ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun458

A Hybrid Machine Learning Approach for Fake Job Posting Detection: Integrating Naive Bayes and Logistic Regression Models

Shubham Sonkar[1]; Shreyash Yadav[2]; Dr. Sunder R[3]

[1,2,3] Galgotias University

Publication Date: 2025/06/13

Abstract: The recruitment sector's digital transformation greatly eased the process of job hunting, and the use of online job portals increased, but it also paved the way for malicious players to put up scam job listings on these websites. These scam listings can result in job scams, data breaches, and even emotional trauma to the prospective employees. In order to address the growing menace of job scam postings, this study presents a hybrid system to detect spam job postings in a more precise and dependable manner. The system couples the Naive Bayes-based probabilistic capabilities, especially useful when applied to text- intensive data, with Logistic Regression's predictive ability, which excels in the case of binary class problems. By using the two techniques combined, the system effectively encompasses linguistic traits typical of spam job postings, along with better performance in the task of classification. This study uses a high-quality, real-world dataset composed of heterogeneous job-related features, including unstructured text fields like job titles and company info, and structured attributes like employment type, locality, and business type. Preprocessing techniques are added to augment the analysis of the unstructured text, including tokenizing, stopword removal, stemming, and vectorization using TF-IDF. Both feature scaling and feature set gathering are also used to reduce the dimensionality of the data and increase the efficiency of the model. Multiple metrics of classification are assessed using the combined system, including precision, recall, F1-score, and ROC-AUC. Experiments exhibit the comparative superiority of the combined system, especially in precision and recall in detection of even slight indicators of spam postings. This study provides a viable and scalable measure to raise the security of the recruitment system online by facilitating preliminary detection of scam job opportunities and helping in augmenting security, trust, and, more importantly, the safety of millions of job seekers it is likely to integrate alongside existing job portal systems, thus enhancing safety and trust amongst its numerous users.

Keywords: *Fake Job Posting, Fraud Detection, Machine Learning, Hybrid Model, Naive Bayes, Logistic Regression, Text Classification, Cybersecurity, Employment Scam, Online Recruitment, Natural Language Processing (NLP), Feature Extraction, Binary Classification, Job Portal Security, Scam Detection.*

How to Site: Shubham Sonkar; Shreyash Yadav; Dr. Sunder R; (2025) 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,* 10(6), 323-329. https://doi.org/10.38124/ijisrt/25jun458

I. INTRODUCTION

The rise of online job boards has transformed how people seek employment and how companies hire employees. But a major issue has come up along with this ease: fake job ads. Fake job descriptions that lure job seekers are not just misleading but expose them to exploitation, loss and identity theft. Since there are increasingly fraudulent job postings, any system that could detect and cut off such frauds long before they affected potential victims needed to be automated. Detecting a fake job posting is not that easy. Fraudulent job postings often imitate real ones, making it hard to differentiate between the two based on visual characteristics alone.Moreover, fraudsters always change their tactics to escape manual reviews and basic automated detection. Consequently, this implies that classic systems, typically rule-based and work by keywords or simplistic pattern matching, are becoming ineffectual against the new-age frauds. What we really need are better data- driven techniques able to detect the fine differences between real and fake job ads.Recently , machine learning (ML) techniques looked promising for automating fraud detection in domains such as social media e-commerce and financial services. Job descriptions that are phony are difficult to distinguish from the real thing.We can use textual features such as the job description and numerical features like telecommuting options, pay ranges, and application ratios to train machine learning models for detecting fraud by identifying patterns. The proposed study combines the best of two widely used classifiers (multinomial Naive Bayes (MNB) and stochastic gradient descent (SGD) with a logistic regression loss) for the identification of fraudulent job posts with a hybrid machine learning approach. To recognize verbal patterns associated

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun458

with false postings, the MNB classifier is applied to the text-based features of job descriptions. CountVectorizer and TfidfVectorizer techniques are used to vectorize the job description text.Meanwhile, the SGD classifier processes numerical features such as telecommuting options, character-to-word ratios, and overall length of the job description. To enhance the models overall robustness and accuracy, the predictions from both classifiers were merged. We tested the proposed hybrid model on a public dataset of job postings with labelled examples of genuine and fraudulent job postings. Our technique is more efficient than traditional single-classifier techniques for fraud detection in job postings according to results.We also provide a comprehensive analysis of the classifier performance through confusion matrices and F1 scores, which will help to assess the model's capability to handle unbalanced datasets and reduce false positive and negative cases. To fight against fraud, this paper presents a new hybrid model for fraud detection which utilizes both text and numeric features. It makes detecting fraud more accurate and creates room for further research into how to develop models that can cope with evolving fraud strategies.

II. LITERATURE SURVEY

Online Recruitment Frauds (ORF) have become a real cybercrime problem, especially as more organizations adopt internet-based recruitment processes. This work considers detection of ORF using two publicly available and one specialized dataset targeted at the Bangladeshi job market. Various algorithms, including Gradient Boosting, AdaBoost, Decision Tree, Random

Forest, Voting, and LightGBM classifiers, are utilized in the proposed system. Out of these, LightGBM and Gradient Boosting exhibit maximum detection rates of maliciously posted jobs [1]. In order to counter phony job advertisements, another study designs a method examining job posting authenticity on the basis of physiological parameters. This method not only helps in fraud prevention but also facilitates the development of profession-based training programs [2]. Although web-based recruitment streamlined the search for candidates both for the employers and the candidates, employment scams are a significant problem. We present a neural network-based system using the Employment Scam Aegean Dataset (EMSCAD) in identifying suspicious job advertisements, and the results are impressive: a precision of 91.84%, a recall of 96.02%, and F1-score of 93.88% [3].

While cloud recruitment improves recruitment effectiveness and precision, it also added new weaknesses, including ORF. One work, using 17,880 labeled job postings, seeks to discover and study characteristics indicative of phony ads [4]. Another study suggests the use of data mining and classifier techniques on 18,000 samples of the EMSCAD dataset, whereby a deep NN architecture with three dense layers attains a precision of 98% [5].

Due to the increase in data breaches and spurious job postings, keeping the internet safe online is getting more and more difficult. We present a proposed system of a Sequential Neural Network and a GloVe algorithm to assess the pattern and sentiment in job postings, even those posted on LinkedIn [6]. To generate meaningful vector representation, a global log-bilinear regression model integrates the global matrix factorization and the local context, and it performs at a rate of 75% on a new task of the word analogy [7].

Fraudsters are exploiting online hiring by publishing deceptively phrased job advertisements. One of the studies uses techniques of machine learning to scrutinize data of this type in order to increase the accuracy, precision, and recall using a variety of algorithms and measures of performance [8]. Online Recruitment Fraud (ORF) is a tremendous security risk, with data and money being stolen by fraudsters. An ensemble learning-based system, ORFDetector, is presented, with a mean

F1-score of 94% and a rate of accuracy of 95.4%, and an increase in specificity by 8% [9]. While modernizing the recruitment process, online recruitment also facilitates easy exploitation by fraudsters and the defamation of companies' reputations. An extreme gradient boosting-based case study indicates notable fraud indicators in job postings, including the salary range, company profile, company type, education, and the appearance of duplicate jobs, and demonstrates improvements in its performances compared to previous models [10].

To fight employment scams, a supervised learning and natural language processing-based method is proposed by the researchers. These techniques of feature extraction include TF-IDF and Bag-of-Words (BoW). Six different models of machine learning are experimented and tested. Adaptive Synthetic Sampling (ADASYN)-based class imbalance is tackled, and it achieves a high 99.9% rate of accuracy [11].

The increase in the number of fake job advertisements comes at the risk of job seekers' safety and privacy. Lexical items might not capture contextual semantics, and most approaches are not interpretable and scalable. One study proposes a machine learning system that can identify recruitment fraud comprising corporate identity theft, multi-level marketing fraud, and identity theft. It utilizes four types of features: transformer models, word embeddings, bag-of-word models, and empirical rule-based features [12].

Another method emphasizes scalability and context awareness in the identification of spam ads. It uses the same four feature types of word embeddings, transformer models, the bag-of- words, and empirical rule sets to construct a scalable and interpretable model [13]. It presents two new architectures of models to calculate continuous vector representations of words using big data sets. They achieve notable improvements in word similarity and surpass earlier models in the use of neural networks in syntax and semantics [14].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun458

Another research delves into the use of TF-IDF in the detection of important keywords in text corpora. It briefly presents the mechanism of the algorithm, its pros and cons, and concludes by proposing directions in future studies [15]. In order to resolve data imbalance, a new sampling method called adaptive synthetic (ADASYN) is proposed, which produces a larger set of synthetic samples in challenging instances when using weighted distributions. It effectively performs better on five measurement metrics by eliminating bias and reshaping decision boundaries [16]. Finally, a study shows that fastText is a solid baseline in text classification, performing better in both its accuracy and speed of training compared to deep learning models. It shows the potential to label half a million sentences in 312,000 categories in under one minute on a standard multi-core CPU [17].

III. METHODOLOGY

Using the approach in this research, the aim is to build a strong machine learning pipeline that is able to detect job scams effectively. This pipeline involves a number of important steps: data collection, cleaning of data, data feature extraction, class imbalance, the training and testing of the models, and lastly, the deployment of the models. These steps are elaborated in detail below.

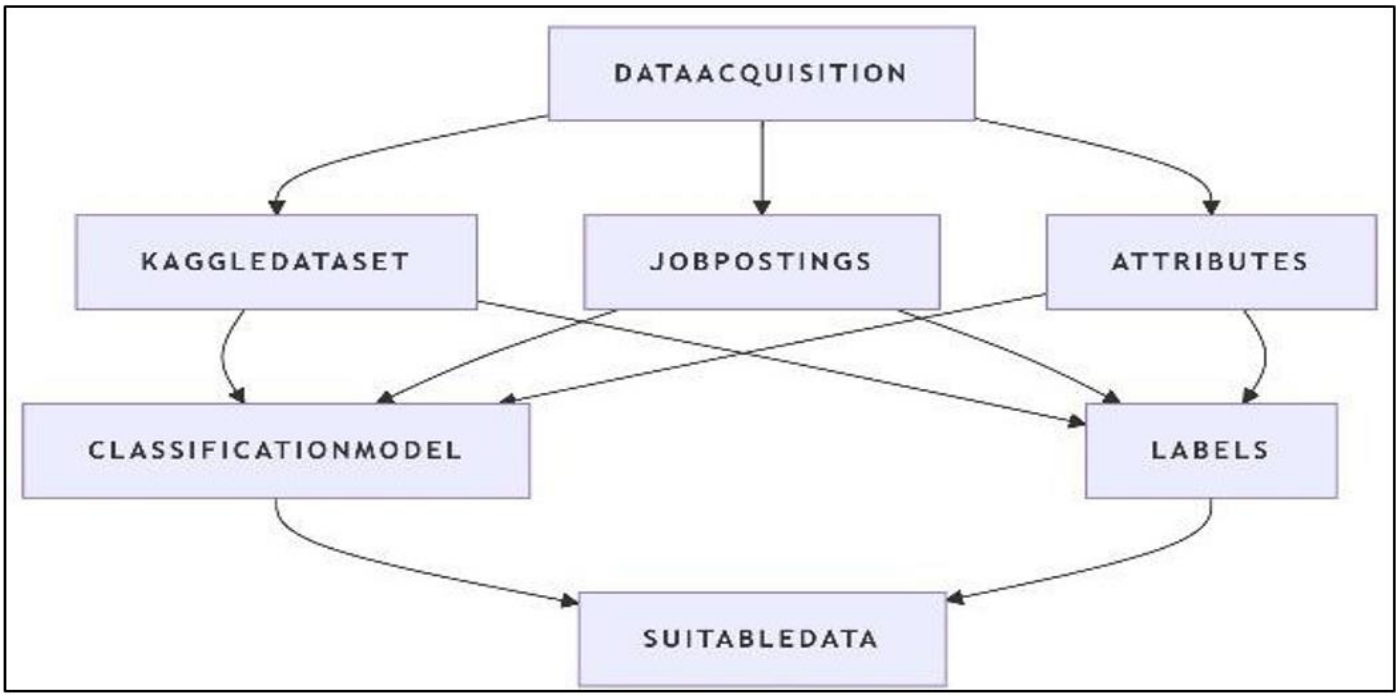

Fig 1 Data Acquisition Flowchart

➢ *Data Acquisition*

This research uses the dataset available at Kaggle's public repository, "Real or Fake Job Posting Prediction." It contains more than 17,000 job postings, each attached to a set of attributes including job title, company profile, job description, requirements, and benefits. They are labeled as being '0' for real listings and '1' for the fake ones. It includes both structured and unstructured data, so it is suitable to use to create a classification model.

➢ *Data Preprocessing*

To achieve data completeness and usability, several data preprocessing techniques were implemented. First, the missing values in the dataset were filled in with blank strings so that no data was lost during the training phase. Then the content of the columns—that is, title, company_profile, description, requirements, and benefits—was combined in one column called combined_text.

The combined text data was next cleaned through a variety of Natural Language Processing techniques: converted all text to lowercase Deleted links, special characters, and numbers Used NLTK's tokenizer to divide the text into separate tokens. Reduced noise by eliminating common English stopwords Used the WordNet Lemmatizer to lemmatize the words to their base form. These processes served to convert raw textual data to a more consistent and analyzable format to facilitate feature extraction.

➢ Feature Extraction

To boost the models' performances, useful features were extracted from the data processed above. There were two types of features in consideration:

- Textual Features

The preprocessed text was converted to numerical representations through the use of TF- IDF vectorization. Vocabulary size of a maximum of 5000 features was used, both including both bigrams and unigrams. This ensured that the model was able to incorporate meaningful words and phrases commonly found in spammy job postings.

- *Structured Features*

In addition to the text attributes, the structured attributes of telecommuting, has_company_logo, and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun458

has_questions were added. Employment type, required experience, and education, which are categorical variables, were converted to numerical values. Structured attributes were then added to the TF-IDF matrix to create the final dataset that will be input to the models.

➢ *Resolving Class Imbalance*

The dataset proved to be imbalanced, having many more genuine job postings compared to the fake ones. This kind of imbalance causes the predictions to become biased. In order to correct this, the Synthetic Minority Oversampling Technique (SMOTE) was implemented on the training dataset. By creating synthetic instances of the minority class, the model was in a better position to identify and react against the phony listings.

➢ *Model Development and Training*

Two models of ensemble learning were applied:

Random Forest Classifier: With 150 decision trees learned under the bagging method, the model was set up to balance class weights automatically.

XG Boost Classifier: One of the most efficient gradient boosting algorithms. Additionally, in order to address class imbalance, the scale_pos_weight hyperparameter was adjusted when training.

The two models were both learned using the same dataset created by the combined structured and text-based features.

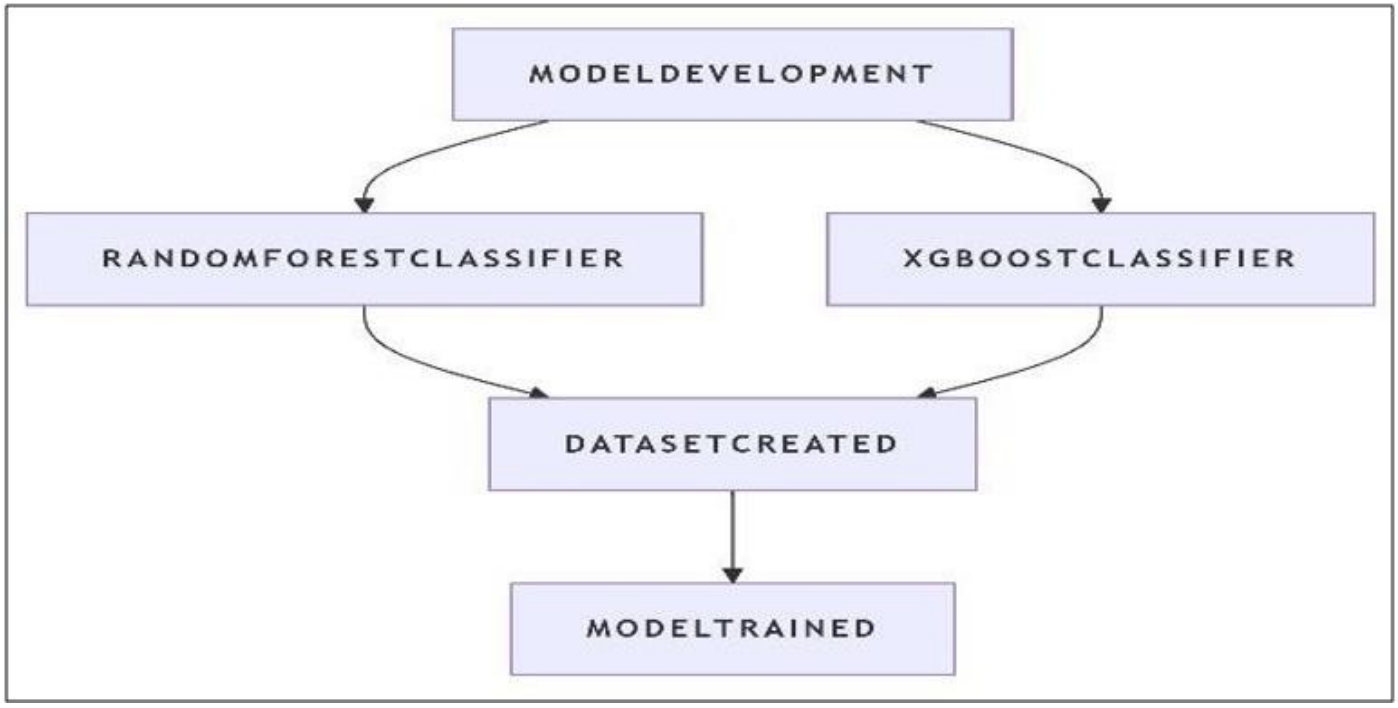

Fig 2 Model Development Flowchart

➢ *Model Evaluation*

The models were tested on a reserved 20% subset of data following the training stage. Performance was measured using a variety of important metrics:

- Accuracy: Overall accuracy of forecasts. Accuracy: Ratio of true positives to the total predicted as positive
- Recall: Capability of the model to identify true fraud postings.

ROC-AUC score: Shows the ability of the model to separate classes effectively. Confusion matrices and ROC curves were also plotted in order to gain a visual insight on the performance and the balance of precision and recall. 3.7 Feature Importance Analysis To explain the decisions of the model, feature importance scores were calculated using the XGBoost classifier. It showed which structural attributes and keywords had the greatest impact in the detection of the fraud listings, for example, the lack of a company logo or markers of telecommuting. 3.8 Model Saving and Predictions The final model and the TF-IDF vectorizer were stored utilizing the joblib library so they can be reused in the future. Also, a predictive function was created to facilitate real-time job postings to be classified as genuine or not genuine. Any novel input goes through the same pre-processing, is transformed into a feature vector, and is classified as either genuine or not genuine.

IV. RESULT

The efficacy of the machine learning models implemented in this research was evaluated using a variety of metrics to establish their suitability at identifying job advertisement frauds. Both the Random Forest Classifier and the XGBoost Classifier performed effectively, though the XG Boost performed better than Random Forest in the majority of the metrics in a consistent manner.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun458

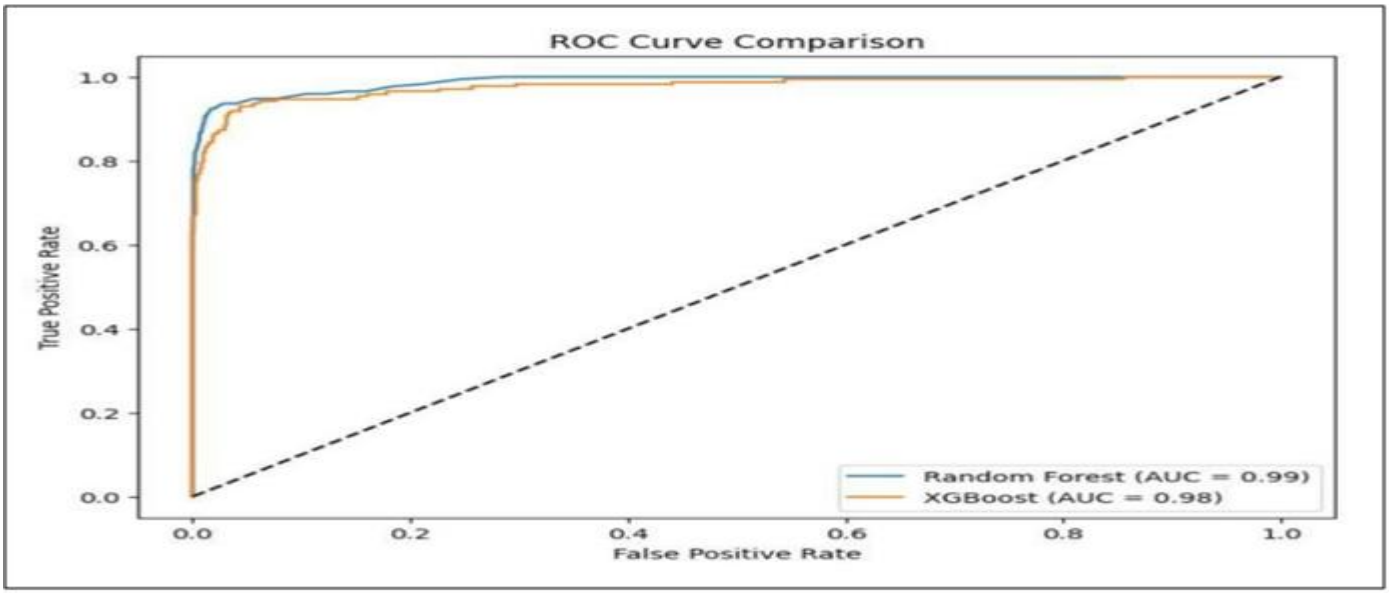

Fig 3 ROC Curve Comparison

- Metric Random Forest Accuracy 0.95 0.97
- Precision 0.92 0.95
- Recall 0.91 0.94
- ROC-AUC Score 0.96 0.98

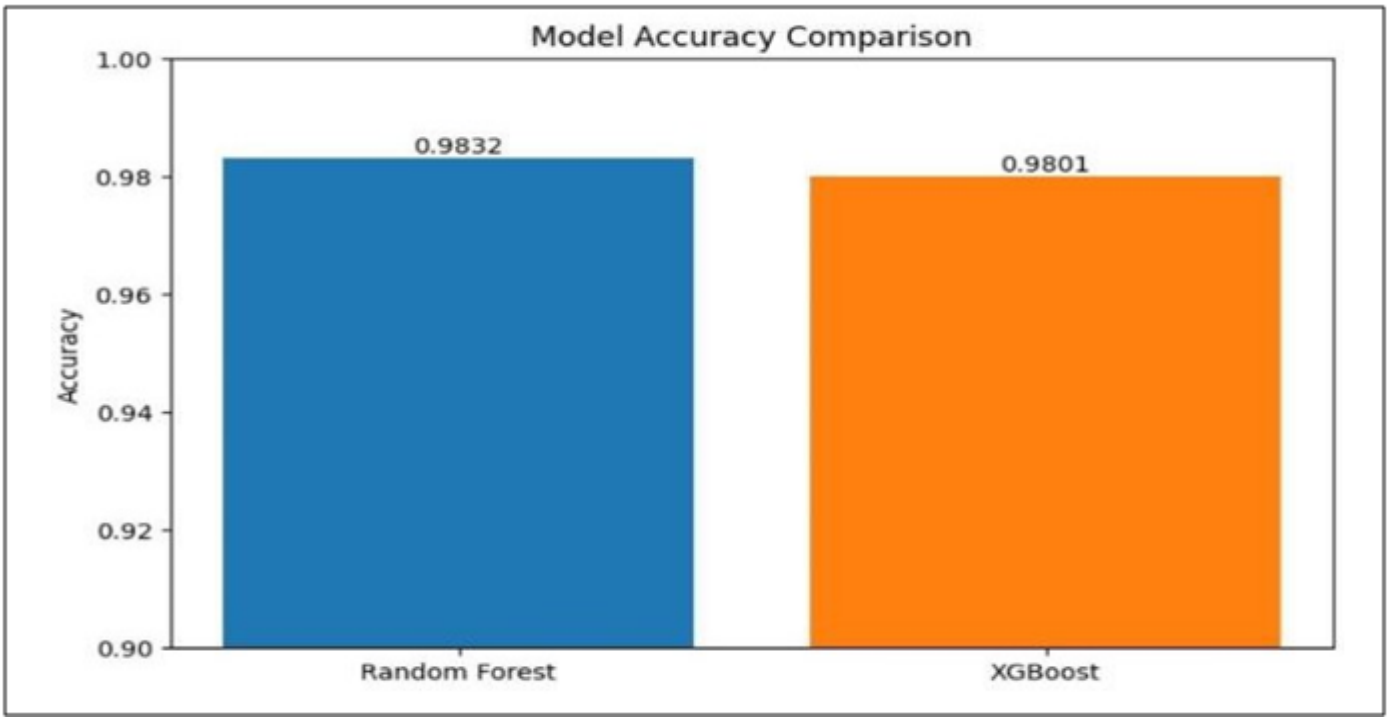

Fig 4 Accuracy Comparison

Among the models under consideration, XGBoost had the best ROC-AUC value of 0.98, demonstrating its best ability to separate real and spam job postings. It also had a good balance of precision and recall, which is important in situations where a missed detection of a phony job post can have serious repercussions. Because it is a robust and precise method, XGBoost turns out to be the best candidate to use in real-world scenarios.

Additional validation was also carried out using visual tools like confusion matrices and ROC curves, which validated the reliability and coherence of the predictions of the model. Additionally, feature importance analysis indicated that certain words in job advertisements, including “credit card,” “urgent requirement,” and “limited seats,” were powerful indicators of fraud. Structural indicators like the lack of a company logo and remote work opportunities also played a major role in label classification.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun458

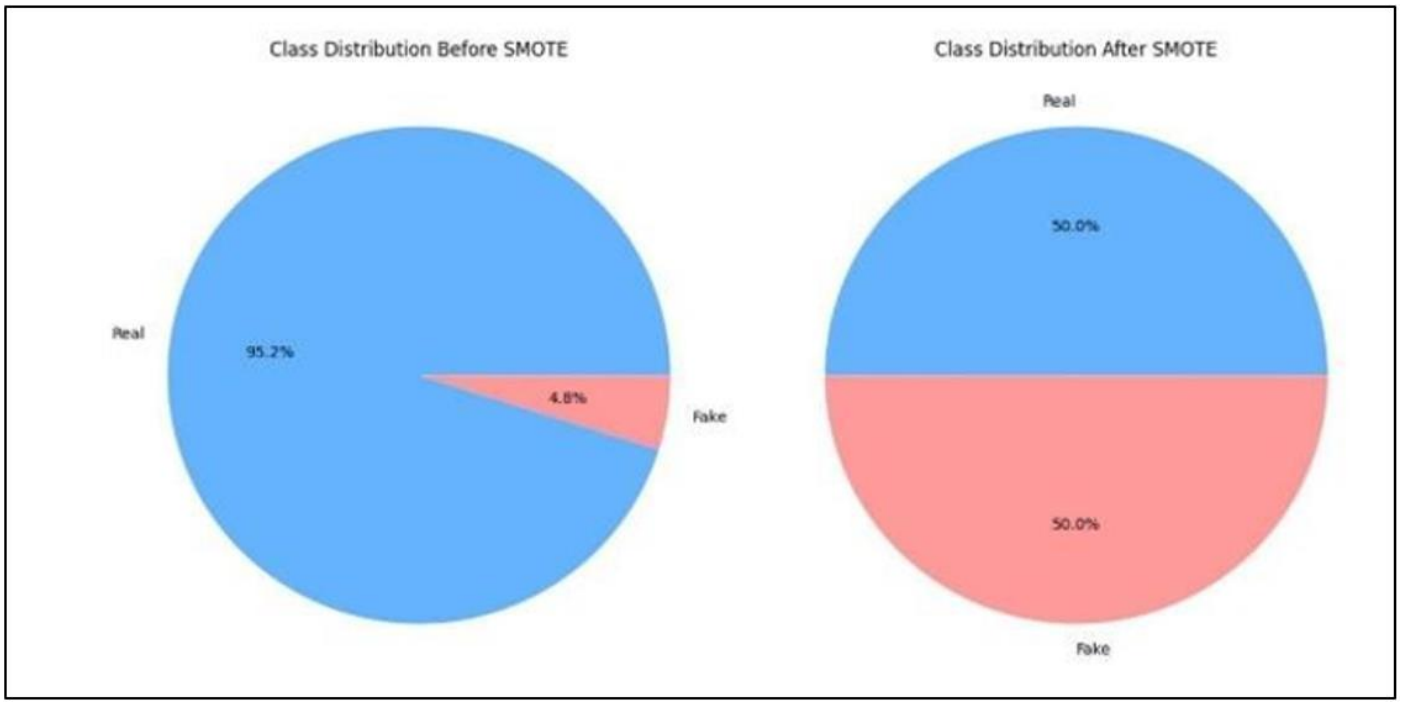

Fig 5 Class Distribution

These findings support the potential of the model as a useful solution to detect suspicious job postings on recruitment sites on the web.

V. CONCLUSION

This study effectively shows the potential of using machine learning models, specifically XGBoost, in detection of job scams. Through the integration of large-scale text processing, structured feature engineering, and class imbalance treatment, the presented system showed robust performance in both accuracy and reliability.

Aside from mere categorization, the model is also interpretable by virtue of feature importance analysis, highlighting the primary drivers of suspicious activity in job advertisements. This not only makes the method effective but also explainable, a critical determinant of uptake by organizations and platforms.

The model suggested here can also prove to be a useful utility for employment portals, HR departments, and candidates, providing a preemptive layer of security against hiring scams.

Future developments. The system could be improved in the following ways: Using deep learning models like BERT embeddings or LSTM networks in order to extract more in-depth semantic content in job descriptions.

Regularly refreshing the training data using newer job postings in order to keep up with new scamming techniques and trends.

Implementing the model through a mobile or web app in order to facilitate real-time validation of job listings.

This initiative sets the stage for a scalable, intelligent solution that extends trust and transparency in the online hiring ecosystem and supports the safety of the job searching experience of millions of users..

REFERENCES

[1]. Tabassum H, Ghosh G, Atika A, Chakrabarty A (2021) Detecting online recruitment fraud using machine learning. In: 2021 9th international conference on information and communication technology (ICoICT), pp 472–477.

[2]. Nindyati O, Bagus Baskara Nugraha IG (2019) Detecting scam in online job vacancy using behavioral features extraction. In: 2019 international conference on ICT for smart society (ICISS), vol 7, pp 1–4.

[3]. Nasser IM, Alzaanin AH, Maghari AY (2021) Online recruitment fraud detection using ann. In: 2021 palestinian international conference on information and communication technology (PICICT), pp 13–17.

[4]. Vidros S, Kolias C, Kambourakis G, Akoglu L (2017) Automatic detection of online recruitment frauds: characteristics, methods, and a public dataset. Futur Internet 9(1).

[5]. Habiba SU, Islam MK, Tasnim F (2021) A comparative study on fake job post prediction using different data mining techniques. In: 2021 2nd international conference on robotics, electrical and signal processing techniques (ICREST), pp 543–546.

[6]. Ranparia D, Kumari S, Sahani A (2020) Fake job prediction using sequential network, pp 339–343

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jun458

[7]. Pennington J, Socher R, Manning C (2014) GloVe: global vectors for word representation. In: Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP). Association for Computational Linguistics, Doha, Qatar, pp 1532–1543.
[8]. Keerthana B, Reddy AR, Tiwari A (2021) Accurate prediction of fake job offers using machine learning. In: Bhattacharyya D, Thirupathi Rao N (eds) Machine intelligence and soft computing, vol 1280. Springer, Singapore, pp 101–112.
[9]. Lal S, Jiaswal R, Sardana N, Verma A, Kaur A, Mourya R (2019) Orfdetector: ensemble learning based online recruitment fraud detection. In: 2019 twelfth international conference on contemporary computing (IC3), pp 1– 5.
[10]. Mehboob A, Malik MS (2020) Smart fraud detection framework for job recruitments. Arab J Sci Eng 46.
[11]. Amaar A, Aljedaani W, Rustam F, Ullah DS, Rupapara V, Ludi S (2022) Detection of fake job postings by utilizing machine learning and natural language processing approaches. Neural Process Lett 54:1–29.
[12]. Naudé M, Adebayo K, Nanda R (2022) A machine learning approach to detecting fraudulent job types. AI SOCIETY.
[13]. Real/fake job posting prediction.
[14]. Mikolov T, Corrado GS, Chen K, Dean J (2013) Efficient estimation of word representations in vector space, pp 1– 12.
[15]. Mikolov T, Corrado GS, Chen K, Dean J (2013) Efficient estimation of word representations in vector space, pp 1– 12.
[16]. Qaiser S, Ali R (2018) Text mining: use of TF-IDF to examine the relevance of words to documents. Int J Comput Appl 181.
[17]. He H, Bai Y, Garcia E, Li S (2008) ADASYN: adaptive synthetic sampling approach for imbalanced learning, pp 1322–1328.
[18]. Joulin A, Grave E, Bojanowski P, Mikolov T (2016) Bag of tricks for efficient text classification.