

Transformer-Based Hybrid Machine Learning System for Detecting Fake Job Postings on LinkedIn

Akanksha Gavhane¹, Manisha Bharambe², Yogeshri Gaidhani³

¹Student, Department of Computer Science, M.E.S' Abasaheb Garware College, Pune, INDIA.

²Professor, Department of Computer Science, M.E.S' Abasaheb Garware College, Pune, INDIA

³Associate Professor, Department of Computer Science, M.E.S' Abasaheb Garware College, Pune, INDIA

Abstract - The rapid expansion of online recruitment platforms, particularly LinkedIn, has significantly increased employment opportunities while simultaneously giving rise to fraudulent job postings. These fraudulent posts often use misleading tactics such as vague or exaggerated keywords like "DM me," "comment interested," "urgent hiring," and "work from home", redirecting applicants to Google Forms, WhatsApp groups, or anonymous sites instead of official application portals. The absence of verified company information, job descriptions, salary, and location, unrealistic salary offers such as large pay scales for interns, and unauthorized recruitment processes such as use of fake posters, demand of application fees, or fake HR engagement may not only waste applicants' time but also expose them to financial and identity theft risks. To address this issue, this research proposes a fraud detection system that utilizes Machine Learning and Natural Language Processing techniques to automatically identify fraudulent job postings. Transformer-based embeddings are used for extracting contextual text features to capture semantic meanings in the post, and classification models such as Logistic Regression, Random Forest and XGBoost are applied to distinguish between legitimate and fake job listings. Along with this, structured metadata features and fraud keyword indicators are used to enhance detection capability. The Synthetic Minority Oversampling Technique (SMOTE) is applied during model training to address class imbalance. The proposed system aims to improve fake job detection accuracy and contribute to a more secure and trustworthy online recruitment environments.

Key Words: Fake Job Detection, LinkedIn, Fraud Detection, Machine Learning, Natural Language Processing, Transformer Embeddings, XGBoost, SMOTE, Contextual NLP

1. INTRODUCTION

Online recruitment platforms have transformed the job search process by providing easy accessibility to employment opportunities. LinkedIn alone hosts millions of job postings worldwide. With over 14 million job postings uploaded monthly on LinkedIn, identifying fraudulent job postings manually has become difficult. Job seekers on LinkedIn often face various forms of recruitment fraud. Common issues include fake job engagements claiming to

represent multinational companies, where unauthorized individuals pose as HR representatives. Fraudulent postings sometimes use images of corporate employees, particularly female professionals, to attract attention and build false credibility. Additionally, scammers frequently promote fake remote job opportunities offering unrealistically high salaries, especially targeting fresh graduates and entry-level candidates.

Many fraudulent recruiters direct applicants to join WhatsApp groups, fill anonymous online forms, or pay hiring and documentation fees. These postings often lack official company career portal links and instead encourage job seekers to like or comment with phrases such as "Interested" to increase engagement. Other suspicious indicators include missing salary details, unclear job locations, absence of company's online presence, and misleading statements such as "Interview is manageable, charges applied", "DM me", "work from home earn", "no experience needed" or "Limited period offer." Fraudsters also commonly use urgency-based marketing phrases like "Urgent hiring," "Follow this page," or "Closing applications soon" to pressure candidates into quick responses. These deceptive practices highlight the growing need for automated detection systems capable of identifying suspicious job postings and protecting job seekers from recruitment fraud.

Sathwika et al. [7] proposed a Machine Learning-based approach for detecting fake job postings using classification techniques such as Random Forest, Support Vector Machine, and Logistic Regression, demonstrating improved detection accuracy. Similarly, Deka et al. [3] conducted a comprehensive review of Machine Learning techniques for identifying fraudulent job advertisements and emphasized the importance of feature engineering and NLP-based analysis in improving classification performance. Machine learning approaches have shown promising results in detecting recruitment fraud by identifying hidden patterns within job posting data. Dutta and Bandyopadhyay [8] developed a classification-based detection framework using multiple Machine learning algorithms and reported that ensemble-based models provide better prediction accuracy compared to individual classifiers. Furthermore, recent research by Vrinda et al. [12] introduced a deep learning-based fake job detection model using advanced NLP techniques, highlighting the effectiveness of transformer-based language models in identifying suspicious textual

patterns in job advertisements. Apart from classification algorithms, several studies have focused on improving fraud detection models using data augmentation and advanced analytical techniques. Anderson et al. [2] emphasized the importance of synthetic data generation for enhancing fraud detection models when labelled datasets are limited. Similarly, Johnson and Lee [4] demonstrated that decision tree-based and hybrid Machine Learning models improve classification accuracy by capturing complex feature relationships. Additionally, Kumar and Patel [5] highlighted the necessity of integrating intelligent security mechanisms into web-based recruitment platforms to prevent fraudulent activities and improve trust in online job portals.

Based on the review of existing literature, it is seen that most studies focus on general fraud detection such as spam emails, phishing websites, and fraudulent e-commerce listings, while fake job postings on professional platforms like LinkedIn remain underexplored. These systems heavily rely on user awareness rather than automated detection. Keyword-based fake company pages, and engagement tricks. There is no comprehensive system that integrates linguistic analysis, metadata verification, and fraud indicators specifically for detecting fake job postings. Therefore, this research aims to develop an integrated fake job detection system that combines NLP preprocessing, hybrid feature engineering, and multiple supervised Machine Learning algorithms to improve detection accuracy and real-world applicability.

NLP techniques can be used to preprocess job descriptions, extract meaningful features, and identify suspicious linguistic patterns commonly associated with fraudulent postings. These extracted features can then be used by Machine Learning classification algorithms to detect fraudulent job advertisements with improved accuracy and efficiency. Multiple supervised Machine Learning algorithms, including Logistic Regression, Random Forest, and Extreme Gradient Boosting (XGBoost), are implemented to analyze job posting patterns and classify them into genuine or fraudulent categories. The performance of these models is evaluated using standard evaluation metrics such as accuracy, precision, recall, F1-score, confusion matrix, and ROC-AUC analysis.

2. PROPOSED METHODOLOGY

The dataset used in this study is the *Real or Fake Job Posting Prediction Dataset* available on Kaggle, which contains job postings labelled as fraudulent or genuine along with various textual and metadata features such as job title, description, company profile, location, and salary information. The dataset contains 17,880 rows and 20 columns with 17,014 jobs labelled as genuine and 866 jobs as fake. The proposed system utilizes Natural Language Processing (NLP) techniques along with Machine Learning classification models to detect and classify fake job postings. Transformer-based contextual embeddings using

SentenceTransformer are applied to extract semantic features from job posting text. In addition, fraud keyword-based features and structured metadata attributes such as company logo presence, employment type, and experience requirements are combined to enhance fraud detection capability. The Synthetic Minority Oversampling Technique (SMOTE) is applied to address class imbalance, and multiple Machine Learning algorithms are then implemented to classify job postings as genuine or fraudulent. The performance of these models is evaluated using standard evaluation metrics to determine the most effective model for accurate fake job detection.

2.1 Models Used:

[A] Random Forest Classification

Random Forest is a classification algorithm used in supervised Machine Learning for categorizing data into different classes. The algorithm uses multiple decision trees, forming a “forest” of decision trees. It improves the performance of a model by combining multiple classifiers to solve complex problems. Random Forest is based on the concept of ensemble learning, as it does not rely on a single decision tree. Instead, it predicts the final output based on the majority voting of predictions obtained from each tree. It achieves this by using techniques such as bagging and bootstrap sampling. Random Forest includes several important hyperparameters such as *n_estimators*, *max_depth*, *max_features*, *max_samples*, *min_samples_split*, *max_leaf_nodes*, and *bootstrap*. Techniques such as GridSearchCV and RandomizedSearchCV can be used to tune these hyperparameters to improve model performance. Random Forest has been widely used in fraud detection and classification problems due to its ability to handle high-dimensional data and complex feature interactions [6].

[B] XGBoost Classification

XGBoost (Extreme Gradient Boosting) is a supervised Machine Learning classification algorithm widely used for solving complex classification and regression problems. It is an advanced implementation of gradient boosting that improves model accuracy and efficiency by combining multiple weak learners, typically decision trees. XGBoost works by building decision trees sequentially, where each new tree focuses on correcting the errors made by the previous trees. Instead of giving equal importance to all trees, it assigns weights to reduce prediction errors and improve overall performance. The algorithm uses gradient descent optimization to minimize the loss function and enhance prediction accuracy. It also includes regularization techniques that help prevent overfitting and improve model generalization.

XGBoost provides several hyperparameters such as *n_estimators*, *learning_rate*, *max_depth*, *subsample*, *colsample_bytree*, *gamma*, and *reg_lambda*, which control

tree complexity and learning behaviour. Due to its computational efficiency and high predictive performance, XGBoost has been successfully applied in classification and fraud detection studies [12].

[C] SMOTE

SMOTE is a popular technique used to handle class imbalance in a dataset where one class outshines other leading to bias in the result. To improve the performance of the model and reduce the bias, it creates synthetic samples for minority class.

[D] Sentence Transformer

Sentence Transformer is a transformer-based Natural Language Processing (NLP) technique used to capture the contextual meaning of text. Unlike traditional methods such as TF-IDF, which focus on word frequency, Sentence Transformer converts job posting text into embeddings that represent semantic relationships between words and sentences. In this research, the SentenceTransformer model ('all-MiniLM-L6-v2') is used to generate contextual embeddings from job postings. These embeddings help detect hidden fraud patterns, misleading phrases, and suspicious recruitment language. The generated embeddings are combined with metadata and fraud keyword features to improve the accuracy of fake job detection.

[E] AUC-ROC

Area Under the Receiver Operating Characteristic Curve (AUC-ROC) is a performance metric used to evaluate the performance of classification models using various thresholds. The ROC curve is used to show the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) using a graphical plot with a diagonal line (AUC = 0.5) representing a random classifier. AUC ranges from 0 to 1. A curve closer to the top-left corner indicates better performance. Irjet Template sample paragraph .Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

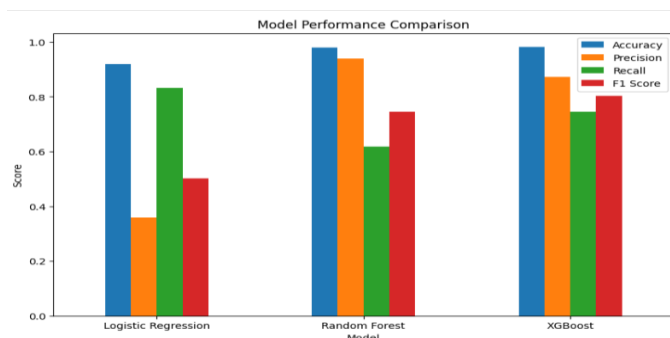


Chart -1: Model Performance Comparison chart

Table -1: Model Evaluation

	Model	Accuracy	Precision	Recall	F1 Score	ROC-AUC
0	Logistic Regression	0.919743	0.358209	0.832370	0.500870	0.947770
1	Random Forest	0.979586	0.938596	0.618497	0.745645	0.979739
2	XGBoost	0.982383	0.871622	0.745665	0.803738	0.975231

As shown in Figures, XGBoost achieved the highest overall performance with the best F1-score and recall, indicating highest capability in identifying fraudulent job postings. While Logistic Regression achieved perfect precision, its recall value was significantly lower, suggesting that it failed to detect a large number of fraudulent cases. Random Forest showed balanced performance but was slightly outperformed by XGBoost in terms of recall and F1-score. Therefore, XGBoost was selected as the most effective model for fake job detection.

2.2 System Architecture

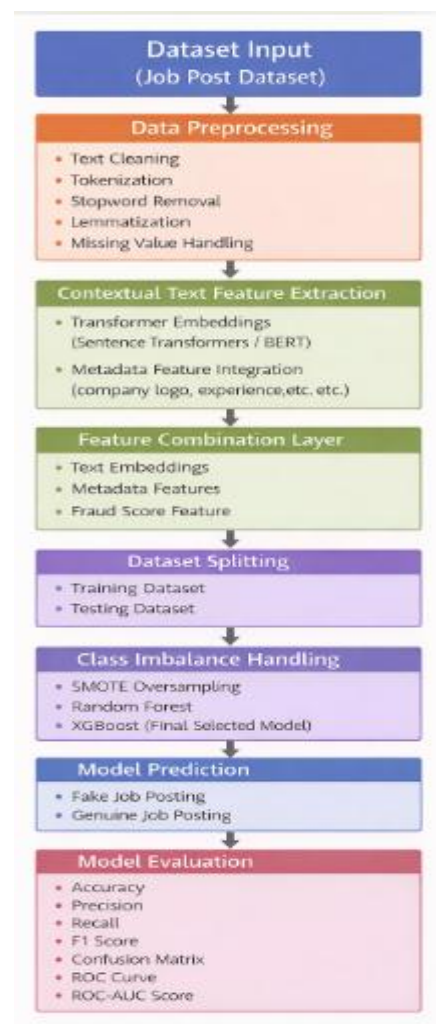


Fig. 1 : System Architecture

The proposed system architecture includes multiple stages such as data preprocessing, transformer-based contextual feature extraction, fraud keyword detection, metadata feature integration, feature combination, class imbalance handling using SMOTE, and Machine Learning classification.

2.3 Result

The performance of the proposed fake job detection system was evaluated using multiple supervised Machine Learning algorithms. The classification results were analyzed using evaluation metrics such as accuracy, precision, recall, and F1-score to determine the effectiveness of the models in identifying fraudulent job postings.

	precision	recall	f1-score	support
0	0.99	0.99	0.99	3403
1	0.87	0.75	0.80	173
accuracy			0.98	3576
macro avg	0.93	0.87	0.90	3576
weighted avg	0.98	0.98	0.98	3576

Fig. 2- Classification Report

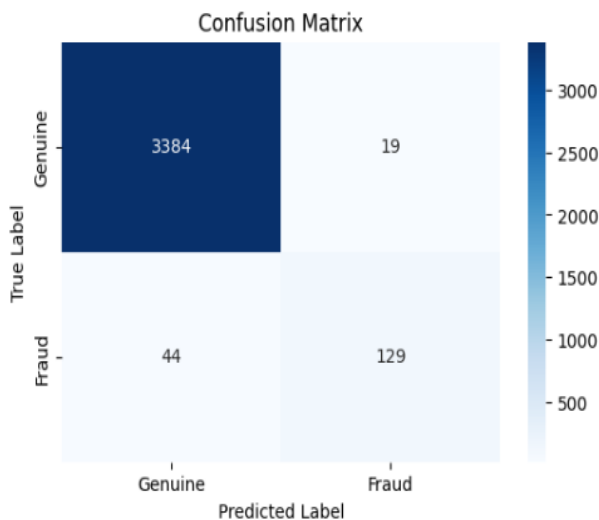


Fig. 3 – Confusion Matrix

From Fig 5, It is seen that the majority of fraudulent and genuine job postings were correctly classified, and the model achieved an overall accuracy of 98%.

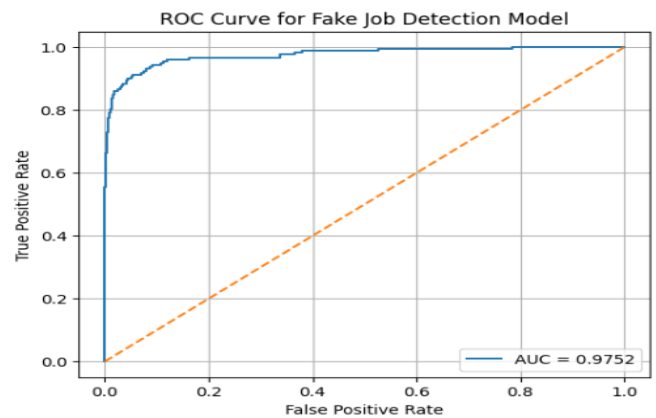


Fig. 4 – ROC-AUC Curve

3. CONCLUSIONS

This research demonstrates that Machine Learning, combined with NLP-based text analysis, can accurately classify fake and genuine LinkedIn job postings. Parameters such as salary range, location, job description, company profile completeness, and job description patterns play a crucial role in fake job post detection. By analyzing a large dataset and applying statistical tests (ANOVA, Chi-square, and t-tests), it was confirmed that certain features significantly differentiate fake from real jobs. This work contributes to improving online job safety and can support LinkedIn and similar platforms in flagging fake jobs. Future improvements may include expanding the model to handle multilingual postings, integrating real-time web scraping APIs, and improving model generalization with deep learning techniques.

REFERENCES

- [1] Amrutha P, Kavya H. V, "Fake Job Detection", Zhuzao/Foundry Journal, Vol. 28, Issue 8, pp. 232–240, 2024.
- [2] Anderson, L., Brown, D., & Harris, M. (2022). "Synthetic Data Generation for Fraud Detection in Marketing Analytics." IEEE Transactions on Big Data (TBD), ISSN 2332-7790, Vol. 8(4), pp. 1125–1138.
- [3] Dipjyoti Deka, Rituparna Seal, Shubham Banik, "Unmasking Fraudulent Job Ads: A Critical Review of Machine Learning Techniques for Detecting Fake Jobs", International Journal on Emerging Research Areas (IJERA), Vol. 3, Issue 1, pp. 59–62, 2023.
- [4] Johnson, R., & Lee, C. (2023). "Comparative Analysis of Decision Tree Algorithms for Fraudulent Pattern Detection." Proceedings of the IEEE International Conference on Data Mining (ICDM), ISSN 1550-4786, Vol. 3, pp. 221–229.

- [5] Kumar, P., & Patel, R. (2021). "Modern Web Application Security and Fraudulent Activity Detection." IEEE Transactions on Dependable and Secure Computing (TDSC), ISSN 1545-5971, Vol. 18(5), pp. 1458–1470.
- [6] Praveen B., "Deep Learning Framework for Detecting Fraudulent Online Job Postings", Anusandhanvallari Research Journal, Vol. 2023, Issue 1, pp. 170–177, 2023.
- [7] Sathwika Ch. P. Shirin, G. Meghana, A. Anokh, V. Prathima, "Fake Job Posting Detection", Journal of Emerging Technologies and Innovative Research (JETIR), Vol. 11, Issue 3, pp. K110–K114, 2024.
- [8] Shawni Dutta, Samir Kumar Bandyopadhyay, "Fake Job Recruitment Detection Using Machine Learning Approach", International Journal of Engineering Trends and Technology (IJETT), Vol. 68, Issue 4, pp. 48–53, 2020.
- [9] Sheeza Habeeba Khan, I. Samuel Peter James, "Deep Learning Based Methods for Online Recruitment Fraud Detection", International Journal of Engineering Science and Advanced Technology (IJESAT), Vol. 25, Issue 9, pp. 87–93, 2025.
- [10] Shivani K., P. Ajay, Ch. Abhishek Reddy, B. ShreeVardhan, D. Pushpa, "Detecting Real or Fake Job Postings Using Machine Learning", International Journal of Research Publication and Reviews (IJRPR), Vol. 6, Issue 4, pp. 5326–5331, 2025.
- [11] Shubham Sonkar, Shreyash Yadav, R. Kumar, "A Hybrid Machine Learning Approach for Fake Job Posting Detection: Integrating Naive Bayes and Logistic Regression Models", International Journal of Innovative Science and Research Technology (IJSRT), Vol. 10, Issue 6, pp. 323–329, 2025.
- [12] Vrinda S, Thushara S, Bindu N, "Fraudulent Online Job Advertisement Detection using Machine Learning Models", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Vol. 13, Issue 9, pp. 16815–16819, 2024.