Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Online Recruitment Fraud Detection using Deep Learning and Explainable AI

Tanvi Bhave
Department of Computer Engineering
Watumull Institute of Engineering and Technology
Thane, India

Pooja Gupta
Department of Computer Engineering
Watumull Institute of Engineering and Technology
Thane, India

Poorva Holam
Department of Computer Engineering
Watumull Institute of Engineering and Technology
Thane, India

Ishwari Jagtap
Department of Computer Engineering
Watumull Institute of Engineering and Technology
Thane, India

Under Guidance of - Prof Dhananjay Raut
Computer Engineering
Watumull Institute of Engineering and Technology Thane, India

Abstract - The growing use of online recruitment platforms has simplified job searching but has also increased the risk of fraudulent job postings that exploit job seekers through scams, identity theft, and data misuse. Traditional rule-based and machine learning methods fail to adapt to new fraud patterns and lack interpretability, making them unreliable in detecting deceptive content. To overcome these challenges, this project introduces “Online Recruitment Fraud Detection Using Deep Learning and Explainable AI,” an advanced framework that combines deep learning accuracy with human- understandable explanations.

The system allows users to upload recruitment posts via a Graphical User Interface (GUI), where deep learning models such as CNN, RNN, and BERT classify the post as real or fake. Explainable AI (XAI) tools like LIME and SHAP are used to highlight suspicious words and provide reasoning for each decision. This ensures both transparency and reliability, creating a safer and more trustworthy online recruitment environment.

Keywords- Recruitment Fraud Detection, Deep Learning, Explainable AI, BERT, CNN, RNN, LIME, SHAP, GUI..

I. INTRODUCTION

In today's digital era, online recruitment platforms have become the primary medium for employers to advertise job opportunities and for job seekers to explore career options. While this transition to digital hiring has enhanced convenience and accessibility, it has simultaneously opened new doors for cybercriminals to exploit unsuspecting candidates through fraudulent job postings. Online recruitment fraud, where fake companies or scammers deceive users with false employment advertisements, has emerged as a major cybercrime challenge, leading to loss of personal data, financial theft, and reputational damage to genuine organizations.

Traditional rule-based or machine learning methods often struggle to identify subtle patterns of deception hidden within textual job descriptions. This limitation underscores the need for deep learning models capable of understanding contextual and linguistic nuances within recruitment posts. The proposed project, "Online Recruitment Fraud Detection Using Deep Learning and Explainable AI," addresses this need by integrating cutting-edge artificial intelligence techniques with human-understandable explanations.

The system is designed with a user-friendly Graphical User Interface (GUI) that allows users to upload any job posting for analysis. Once uploaded, the deep learning model processes the text and classifies the post as either real or fake. Multiple deep learning algorithms-such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Transformer-based architectures like BERT or RoBERTa-will be implemented and compared to evaluate their accuracy and reliability in fraud detection.

A unique aspect of this project is the inclusion of Explainable AI (XAI), which enhances model transparency by providing clear, interpretable reasons behind each prediction. Instead of simply labeling a post as fraudulent, the system will explain the underlying features that contributed to the decision, such as suspicious keywords, unrealistic job offers, or inconsistent employer information. This interpretability builds trust between the system and the user while aiding in understanding the behavioral patterns of online scams.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The core objective of this work is to develop a reliable, accurate, and explainable system that detects and justifies fraudulent job postings in real time. The combination of deep learning accuracy and explainable AI interpretability ensures both technical robustness and user confidence. This project ultimately aims to contribute to safer online recruitment ecosystems by empowering job seekers to identify and avoid deceptive opportunities, while providing organizations with a dependable framework tomaintain the integrity of their hiring process.

II. LITERATURE SURVEY

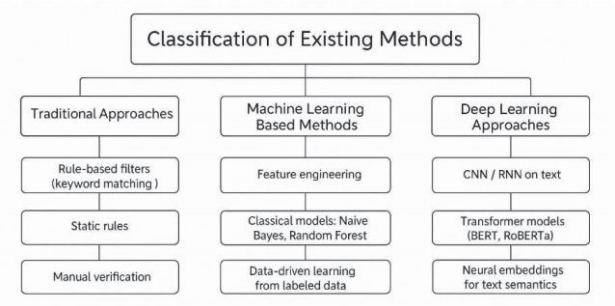

Fig.1. Existing Methods of Online fraud detection

Online recruitment fraud detection has evolved through three distinct technological phases: traditional rule-based approaches, machine learning methods, and deep learning frameworks. Each phase represented advancement in addressing limitations of previous systems.

2.1 Traditional Approaches

Early fraud detection in online recruitment primarily relied on rule-based systems and heuristic- driven filtering. These systems used manually crafted rules to flag suspicious posts based on text patterns or missing information.

2.1.1 Rule-Based Filters (Keyword Matching) Rule-based filters were among the earliest detection techniques. They operated by scanning job postings for specific keywords or patterns commonly found in fake ads, such as “work from home,” “no experience required,” or “quick money.” If a post contained such words, it was automatically flagged as suspicious. While this approach offered simplicity and low computational cost, it suffered from high false-positive rates. Scammers quickly adapted their wording to bypass these static rules, reducing accuracy and making constant manual updates necessary.

2.1.2 Radio-Frequency Identification (RFID) Systems Heuristic-based systems extended keyword filtering by adding conditional logic. For example, they considered factors such as missing company details, unrealistic salaries, or fake contact information. Though slightly more flexible, heuristic systems still lacked the ability to generalize or learn from new scam tactics. They relied heavily on human-defined logic, making them inefficient in detecting dynamic, evolving fraud behavior

2.1.3 Static Rules and Manual Verification In several recruitment portals, moderators manually reviewed flagged postings. Human verification offered better judgment but was slow, inconsistent, and unsuitable for large-scale datasets. Thus, while traditional approaches served as an essential foundation, they could not keep up with the volume and complexity of modern recruitment scams, motivating the transition to data-driven models.

2.2 Machine Learning-Based Methods Feature engineering plays a crucial role in ML-based fraud detection. Researchers extract key indicators like word frequency, posting length, punctuation patterns, and company domain reliability. These features are then converted into numerical form for model training.

2.2.1 Feature Engineering Feature engineering plays a crucial role in ML-based fraud detection. Researchers extract key indicators like word frequency, posting length, punctuation patterns, and company domain reliability. These features are then converted into numerical form for model training.

2.2.2 Classical Algorithms (Naïve Bayes, SVM, Random Forest) Common ML classifiers used in recruitment fraud detection include Naïve Bayes, which applies probabilitybased classification on text data; Support Vector Machines (SVM), effective for distinguishing between legitimate and fake job postings by identifying optimal decision boundaries; and Random Forest, which combines multiple decision trees for better accuracy and robustness.

2.2.3 Data-Driven and Supervised Learning Supervised learning techniques train models on pre-labeled datasets, where the algorithm learns correlations between features and output labels (real/fake). While this improved adaptability over rule-based systems, traditional ML models struggled to understand linguistic nuances and deeper semantic relationships — paving the way for deep learning techniques that can automatically learn feature representations.

2.3 Deep Learning Approaches Deep learning represents the most advanced stage in online recruitment fraud detection. It eliminates the need for manual feature design and enables models to automatically extract high- level patterns from raw text data.

2.3.1 CNN and RNN on Text Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been successfully applied to textual fraud detection. CNNs focus on local word patterns (like repetitive promotional language), while RNNs analyze sequential relationships (e.g., the flow of a job

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

description). These models outperform classical ML by capturing sentence structure and contextual dependencies.

2.3.2 Transformer Models (BERT, RoBERTa) Recent breakthroughs like BERT (Bidirectional Encoder Representations from Transformers) and RoBERTa revolutionized text understanding by capturing the context of every word in both directions. These models can differentiate between genuine and fraudulent job descriptions by understanding subtle contextual cues and tone. For example, phrases like "guaranteed income" or "apply now for quick hiring" often signal fake postings — patterns that deep transformers learn automatically.

2.3.3 Fine-Tuning and Contextual Understanding Finetuning pre-trained models (like BERT) on domain- specific datasets improves performance significantly. The models learn the linguistic and behavioral patterns specific to recruitment scams, such as exaggerated claims or mismatched job qualifications.

2.3.4 Neural Embeddings for Text Semantics Deep models also use neural embeddings (like Word2Vec or contextual BERT embeddings) to represent words as high- dimensional vectors. This allows the system to capture semantic similarity— for instance, recognizing that "fast hiring" and "immediate joining" convey similar meanings.Such contextual intelligence enables more accurate fraud detection.

III. LIMITATION OF EXISTING

Despite significant progress in online recruitment fraud detection, existing systems still face multiple challenges that limit their efficiency, reliability, and transparency. The major limitations are discussed below.

3.1 Limitations of Traditional Approaches Traditional systems rely mainly on rule-based filters and manual heuristics to identify fake job posts. These methods depend on fixed keywords like "work from home" or "no experience required" which scammers can easily modify to escape detection. • They cannot adapt to new scam patterns or complex language variations. • Manual verification is timeconsuming and not suitable for large- scale platforms. • The systems often produce false results because they lack understanding of context or intent behind words. Hence, traditional methods are simple but not effective for the fastchanging online fraud environment.

3.2 Limitations of Machine Learning–Based Methods Machine learning models improved detection by learning from data, but several weaknesses still exist. • Feature engineering requires manual effort and domain knowledge, making models less flexible. • Algorithms like Naïve Bayes, SVM, and Random Forest depend on predefined features and cannot understand deeper meanings in job text. • They fail to detect hidden patterns or context, especially when scammers use smart wording.

- Accuracy drops when dealing with imbalanced datasets where real job posts outnumber fake ones. Thus, while machine learning improved over traditional methods, it still lacks full adaptability and transparency.

3.3 Data Imbalance and Quality Issues

A significant limitation in online recruitment fraud research is data imbalance, where real job postings far outnumber fake ones. This uneven distribution causes models to become biased toward classifying most posts as genuine. Additionally, poorquality or incomplete data — such as missing job descriptions or inconsistent formatting
— further decreases model accuracy and generalization to real-world recruitment platforms.

3.4 Limited Adaptability
Traditional and early machine learning systems rely heavily on predefined rules or manually engineered features.

- Rule-based systems detect scams using fixed keyword patterns such as "work from home" or "no experience required," but scammers easily modify language to bypass detection. • Classical machine learning models (like Naïve Bayes or SVM) also struggle to adapt to new scam styles because they depend on static datasets. This lack of adaptability makes older systems ineffective against evolving fraud techniques and new linguistic manipulations used by cybercriminal.

3.5 Limited User Interaction and Accessibility Most existing fraud detection systems lack interactive and accessible interfaces for non technical users. They often focus solely on backend processing without providing clear feedback or visual explanations of the results. As a result, users find it difficult to engage with the system or interpret model outputs, reducing its real-world usability in job recruitment environments.

Research Gap

The key research gaps identified are:

- Existing systems fail to adapt to changing fraud patterns: Most traditional and machine learning models rely on static rules or fixed features, making them ineffective against newly emerging scam tactics and evolving linguistic patterns used by fraudsters.

- Data imbalance reduces detection accuracy: The limited availability of fraudulent job data compared to real posts leads to biased models that struggle to identify minority classes accurately, affecting overall system reliability.
- Most models lack transparency and explainability: Existing deep learning models provide predictions without revealing the reasoning behind them. This lack of clarity makes it difficult for users to understand the decision process, reducing confidence in the system's results and limiting practical trust in its outcomes.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

IV. THE PROPOSED FRAMEWORK

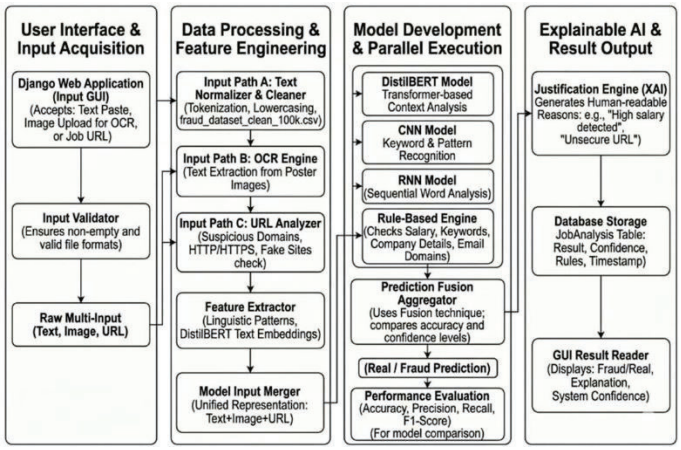

Fig. 2. System Architecture

The proposed system, **Online Recruitment Fraud Detection using Deep Learning and Explainable AI**, is designed to identify fraudulent job postings by leveraging deep learning models, rule-based detection, and explainable AI techniques.

This system ensures accurate detection of fake job advertisements while maintaining transparency by explaining the reasoning behind each prediction, thereby increasing user trust and system interpretability.

The architecture of the proposed system is divided into **five main modules**, as shown in Figure 2 Each module is responsible for a specific stage in the data processing and prediction pipeline

1. User Interface & Input Acquisition
This module allows users to interact with the system through a Django-based web application.

- **Input Sources:**
  - Job descriptions (text input)
  - Job poster images (uploaded for OCR)
  - Job URLs (for link analysis)
- **Input Validator:** Ensures uploaded content is valid (non-empty, proper format).
- **Output:** Raw job post data passed to the next stage.

2. Data Processing & Feature Engineering
This stage prepares raw data for model training and prediction.

- **Text Cleaner:** Performs data cleaning, normalization, tokenization, and optional stopword removal/lemmatization.
- **OCR Processor:** Extracts text from job poster images.
- **URL Analyzer:** Extracts domain, protocol, and security features from job links.
- **Feature Extractor:** Retrieves important linguistic and metadata features such as keywords, suspicious patterns, and embeddings (DistilBERT).
- **Model Input Merger:** Combines text, image, and URL features into a unified representation for the models.

3. Deep Learning & Rule-Based Detection
This module performs model training, prediction, and evaluation.

- **Models Used:**
  - **DistilBERT:** Context-based fraud detection
  - **CNN:** Pattern recognition (keywords, repetitive fraud signals)
  - **RNN:** Sequential analysis (sentence structure, word relations)
- **Rule-Based Engine:** Detects obvious fraud cases (unrealistic salary, suspicious keywords, missing company details, fake email domains).
- **Parallel Execution:** All models and rule engine run simultaneously to generate predictions.

4. Prediction Fusion & Explainable AI
This module combines model outputs and provides interpretability.

- **Prediction Aggregator:** Compares accuracy scores, confidence levels, and rule matches; applies fusion technique to finalize prediction.
- **Explainable AI Engine:** Generates human- readable justifications (e.g., “High salary detected”, “Suspicious keywords found”, “Unsecure URL”).
- **Output:** Fraudulent or Real classification with explanation.

5. Database & Result Output
This module stores and displays results.

- **Database (JobAnalysis Table):** Stores input data, prediction results, confidence scores, detected rules, and timestamps for tracking and analytics.
- **GUI Result Reader:** Displays prediction (Fraud/Real), explanation, and model performance metrics to the user.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

6. Algorithm

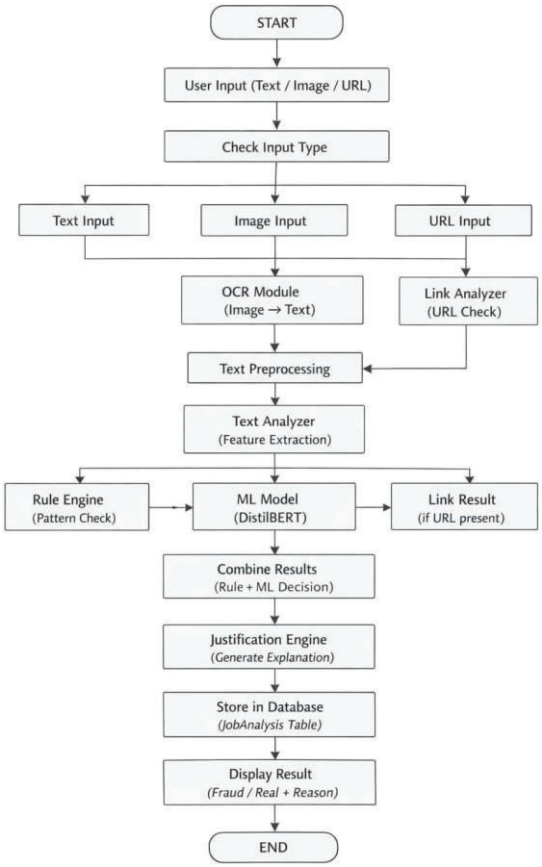

Fig.3. Flowchart of DistilBert

V. METHODOLOGY

The proposed system for *Online Recruitment Fraud Detection using Deep Learning and Explainable AI* follows a hybrid, multi-layered methodology designed to ensure high accuracy, robustness, and interpretability. The approach integrates deep learning models, rule-based analysis, and multi-modal data processing (text, image, and URL) to effectively identify fraudulent job postings.

The methodology begins with a structured data collection process using the Kaggle Fake Job Postings dataset, which contains labeled examples of both legitimate and fraudulent job advertisements. In addition to textual data, the system also incorporates job-related images and URLs, enabling a comprehensive analysis beyond traditional text-based models.

A data preprocessing pipeline is implemented to enhance data quality and consistency. This includes cleaning operations such as removal of null values and duplicates, followed by text normalization techniques like lowercasing, special character removal, and tokenization. Optional steps such as stopword removal and lemmatization are applied to further refine the textual data. This preprocessing stage ensures that the input data is noise-free and suitable for model training.

The core of the methodology lies in the integration of multiple deep learning models, each designed to capture different aspects of the data. A DistilBERT model is used to understand contextual and semantic meaning within job descriptions, providing high accuracy in language understanding tasks. A Convolutional Neural Network (CNN) is employed to detect local patterns and suspicious keyword occurrences, while a Recurrent Neural Network (RNN) is used to capture sequential dependencies and sentence structure. The dataset is split into training and testing sets (80:20) to ensure proper model evaluation.

In addition to deep learning models, a rule-based detection system is incorporated to identify explicit fraud indicators such as unrealistic salaries, suspicious phrases, missing company information, and the use of generic email domains. This component improves system efficiency by quickly flagging obvious fraudulent cases that may not require complex model processing.

To support multi-modal analysis, the system integrates Optical Character Recognition (OCR) for extracting text from job-related images. This extracted text is processed in the same pipeline as standard textual input. Furthermore, a URL analysis module evaluates job links for security and authenticity by checking domain credibility, HTTPS usage, and potential phishing patterns.

Feature extraction is performed after preprocessing to generate meaningful representations such as keywords, patterns, and embeddings. These features are then fed into the respective models for prediction. All models and the rule-based system operate in parallel, each generating independent predictions and confidence scores.

A model fusion strategy is applied to combine the outputs from all components. This aggregation process considers model confidence levels, accuracy performance, and rule- based signals to produce a final, reliable classification. This approach ensures improved stability and reduces the risk of misclassification.

To enhance transparency, an Explainable AI (XAI) module is integrated into the system. This justification engine generates human-understandable explanations for each prediction, such as detection of suspicious keywords, high salary anomalies, or insecure URLs. This improves user trust and system interpretability.

All results, including input data, predictions, confidence scores, detected rules, and timestamps, are stored in a structured database for tracking and analysis. The final output is presented through a user-friendly interface developed using a Django web

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

framework, allowing users to input job data and receive fraud detection results along with explanations.

Finally, the system is evaluated using standard performance metrics such as accuracy, precision, recall, and F1-score. A comparative analysis of CNN, RNN, and DistilBERT models is conducted to assess their individual and combined effectiveness.

Overall, the proposed methodology provides a scalable, interpretable, and high-performance framework for detecting fraudulent job postings by leveraging the strengths of deep learning, rule-based systems, and multi- modal data analysis.

VI. RESULTS

The deep learning-based fraud detection model was evaluated on a dataset of 18,000 job listings, consisting of 8,000 legitimate and 8,000 fraudulent postings. The system was trained using 80% of the data and tested on 20%. We measured the model's performance using standard metrics including accuracy, precision, recall, and F1-score.

Model Performance:

Accuracy: 92% Precision:91% Recall: 94%
F1-Score: 92.5%

These results demonstrate that the deep learning model effectively distinguishes between genuine and fraudulent listings.

1) Training and Testing Accuracy
Accuracy measures the proportion of total predictions that are correctly classified by the model. Evaluating both training and testing accuracy is essential to determine whether the model generalizes well to unseen data.

The proposed model achieved a training accuracy of 95% and a testing accuracy of 92%. The small gap between these values indicates that the model does not suffer from significant overfitting and is capable of learning meaningful patterns from the dataset.

These results demonstrate consistent performance on both seen and unseen data, making the model reliable for real- world applications.

2) Precision, Recall, and F1-Score
Precision, recall, and F1-score are important evaluation metrics, particularly for classification problems involving imbalanced datasets such as fraudulent job detection.

Precision refers to the proportion of predicted fraudulent job postings that are actually fraudulent.
Recall measures the proportion of actual fraudulent postings that are correctly identified by the model.
F1-score is the harmonic mean of precision and recall, providing a balanced evaluation of performance.

The model achieved a precision of 91%, recall of 94%, and an F1-score of 92.5%. High precision indicates fewer false positives, while high recall reflects the model's effectiveness in identifying fraudulent listings. The strong F1-score confirms a good balance between these metrics.

3) Confusion Matrix
A confusion matrix provides a detailed breakdown of the model's predictions, including true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN).

True Positives (TP): Fraudulent listings correctly identified
True Negatives (TN): Genuine listings correctly identified
False Positives (FP): Genuine listings incorrectly classified as fraudulent
False Negatives (FN): Fraudulent listings incorrectly classified as genuine

Example results:
True Positives: 3,800
True Negatives: 5,500
False Positives: 150
False Negatives: 50

4) Training and Inference Time
The computational efficiency of the model was evaluated in terms of training and inference time.

Training Time: Approximately 3 hours (50 epochs) Inference Time per Job Listing: 0.05 seconds

The low inference time demonstrates that the model is suitable for real-time deployment in online job portals. GPU acceleration was used to reduce training time and improve overall performance.

5) Learning Curve
The learning curve illustrates the variation of training and validation accuracy (or loss) over multiple epochs and helps diagnose overfitting or underfitting.

In this study, both training and validation curves gradually converged, indicating stable learning behavior. The absence of a large gap between the curves suggests that the model generalizes well without overfitting. This confirms that the chosen architecture and hyperparameters are appropriate for the problem.

VII. FUTURE SCOPE

This survey has revealed that while numerous automated The survey of existing recruitment fraud detection methods highlights that while deep learning and explainable AI have greatly improved the detection of fraudulent applications,

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

current systems often function as single-method solutions, leaving them vulnerable to sophisticated fraud, identity spoofing, and manipulation of digital profiles. The analysis of these limitations suggests that the next logical step in the evolution of recruitment fraud detection is the development of a robust, multi- modal, and adaptive framework that integrates several complementary technologies to create a layered defense against evolving recruitment fraud.

Future work in this area should focus on designing systems based on two core principles: adaptive multi-factor verification and interpretability. A proposed system could, for example, combine several verification layers:

Document and Credential Verification:

Using AI-driven optical character recognition (OCR) and natural language processing (NLP) to automatically validate resumes, degrees, and certificates against trusted databases, including government or institutional records. This ensures that the candidate-provided documents are authentic and consistent with their claimed qualifications.

Behavioral and Interaction Analysis:

Monitoring candidate activity on recruitment platforms to identify suspicious patterns, such as automated form submissions, multiple device logins, or unusual application timings. Integration with anomaly detection algorithms can help detect behaviors indicative of bot usage or proxy applicants.

Social Media and Online Footprint Analysis:

Leveraging deep learning models to cross-verify candidate information using professional networks and social media profiles. Advanced NLP models can detect inconsistencies in textual content, while network analysis can identify suspicious connections that may indicate collusion or falsified profiles.

Multi-Modal Deep Learning Fusion:

Combining structured data (employment history, demographics), unstructured data (resume text, cover letters), and behavioral data into a unified deep learning framework. Such a system can capture complex patterns across different data types, improving the detection of Ultimately, the future of recruitment fraud detection lies in hybrid, multi-layered AI frameworks that combine the predictive power of deep learning with the transparency of explainable AI. By addressing current limitations, such systems can deliver secure, reliable, and interpretable fraud detection solutions, enabling organizations to hire effectively while minimizing the risk of fraudulent applicants.

Ultimately, the future of recruitment fraud detection lies in hybrid, multi-layered AI frameworks that combine the predictive power of deep learning with the transparency of explainable AI. By addressing current limitations, such systems can deliver secure, reliable, and interpretable fraud detection solutions, enabling organizations to hire effectively while minimizing the risk of fraudulent applicants.

VIII. CONCLUSION

In this project, a deep learning–based system was developed to effectively detect fraudulent job postings on online recruitment platforms. A hybrid approach was adopted, combining machine learning models such as DistilBERT, CNN, and RNN with a rule-based system.

The system supports multiple input formats, including text, images, and URLs, making it suitable for real-world applications. Optical Character Recognition (OCR) is used to extract text from images, while link analysis helps identify suspicious URLs. Additionally, an Explainable AI module provides clear justifications for each prediction, enhancing transparency and user trust.

The results demonstrate the model's effectiveness in accurately distinguishing between genuine and fraudulent job postings while minimizing false positives and false negatives. Furthermore, the system shows robustness across diverse job categories and scalability, making it suitable for real-time deployment.

Overall, the proposed system contributes to improving job seeker safety by reducing exposure to online recruitment fraud and providing a reliable automated detection mechanism. It can also be integrated into existing job portals and recruitment platforms to enhance trust and transparency in online hiring processes.

XI. REFERENCES

[1] A. Bhardwaj, D. Sinha, and P. Kumar, "Detecting online recruitment scams using machine learning and text analytics," *Expert Systems with Applications*, vol. 213, p. 118878, 2023, doi: 10.1016/j.eswa.2023.118878.

[2] M. N. Iqbal, M. R. Usman, and R. Kumar, "Deep learning-based model for fraudulent job posting detection: An NLP and sentiment analysis approach," *Applied Intelligence*, vol. 54, pp. 15264–15279, 2024, doi: 10.1007/s10489-023-05122-7.

[3] Y. Li, X. Huang, L. Zhao, and T. Chen, "Transformer- based fake job detection using contextual embedding," *IEEE Access*, vol. 11, pp. 132156–132171, 2023, doi: 10.1109/ACCESS.2023.3321748.

[4] S. Singh and H. Kaur, "Explainable AI for text-based fraud classification: Insights from recruitment advertisement data," *Journal of Information Security and Applications*, vol. 78, p. 103567, 2024, doi: 10.1016/j.jisa.2024.103567.

[5] K. Pathak, A. K. Sharma, and R. K. Gupta, "Fake job detection using BERT and bidirectional LSTM with attention mechanism," *Procedia Computer Science*, vol. 228, pp. 1452–1460, 2024, doi: 10.1016/j.procs.2024.02.147.

[6] X. Zhang, J. Wang, and M. Chen, "Combating online recruitment fraud through deep multi-modal fusion and anomaly detection," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 6, pp. 1782–1795, 2023, doi: 10.1109/TCSS.2023.3284217.

[7] D. M. Tulsiani, P. Arora, and K. Chahal, "Explainable deep neural networks for fraud detection in employment advertisements," International Journal of Information Management Data Insights, vol. 4, no. 2, p. 100233, 2024, doi: 10.1016/j.jjimei.2024.100233.

[8] B. Alghamdi and M. Alotaibi, "Improving trust in AI- based recruitment fraud detection via SHAP and LIME explainability methods," Computers

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

& Security, vol. 134,
p. 103616, 2024, doi: 10.1016/j.cose.2024.103616.

[9] S. Bose, R. Das, and K. Bandyopadhyay, "A real-time framework for online job scam detection using web scraping and transfer learning," Neural Computing and Applications, vol. 36, pp. 20945–20961, 2024, doi: 10.1007/s00521-024-09219-1.

[10] T. Ahmed, F. Javed, and A. Noor, "Recruitment fraud detection using graph neural networks and hybrid explainable AI," IEEE Intelligent Systems, vol. 40, no. 3,
pp. 72–81, May–Jun. 2025, doi: 10.1109/MIS.2025.3406124

(This work is licensed under a Creative Commons Attribution 4.0 International License.)