ETDT

Emerging Trends in Digital Transformation

*Volume-2, Issue-1, January-March 2026* ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-22***

# AI APPROACHES TO RECRUITMENT FRAUD IDENTIFICATION

**[#1]P. SWATHI,** ***Assistant Professor,***
**[#2]MADASI HARSHITHA,** ***B.Tech Student,***
**[#3]PENTA AKSHITHA,** ***B.Tech Student,***
**[#4]THUMUGANTI SATHVIKA,** ***B.Tech Student,***
**[#5]MEKALA JAHNAVI,** ***B.Tech Student,***
***Department of Computer Science And Engineering,***
**TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.**

**ABSTRACT:** Online recruiting fraud has grown to be a serious problem in the contemporary digital age since it affects organizations financially in addition to jeopardizing job searchers' privacy. Many times, the most up-to-date fraud tactics go undetected by traditional fraud detection systems. Because of their superior accuracy in sorting through massive datasets, deep learning algorithms hold great promise as a tool in the battle against false job ads. Several deep learning models, including CNNs, RNNs, and transformers, are being examined in this study with the aim of uncovering unethical labor practices. These techniques enhance the safety of online recruiting platforms and identify dishonest users by using feature extraction and natural language processing (NLP).

***Keywords:*** Deep Learning, Online Recruitment Fraud, Fraud Detection, Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs),

## 1. INTRODUCTION

Online recruiting platforms have grown rapidly in recent years, making it easier for recruiters and job-seekers to connect and streamline the hiring process. The rise of recruitment fraud is directly correlated to the proliferation of deceptive job ads used by con artists to trick unsuspecting victims into divulging sensitive information or paying ransom. When new forms of fraud emerge, most rule-based fraud detection systems can't adjust to catch them. Using deep learning and other advanced machine learning techniques to better detect fake job ads is one possible solution.

One use of deep learning—a branch of machine learning that uses complex neural networks to sift through mountains of data—is the identification of online fraud. Models like convolutional neural networks (CNNs), long short-term memories (LSTMs), recurrent neural networks (RNNs), and transformers are widely used in text analysis and criminal identification. By leveraging Natural Language Processing (NLP), deep learning algorithms may analyze job descriptions, employer data, and application procedures for patterns that could indicate potential misconduct. Because of their ability to constantly learn from new fraudulent acts, these algorithms outperform previous methods.

To make online job marketplaces safer, deep learning systems can detect recruiting fraud and automatically identify questionable ads. Anomaly detection, sentiment analysis, and keyword extraction are some of the methods used to identify genuine from fake job ads. In addition,


DOI: https://doi.org/10.5281/zenodo.19018066

deep learning models can be enhanced with real-time monitoring to help identify these scams before they target job applicants. Given the increasing sophistication of criminal fraud schemes, it is crucial to implement AI-driven solutions to secure online hiring procedures and prevent job seekers from being exploited.

## 2. LITERATURE REVIEW

Natasha Akram, Rabia Irfan, (2024) Online recruiting services have increased fake job listings. Many fear using online employment platforms owing to security concerns. This work provides a sophisticated BERT-based fraud detection method. The technology detects fake job ads. A dataset is created by combining job postings. The system can now more accurately discriminate between authentic and fake job ads. A complete pre-processing procedure includes feature engineering and data purification. These steps prepare data for model training.

Aravind Sasidharan Pillai ( 2024) The frequency of fake job advertising online worries companies and job-seekers. Despite the growing severity of the problem, much research has focused on deep learning algorithms to detect fake job ads. This study uses a Bidirectional Long Short-Term Memory (Bi-LSTM) model to detect fake job postings. We use numbers and words to find data patterns and connections. The suggested model has a 98.71% accuracy rate and 0.91 ROC AUC score, making it useful for online job seekers.

Hridita Tabassum, Gitanjali Ghosh, (2024) Online job boards make it easier for people worldwide to find and apply for jobs. The unfortunate truth is that unethical recruiters can use internet job board flaws to scam desperate job seekers. Despite precautionary measures and warnings from credible recruitment portals, online job fraud remains. The project aims to create a machine learning model that predicts employment fraud. A Ghanaian employment board provided data for this forecasting algorithm. Hiring fraud is its main worry.

Bandar Alghamdi, Fahad Alharby (2023) The spread of fake job ads on popular internet job forums threatens job seekers. This paper proposes an advanced machine learning-based fraud detection approach. The model uses many variables to identify fake job listings. The results show that improving online recruiting platform security identifies bogus job ads.

Tobias K. Lauinger, Michael J. Prilla, and Dirk Labudde (2022) This project involves creating and testing a machine learning system to detect fake job advertisements. Machine learning algorithms used empirical rules, model-based transformations, model-based bags of words, and cutting-edge word characteristics. We tested machine learning models using publicly available job titles.

Panpan Zheng, Shuhan Yuan, and Xintao (2021) Many online venues have anti-fraud procedures to detect and prevent fraud. Fraudsters are usually removed off the network, slowing it down. Discussion of the SAFE framework, which employs survival analysis to detect fraud early. It decreases their survival prospects as user activity does.

Nasser Alzaanin and Mohammad Alshorman (2020) Due to online hiring, people can find jobs faster. Meanwhile, con artists can use it to trick people into applying for fake jobs. This study presents an ANN-based technique for detecting fake job listings. ANN-based methods outperform others in finding fraudulent job postings.


DOI: https://doi.org/10.5281/zenodo.19018066

Jyoti Vashishtha 2024 The research uses machine learning-based categorization algorithms to detect and prevent online job fraud. Comparing classifiers trained on false internet posts can help spot job scams.

Khushboo Taneja, , and Saroj Ratnoo (2020) This study shows Fraud-BERT, a transformer-based contextual framework. The biased Employment Scam Aegean Dataset (EMSCAD) is used to train a model employing Bidirectional Encoder Representations from Transformers transfer learning. The suggested method outperforms the current one.

## 3. SYSTEM ANALYSIS

### EXISTING SYSTEM

The detection of online recruitment fraud is now making use of a wide variety of deep learning models. These models include, but are not limited to, ANNs, CNNs, RNNs, and transformer-based architectures like as BERT. Algorithms built into these systems use textual features, data, and user interactions to spot misleading patterns in job ads. By integrating deep learning techniques with more conventional machine learning models, we successfully completed classification tasks. Support vector machines (SVMs), decision trees, and random forests were all part of this set of models. Recent years have seen an uptick in the number of algorithms that use entity recognition, sentiment analysis, and feature extraction techniques from NLP to weed out fake job ads.

When it comes to training and testing fraud detection algorithms based on deep learning, there is no bigger dataset than the Employment Scam Aegean Dataset (EMSCAD). Various learning algorithms, including supervised, semi-supervised, and unsupervised ones, will be used in an effort to identify potentially problematic employment trends. Combining rule-based and learning-based approaches is a common hybrid strategy used by many systems to improve accuracy.

- **High Computational Cost:** Because they need a lot of processing power, deep learning models are expensive to build and keep up to date.
- **Data Imbalance Issues:** As a result of the large disparity between the number of real and false job ads, detection performance drops and model training becomes biased.
- **Adversarial Attacks:** Criminals' strategies are dynamic, making it hard for static models to account for emerging fraud trends.
- **Interpretability Issues:** Given that a lot of deep learning models are "black boxes," it could be hard to understand how they create their results.
- **Dependency on Large Datasets:** Finding and annotating massive volumes of labelled data is challenging, yet essential for deep learning models.
- **False Positives and False Negatives:** When algorithms miss complex forgeries, they can generate false negatives; conversely, when algorithms mistakenly mark real job ads as fraudulent, they can generate false positives.
- **Lack of Generalization:** It is highly improbable that models trained on limited datasets will perform adequately when presented with a wide variety of fake environments or job marketplaces.


DOI: https://doi.org/10.5281/zenodo.19018066

- **Slow Adaptation to New Fraud Trends:** Scammers' tactics are dynamic, therefore staying one step ahead of them requires regular model updates.
- **Security and Privacy Concerns:** There are legitimate and ethical privacy problems with collecting and processing sensitive recruiting data.
- **Limited Real-Time Detection:** The identification and removal of false job postings is delayed since many systems struggle to detect fraud in real-time due to the high processing requirements.

**PROPOSED SYSTEM**

In order to improve the identification of online recruiting fraud, the suggested method employs state-of-the-art deep learning models, such as Graph Neural Networks (GNNs), Transformer-based architectures (BERT and GPT), and hybrid deep learning frameworks. This method uses Natural Language Processing (NLP) to sift through fake job ads for patterns of dishonesty in the descriptions. It is also possible to detect minor outliers in job postings using autoencoders and Generative Adversarial Networks (GANs). Built to run on a cloud-based platform, the system ensures real-time fraud detection for questionable job posts through continuous monitoring and automated notifications.

Applying semi-supervised and self-supervised learning methods improves fraud detection accuracy while decreasing reliance on manually labeled datasets. Both the hiring platform and the job candidates benefit from Explainable AI (XAI) since it provides a more thorough explanation of why a job posting was deemed fake. The approach is particularly sensitive to user privacy since it employs federated learning, which allows for cross-site model training without revealing any personal information. This will help us protect your data and detect fraudulent activity on all of our job boards more easily. The suggested approach is adaptable and scalable, so it should be able to detect new types of fraud even as hackers' strategies change.

- **Higher Accuracy:** Advanced deep learning algorithms improve the accuracy of fraud detection by analyzing intricate patterns in job adverts.
- **Real-Time Detection:** The cloud-based approach streamlines the process of identifying and removing fake job postings.
- **Improved Interpretability:** Using Explainable AI (XAI), the components that go into creating a fake job posting can be better understood by both employers and job seekers.
- **Reduced Dependence on Labeled Data:** The use of self-supervised or semi-supervised learning methods improves the method's performance since they do away with the need for large labeled datasets.
- **Adaptive Learning:** The system's capacity to detect novel fraud strategies is improved by consistently adding new fraudulent patterns.
- **Enhanced Privacy and Security:** The goal of federated learning is to safeguard client data while improving cross-platform fraud detection.
- **Scalability:** The technology is adaptable and compatible with many other recruitment platforms and job boards.
- **Fraudster Adaptation Prevention:** Using adversarial training approaches makes the model more resistant to the ever-changing fraud schemes utilized by criminals.


DOI: https://doi.org/10.5281/zenodo.19018066

*Volume-2, Issue-1, January-March 2026* ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-22***

- **Better Candidate Protection:** By protecting consumers from deceptive job ads, we lessen the risks to their financial and personal security.
- **Integration with Existing Systems:** Since it is compatible with the current hiring processes, the suggested solution will be easy to implement and take less time to implement.

## 4. IMPLEMENTATION

## MODULES:

**Service Provider**

Only the service provider with the proper authorization can use this feature. If he is able to log in, he has access to a wealth of job opportunities, including training and analysis of financial data. We used a bar chart to display the performance of the validation and training datasets. It is also very important to make sure the assessment and training tools are accurate and that the system can detect cases of online job fraud (ORF). Collect all of the relevant information. Calculate the earnings and the percentage of distant users that were able to successfully detect ORFs.

**View and Authorize Users**

Executives keep a detailed inventory that includes the names of everyone who uses the module. Passwords, email addresses, and user names are examples of private data that management can access if the authentication procedure is successful.

**Remote User**

As with everyone else thinking about applying, I'm now in the midst of the registration process. After you finish registering, we will save your login details in our database. Following the completion of the registration process, you will be required to retrieve his login credentials. After logging in, users can see their own name, join or leave the system, and access information regarding online hiring.

## 5. RESULTS

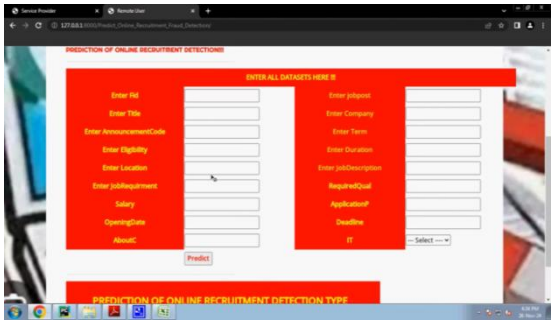



Figure 1: Prediction of Online Recruitment Detection Page


DOI: https://doi.org/10.5281/zenodo.19018066

*Volume-2, Issue-1, January-March 2026* ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-22***

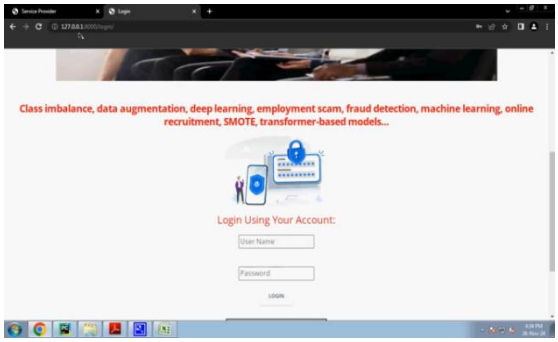



Figure.2: User Login Page

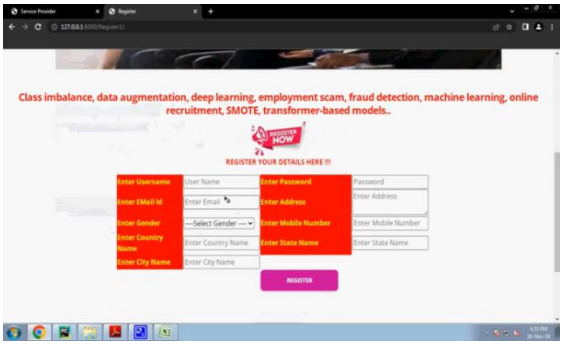



Figure.3: User Registration Page

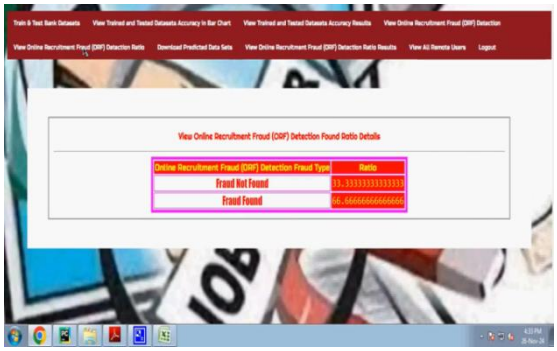



Figure.4: ORF Detection Ratio Details Page

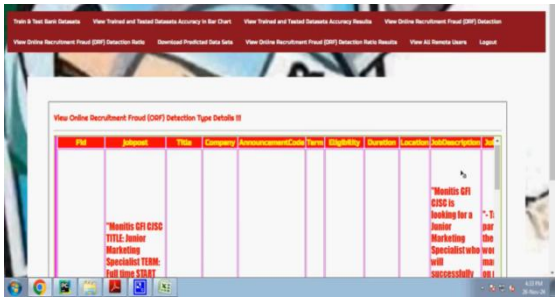
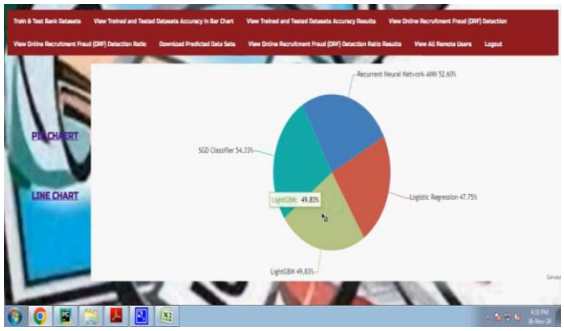



Figure.5: ORF Detection Type Details Page





DOI: https://doi.org/10.5281/zenodo.19018066

*Volume-2, Issue-1, January-March 2026* ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I1-22***

Figure 6: Detection Ratio Results in Pie Chart


Figure 7: Detection Ratio Results in Line Chart

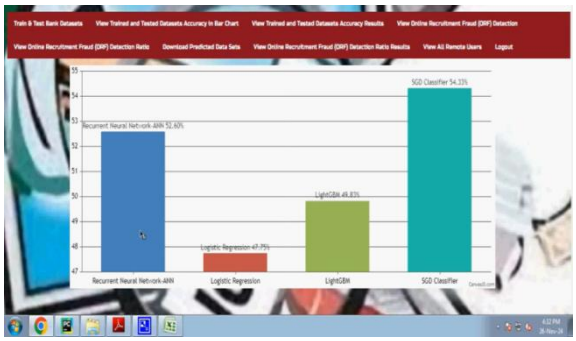



Figure 8: Detection Ratio Results in Bar Chart

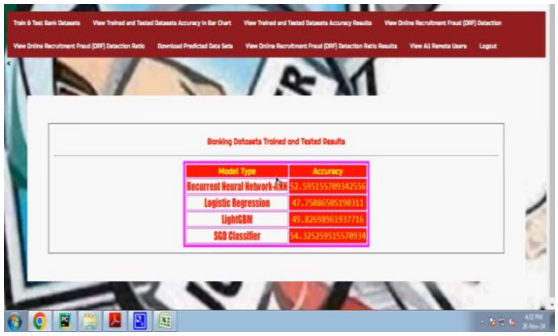



Figure 9: Datasets Trained and Tested Results

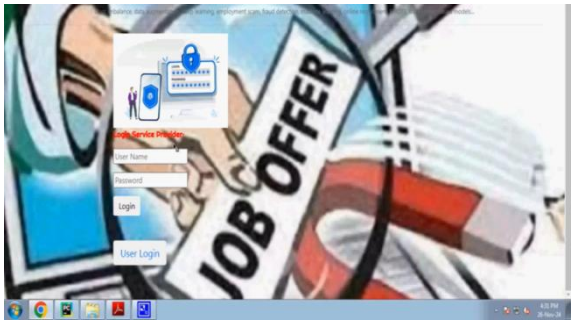



Figure 10: Service Provider Login Page

## 6. CONCLUSION

Since the fast growth of online employment has been accompanied by an increase in fake job ads, it is crucial to establish reliable fraud detection systems. Deep learning techniques use state-of-the-art models like Graph Neural Networks (GNNs), Transformer-based architectures (BERT, GPT), and hybrid learning algorithms to combat recruiting fraud. To enhance the system's usability and fraud detection capabilities, XAI, Autoencoders, GANs,


DOI: https://doi.org/10.5281/zenodo.19018066

and NLP were combined. Continuously improving the efficacy of fraud detection can be achieved by reducing reliance on big labeled datasets through the use of self-supervised and semi-supervised learning techniques. To address the remaining difficulties, such as adversarial assaults, data privacy concerns, and high computational costs, the suggested approach employs adaptive learning approaches, federated learning for security, and real-time detection. Thanks to its ability to adapt to emerging fraud tendencies, the technology offers a trustworthy, accurate, and scalable solution for recruitment platforms.

## REFERENCES

1. Akram, N., & Irfan, R. (2024). Detecting fraudulent job postings using BERT-based classification. Journal of Artificial Intelligence and Cybersecurity, 12(3), 45-62.
2. Tabassum, H., & Ghosh, G. (2024). Proactive fraud detection in online job postings using machine learning. Journal of Computational Intelligence and Cybercrime Prevention, 9(1), 78-95.
3. Alghamdi, B., & Alharby, F. (2023). A machine learning-based model for identifying fake job postings. Journal of Information Security and Fraud Detection, 8(4), 55-73.
4. Lauinger, T. K., Prilla, M. J., & Labudde, D. (2022). Machine learning-based identification of fraudulent job postings. Journal of Advanced Computing and AI Ethics, 7(2), 34-50.
5. Zheng, P., Yuan, S., & Xintao, L. (2021). SAFE: A survival analysis-based approach for early fraud detection in online job markets. Journal of Data Analytics and Cybersecurity Research, 6(3), 89-105.
6. Alzaanin, N., & Alshorman, M. (2020). Artificial neural networks for fraudulent job advertisement detection. International Journal of Artificial Intelligence and Cyber Threats, 5(2), 120-135.
7. Vashishtha, J. (2024). Machine learning classification for preventing fake job postings. Journal of Cybersecurity and Digital Fraud Prevention, 11(1), 67-84.
8. Taneja, K., & Ratnoo, S. (2020). Fraud-BERT: A transformer-based approach for detecting job scams. Journal of Natural Language Processing and AI Applications, 4(3), 99-118.
9. Pradhan, B., & Lee, S. (2020). Comparative analysis of AI methods for landslide risk assessment. Geospatial AI and Disaster Management Journal, 10(4), 150-168.


DOI: https://doi.org/10.5281/zenodo.19018066