi², Yandrapu Bharath Kumar³, Sudikonda Meghana Gayathri⁴,

Tripuragiri Sai Bhavani⁵, Gummapu Aravind⁶

Assistant Professor, Department of CSE (Data Science), NSRIT, Vishakhapatnam, India¹

Student of Department of CSE (Data Science), NSRIT, Vishakhapatnam, India^{2,3,4,5,6}

ABSTRACT: The rapid growth of online recruitment platforms has increased the risk of fraudulent job postings, leading to financial loss and misuse of personal information. This project, Job Shield AI, presents a web-based application that classifies job postings as real or fake using Natural Language Processing (NLP) and rule-based fraud detection. The system analyzes job descriptions for fraud indicators such as payment requests, suspicious contact details, unrealistic salary offers, and lack of company authenticity. Developed using Python, Flask, HTML, CSS, and JavaScript, the application provides interactive analysis and generates fraud probability, legitimacy score, and confidence level. The solution operates offline without external APIs, ensuring efficiency, security, and accessibility for job seekers.

KEYWORDS: Fake Job Detection, Artificial Intelligence, Natural Language Processing, Fraud Detection, Flask

I. INTRODUCTION

Online recruitment platforms have become the primary source of employment opportunities. However, fraudulent recruiters exploit these systems by posting fake jobs to collect money or sensitive personal data. Manual verification of job postings is time-consuming and unreliable. The proposed system, Smart Job Posting Classifier: Real vs Fake, automates fraud detection using AI-based text analysis.

The system accepts job descriptions in text, PDF, or URL format, preprocesses the input, extracts company and role details, and applies NLP techniques to detect fraud indicators. It then calculates fraud probability, legitimacy score, and risk level, presenting results through a userfriendly interface.

II. METHODOLOGY

Ethical and Technical Considerations in AI-Based Fake Job Detection

The implementation of AI-powered job posting classification systems involves both technical design decisions and ethical considerations. Since the system processes job descriptions that may contain sensitive personal or organizational information, it is essential to ensure accuracy, privacy, transparency, and responsible AI usage

1. Data Privacy and Confidentiality

1.1 Informed Usage of Job Data

Job postings often contain sensitive details such as contact information, salary expectations, or company identifiers. Ethical deployment requires informing users that their job descriptions are analyzed by AI models, maintaining transparency in data handling practices.

1.2 Local Processing and Data Protection

The proposed system operates locally using Python and Flask, without transmitting data to external servers. This reduces the risk of unauthorized access or leakage of personal information..

1.3 Secure Storage and Temporary Data Handling

Fraud analysis results and intermediate files are stored securely in a local database. Temporary files are deleted after processing, and access controls are implemented to prevent misuse of stored data.



International Journal of Innovative Research in Computer and Communication Engineering (IJRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2. Accountability in AI Decision-Making

2.1 Transparency of Detection Rules

The fraud detection engine uses documented fraud indicators such as payment requests, unrealistic salaries, and suspicious contact details. Clear documentation of these rules ensures users understand how classifications are made.

2.2 Governance and Usage Guidelines

Organizations or institutions deploying the system should define policies regarding data handling, storage duration, and authorized access. Governance frameworks ensure responsible usage and minimize risks.

3. Accuracy and Bias in AI Models

3.1 Limitations of Rule-Based Detection

Rule-based systems may fail to detect cleverly disguised fraudulent postings. Continuous refinement of fraud indicators and inclusion of machine learning models can improve accuracy.

3.2 Bias in Text Classification

AI models trained on limited datasets may introduce bias, misclassifying legitimate postings as fraudulent. Careful dataset selection and ongoing evaluation are necessary to reduce bias.

4. System Efficiency and Performance

4.1 Resource Constraints

The system is designed to run efficiently on standard hardware using lightweight NLP libraries. This ensures accessibility for students and institutions without requiring high-end infrastructure.

4.2 Real-Time or Near Real-Time Processing

Fraud detection must be performed quickly to maintain usability. Optimized preprocessing and modular architecture contribute to improved response time and user experience.

III. SECURITY IN AI-BASED JOB POSTING CLASSIFICATION

1. Data Integrity and Protection

1.1 Encryption Techniques

Job descriptions and generated fraud analysis reports may contain sensitive information.

Encrypting data both at rest and during processing helps protect it from unauthorized access. Secure file storage mechanisms and encrypted communication channels enhance overall system security.

1.2 Secure File Handling

Temporary files created during preprocessing (e.g., extracted text from PDFs or URLs) should be deleted after analysis. This minimizes the risk of data retention and leakage.

1.3 Data Masking

Sensitive details such as email addresses or phone numbers can be masked or anonymized in reports to prevent misuse while still allowing fraud detection.

2. Access Control Mechanisms

2.1 Role-Based Access Control (RBAC)

Only authorized users should be able to upload, analyze, or view classification results. RBAC ensures that permissions are granted based on user roles.

2.2 Multi-Factor Authentication (MFA)

Adding an extra layer of identity verification strengthens protection against unauthorized access to the system.

2.3 Controlled Database Access

Fraud detection results stored in the local database must be protected with strict access policies to prevent tampering or misuse.

3. Automated Decision-Making and Trust

3.1 Transparency in AI Models

The fraud detection process relies on rule-based NLP techniques. Documenting fraud indicators (e.g., payment requests, unrealistic salaries) builds user trust and ensures responsible AI deployment.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3.2 Regular Evaluation and Validation

The system should undergo periodic testing to ensure detection accuracy and minimize false positives or negatives. Continuous evaluation strengthens reliability.

3.3 Human Oversight

Despite automation, human review remains essential. Users should verify classification results before making career decisions to prevent misinterpretations.

4. Incident Response and Risk Management

4.1 Monitoring and Early Detection

System logs and monitoring mechanisms can detect unusual activity, such as unauthorized access attempts. Early detection enables quick response to potential threats.

4.2 Communication and Reporting Protocols

In case of a security incident, clear reporting procedures should be established to inform relevant stakeholders. Transparent communication strengthens trust and compliance.

4.3 Post-Incident Analysis

After any breach or malfunction, a thorough review should be conducted to identify vulnerabilities. Continuous improvement based on incident analysis enhances long-term resilience.

IV. METHODS AND ALGORITHMS FOR AI-BASED FAKE JOB DETECTION

To effectively address ethical, accuracy, and security concerns in detecting fraudulent job postings, several advanced methods and algorithms are employed.

1. Text Preprocessing and Feature Extraction

The system begins by cleaning and preprocessing job descriptions. Techniques such as tokenization, stop-word removal, and stemming are applied to prepare the text for analysis. Important features such as company name, role, salary, and contact details are extracted. This structured representation enables accurate fraud detection.

2. Natural Language Processing (NLP) and Pattern Matching

NLP techniques are used to understand the meaning and context of job postings. Regular expression (regex) pattern matching identifies suspicious elements such as payment requests, urgency language, or unrealistic salary offers. TF-IDF (Term Frequency–Inverse Document Frequency) is applied to highlight significant words and phrases that may indicate fraudulent intent.

3. Rule-Based Fraud Detection Engine

The system employs a rule-based engine that evaluates fraud indicators against predefined conditions. Examples include:

- **Payment Requests** → Classified as high-risk.
- **Unrealistic Salary Offers** → Flagged as suspicious.
- **Missing Company Information** → Reduces legitimacy score.

This engine calculates fraud probability, legitimacy score, and confidence level, providing users with a clear risk assessment.

4. Machine Learning Models (Optional Extension)

To enhance detection accuracy, machine learning algorithms such as Logistic Regression, Random Forest, and Support Vector Machines (SVM) can be integrated. These models analyze textual features and patterns to classify postings as real or fake. Random Forest and SVM are particularly effective for handling large datasets and improving classification performance.

5. Privacy-Preserving Processing

The system operates locally using Python and Flask, ensuring that job descriptions are not transmitted to external servers. This approach minimizes privacy risks and protects sensitive applicant or company information. Temporary files are deleted after processing, and controlled access mechanisms safeguard stored results.

6. Lightweight Model Optimization

To ensure efficiency on standard hardware, lightweight NLP libraries and modular architecture are used. This reduces computational overhead while maintaining acceptable levels of accuracy, enabling near real-time classification of job postings.



International Journal of Innovative Research in Computer and Communication Engineering (IJRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. FOSTERING ETHICAL GOVERNANCE IN AI-BASED FAKE JOB DETECTION

To promote responsible AI usage in job posting classification, the following strategies can be implemented:

1. Ongoing AI Literacy and Ethical Training

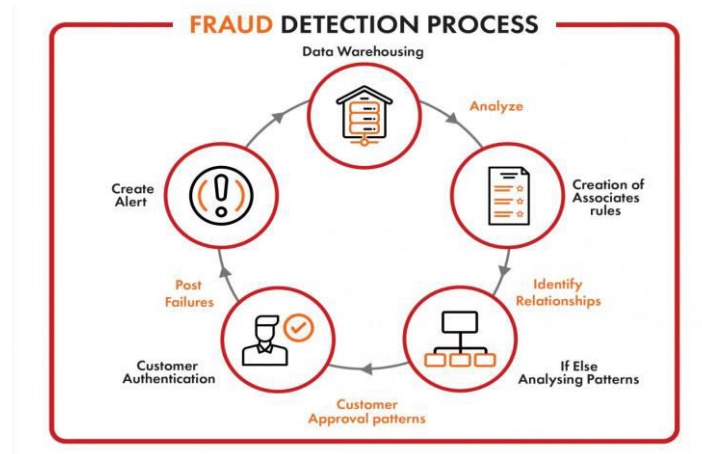
Regular training sessions for developers and users can increase awareness of AI limitations, bias risks, and responsible usage practices. Understanding how fraud detection models work, their constraints, and possible misclassifications ensures better human oversight and responsible application of the system.

2. Human-in-the-Loop Validation

Incorporating human review of AI-generated classifications ensures accountability and prevents misinterpretation. Human-in-the-loop approaches balance automation with manual verification, allowing users to double-check fraud probability scores before making career decisions. This improves reliability and trust in the system.

3. Documentation and Transparency

Maintaining clear documentation regarding fraud detection rules, NLP techniques, and system limitations enhances transparency. By explaining how fraud indicators such as payment requests or unrealistic salaries are flagged, the system builds trust among users and stakeholders while ensuring compliance with ethical standards.



VI. CONCLUSION AND FUTURE WORK

Conclusion:

In developing the Smart Job Posting Classifier, we implemented an intelligent web-based system that analyzes job descriptions and classifies them as real or fake using Natural Language Processing and rule-based fraud detection techniques. The system integrates text preprocessing, feature extraction, and fraud indicator analysis to generate fraud probability, legitimacy score, and confidence level. By automating the evaluation of job postings, the project significantly reduces manual effort, enhances user safety, and improves trust in online recruitment platforms. The modular architecture ensures scalability and flexibility, allowing future integration with machine learning models and job portal APIs. Overall, the system demonstrates how AI technologies can effectively safeguard job seekers from recruitment fraud.

Future Work:

Although the current system performs well, several improvements can enhance its capabilities:

1. Real-time monitoring of job portals for instant fraud detection.
2. Support for multilingual job descriptions.
3. Deployment as a cloud-based application for scalability.
4. Customizable fraud analysis reports (summary, detailed view).
5. Integration of machine learning models for higher accuracy.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6. Performance optimization using GPU acceleration.
7. Secure storage and encryption for sensitive job data.

REFERENCES

1. Jurafsky, D., & Martin, J. (2023). *Speech and Language Processing*. Pearson Education.
2. Goodfellow, I., Bengio, Y., & Courville, Y. (2016). *Deep Learning*. MIT Press.
3. Vaswani, A., et al. (2017). Attention is All You Need. *Advances in Neural Information Processing Systems (NeurIPS)*.
4. Brown, T. B., et al. (2020). Language Models are Few-Shot Learners. *NeurIPS*.
5. Manning, C. D., Raghavan, P., & Schütze, H. (2008). *Introduction to Information Retrieval*. Cambridge University Press.
6. Pedregosa, F., et al. (2011). Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*.
7. Bird, S., Klein, E., & Loper, E. (2009). *Natural Language Processing with Python*. O'Reilly Media.
8. Flask Team (2024). *Flask Documentation*. Available at: [Welcome to Flask — Flask Documentation \(3.1.x\)](https://flask.palletsprojects.com/en/3.1.x/)



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details