International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Online Recruitment Fraud Detection Using Deep Learning Approaches

Gunnala Varshitha[1], Kadam Sowmya[2], Kallem Sheshma[3], Kemidi Sowmya[4], R. A. Manikandan[5]

[1,2,3,4]Student, Department of CSE – Artificial Intelligence & Machine Learning, Malla Reddy University Hyderabad, India
[5]Professor, CSE-AI&ML, Malla Reddy University

Abstract
Online recruitment platforms have significantly simplified the job search process by enabling organizations to publish job vacancies digitally. However, these platforms are increasingly exploited by cybercriminals who post fraudulent job advertisements to deceive job seekers and collect sensitive information or illegal payments. Online Recruitment Fraud (ORF) can lead to financial loss, identity theft, and emotional distress for victims. This research proposes a deep learning framework for detecting fraudulent job postings using transformer-based language models. The proposed system utilizes contextual embeddings generated from BERT and RoBERTa combined with a CNN2D classifier to improve classification accuracy. To address the class imbalance problem in the dataset, the SMOTE oversampling technique is applied during preprocessing. Experimental results demonstrate that the hybrid BERT + CNN2D architecture achieves an accuracy of 98.68%, outperforming traditional machine learning models. The results indicate that transformer-based models can effectively capture contextual patterns in job descriptions and significantly improve fraud detection performance.

Keywords: Online Recruitment Fraud, BERT, RoBERTa, CNN2D, SMOTE, Natural Language Processing, Fraud Detection.

1. INTRODUCTION

With the expansion of digital platforms, online recruitment systems (E-recruitment) have become the primary method for hiring and job searching. Organizations publish job advertisements through portals, specifying job roles, requirements, salary details, and benefits. While this transformation improves efficiency and accessibility, it also opens opportunities for cybercriminals to advertisements. post fraudulent job Online recruitment fraud involves fake job postings designed to extract personal information, collect illegal fees, or conduct phishing activities. These fraudulent activities increased significantly during the COVID-19 pandemic due to rising unemployment rates and heavy dependence on online platforms. Traditional fraud detection systems rely on conventional machine learning algorithms such as Naïve Bayes, Decision Trees, and Random Forest. Although these methods provide moderate performance, they fail to capture deep contextual relationships in textual job descriptions. To overcome these limitations, this study proposes a deep learning-based framework leveraging transformer-based models such as BERT and RoBERTa, combined with class balancing using SMOTE

and classification enhancement. In addition to financial exploitation, online recruitment fraud poses serious cybersecurity and privacy risks, as fraudulent postings often aim to collect sensitive personal information such as identification documents, banking details, and login credentials. The sophistication of fraudulent advertisements has increased over time, making them difficult to distinguish from legitimate job postings. Fraudsters frequently mimic reputable organizations, use professional language, and create convincing company profiles to deceive applicants. Consequently, there is a growing need for intelligent, automated, and adaptive detection systems that can analyze textual content at a deeper semantic level and identify subtle patterns indicative of fraudulent intent. The integration of advanced deep learning techniques into recruitment fraud detection systems therefore represents a critical step toward strengthening digital trust and safeguarding job seekers in the evolving online employment landscape.

2. LITERATURE REVIEW

Extensive research has been conducted on fraud detection using machine learning and deep learning approaches. Early studies primarily focused on traditional supervised learning algorithms, including Naïve Bayes, Support Vector Machines, Decision Trees, and Random Forest models. These methods demonstrated moderate success in identifying fraudulent job postings based on structured features such as company information, salary range, and keyword frequency. However, their effectiveness was limited by reliance on manual feature extraction and inability to interpret complex semantic structures within textual content. With the advancement of deep learning techniques, researchers began exploring neural network- based models for text classification tasks. Recurrent Neural Networks and Long Short- Term Memory networks were applied to capture sequential dependencies in textual data. Although these models improved performance compared to traditional approaches, they faced challenges in dependencies efficiently. and handling large-scale long-range datasets More recently, transformer-based language models have significantly advanced natural language processing tasks by enabling bidirectional contextual understanding. These models have achieved state-of-the-art

3. DATASET DESCRIPTION

The dataset used in this study consists of job postings collected from publicly available online recruitment platforms. The dataset includes both legitimate and fraudulent job advertisements to facilitate supervised learning. Each record contains textual attributes such as job title, job description, requirements, company profile, employment type, location, and salary information. The dataset exhibits significant class imbalance, as fraudulent postings represent a smaller proportion compared to legitimate listings. This imbalance can negatively impact model performance by biasing predictions toward the majority class. Since the dataset is text-based and inherently unstructured, it requires extensive preprocessing and transformation into numerical representations suitable for deep learning models. The inclusion of diverse job categories and geographical sources ensures that the model generalizes effectively recruitment scenarios.

4. DATA PREPROCESSING

Data preprocessing is a critical step in preparing textual job postings for deep learning analysis. Initially, the dataset is examined for missing, inconsistent, or duplicate entries, which are appropriately handled to

ensure data integrity. Text cleaning procedures are applied to remove special characters, URLs, HTML tags, punctuation, and irrelevant symbols. Stop words are eliminated to reduce noise, while meaningful tokens are preserved for semantic interpretation. Following text cleaning, tokenization and encoding are performed using transformer based tokenizers to convert textual data into contextual embeddings. These embeddings capture semantic relationships and bidirectional context within job descriptions. Due to the presence of severe class imbalance, a synthetic minority oversampling technique is applied to generate additional samples for the minority fraud class. This balancing process ensures that the model does not become biased toward legitimate postings during training. The processed dataset is then divided into training and testing subsets using an 80:20 split, preserving randomness while preventing data leakage. These preprocessing steps collectively enhance model stability, convergence speed, and predictive accuracy.

5. SYSTEM ARCHITECTURE

The proposed system architecture is designed to provide an efficient and modular framework for detecting online recruitment fraud. The architecture begins with the dataset input layer, where raw job posting data is uploaded into the system. The preprocessing layer performs cleaning, tokenization, embedding generation, and dataset balancing. The feature extraction component utilizes transformer-based embeddings to generate high-dimensional contextual representations of textual data. These embeddings are subsequently passed into a convolutional neural network classifier, which extracts discriminative patterns and performs binary classification to determine whether a job posting is fraudulent or legitimate. The evaluation component compares predicted labels with actual outcomes using standard performance metrics such as accuracy, precision, recall, and F1-score.

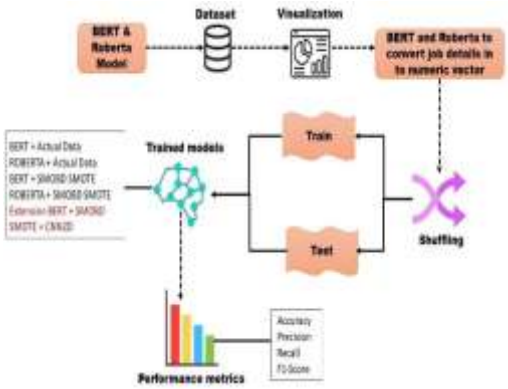

Fig. 1. Proposed system architecture.

6. SOFTWARE REQUIREMENTS

The proposed Online Recruitment Fraud detection system is developed using Python due to its flexibility and strong support for machine learning applications. Libraries such as NumPy and Pandas are used for data preprocessing, while Matplotlib and Seaborn are used for visualization.TensorFlow, and Keras are used to implement transformer-based and deep learning models. Scikit-learn supports dataset splitting, evaluation metrics, and SMOTE-based class balancing. The system interface is deployed using the Flask framework, with SQLite for database management. Development and testing are performed using Anaconda and Jupyter Notebook, and the system is compatible with Windows, Linux, and macOS

7. HARDWARE REQUIREMENTS

The system requires a computer with at least an Intel Core i5 processor, 8 GB RAM (16 GB recommended), and 50 GB storage for datasets and models. Although the system can run on a CPU, a GPU-enabled system is recommended to accelerate training of transformer-based models. A stable operating system such as Windows 10 or later ensures compatibility with required libraries and frameworks.

8. APPLICATION WORKFLOW

The workflow of the proposed Online Recruitment Fraud detection system begins with importing the required libraries for data processing and model development. The system then verifies the execution environment to ensure proper configuration. If verification fails, the process stops; otherwise, it proceeds to the next stage. The dataset containing job postings is loaded and explored to understand its structure and class distribution. Exploratory analysis and visualization techniques are applied to examine patterns and identify class imbalance. The textual job details are then converted into numerical representations using transformer based models such as BERT and RoBERTa, which generate contextual embeddings for classification. After vectorization, the dataset is shuffled to remove ordering bias and divided into training and testing subsets. Multiple deep learning models are built and trained using actual and SMOTE- balanced data, including an extended hybrid model combining contextual embeddings with a CNN2D classifier. Once training is completed, the system allows administrative access for analyzing new job postings. The trained model classifies each posting as legitimate or fraudulent, and the application terminates after logout.

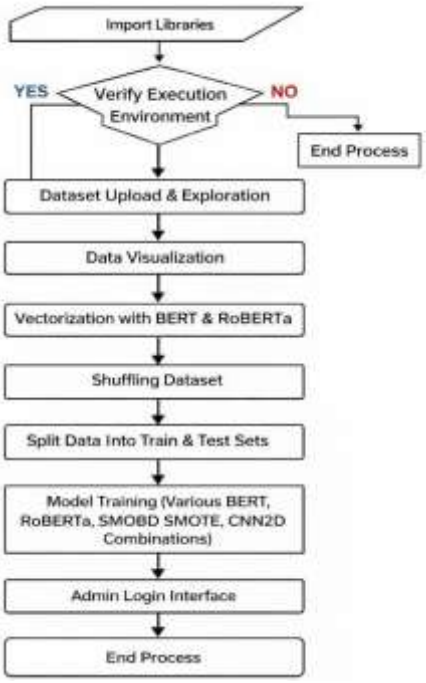

Fig. 2. Workflow of the Fraud Detection System

9. IMPLEMENTATION

The proposed Online Recruitment Fraud detection system is implemented using Python and advanced

deep learning libraries, following a structured and modular design approach to ensure scalability, maintainability, and clarity. The implementation process begins with loading the recruitment dataset and performing comprehensive preprocessing operations to prepare the data for model training. Textual data cleaning is carried out by removing missing values, duplicate records, special characters, hyperlinks, and irrelevant symbols. Stop words are eliminated to reduce noise, while meaningful textual information is preserved for semantic analysis. Exploratory Data Analysis is conducted to examine dataset distribution and identify the imbalance between legitimate and fraudulent job postings. After preprocessing, the textual job descriptions are transformed into contextual numerical representations using transformer-based language models such as BERT and RoBERTa. These models generate high- dimensional embeddings that capture bidirectional semantic relationships within the text. Since the dataset exhibits significant class imbalance, SMOTE based oversampling techniques are applied to synthetically generate additional samples for the minority fraud class. This balancing process ensures that the classification models learn fraud-related patterns effectively without bias toward the majority class. The processed dataset is then shuffled to eliminate ordering bias and divided into training and testing subsets using an appropriate ratio to ensure fair performance evaluation. Multiple deep learning models are implemented under identical experimental conditions. These include BERT trained on actual data, RoBERTa trained on actual data, BERT trained on SMOTE- balanced data, RoBERTa trained on SMOTE- balanced data, and an extended hybrid architecture combining BERT embeddings with a CNN2D classifier. The models are trained iteratively to minimize classification loss and optimize predictive performance. Evaluation metrics such as accuracy, precision, recall, and F1-score are computed to assess model effectiveness. Finally, the best-performing model is integrated into a Flask-based web application that provides a secure admin login interface and enables real-time fraud detection for new job postings.

10. RESULTS AND PERFORMANCE ANALYSIS

The performance of the proposed Online Recruitment Fraud detection system is evaluated using standard classification metrics, including accuracy, precision, recall, and F1 score. All implemented models are trained and tested on the same preprocessed datasets to ensure a fair and consistent comparison. Experimental results indicate that transformer based models significantly outperform traditional machine learning approaches in identifying fraudulent job postings. The models trained on balanced datasets demonstrate improved recall for the minority fraud class, highlighting the effectiveness of SMOTE-based oversampling in addressing class imbalance. Among all implemented architectures, the hybrid model integrating BERT embeddings with a CNN2D classifier achieves the highest overall performance. The model attains an accuracy of 98.68%, with strong precision and recall values, indicating reliable classification capability. Confusion matrix analysis further reveals a reduction in false negatives, which is critical in fraud detection systems where missing fraudulent postings can have serious consequences. Graphical analysis of model performance demonstrates that contextual embeddings extracted from transformer-based architectures capture subtle linguistic patterns commonly used in fraudulent job advertisements. The integration of convolutional layers enhances feature extraction by identifying local semantic patterns within embeddings. Overall, the experimental findings confirm that the proposed deep learning framework provides accurate, stable, and robust fraud detection performance under the evaluated conditions.

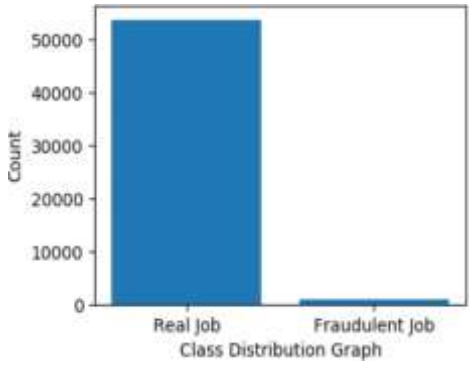

Fig. 3. Class Distribution Graph

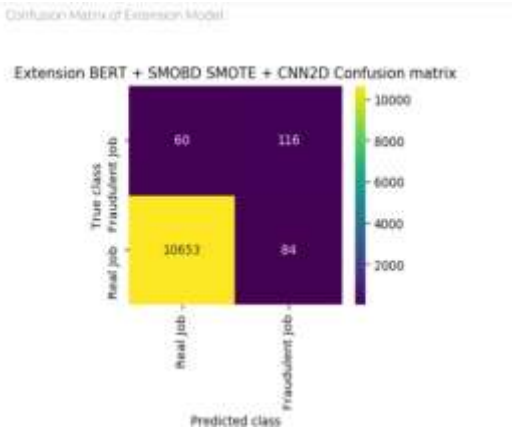

Fig. 4. Confusion Matrix

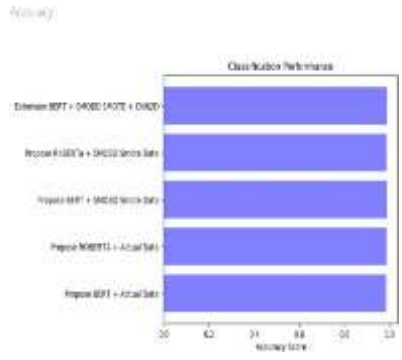

Fig. 5. Accuracy

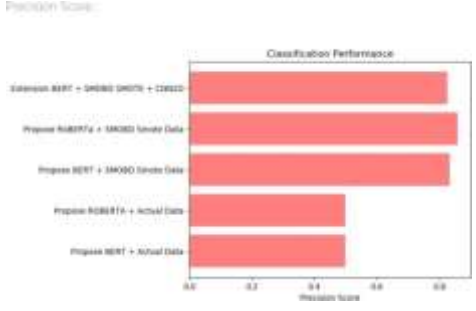

Fig. 6. Precision

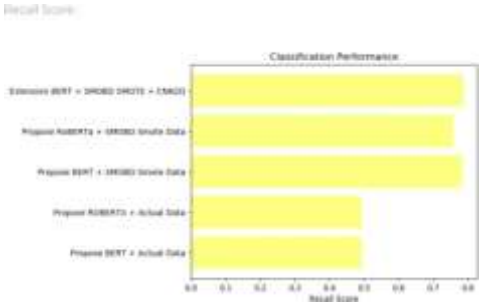

Fig. 7. Recall

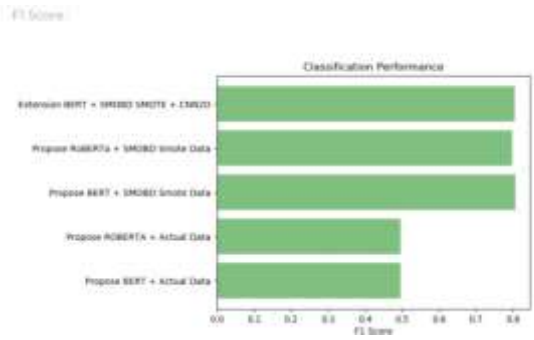

Fig. 8. F1 Score

detection capability. Expanding the system to support multilingual job postings would enable broader applicability across global recruitment platforms. Furthermore, deploying the model on cloud based infrastructure with real-time API integration can improve scalability and accessibility. Continuous retraining with updated datasets will ensure adaptability to evolving fraud strategies and maintain long term system effectiveness. This study presents a comprehensive deep learning–based framework for detecting online recruitment fraud using transformer-based contextual embeddings combined with a CNN classifier. The proposed system effectively processes textual job posting data, addresses class imbalance challenges, and achieves high classification accuracy. Experimental results demonstrate that the hybrid architecture significantly improves fraud detection performance compared to baseline models. Overall, the system provides a reliable, scalable, and intelligent solution for enhancing security in online recruitment environments and protecting job seekers from fraudulent activities. With further advancements and real time deployment, the framework can support large- scale digital recruitment platforms and contribute

MODEL PERFORMANCE COMPARISON

TABLE I

Model	Accuracy
BERT	96.8%
RoBERTa	97.5%
BERT + SMOTE	97.9%
BERT+CNN2D	98.68%

11. FUTURE WORK

Future improvements to the proposed Online Recruitment Fraud detection system may focus on incorporating mechanisms and advanced ensemble attention learning architectures to further enhance classification accuracy. The inclusion of additional metadata features such as recruiter verification status, posting frequency, and behavioral analytics can strengthen fraud to safer employment ecosystems.

12. CONCLUSION

This research presents a transformer-based deep learning framework for detecting online recruitment fraud using advanced natural language processing techniques. The proposed system leverages contextual embeddings generated from BERT and RoBERTa models combined with a CNN2D classifier to effectively analyze textual job posting data. By capturing deep semantic relationships within job descriptions, the system is able to identify subtle patterns that distinguish legitimate job postings from fraudulent ones.A key challenge addressed in this study is the class imbalance present in recruitment datasets, where fraudulent postings occur less frequently than legitimate listings. To overcome this issue, the SMOTE oversampling technique is applied during preprocessing to balance the dataset and improve the learning capability of the models. Experimental results demonstrate that transformer-based architectures significantly outperform traditional machine learning approaches for this task. Among the evaluated models, the hybrid BERT + CNN2D architecture achieved the highest performance, reaching an accuracy of 98.68% along with strong precision, recall, and F1-score values.The integration of deep learning models with contextual language representations enables the system to detect complex linguistic patterns commonly used in fraudulent job advertisements. Additionally, the deployment of the model through a Flask-based web application allows administrators to analyze and classify new job postings in real time, making the system practical for real-world recruitment platforms.Overall, the proposed framework provides an accurate, scalable, and reliable solution for detecting online recruitment fraud. By enhancing automated fraud detection capabilities, this system can help protect job seekers from financial exploitation, identity theft, and misleading employment opportunities while improving the security and trustworthiness of digital recruitment environments.

REFERENCES

1. G. O. Alandjani, “Online fake job advertisement recognition and classification using machine learning,” 3C TIC, Cuadernos de Desarrollo Aplicados a las TIC, vol. 11, no. 1, pp. 251–267, Jun. 2022.

2. A. Adhikari, A. Ram, R. Tang, and J. Lin, "DocBERT: BERT for document classification," arXiv preprint, Apr. 2019.
3. I. M. Nasser, A. H. Alzaanin, and A. Y. Maghari, "Online recruitment fraud detection using ANN," in Proc. Palestinian Int. Conf. Inf. Commun. Technol. (PICICT), Sep. 2021, pp. 13–17.
4. C. Lokku, "Classification of genuinity in job posting using machine learning," Int. J. Res. Appl. Sci. Eng. Technol., vol. 9, no. 12, pp. 1569–1575, Dec. 2021.
5. S. U. Habiba, M. K. Islam, and F. Tasnim, "A comparative study on fake job post prediction using different data mining techniques," in Proc. 2nd Int. Conf. Robot., Electr. Signal Process. Technol. (ICREST), Dhaka, Bangladesh, Jan. 2021, pp. 543–546.
6. V. Itnal, I. Pande, S. Nimkar, et al., "Fake/Real Job Posting Detection Using Machine Learning," Int. J. Research and Analytical Reviews (IJRASER), 2025.
7. K. Taneja et al., "Fraud-BERT: Transformer based context aware online recruitment fraud detection," Discover Computing, 2025.
8. E. Baraneetharan, "Detection of Fake Job Advertisements Using Machine Learning Algorithms," Journal of Artificial Intelligence and Capsule Networks, vol. 3, pp. 200–210, 2022.