



## Online Recruitment Fraud Detection Using Deep Learning Approaches

ivaranjani. D<sup>1</sup>, Sri Harini. G<sup>2</sup>, Sivaranjani. M<sup>3</sup>

<sup>1, 2</sup>Student-Department of computer science and engineering, Paavai Engineering College, Namakkal, India.

<sup>3</sup>Associate professor- Department of Computer Science and Engineering, Paavai Engineering College, Namakkal, India.

**Email ID:** [dharmaraje124@gmail.com](mailto:dharmaraje124@gmail.com)<sup>1</sup>, [sriharini9597@gmail.com](mailto:sriharini9597@gmail.com)<sup>2</sup>, [ranjanimecse@gmail.com](mailto:ranjanimecse@gmail.com)<sup>3</sup>

### Abstract

Online recruitment platforms have become widely used for job searching and hiring processes. However, the increasing popularity of these platforms has also led to a rise in fraudulent job postings that mislead job seekers and cause financial and personal data losses. This paper presents a deep learning-based approach for detecting online recruitment fraud by analyzing job descriptions and related textual information. Advanced natural language processing techniques and deep learning models such as GPT-2, XLNet and Long Short-Term Memory (LSTM) are utilized to classify job postings as genuine or fraudulent. Experimental results show that the proposed system effectively improves detection accuracy and reduces the risk of online recruitment fraud. The proposed framework focuses on extracting meaningful linguistic and contextual features from job advertisement to identify hidden fraud patterns that are difficult to detect using traditional machine learning methods. Text preprocessing, tokenization and embedding techniques are applied to convert unstructured job posting data into numerical representations suitable for deep learning models. By leveraging transformer-based architectures along with sequential neural networks, the system captures both semantic meaning and contextual dependencies present in recruitment content. This enables the model to differentiate subtle differences between legitimate and deceptive job descriptions. Furthermore, the developed fraud detection model contributes to enhancing trust and safety in online recruitment environments by enabling automated screening of job postings at scale. The approach can assist recruitment platforms and regulatory authorities in identifying suspicious listings before they reach potential applicants. The experimental evaluation demonstrates that deep learning-based classification significantly outperforms conventional approaches in terms of precision and recall. The proposed system can be integrated into real-world recruitment platforms to provide early fraud detection, thereby protecting job seekers and improving the reliability of online hiring ecosystems.

**Keywords:** Online Recruitment Fraud, Deep Learning, Natural Language Processing, Fraud Detection, Text Classification, Job Posting Analysis, Machine Learning, Cybersecurity

### 1. Introduction

Online recruitment platforms have transformed the hiring process by enabling organizations and job seekers to connect quickly and efficiently. With the widespread use of digital job portals and social media recruitment channels, candidates can apply for employment opportunities across geographic boundaries. However, the rapid growth of these platforms has also created opportunities for fraudulent actors to exploit job seekers through fake job advertisements and deceptive recruitment practices. Such fraudulent activities not only cause financial losses but also lead to identify theft and psychological distress among victims. Online

recruitment fraud has become a serious cybersecurity concern in recent years. Fraudsters often design job postings that closely resemble legitimate advertisements, making it difficult for individuals to distinguish between genuine and fraudulent opportunities. These deceptive postings may request application fees, personal documents, or sensitive information under the pretense of employment processing. Traditional fraud detection mechanisms, such as manual verification and rule-based filtering, are inadequate for handling the large volume and complexity of online job postings. To address this challenge, automated detection systems based on



artificial intelligence have gained attention. Machine learning and deep learning techniques have demonstrated strong capabilities in analyzing large textual datasets and identifying hidden patterns within unstructured data. In particular, natural language processing methods enable computational models to understand contextual and semantic relationships in job descriptions, which are essential for distinguishing fraudulent content from legitimate postings. These techniques provide scalable and efficient solutions for fraud detection in online recruitment environments. Recent advancements in deep learning architectures, including recurrent neural networks and transformer-based models, have significantly improved text classification performance. Models such as Long Short-Term Memory (LSTM), GPT-based architectures, and XLNet can capture contextual dependencies and linguistic nuances present in job advertisements. By learning complex language patterns associated with fraudulent postings, these models can enhance detection accuracy compared to conventional machine learning approaches. This paper proposes a deep learning-based framework for detecting online recruitment fraud using textual features extracted from job postings. The proposed system applies natural language processing techniques and advanced deep learning models to classify recruitment advertisements as genuine or fraudulent. The objective of this study is to improve fraud detection accuracy, reduce false classifications and provide a scalable automated solutions for securing online recruitment platforms. The increasing availability of online recruitment data and advancements in computational resources have enabled the development of intelligent fraud detection systems that operate in real time. Automated screening of job advertisements using deep learning models can significantly reduce the reliance on manual verification processes and improve detection speed. Such systems are capable of continuously learning from new data, adapting to evolving fraud patterns, and enhancing detection robustness over time. This capability is essential in modern recruitment ecosystems, where fraudulent techniques frequently change to bypass conventional filtering methods.

Furthermore, integrating deep learning-based fraud detection into online recruitment platforms can improve user trust and platform credibility. Early identification of fraudulent postings protects job seekers from potential exploitation and helps organizations maintain a secure hiring environment. By providing accurate and scalable fraud classification, the proposed framework contributes to strengthening cybersecurity measures in digital recruitment systems. Consequently, the adoption of intelligent detection models can support safer online employment processes and promote confidence in digital hiring technologies. Despite the progress achieved through deep learning-based classification, detecting online recruitment fraud remains challenging due to the dynamic and adaptive nature of fraudulent content. Fraudsters continuously modify linguistic patterns, job structures, and presentation styles to resemble legitimate postings and evade automated detection mechanisms. This evolving behavior necessitates robust models capable of generalizing across diverse textual variations and maintaining performance over unseen data. Therefore, incorporating contextual feature learning and semantic representation techniques becomes essential for improving the resilience and reliability of recruitment fraud detection systems. Consequently, developing a scalable and adaptive fraud detection framework is crucial for sustaining secure digital recruitment environments. By leveraging deep learning architecture that capture contextual semantics and long-range textual dependencies, the proposed approach aims to address the limitations of conventional detection methods. The integration of such intelligent models within recruitment platforms can enable continuous monitoring of job postings and timely identification of suspicious content. This progression from problem recognition to intelligent automated detection underscores the significance of deep learning in strengthening cybersecurity within online recruitment ecosystems.

## **2. Related Works**

The problem of online recruitment fraud detection has gained increasing research attention due to the rapid growth of digital hiring platforms and the



associated rise in deceptive job postings. Early studies primarily relied on traditional machine learning techniques such as Naïve Bayes, Decision Trees, and Support Vector Machines to classify job advertisements based on manually engineered textual features. These approaches utilized keyword frequency, metadata attributes and statistical patterns to differentiate fraudulent postings from legitimate ones. Although such models provided baseline detection capability, their performance was limited by their inability to capture contextual semantics and complex linguistic structures present in recruitment content. Subsequent research focused on improving fraud detection accuracy through enhanced feature extraction and natural language processing techniques. Methods such as term frequency-inverse document frequency (TF-IDF), n-gram analysis, and syntactic feature modeling were incorporated to represent textual information more effectively. These techniques improved classification performance compared to simple keyword-based methods; however, they still relied heavily on handcrafted features and lacked adaptability to evolving fraud patterns. As fraudulent job postings became more sophisticated in their language and structure, the limitations of traditional feature-based models became increasingly evident. With the advancement of deep learning, researchers began applying neural network architectures to textual fraud detection tasks. Recurrent neural networks (RNN) and Long Short-Term Memory (LSTM) models demonstrated improved capability in capturing sequential dependencies and contextual sequential dependencies and contextual relationships within job descriptions. These models enabled automated feature learning directly from textual data, reducing reliance on manual feature engineering. Studies reported that LSTM-based approaches significantly enhanced detection accuracy and recall compared to classical machine learning algorithms in recruitment fraud classification tasks. More recent studies have explored transformer-based architecture and pre-trained language models for recruitment fraud detection. Models such as GPT-based architecture, BERT, and XLNet have shown superior performance in text classification due to their ability to learn deep

contextual representations and bidirectional language dependencies. These models effectively identify subtle linguistic cues and semantic inconsistencies commonly found in fraudulent job postings. Experimental comparisons in existing literature indicate that transformer-based approaches outperform both traditional machine learning and earlier deep learning models in fraud detection scenarios involving complex textual datasets. In addition to textual analysis, some research has incorporated hybrid detection frameworks combining textual features with metadata attributes such as company information, salary patterns and posting behavior. These multimodal approaches aim to improve robustness by analyzing both linguistic and structural characteristics of recruitment advertisements. While such methods demonstrate improved detection reliability, they often require extensive feature integration and domain-specific preprocessing, which may limit scalability across diverse recruitment platforms. Despite significant advancements, existing research still faces challenges related to dataset imbalance, evolving fraud strategies, and model generalization across different recruitment domains. Many models are trained on limited datasets that may not fully represent real-world recruitment variability. Consequently, maintaining consistent detection accuracy across unseen job postings remains a key research concern. These limitations highlight the need for adaptive deep learning frameworks capable of learning robust semantic representations and maintaining performance under dynamic fraud conditions. Based on the insights from prior studies, the present work proposes a deep learning-based recruitment fraud detection framework that leverages advanced natural language processing and contextual representation learning. By integrating transformer-based and sequence-based deep learning models, the proposed approach aims to improve classification accuracy, reduce false detections, and enhance scalability for real-world online recruitment environments. Another research direction in recruitment fraud detection involves the use of ensemble and hybrid deep learning frameworks to improve classification robustness. Ensemble models combine predictions



from multiple classifiers such as convolutional neural networks, recurrent neural networks, and transformer-based architectures can capture both local textual patterns and long-range contextual dependencies present in job postings. This integrated learning strategy enhances detection stability and reduces misclassification caused by ambiguous recruitment language. However, ensemble approaches often introduce increased computational complexity and training cost, which may limit their deployment in large-scale recruitment platforms. Furthermore, recent investigations have explored explainable artificial intelligence techniques for fraud detection to improve model transparency and interpretability. In recruitment environments, understanding why a job posting is classified as fraudulent is important for platform administrators and users. Explainable models analyze influential textual features and semantic cues contributing to classification decisions, thereby supporting trust in automated detection systems. Although explainability enhances usability and regulatory compliance, balancing interpretability with high detection accuracy remains an open research challenge. These considerations emphasize the importance of developing deep learning-based recruitment fraud detection systems that are not only accurate and scalable but also interpretable and practical real-world deployment.

### **3. Literature Review**

The detection of fraudulent activities in online recruitment platforms has become an important research area due to the increasing prevalence of deceptive job postings on digital employment portals. Early studies on recruitment fraud detection primarily utilized traditional machine learning algorithms such as Naïve Bayes, Decision Trees, and Support Vector Machines[3]. These approaches relied on manually engineered textual features, including keyword frequency, lexical patterns, and metadata attributes extracted from job advertisements. Although these methods provided baseline classification capability, their effectiveness was limited by their dependence on shallow feature representations and inability to capture contextual meaning in recruitment content. To enhance textual representation, subsequent

research incorporated natural language processing techniques such as term frequency-inverse document frequency (TF-IDF), n-gram modeling and syntactic feature extraction. These approaches improved classification performance by representing recruitment text more effectively than simple keyword matching. However, they still depended on handcrafted feature engineering and lacked adaptability to evolving fraud patterns. As fraudulent job postings became increasingly sophisticated in language and presentation, the limitations of feature-based models became more evident, particularly in detecting subtle semantic inconsistencies within job descriptions. With advancements in deep learning, researchers began exploring neural network-based models for automated recruitment fraud detection. Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) architectures demonstrated improved capability in capturing sequential dependencies and contextual relationships within textual data. By automatically learning features from job descriptions, LSTM-based approaches reduced reliance on manual feature extraction and improved detection accuracy compared to traditional classifiers. Several studies reported significant improvements in recall and precision when applying LSTM models to recruitment fraud classification tasks. More recently, transformer-based language models have emerged as state-of-the-art approaches for text classification and fraud detection. Architectures such as GPT-based models, BERT, XLNet learn deep contextual semantic representations through attention mechanisms and bidirectional language modeling. These models effectively identify subtle linguistic cues, semantic anomalies and contextual inconsistencies that often characterize fraudulent job postings[2]. Comparative studies in existing literature indicate that transformer-based approaches outperform both conventional machine learning and earlier deep learning methods in detecting complex textual fraud patterns within recruitment datasets.

### **4. Problem Statement**

The rapid growth of online recruitment platforms has significantly increased the volume of job advertisements published across digital



environments. While these platforms provide convenient access to employment opportunities, they have also become attractive channels for fraudulent actors to disseminate deceptive job postings. Online recruitment fraud involves the creation of fake job advertisements intended to mislead applicants, extract sensitive personal information, or obtain financial payments under false recruitment claims. The presence of such fraudulent postings undermines the credibility of recruitment platforms and exposes job seekers to substantial risks, including identifying theft, financial loss and exploitation. Detecting fraudulent job postings within large-scale recruitment datasets presents a complex and challenging task. Fraudulent advertisements are often deliberately designed to closely resemble legitimate job postings in structure, language and presentation. They may contain realistic job titles, company descriptions and requirements, making manual verification difficult and time-consuming[1]. Additionally, fraudsters continuously modify linguistic patterns and content strategies to evade detection, resulting in dynamic and evolving fraud characteristics. This variability reduces the effectiveness of conventional rule-based and keyword-driven detection systems. Existing automated fraud detection approaches based on traditional machine techniques rely heavily on handcrafted textual features and shallow statistical representations. Such methods are limited in their ability to capture contextual semantics, long-range dependencies and subtle linguistic anomalies present in recruitment content. Consequently, these approaches often produce higher false positives and false negatives, reducing detection reliability. Furthermore, many existing models lack scalability and adaptability when applied to diverse recruitment platforms and unseen job postings. Another major challenge in recruitment fraud detection is the imbalance and heterogeneity of available datasets. Genuine job postings significantly outnumber fraudulent ones, creating class imbalance that negatively affects classification performance. Moreover, recruitment data varies across industries, geographic regions, and job categories, requiring models to generalize across heterogeneous textual distributions. Many existing detection systems are

trained on limited datasets and therefore struggle to maintain accuracy when deployed in real-world environments with evolving fraud patterns. Therefore, there is a critical need for an intelligent, scalable and adaptive detection framework capable of accurately distinguishing fraudulent job advertisements from legitimate postings using textual information. Such a system should automatically learn contextual and semantic features from recruitment content, remain robust against evolving fraud strategies and perform effectively across diverse recruitment domains[4]. Addressing these challenges motivates the development of a deep learning-based online recruitment fraud detection approach that leverages advanced natural language processing and contextual representation learning to improve detection accuracy and reliability Figure 1.

## **5. Proposed System**

The proposed system presents a deep learning-based framework for automatically detecting fraudulent job postings in online recruitment platforms. The primary objectives of the system is to accurately classify recruitment advertisements as genuine or fraudulent by analyzing textual content and contextual information present in job descriptions. Unlike traditional rule-based or feature-engineered detection methods, the proposed approach leverages advanced natural language processing and deep learning techniques to learn semantic and contextual representations directly from recruitment data. This enables the system to identify subtle linguistic patterns and anomalies associated with fraudulent postings[5]. The overall architecture of the proposed system consists of multiple stages, including data acquisition, preprocessing, feature representation, deep learning-based classification and fraud prediction. Initially, recruitment data is collected from publicly available job posting datasets containing labeled examples of genuine and fraudulent advertisements. The collected data includes attributes such as job title, company profile, job description, requirements and employment details. This diverse textual information provides a comprehensive basis for training deep learning models to capture fraud-related patterns across different recruitment domains. In the processing

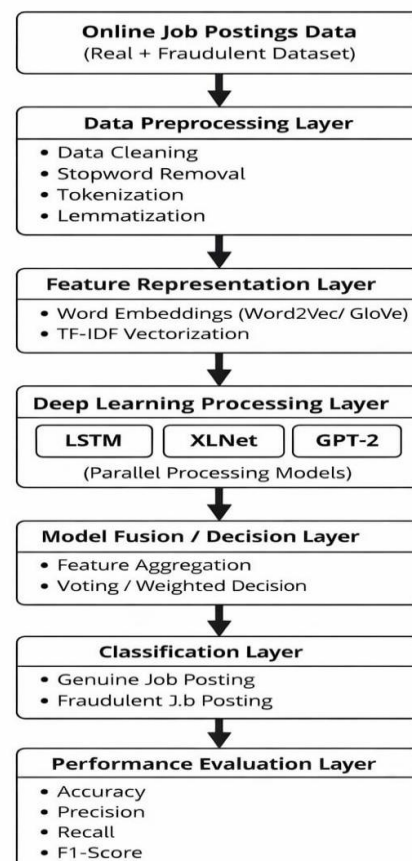
stage, raw recruitment text undergoes cleaning and normalization to remove noise and irrelevant information. This includes eliminating special character, stop words, duplicate entries and incomplete records. Tokenization and text standardization are then applied to convert textual content into structured sequences suitable for computational analysis. To enhance semantic representation, techniques such as word embedding or contextual encoding are employed to transform textual data into numerical feature vectors that preserve linguistic meaning and contextual relationships.

## 6. Dataset Description

The performance of the proposed online recruitment fraud detection system is evaluated using a labeled dataset of job advertisements collected from publicly available online recruitment sources. The dataset contains both genuine and fraudulent job postings, enabling supervised training and evaluation of deep learning models. Each job advertisement entry includes multiple textual and categorical attributes such as job title, company profile, job description, required qualifications, employment type, location, salary information and recruitment requirements. These attributes provide rich contextual information necessary for distinguishing legitimate recruitment postings from deceptive ones. The dataset exhibits characteristics typical of real-world recruitment environments, including diversity in job domains, organizational types and employment conditions. Genuine postings represent legitimate employment opportunities across industries such as information technology, healthcare, finance and administrative services. Fraudulent postings, on the other hand, often contain misleading or exaggerated claims, incomplete company details, unrealistic salary offers or requests for upfront payments. The presence of such heterogeneous textual patterns enables the deep learning models to learn semantic differences between authentic and deceptive recruitment content. Before model training, the dataset undergoes preprocessing to ensure data quality and consistency. Missing values, duplicate entries, and incomplete job advertisements are removed to prevent bias in classification. Textual attributes are cleaned by

eliminating special characters, irrelevant symbols and formatting inconsistencies. Stop-word removal and tokenization are applied to standardize textual sequences. This preprocessing stage ensures that the dataset accurately represents meaningful recruitment information while reducing noise that could negatively affect model performance. An important characteristic of recruitment fraud datasets is class imbalance, where genuine job postings significantly outnumber fraudulent ones. Such imbalance can bias models toward predicting the majority class. To address this issues, techniques such as balanced sampling or class weighting may be applied during training to ensure fair learning across both categories. Maintaining balanced representation helps improve detection accuracy for fraudulent postings, which are typically less frequent but more critical to identify.

## 7. System Architecture



**Figure 1** System Architecture of Online Recruitment Fraud Detection Using Deep Learning Models



## 8. Results And Discussion

The performance of the proposed online recruitment fraud detection system was evaluated using labeled recruitment datasets containing both genuine and fraudulent job postings. The dataset was divided into training and testing subsets to assess the generalization capability of the deep learning models. The training data was used to learn semantic patterns associated with recruitment fraud, while the testing data evaluated classification accuracy on unseen job postings. Standard evaluation metrics such as accuracy, precision, recall and F1-score were employed to measure detection effectiveness. To analyze classification performance, the proposed deep learning framework was compared with conventional machine learning approaches commonly used in recruitment fraud detection. Traditional classifiers such as Support Vector Machines (SVM) and Naïve Bayes served as baseline models. Experimental results indicate that the proposed deep learning models significantly outperform traditional methods in detecting fraudulent job advertisements. This improvement is attributed to the ability of deep learning architectures to capture contextual semantics and linguistic dependencies within recruitment text. To analyze classification performance, the proposed deep learning framework was compared with conventional machine learning approaches commonly used in recruitment fraud detection. Traditional classifiers such as Support Vector Machine (SVM) and Naïve Bayes served as baseline models. Experimental results indicate that the proposed deep learning models significantly outperform traditional methods in detecting fraudulent job advertisements[6]. This improvement is attributed to the ability of deep learning architectures to capture contextual semantics and linguistic dependencies within recruitment text. The Long Short-Term Memory (LSTM) model demonstrated strong capability in identifying sequential linguistic patterns associated with fraudulent postings. It effectively captured contextual flow and semantic inconsistencies present in job descriptions. However, transformer-based architectures achieved superior performance due to their attention mechanisms and bidirectional

contextual representation learning. These models identified subtle anomalies such as unrealistic claims, missing organizational information and deceptive recruitment language more accurately than sequence-only models. Quantitative evaluation results showed that the transformer-based deep learning model achieved the highest detection accuracy and F1-score among all evaluated approaches. The model also demonstrated improved recall, indicating effective identification of fraudulent postings without overlooking suspicious advertisements. Reduced false positives were observed compared to traditional machine learning methods, highlighting the reliability of contextual deep learning representations in recruitment fraud classification tasks. The experimental analysis also examined the robustness of the proposed system across diverse recruitment categories and textual variations. The model maintained stable performance across different job domains and posting styles, indicating strong generalization capability.

## Conclusion

In this research, the problem of ORF detection is analyzed thoroughly. This paper presented a novel dataset of fake job postings. The proposed data is a combination of job postings from three different sources. Upon conducting EDA, it was discovered that the class distribution within the collected dataset was highly imbalanced. To rectify this class distribution imbalance, the top ten highly effective SMOTE variants were implemented on the imbalanced data. Subsequently, a type error analysis was conducted to investigate the impact of employing SMOTE variants on predictive models. Transformer-based classification models, BERT and RoBERTa, were implemented on both the imbalanced and balanced data, and the results were compared to derive more comprehensive insights from the experiments. Diverse evaluation metrics were employed to compare the performance of the implemented techniques. Due to the class imbalance issue, only accuracy as an evaluation metric failed to provide an accurate representation of the overall performance. Because high predictive accuracy for the majority class can be misleading, as it may overshadow the minority class, leading to incomplete



assessment. Thus, this study prioritized enhancing balanced accuracy and recall as evaluation metrics. All implemented approaches exhibited commendable performance. However, based on the type error and classification results, it was observed that BERT, in conjunction with the SMOBD SMOTE technique, demonstrated exceptional performance on our data and achieved optimal outcomes. The experiments performed in this research can provide valuable directions to job-seekers and reputed organizations to better understand fact-based insights about employment scam and their effects on society. Consequently, people would not fall into the trap of employment scams anymore. By distinguishing ORF, the people who were wasting their time and money on those fraudulent activities can be vigilant now. Conventional fraud detection without considering class imbalance problems can lead to misleading conclusions for both job-seekers and organizations. To get a true set of results, it is necessary to handle this problem as well. In this research, we extensively improved the system's performance and gained valuable results based on balanced data; still, it has many gaps that can be covered in the future. All sets of analyses are performed on the job postings advertised in the English language only. In the present research, a range of SMOTE variants were employed to address class distribution imbalance. To attain even more precise results, the utilization of hybrid oversampling techniques can be considered. For future research, explainable AI and novel transformer based hybrid models need to be explored.

#### Reference

- [1]. P. Kaur, "E-recruitment: A conceptual study," *Int. J. Appl. Res.*, vol. 1, no. 8, pp. 78-82, 2015.
- [2]. J. Howington, "Survey: More millennials than seniors victims of job scams," *Flexjobs*, CO, USA, Sep. 2015. Accessed: Jan. 2024 [Online]. Available: [www.flexjobs.com/blog/post/survey-results-millennials-seniors-victims-job-scams](http://www.flexjobs.com/blog/post/survey-results-millennials-seniors-victims-job-scams).
- [3]. S.Bansal, "[real or fake]fake jobposting prediction," *Kaggle*, 2020.
- [4]. A. Adhikari, A. Ram, R Tang, and J.Lin, "Docbert: Bert for document classification,"

arXiv preprint arXiv:1904.08398, 2019.

- [5]. Y. Hu, J. Ding, Z. Dou, and H. Chang, "Short-text classification detector: A bert-based mental approach," *Computational intelligence and Neuro-science*, vol. 2022, 2022.
- [6]. I. M. Nasser, A. H. Alzaanin, and A. Y. Maghari, "Online recruitment fraud detection using ann," in *2021 Palestinian International Conference on Information and Communication Technology (PICICT)*, IEEE, 2021, pp.13.