

Identification of Online Recruitment Fraud (ORF) through Predictive Models

Riktesh Srivastava

City University College of Ajman, Ajman, UAE

riktesh.srivastava@gmail.com

Abstract

Job postings online have become popular these days due to connecting to job seekers around the world. There are also instances where the fraudulent employer posts a job online and expects people to apply to these postings. These fraudulent employers impend job seekers' privacy, spawns fake job offers, and wanes. We perceived that most of the Online Recruitment Fraud (ORF) has matching features. Though the user cannot categorize them, we propose using various predictive models like Support Vector Machine (SVM), Artificial Neural Network (ANN), Random Forest, Naïve Bayes, or Logistics Regression to detect them effortlessly. Dataset with 17780 job postings was downloaded from Kaggle to identify which proposed model best predicts the fraudulent job posting. The dataset includes 14 features to determine whether online job posting is fraudulent or non-fraudulent. 70% of these job postings train the model, and the remaining 30% test the model's efficiency. The outcomes of each model are predicted using four evaluation metrics - Classification Accuracy (CA), Precision, Recall and F-1 score. The research found its suitability from two sides: the websites can identify fake jobs before being published, and job seekers are sheltered from fraudulent job postings.

Keywords:

Artificial Neural Networks, Logistic Regression, Stochastic Gradient Descent, CA, Precision, Recall, Online Recruitment Fraud (ORF).

1. Introduction

The advent of the online platform has advantages and disadvantages. On the practical side, we can share ideas, news, and other information. It is exceedingly challenging to classify which news and information are deceitful and actual on the disadvantageous side. One of the increasingly online incidents is fake job postings, often termed Online Recruitment Fraud (ORF) (Vidros et al., 2017). (Ryan, 2018) assertions that almost 90% of the job seekers fall prey to ORF. (Mehta, 2020) ORF has become an industry in India, with an unemployment rate of 7.9%; job seekers easily fall victim to these rackets. Also, in 2021, fake jobs cheated 27,000 people in India by posting 13,000 vaccines online (DNA, 2021). Agency Central, a recruitment agency in the UK, remarks a 300% rise in ORF from September 2014 to September 2016 and is expected to grow even more (Agency Central, 2019). It further states that only 17% of students and graduates in the UK are aware of ORF. The article published in CNN states that more than 16,000 fell prey to online employment scams in the US, with more than \$59 million in losses (CNN, 2021).

The motivation of the study is thus based on the fact that ORF is on the rise worldwide. The people involved in ORF are sneaky and use sophisticated technology to conduct scam unsuspecting job searches (Phillips, 2021). Some of the various common cheats used by almost all in ORF are: conducting interviews over messaging services, asking for personal information, and the company asks for payment before joining (Porter, 2021).

The study finds its objective to identify and analyze the factors that cause job seekers to believe in job postings online by identifying the variables that impact them. First, the study uses a selected predictive model to analyze the data with 14 features. The predictive models use three accuracy standards - classification accuracy, precision, and recall to test the effectiveness of the proposed model. The results obtained help the adoption of the best predictive model to identify the causes of fraudulent jobs.

The rest of the paper is as follows; In Section 2, the literature review to identify the use of predictive modelling for ORF is identified. Section 3 does the research methodology that mentions the business

understanding, data understanding, and data preparation for data analysis. Section 4 is devoted to data modelling, which exemplifies the model construction phase and executed predictive model. Section 5 presents the analysis results, comparing using five accuracy standards for the proposed models. The outcome deployment is in section 6, based on the predictive models for 30% of the test data.

2. Literature Review

There is enough literature about online crime detection models of different forms available. Almost all of them apply different predictive models for identifying ORF. (Alharby & Alghamdi, 2019) performed the ORF using the Random Forest algorithm and gauged classification accuracy to assess the model's effectiveness. Another suggested approach for ORF is Hierarchical Clusters-based Deep Neural Networks (HC-DNN), which conducts the fraud detection through cross-validation (Kim et al., 2019) and calculates the precision for ascertaining the efficacy of the model. (Lal et al., 2019) proposed the ensemble learning-based model for ORF detection and evaluated it based on the calculating recall parameter

with 94% and 95.4% score of F1-score and accuracy. (Cao et al., 2019) introduced a model called TitAnt to classify between fraudulent and non-fraudulent job postings. (Choi, 2020) conducted the study using two classifiers - single and ensemble classifiers to classify the fraudulent job posts. (Ranparia et al., 2020) used natural language processing (NLP) to analyze the sentiments and patterns of online job postings to predict the fraudulent jobs posted on LinkedIn. (Nasser & Alzaanin, 2020) conducted the study using multiple predictive models as Multinomial Naïve Bayes, Support Vector Machine, Decision Tree, K-Nearest Neighbours and Random Forest to differentiate between fraudulent and non-fraudulent job postings. (Shree et al., 2021) used Ensemble algorithm and Logistic Regression, K Nearest Neighbors, and Random Forest predictive models to analyze job scams. (Shibly et al., 2021) performed the test of identifying the fraudulent job postings online using the combination of decision trees and random forest algorithms. (Shishupal et al., 2021) used NLP algorithm to classify job postings as fake or real.

The present study uses five predictive models, Random Forest, Artificial Neural Network, Naïve Bayes, Logistic Regression and Support Vector Machine, to classify fraudulent and non-fraudulent job postings. The efficiency and effectiveness of the predictive models are judged using four different accuracy standards - CA, Precision, Recall and F1-score, respectively.

3. Research Methodology

The research methodology adopted for the study uses the CRISP-DM framework, termed as Cross-Industry Standard Process for Data Mining, methods for thorough data analysis. The CRISP-DM approach is applied to use the five different predictive models for identifying the fraudulent job postings and has 6 phases:

1. *Business understanding*: The understanding of the research objectives (section 3.1)
2. *Data understanding*: The data understanding includes the study about the variables used for the study and also conduct statistical analysis to conclude the dissemination of

data for the dependent variable (section 3.2)

3. *Data preparation for predictive modeling*: Data preparation involves data cleaning for further data analysis. (section 3.3)
4. *Data modeling*: Data modeling elaborate the dataset for training and testing to be used by different predictive models for analysis (section 4)
5. *Results evaluation*: The results are evaluated based on different performance metrics. (section 5).
6. *Outcome deployment*: Use the predictive models to predict fraudulent job postings. (section 6).

3.1 Business Understanding

The research objectives for the study identifies the business understanding for the case. There are two research objectives:

- i. To use five predictive models for identification of ORF, and,
- ii. To evaluate the effectiveness of predictive models for predictive accuracy.

3.2 Data Understanding

The dataset used for the study involves 17780 job postings collected from the Kaggle web source. There are 14 features included in the downloaded dataset, with the details mentioned in Table 1.

Variable name

Title
Location
Department
salary_range
company_profile
Description
Requirements
Benefits
has_questions
employment_type
required_experience
required_education
Industry
Function

Table 1: Variables for Data Analysis

Apart from the mentioned 14 features, the dependent variable, fraudulent, identifies 1 when the job posting is fraudulent and 0 when identified as non-fraudulent.

The predictive models used for the study divides the data randomly into two different subsets: 70% of the data (12516) for training the model and 30% of the data (5364) for testing the model.

Independent variables	Dependent variable (1=fraudulent/0=non-fraudulent)
title location department salary_range company_profile description requirements benefits has_questions employment_type required_experience required_education industry function	Fraudulent

Table 2: Independent and Dependent variables

3.2.1 Descriptive Analysis for general variables

Descriptive analysis helps in detecting the dissemination of the target variable in the dataset. As shown in Figure 1, 56% of job postings online are for full-time jobs and 44% (22% each) for part-time and contract jobs.

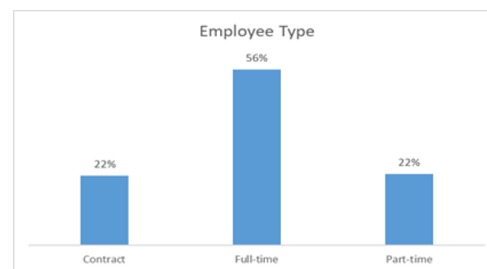


Figure 1: Distribution of fraudulent job postings based on Employee Type

Interestingly, experience-wise, the fraudulent job postings are more for associate and mid-senior levels. The fraudulent job postings are also high for newcomers (entry-level and Internship) and their

minimum for executive-level jobs. Figure 2 mentions in detail the experience-wise ORF.

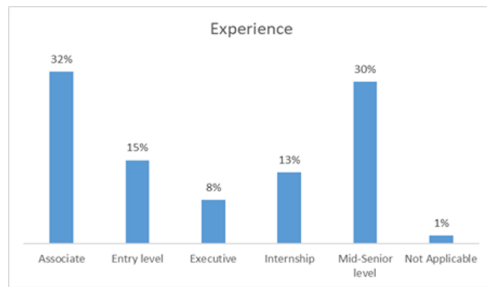


Figure 2: Distribution of fraudulent job postings- Experience-wise

In figure 3, we reported the fraudulent job postings as a function of the education level. The dataset has four education fields: associate degree, bachelor's degree, master's degree, and high school or equivalent. Figure 3 also mentions that the highest fraudulent job postings are for bachelor's degree, while the number decrease for master's degree. Job postings with associate degrees and unspecified education levels do not have any fraudulent job postings.

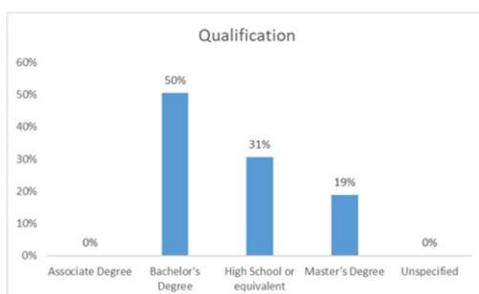


Figure 3: Distribution of fraudulent job postings based on the education level

Figure 4 shows the distribution of fraudulent job postings industry-wise. Almost one-third of the job postings did not mention any industry-specific information. The job postings with the highest percentage of fraudulent job postings are oil & energy, with 12% reported cases. Accounting and Healthcare reported 6% fraudulent job postings and Marketing with 5% cases. The criteria used to select data were to identify the reported cases, where the number of fraudulent job postings was > 10.

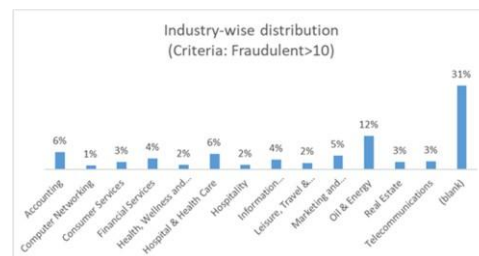


Figure 4: Distribution of fraudulent job postings industry wise

Figure 5 displays the distribution of job postings and reported fraudulent jobs listed based on function-wise. The criteria used for selection of data is where the reported cases > 5%. The unspecified (blank) reported the highest cases with 31% of cases. Amongst the

mentioned functions, IT reported the highest cases with 10% of fraudulent job postings.

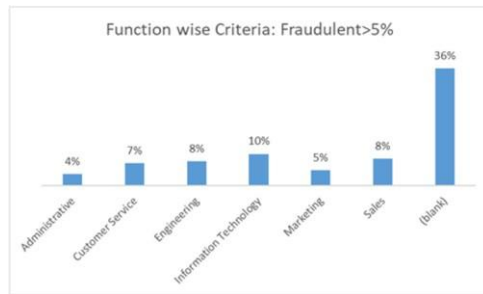


Figure 5: Distribution of fraudulent job postings function-wise

3.3 Data preparation for predictive modeling

Data preparation is the most essential and critical step for predictive modeling. Data preparation for the study was conducted to map the textual values to numeric values for in-depth analysis. (see table 3).

Variable Name	Variable type	Transformation
employment_type	Text	Text to Numeric Contract to 0, Part time to 1, Full time to 2
required_experience	Text	Text to Numeric Associate to 0, Entry level to 1, Executive to 2, Internship to 3, Mid-Senior level to 4, and Not Applicable to 5.
required_education	Text	Text to Numeric Unspecified to 0, Associate Degree to 1, Bachelor's Degree to 2, High School or equivalent to 3, and Master's Degree to 4.
industry	Text	Text to Numeric Airlines/Aviation to 1, Banking to 2, Building Materials to 3, Civic & Social Organization to 4, Computer Software to 5, Construction to 6, Consumer Electronics to 7, Consumer Services to 8, Education Management to 9, Entertainment to 10, Events Services to 11, Facilities Services to 12, Financial Services to 13, Food & Beverages to 14, Hospital & Health Care to 15, Information Technology and Services to 16, Internet to 17, Management Consulting to 18, Marketing and Advertising to 19, Oil & Energy to 20, Online Media to 21, Retail to 22, Staffing and Recruiting to 23, Telecommunications to 24, and Wholesale to 25.
function	Text	Text to Numeric Administrative to 1, Advertising to 2, Business Development to 3, Consulting to 4, Customer Service to 5, Data Analyst to 6, Distribution to 7, Education to 8, Engineering to 9, General Business to 10, Health Care Provider to 11, Human Resources to 12, Information Technology to 13, Management to 14, Marketing to 15, Part-time to 16, Product Management to 17, Production to 18, Project Management to 19, Quality Assurance to 20, Sales to 21, and Supply Chain to 22.

Table 3: Variables transformation

4. Data Modeling

The fraudulent job posting classification is driven using five different predictive models. All five predictive models use the binary classifications of the job postings as fraudulent (1) and non-fraudulent (0). The section describes the mathematical formulation of each of the selected predictive models and the mechanism of its classification. The selection of the model is based on the Receiver Operating Characteristic (ROC) curve accordingly.

4.1 Logistic Regression

Logistic regression is a predictive model that can classify the jobs as fraudulent and not fraudulent in binary format. With the 14 features in the downloaded dataset, the logistic regression

$$h_{\theta}(X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x + \dots + \beta_{12} x + \beta_{13} x + \beta_{14} x)}} \quad (1)$$

For the study, Y variable is independent variable Y with dependent variables as $(X) \in \{x_1, x_2, x_3, x_4, \dots, x_n\}$.

$$Y = w_0 + w_1 x_1 + w_2 x_2 \quad (2)$$

$Y \in [0,1]$ for the binary classification problem, as fraudulent as 1 and not fraudulent as 0.

The function used to calculate is called the sigmoid function, which gives the output a probability value with a minimal cost function. The cost function is as shown in Equation 3. (3)

$$\text{Cost}(h\theta(X), y) = \begin{cases} \log(h\theta(X)), y = 1 \\ -\log(1 - h\theta(X)), y = 0 \end{cases}$$

4.2 Support Vector Machine (SVM)

SVM finds the optimal hyperplane concerning the feature sets to divide the data points into two classes. Several hyperplanes separate the data points into different categories, but SVM help in finding the optimal hyperplane, which directly affects the models' performance. The model trains the data points through the closest information lying on two hyperplanes (classified as fraudulent and non-fraudulent) on either side of the ideal known help vectors. The cost function for the SVM classifier is given mathematically in eq. 4.

$$J(\theta) = \frac{1}{2} \sum_{j=1}^n \theta_j^2$$

4.3 Naïve Bayes

Naive Bayes is a probabilistic predictive model that depends on

the Bayes Theorem, as mentioned in eq. 5

$$P\left(\frac{A}{B}\right) = P\left(\frac{B}{A}\right) * \frac{P(A)}{P(B)} \quad (5)$$

The text data of the job description is converted into vectors. These encoding text in the form of numbers will help to decide whether the vector representation of news belongs to a fraudulent or on-fraudulent. A Naive Bayes classifier is trained with a given set of features so that fraudulent job descriptions are automatically categorized into fraudulent or non-fraudulent using the probabilities defined in the Bayes theorem. From the Bayes Theorem, Replacing A and B from eq. 5 to X and Y as feature matrix and response vector respectively, the eq. 6 will become:

$$P\left(\frac{X}{y}\right) = P\left(\frac{y}{X}\right) * \frac{P(X)}{P(y)} \quad (6)$$

Thus, the probability of predicting a target with class k has given feature matrix X, given a particular class (fraudulent or non-fraudulent) of y times the probability of belonging to a specific class.

4.4 Artificial Neural Network (ANN)

There are two steps to outline the ANN experimental setup for class (4) fraudulent employers. Logistic Regression for activation layer and Stochastic Gradient Descent (SGD) to identify the cost.

The present section explains the mathematical representation for each of the two steps in conjunction.

Apart from these 14 features, we also have classification as fraudulent or not (binary classifier labelled as 1, for fraudulent and 0, for non-fraudulent). These data are grouped into a matrix, column corresponds to features, and row represents a single data point $X, X \in \mathbb{R}^{(m \times n)}$. We will then have a vector containing the outputs, either 0 for not fraudulent or 1 for fraudulent. For ANN, we also define the weight vector (adjust the values as per the cost function) $w, w \in \mathbb{R}^n$. The weighted sum is characterized as:

$$w_1x_1 + w_2x_2 + \dots + w_mx_m \quad (7)$$

which is as:

$$\sum_{i=1}^m w_i x_i = w^T x \quad (8)$$

where w^T is "transpose w ".

The Logistic Regression uses probabilistic logistic function based on equation (8) and is as:

$$P(w^T x) = \frac{1}{1 + e^{-w^T x}} \quad (9)$$

Based on equation (9), if the weighted sum for a data point is nearing 1, then we can predict the data point to have a class 1, 0 otherwise, which is as:

$$P(\hat{y} = 1 | x; w) = \frac{1}{1 + e^{-w^T x}}, \text{ for class 1} \quad (10)$$

For correct classification, Stochastic Gradient Descent (SGD) iterates the cost function as

$$C = \frac{1}{2} \sum (\hat{y} - y)^2 \quad (11)$$

where initial $y = 0$, and $\hat{y}$ is based on equation (10).

4.5 Random Forest

The random forest predictive model uses decision trees and fits multiple decision trees using averaging to improve the predictive accuracy and control over-fitting. The random forest predictive model uses the Gini index to measure a variable's probability of being wrongly classified when randomly chosen. The degree of the Gini index varies between 0 and 1 and is denoted as:

$$Gini\ Index = 1 - \sum_{i=1}^c (p_i)^2$$

where p_i is the probability of an object being classified to a particular class, and c refers to the classes (fraudulent and not fraudulent).

The analysis and adoption of the model are based on the ROC curve. ROC curve is considered the most accurate and straightforward method of classifying the classes as 0 or 1. By analogy, the ROC curve

states higher the AUC (Area Under Curve), the better is the predictive model is at differentiating between fraudulent and non-fraudulent job postings.

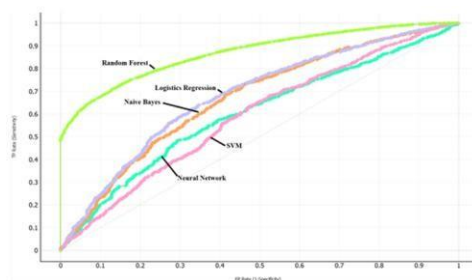


Figure 6: ROC curve of five predictive models

The AUC values for five different predictive models is given in Table 4 as:

Predictive Models	AUC
SVM	0.590
Random Forest	0.869
Neural Network	0.600
Naïve Bayes	0.668
Logistic Regression	0.680

Table 4: AUC values for five predictive models

Based on table 4, the AUC value for Random Forest predictive model gives the highest value and is thus suitable to predict the job postings as fraudulent and non-fraudulent. For detailed analysis, in the following section, we will use four accuracy standards for all the

five predictive models and then select the suitable ones.

5. Results Evaluation

The data modeling process involves selecting machine learning techniques for predictive modeling. The artificial neural networks (ANN) model is used to recognize fraudulent job postings online. The accuracy standards from the confusion matrix are classification accuracy, precision, and recall (see Table 4)

Accuracy Standards	Evaluation Criteria
Classification Accuracy: It is the ratio of the number of correct predictions from total data points.	Classification Accuracy > 0.5
$\text{Classification Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$	
Precision: Precision is the ratio between the True Positives (TP) and all the positives.	Precision > 0.5
$\text{Precision} = \frac{TP}{TP + FP}$	
Recall: Recall is the measure of our model correctly identifying True Positives (TP).	Recall > 0.5
$\text{Recall} = \frac{TP}{TP + FN}$	
F1-Score: F-1 is the weighted harmonic mean for Precision and Recall and creates a balance between Precision and Recall.	F1 > 0.5
$F1 = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$	

Table 5: Accuracy Standard to evaluate fraudulent job postings

	CA	Precision	Recall	F-1 Score
SVM	0.797	0.913	0.797	0.848
Random Forest	0.952	0.948	0.952	0.930
Neural Network	0.951	0.905	0.951	0.928
Naïve Bayes	0.951	0.917	0.951	0.928
Logistic Regression	0.951	0.905	0.951	0.928

Table 6: Evaluation Metrics

This phase assesses the predictive models' abilities using four accuracy criteria (classification accuracy, precision, recall, and F-1 score) from the confusion matrix, summarized in Table 5. The

outcomes are for 70% of the dataset for training the predictive models.

As mentioned in table 6, the Random Forest predictive model recognizes almost 95% accuracy for all four accuracy criteria.

Table 7 testifies the confusion matrix of the Random Forest predictive model, which suitably classified the job postings as fraudulent or non-fraudulent with 95.2% accuracy for 30% of the test data.

	CA	Precision	Recall	F-1 score
Random Forest	0.950	0.907	0.950	0.928

Table 7: Random Forest's predictive model outcomes for test data

Random Forest predictive model obtained:

- The true-negative rate (TNR) gave 100% results, indicating that the job postings which were non-fraudulent were classified correctly by the model;
- The true-positive rate (TPR) is also 95%, claiming that the proposed model classified 5096 job postings correctly, out of the 5364.

6. Outcome deployment

This paper uses the ANN predictive model approach to study fraudulent job postings online for the downloaded Kaggle dataset. The results were analyzed using three performance metrics for assessing the proposed model: classification accuracy (CA), precision, recall, and F-1 score. The experiment revealed that the ANN provides acceptable outcomes (CA=0.950, precision=0.907, recall=0.950, and F-1 score=0.928).

The prospective future work for this study will be a further development of the model by deepening analysis on variables used in the models. Data available have restrictions regarding the specifics of defaulters and timeline, which stipulates the behaviour of default job postings.

References

- Agency Central. (2019). *Spotting fake job adverts: What jobseekers need to know*.
<https://www.agencycentral.co.uk/articles/2017-06/what-jobseekers-need-to-know-about-fake-job-ads.htm>
- Alharby, F., & Alghamdi, B. (2019). An Intelligent Model for Online Recruitment Fraud Detection. *Journal of Information Security*, 10(3), 720-726.

<https://doi.org/10.4236/jis.2019.103009>

Cao, S., Yang, X., Chen, C., Zhou, J., Li, X., & Qi, Y. (2019). TitAnt: Online Real-time Transaction Fraud Detection in Ant Financial. *ArXiv:1906.07407 [Cs, Stat]*.

<http://arxiv.org/abs/1906.07407>

Choi, J. K., Hyerin Won, Minsun Shim, Seungah Hong, Eunjung. (2020).

Fake Job Recruitment Detection Using Machine Learning Approach. *International Journal of Engineering Trends and Technology - IJETT*.

<https://www.ijettjournal.org/archive/ijett-v68i4p209s>

CNN, A. E. (2021). *Looking for a job? Make sure it's real first*. CNN.

<https://www.cnn.com/2021/04/24/business/employment-scams-2020-trnd/index.html>

DNA. (2021). *Fake job portals cheated 27,000 employed people, collected Rs 1.09 crore in a month*. DNA India.

<https://www.dnaindia.com/delhi/report-fake-job-portals-cheated-27000-employed-people-collected-rs-109-crore-in-a-month-2854770>

Kim, J., Kim, H.-J., & Kim, H. (2019). Fraud detection for job placement using hierarchical clusters-based deep neural networks. *Applied Intelligence*, 49(8), 2842-2861.

<https://doi.org/10.1007/s10489-019-01419-2>

Lal, S., Jiaswal, R., Sardana, N., Verma, A., Kaur, A., & Mourya, R. (2019). ORFDetector: Ensemble Learning Based Online Recruitment Fraud Detection. *2019 Twelfth International Conference on Contemporary Computing (IC3)*, 1-5.

<https://doi.org/10.1109/IC3.2019.8844879>

Mehta, R. (2020). *Fake job offers: How to avoid getting duped in job scams*. Economics Times.

<https://economictimes.indiatimes.com/wealth/earn/fake-job-offers-how-to-avoid-getting-duped-in-job-scams/articleshow/69173183.cms?from=mdr>

Nasser, I. M., & Alzaanin, A. H. (2020). *Machine Learning and Job Posting Classification: A Comparative Study*. 9, 9.

Phillips, P. (2021). *Council Post: Are Online Scammers Committing Recruitment Fraud In Your Company's Name?* Forbes.

<https://www.forbes.com/sites/forbeshumanresourcescouncil/2021/04/14/are-online-scammers-committing-recruitment-fraud-in-your-companys-name/>

Porter, K. (2021). *Don't fall for online employment and job scams*.

<https://us.norton.com/internetsecuri>

ty-online-scams-avoid-job-
scams.html

Ranparia, D., Kumari, S., & Sahani, A.
(2020). Fake Job Prediction using
Sequential Network. *2020 IEEE 15th
International Conference on
Industrial and Information Systems
(ICIIS)*, 339-343.

<https://doi.org/10.1109/ICIIS51140.2020.9342738>

Ryan, L. (2018). *The Job Search Scam
90% Of Candidates Fall For*. Forbes.
[https://www.forbes.com/sites/lizryan/
/2018/05/06/the-job-search-scam-90-
of-candidates-fall-for/](https://www.forbes.com/sites/lizryan/2018/05/06/the-job-search-scam-90-of-candidates-fall-for/)

Shibly, F., Sharma, U., & Naleer, H.
(2021). Performance Comparison of
Two Class Boosted Decision Tree and
Two Class Decision Forest
Algorithms in Predicting Fake Job
Postings. *Annals of the Romanian
Society for Cell Biology*, 2462-2472-
2462-2472.

[https://www.annalsofrscb.ro/index.p
hp/journal/article/view/2778](https://www.annalsofrscb.ro/index.php/journal/article/view/2778)

Shishupal, Prof. R. S., . V., Mane, S.,
Singh, V., & Wasekar, D. (2021).
Virtual Assistant for Prediction of
Fake Job Profile Using Machine
Learning. *International Journal of
Advanced Research in Science,
Communication and Technology*, 171-
175.

<https://doi.org/10.48175/IJAR SCT-885>

Shree, R. A., Nirmala, D., Sweatha, S.,
& Sneha, S. (2021). Ensemble
Modeling on Job Scam Detection.
Journal of Physics: Conference Series,
1916(1), 012167.

[https://doi.org/10.1088/1742-
6596/1916/1/012167](https://doi.org/10.1088/1742-6596/1916/1/012167)

Vidros, S., Kolias, C., Kambourakis, G.,
& Akoglu, L. (2017). Automatic
Detection of Online Recruitment
Frauds: Characteristics, Methods,
and a Public Dataset. *Future
Internet*, 9(1), 6.

<https://doi.org/10.3390/fi9010006>