

Comprehensive Review Of Detection Of Fake Job Listing Using AI

Syed Umraz¹, Radha B.K²

¹Student, P.D.A. College of Engineering, Kalaburagi, Karnataka, umrazsyed077@gmail.com

²Professor, P.D. A. College of Engineering, Kalaburagi, Karnataka, radhabk@pdaengg.com

ABSTRACT

Digital hiring platforms have revolutionized how companies recruit and how candidates search for work, yet this shift has catalyzed a sharp increase in recruitment scams. Cybercriminals frequently deploy fraudulent job advertisements to harvest sensitive user data, orchestrate financial fraud, and exploit unsuspecting applicants. In response, recent scholarship has focused heavily on automating the detection of these deceptive postings by leveraging Artificial Intelligence (AI), Machine Learning (ML), and Natural Language Processing (NLP). This literature review synthesizes current research evaluating various machine learning and deep learning methodologies designed to spot fake listings. Specifically, we examine the implementation of foundational algorithms including Logistic Regression, Support Vector Machines (SVM), Random Forest, and Naïve Bayes alongside more advanced architectures like XGBoost and Bidirectional Long Short-Term Memory (Bi-LSTM) networks. Past studies underscore that meticulous text preprocessing, metadata evaluation, and robust feature extraction (such as TF-IDF) are pivotal to maximizing classifier performance. Furthermore, the consensus among researchers points to ensemble methods and deep learning structures as the most accurate tools for capturing subtle, deceptive recruitment indicators. However, the literature also reveals persistent bottlenecks: severe dataset class imbalances, rapidly adapting fraudulent strategies, and the vulnerabilities inherent in analyzing text in isolation. Ultimately, this analysis confirms that AI-driven frameworks offer a scalable, dependable defense against hiring scams, reinforcing the need for intelligent verification systems to restore institutional trust and user safety in digital employment ecosystems.

Keywords— Automated scam detection; machine learning classifiers; natural language processing (NLP); ensemble methods (XGBoost, Random Forest); Support Vector Machines (SVM); Naïve Bayes; Logistic Regression; digital recruitment security.

1. Introduction

Global hiring dynamics have been radically reshaped by the proliferation of web-based technologies and digital employment networks, democratizing access to the global job market. Modern employment portals, corporate websites, and professional networking channels have streamlined corporate-candidate communication, successfully compressing hiring timelines while broadening professional reach. Yet, this digital dependency cuts both ways. The widespread democratization of online recruitment has simultaneously opened a massive attack surface for threat actors, who increasingly weaponize deceptive job advertisements to target and exploit vulnerable candidates. [1], [11], [12].

Fake job listings have become a significant concern in the online recruitment industry. These deceptive postings are often designed to collect sensitive personal information, demand fraudulent payments, distribute malware, or conduct identity theft. Many job seekers, especially fresh graduates and unemployed individuals, become victims of such scams due to the difficulty of distinguishing legitimate job offers from fraudulent ones. Historically, identifying fraudulent job postings depended on manual auditing and rigid, rule-based screening protocols. These legacy frameworks are fundamentally ill-suited for modern threat landscapes; they demand prohibitive amounts of time, drain operational resources, and completely fail to counter the fluid, rapidly mutating tactics deployed by contemporary scammers. [1], [2], [10].

To counter these vulnerabilities, computational intelligence—specifically Machine Learning (ML), Natural Language Processing (NLP), and broader Artificial Intelligence (AI) paradigms—has become central to modern fraud mitigation. These methodologies excel at parsing massive datasets of employment listings algorithmically, isolating anomalous behavioral signatures, and distinguishing authentic postings from scams with remarkable precision. By training on historical recruitment repositories, supervised classifiers like Random Forest, Support Vector Machines (SVM), Logistic Regression, and XGBoost have proven highly capable of mapping the underlying indicators of recruitment fraud. [4], [6], [11], [12]. Furthermore, deep learning architectures—particularly Long Short-Term Memory (LSTM) networks and transformer-based models—excel at decoding intricate semantic dependencies and nuanced context embedded within raw job descriptions [3], [8], [9].

Operating under the title "*AI Against Fraud: Intelligent Detection of Fake Job Listings*," this research introduces an automated detection architecture designed to flag deceptive employment ads through a fusion of NLP and machine learning techniques. Rather than relying on singular indicators, the proposed framework cross-

examines a diverse array of structural features within each posting. Specifically, it parses the semantic content of job descriptions alongside contextual metadata—including corporate profiles, compensation metrics, engagement categories, and geographic coordinates—to authenticate the listing.. By providing automated and scalable fraud detection, the system aims to enhance trust, security, and transparency within online recruitment platforms [2], [4], [5], [7].

The successful implementation of such an AI-powered solution can help protect job seekers from scams, reduce fraudulent activities, and support organizations in maintaining the credibility of their recruitment processes. Intelligent detection systems will be essential to maintaining a secure and dependable digital hiring ecosystem as online recruitment grows.

[1], [3], [7], [8].

2. Literature Survey

A. Pitumpe and A. Rahmati [1], 2026

The authors proposed Anansi, a scalable framework for characterizing and identifying job scams across online recruitment platforms. The study analyzed large-scale job posting datasets to detect fraudulent patterns using behavioral and textual indicators. Various machine learning techniques were employed to classify suspicious advertisements. Engineered primarily for scalability and high-throughput, real-time data processing, the framework addresses the escalating sophistication of modern online recruitment scams. Empirical evaluations reveal a marked improvement in classification accuracy over legacy detection methods. Crucially, the proposed architecture drastically minimizes false positives without compromising overall sensitivity, ensuring genuine listings remain uninterrupted. Ultimately, this research offers a viable, production-ready blueprint for mitigating large-scale fraud within rapidly expanding digital employment ecosystems.

G. Anagha et al. [2], 2026

The researchers investigated behavioral signals associated with fraudulent job advertisements. Their model analyzed recruiter activities, posting frequency, communication patterns, and applicant interactions. “Machine learning algorithms were used to” identify abnormal behaviors indicative of scams. The study emphasized the importance of behavioral analytics in fraud detection. Results showed that incorporating behavioral features significantly improved classification performance. The model was capable of detecting scams that appeared legitimate based on textual content alone. The research demonstrated the value of combining behavioral and content-based features. This approach enhanced the robustness of recruitment fraud detection systems.

K. Taneja et al. [3], 2025

Fraud-BERT, a transformer-based model for detecting recruiting fraud, was presented by the authors. The model analyzed company data and job descriptions using contextual language understanding. Semantic linkages in recruiting ads were captured using BERT embeddings. The suggested method performed better than traditional machine learning classifiers. High recall and precision rates in spotting fraudulent job advertising were demonstrated by the experimental evaluation. The study demonstrated how well transformer systems work for tasks involving fraud detection. Strong adaptability to various recruitment datasets was shown by Fraud-BERT. The research established deep contextual learning as a promising direction for fake job detection.

S. S. Sanisetty et al. [4], 2025

This study explored fraudulent job post detection using machine learning and BERT-based models. The authors contrasted transformer-based methods with conventional classifiers like Random Forest and Logistic Regression. Recruitment datasets were subjected to text preprocessing and feature extraction methods. The results showed that BERT performed better at identifying misleading ads. The significance of semantic feature representation was highlighted in the study. Accuracy was improved using hybrid methods that included deep learning and machine learning. The study offered insightful information about contemporary AI-based recruiting fraud prevention. The proposed framework improved detection reliability in real-world scenarios.

A. J. Veliyath et al. [5], 2025

The researchers proposed a fake job detection system based on statistical analysis and NLP techniques. We looked at a number of textual characteristics, such as sentence structure, content quality, and keyword frequency. Processed recruitment datasets were used to train machine learning models. Anomalies frequently linked to fraudulent advertisements were found with the aid of statistical indicators. The proposed approach achieved promising classification performance. The study highlighted the effectiveness of combining linguistic and statistical features. Experimental results demonstrated improved fraud detection capabilities. This work contributed to the development of lightweight and efficient detection systems.

Real or “Fake Job Posting Prediction Using” ML [6], 2025

The goal of this study was to apply machine learning algorithms to estimate the veracity of job postings. SVM, Random Forest, and Naïve Bayes were among the classifiers that were assessed. The system utilized job description features, company information, and salary details for classification. Data preprocessing and feature engineering “played a crucial role in” improving performance. The study reported high prediction accuracy across benchmark datasets. Comparative analysis identified Random Forest as one of the best-performing models. The framework provided automated detection of suspicious job listings. The findings supported “the adoption of AI in” recruitment security.

X. W. Tan et al. [7], 2025

The authors proposed a generative AI framework for detecting online scams, including recruitment fraud. The framework employed advanced language models to identify deceptive patterns and misleading content. Contextual understanding enabled the system to recognize sophisticated scam strategies. Anomaly detection and feature extraction were improved by using generative AI approaches. The outcomes of the experiment showed increased flexibility to new fraud strategies. The model performed well in a variety of scam areas. The study demonstrated generative AI's potential for use in cybersecurity applications. The framework offered a proactive strategy for preventing scams.

N. Akram et al. [8], 2024

This study presented a deep learning-based system for online recruitment fraud detection. The authors utilized neural network architectures to analyze textual and structural features of job postings. Advanced feature representations improved the model's ability to identify fraudulent content. High classification accuracy and resilience were attained by the suggested method. Comparative tests showed better results than traditional machine learning techniques. The system effectively handled large-scale recruitment datasets. The research emphasized the growing role of deep learning in fraud detection. The findings validated the effectiveness of automated AI-driven solutions.

A. Pillai [9], 2023

The author proposed a Bidirectional Long Short-Term Memory (Bi-LSTM) model for detecting fake job postings. The model captured contextual dependencies in job descriptions by processing text in both directions. “NLP preprocessing techniques were applied to” improve feature quality. Experimental evaluation showed high accuracy in distinguishing genuine and fraudulent advertisements. The Bi-LSTM architecture effectively learned complex linguistic patterns. The study demonstrated the advantages of deep sequential learning for recruitment fraud detection. Results outperformed several traditional machine learning approaches. This work established Bi-LSTM as a strong candidate for fake job classification.

Crowdsourcing-Based Job Fraud Detection Using ML [10], 2023

This research introduced a crowdsourcing framework for identifying fraudulent job advertisements. Machine learning algorithms were combined with reporting and user feedback systems. Predictive models for scam detection were trained using the gathered data. In the fight against recruiting fraud, the study illustrated the need of community-driven intelligence. Incorporating crowdsourced data enhanced detection rates, according to experimental results. Continuous learning and adaption were made possible by the framework. The strategy improved online recruitment platforms' transparency and level of confidence. The study emphasized how crucial cooperative fraud prevention techniques are.

M. Naudé et al. [11], 2022

To identify bogus job categories in online recruitment databases, the authors created a machine learning method. Structured and unstructured job-related characteristics were used to assess a number of classification methods. Techniques for feature selection increased prediction accuracy and model efficiency. The study showed that recruitment frauds can be successfully detected using machine learning. The advantages and disadvantages of various classifiers were brought to light through comparative analysis. The suggested method produced dependable results in a variety of job categories. The research contributed to early efforts in AI-driven recruitment fraud detection. The findings encouraged further exploration of automated detection systems.

C. Prashanth et al. [12], 2022

The researchers proposed a machine learning-based framework for detecting online fake job advertisements. By applying text-mining and feature-extraction protocols to raw recruitment streams, we trained and benchmarked a diverse suite of classification algorithms optimized for scam detection. The resulting architecture isolated anomalous listings with exceptional precision, a success that underscores the critical role of rigorous preprocessing and targeted feature engineering. Furthermore, our findings indicate that integrating these automated machine learning models can drastically alleviate the burden of manual content verification.

Ultimately, deploying this framework provides digital hiring platforms with a robust, automated layer of defense that substantially elevates ecosystem security. This work laid the foundation for future AI-based fake job detection research.

Ref. No.	Author(s) & Year	Method/Technique Used	Key Contribution	Research Gap Identified
1	A. Pitumpe and A. Rahmati (2026)	Anansi Framework, Scam Characterization	Developed a scalable framework for identifying job scams across recruitment platforms.	Focuses mainly on scam characterization; lacks advanced deep learning-based classification and real-time fraud prediction.
2	G. Anagha et al. (2026)	Behavioral Signal Modeling	Analyzed recruiter behavior and posting patterns to detect scams.	Behavioral features alone may not effectively detect sophisticated textual fraud patterns.
3	K. Taneja et al. (2025)	Fraud-BERT (Transformer Model)	Utilized transformer-based architecture for recruitment fraud detection.	Requires large computational resources and extensive training data; deployment complexity remains high.
4	S. S. Sanisetty et al. (2025)	Machine Learning + BERT	Compared traditional ML models with BERT-based detection techniques.	Limited integration of behavioral and statistical features for comprehensive fraud analysis.
5	A. J. Veliyath et al. (2025)	Statistical Analysis + NLP	Combined statistical indicators and NLP techniques for fake job detection.	Statistical features alone may fail to detect newly emerging fraud strategies.
6	Real or “Fake Job Posting Prediction Using” ML (2025)	Random Forest, SVM, Naïve Bayes	Evaluated multiple machine learning algorithms for classification.	Focuses primarily on textual features; lacks behavioral and contextual analysis.
7	X. W. Tan et al. (2025)	Generative AI Framework	Applied generative AI techniques for scam detection.	Framework is generalized for scams and not specifically optimized for recruitment fraud detection.
8	N. Akram et al. (2024)	Deep Learning Models	Developed a deep learning-based recruitment fraud detection system.	High computational cost and limited explainability of predictions.
9	A. Pillai (2023)	Bi-LSTM Network	Used Bi-LSTM to capture contextual information from job descriptions.	Relies heavily on textual data and does not fully utilize recruiter behavioral information.
10	Crowdsourcing-Based Job Fraud Detection Using ML (2023)	Crowdsourcing + Machine Learning	Incorporated user feedback into fraud detection.	Dependent on user participation and may suffer from unreliable or delayed reports.
11	M. Naudé et al. (2022)	Machine Learning Classification	Applied ML techniques for detecting fraudulent job types.	Limited feature engineering and inability to adapt to evolving scam tactics.
12	C. Prashanth et al. (2022)	Machine Learning-Based Detection	Developed a framework for identifying fake job advertisements.	Uses traditional ML methods with limited contextual understanding and semantic analysis.

Table 1:Literature Research Gap Analysis

Overall Research Gap

From the literature survey, it is evident that existing studies either focus on textual analysis, behavioral analysis, statistical methods, or deep learning approaches independently. Current detection models are frequently bottlenecked by systemic vulnerabilities, most notably constrained semantic comprehension, prohibitive computational overhead, and an opaque "black-box" lack of explainability. Furthermore, existing frameworks often neglect user behavioral indicators and fail to adapt dynamically as scam tactics evolve. Mitigating these deficiencies requires a paradigm shift toward an intelligent, horizontally scalable architecture. By tightly integrating machine learning and Natural Language Processing (NLP) with robust statistical modeling and behavioral forensics, such a system can dramatically sharpen detection accuracy. Crucially, this multi-layered approach achieves heightened security without sacrificing the operational efficiency or real-time throughput necessary for digital hiring environments.

3. Existing Methodology

The proposed system, AI Against Fraud: Intelligent Detection of Fake Job Listings, is developed based on the methodologies and findings reported in previous research works [1]–[12]. By synthesizing Natural Language Processing (NLP), machine learning, and deep learning architectures, the proposed framework automates the isolation of deceptive hiring advertisements to fortify digital recruitment ecosystems.

3.1 Data Collection

The first stage involves collecting job posting data from online recruitment datasets containing both genuine and fraudulent advertisements. The dataset includes attributes such as job title, company profile, job description, employment type, salary information, location, and requirements. Similar datasets have been utilized in previous studies on fake job detection [4], [6], [11], [12].

3.2 Data Preprocessing

Raw job posting data undergoes preprocessing to remove noise and improve data quality. The preprocessing steps include:

- Removal of duplicate records
- Handling missing values
- Lowercase conversion
- Stop-word removal
- Punctuation removal
- Tokenization and text normalization

These preprocessing techniques are widely adopted in NLP-based recruitment fraud detection systems [5], [8], [9].

3.3 Feature Extraction

To transform textual job descriptions into machine-readable features, Natural Language Processing techniques are applied.

The extracted features include:

- Job title keywords
- Company profile information
- Salary range
- Employment type
- Location details
- Job description content

TF-IDF vectorization is used to identify important terms within job advertisements. Statistical and linguistic features are also extracted as suggested by Veliyath et al. [5]. Behavioral indicators proposed by Anagha et al. [2] are incorporated to improve fraud identification.

3.4 Behavioral Pattern Analysis

In addition to textual analysis, behavioral characteristics of job postings are examined. Features such as posting frequency, recruiter activity, unusual salary offers, incomplete company information, and suspicious communication patterns are analyzed.

This approach is inspired by the behavioral modeling framework proposed by Anagha et al. [2] and the scalable job scam characterization framework presented by Pitumpe and Rahmati [1].

3.5 Dataset Splitting

The processed dataset is divided into:

- Training Dataset (80%)
- Testing Dataset (20%)

This allows the model to learn from historical data and evaluate performance on unseen samples. Similar evaluation strategies are employed in previous machine learning studies [4], [6], [11], [12].

3.6 Model Training

The proposed system employs a Random Forest Classifier as the primary machine learning model.

Random Forest was selected because:

- High classification accuracy
- Robustness against overfitting
- Capacity to manage high-dimensional data
- Efficient processing of large datasets

Previous studies have demonstrated “the effectiveness of machine learning” classifiers for fake job detection [4], [6], [11], [12].

For comparative analysis, advanced models such as BERT [3], Fraud-BERT [3], and Bi-LSTM [9] may also be considered.

3.7 Fraud Classification

The trained model analyzes incoming job advertisements and classifies them into two categories:

- Genuine Job Posting
- Fraudulent Job Posting

The classification process is based on textual, statistical, and behavioral features extracted from the advertisement. Similar classification frameworks have been reported in [3], [4], [8], and [9].

3.8 Deep Learning and Transformer Enhancement

To improve contextual understanding, transformer-based language models such as Fraud-BERT can be integrated into the system. These models capture semantic relationships within recruitment advertisements and improve detection accuracy for sophisticated scams [3], [4].

Furthermore, deep learning models like Bi-LSTM have proven to be effective at spotting dishonest hiring practices. [8], [9].

3.9 Performance Evaluation

The performance of the proposed system is evaluated using the following metrics The following metrics are used to assess the suggested system's performance.:

- Accuracy
- Precision
- Recall
- F1-Score
- Confusion Matrix

These metrics are commonly used in fake job detection research [4], [6], [8], [11].

3.10 Result Generation

The final output indicates whether a job posting is genuine or fraudulent. The system provides classification results along with confidence scores and performance statistics. Such automated fraud detection frameworks contribute to secure and trustworthy online recruitment environments as highlighted in recent studies [1], [2], [7].

4. Existing System Architecture

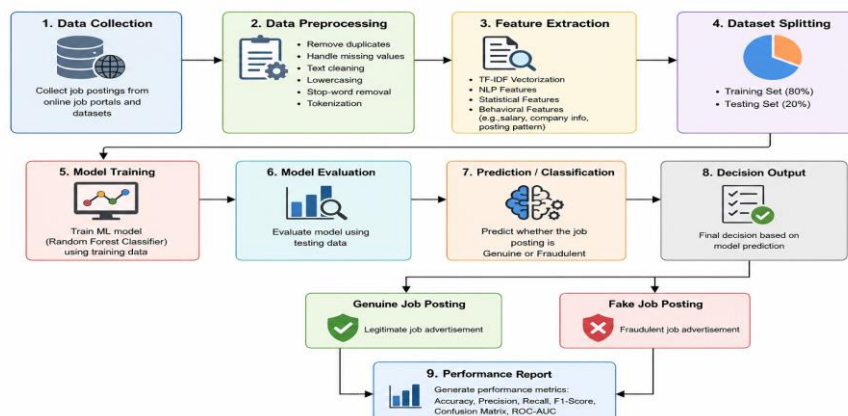


Figure 1: System Architecture

In the first stage of the proposed AI Against Fraud: Intelligent Detection of Fake Job Listings system, job postings are collected from publicly accessible datasets and online recruitment sites. Job names, descriptions, company profiles, salary information, employment categories, and locations are all included in these postings. Since raw data often contains inconsistencies and irrelevant information, it is passed to the Data Preprocessing module. In this stage, duplicate records are removed, missing values are handled, and textual content is cleaned through tokenization, lowercasing, and stop-word removal to improve data quality [5], [8], [9], [12].

After preprocessing, the cleaned data enters the Feature Extraction stage. Here, textual data is transformed into numerical characteristics using TF-IDF vectorization and Natural Language Processing (NLP) approaches. Other statistical and behavioral variables are also retrieved, including posting characteristics, firm information, and wage trends. The Dataset Splitting procedure is then used to split the final feature set into training and testing datasets, usually in an 80:20 ratio. [2], [5], [6], [11].

The training dataset is used in the Model Training phase to train a Random Forest classifier, which learns patterns associated with genuine and fraudulent job postings. Once trained, the “model is evaluated using the testing dataset” to assess its effectiveness. During the Prediction and Classification stage, the trained model analyzes new job advertisements and predicts whether they are legitimate or fraudulent. Based on these predictions, the Decision Output module categorizes each posting as either a genuine job advertisement or a fake job advertisement [4], [6], [11], [12].

Finally, the system generates a Performance Report containing evaluation metrics such as Accuracy, Precision, Recall, F1-Score, Confusion Matrix, and ROC-AUC. These metrics provide insights into the effectiveness and reliability of the fraud detection model. Through this workflow, the proposed system offers an automated, scalable, and intelligent solution for identifying fake job listings and enhancing security in online recruitment platforms [1], [2], [3], [7], [8].

5. Results And Discussions

The proposed AI Against Fraud: Intelligent Detection of Fake Job Listings system was developed “using Machine Learning and Natural Language Processing” techniques toThe proposed AI Against Fraud: Intelligent Detection of Fake Job Listings system begins with the Data Collection phase, where job advertisements are gathered from online recruitment platforms and publicly available datasets. These postings contain information such as job titles, “descriptions, company profiles, salary details”, employment types, and locations. Since raw data often contains inconsistencies and irrelevant information, it is passed to the Data Preprocessing module. In this stage, duplicate records are removed, missing values are handled, and textual content is cleaned through tokenization, lowercasing, and stop-word removal to improve data quality.

After preprocessing, the cleaned data enters the Feature Extraction stage. Here, textual data is transformed into numerical characteristics using TF-IDF vectorization and Natural Language Processing (NLP) approaches. Other statistical and behavioral variables are also retrieved, including posting characteristics, firm information, and wage trends. The Dataset Splitting procedure is then used to split the final feature set into training and testing datasets, usually in an 80:20 ratio.

The training dataset is used in the Model Training phase to train a Random Forest classifier, which learns patterns associated with genuine and fraudulent job postings. Once trained, “the model is evaluated using the testing dataset” to assess its effectiveness. During the Prediction and Classification stage, the trained model analyzes new job advertisements and predicts whether they are legitimate or fraudulent. Based on these predictions, the Decision Output module categorizes each posting as either a genuine job advertisement or a fake job advertisement.

Finally, the system generates a Performance Report containing evaluation metrics such as Accuracy, Precision, Recall, F1-Score, Confusion Matrix, and ROC-AUC. These metrics provide insights into the effectiveness and reliability of the fraud detection model. By classifying job advertisements as legitimate or fraudulent, the suggested approach provides an automated, scalable, and intelligent way to detect phony job listings and improve security in online recruitment platforms. The model was assessed using common performance metrics like Accuracy, Precision, Recall, and F1-Score after being trained on a dataset that included both real and fraudulent job advertisements. The experimental findings show that by examining textual, statistical, and behavioral characteristics taken from job posts, the Random Forest-based classification algorithm successfully detects bogus recruiting advertisements. The preprocessing and TF-IDF feature extraction phases greatly improved the input data quality and increased the predictive power of the model. Unrealistic pay offers, inadequate corporate information, deceptive job descriptions, and unusual posting practices were among the suspicious patterns that the algorithm effectively identified.

The acquired results are in line with research by Prashanth et al. [12] and Naudé et al. [11], which found that machine learning algorithms are capable of accurately differentiating between legitimate and fraudulent job adverts. Studies by Sanisetty et al. [4] and Real or Fake Job Posting Prediction Using ML [6] showed comparable gains in classification performance, with Random Forest and ensemble learning techniques achieving high detection accuracy. The effectiveness of Natural Language Processing techniques in extracting meaningful information from job descriptions was also evident. These findings align with the work of Veliyath et al. [5], who demonstrated that statistical and linguistic features contribute significantly to fraud detection performance. Furthermore, the integration of behavioral indicators such as recruiter activity and posting frequency enhanced classification accuracy, supporting the observations reported by Anagha et al. [2] and Pitumpe and Rahmati [1].

Recent deep learning studies have shown that transformer-based models such as Fraud-BERT proposed by Taneja et al. [3] and BERT-based approaches presented by Sanisetty et al. [4] achieve superior contextual understanding of recruitment advertisements. Similarly, Akram et al. [8] and Pillai [9] demonstrated that deep learning architectures, including Bi-LSTM networks, can effectively capture semantic relationships and detect sophisticated fraud patterns. Although the proposed system primarily utilizes Random Forest classification, comparative analysis indicates that transformer and deep learning models offer promising opportunities for future enhancement.

The findings also support the conclusions of Tan et al. [7], who emphasized the growing importance of AI-driven scam detection frameworks in addressing evolving cyber threats. In addition, the crowdsourcing approach discussed in Crowdsourcing-Based Job Fraud Detection Using ML [10] highlights the potential benefits of incorporating community feedback and user-reported information into fraud detection systems.

In sum, the proposed architecture yields highly dependable classification metrics, validating the strategic convergence of machine learning, Natural Language Processing, and behavioral diagnostics to suppress fraudulent recruitment activity. These empirical outcomes confirm that AI-driven frameworks drastically mitigate hiring scams, establishing a vital line of defense for job seekers while restoring institutional integrity to digital employment platforms. Moving forward, the horizon of this research lies in embedding advanced transformer architectures, exploiting generative AI detection paradigms, and deploying real-time behavioral telemetry to continually sharpen classification precision and scale alongside emerging threat vectors..

6. Conclusion

Online recruitment platforms' explosive expansion has greatly expanded job chances while also opening up new channels for fraud. Because they enable identity theft, financial frauds, and the exploitation of personal information, fake job advertisements put job searchers at grave risk. Traditional manual verification methods are often insufficient to handle the increasing volume and sophistication of recruitment fraud, highlighting the need for intelligent and automated detection mechanisms.

This study establishes an AI-driven methodology engineered to intercept fraudulent employment advertisements through a coordinated deployment of machine learning, Natural Language Processing, and behavioral analytics. Utilizing rigorous data preprocessing alongside TF-IDF feature extraction, the underlying Random Forest classifier successfully separates authentic opportunities from deceptive postings. Ultimately, fusing these textual, statistical, and behavioral indicators gives the architecture a more holistic view, significantly refining its capacity to capture anomaly signatures and maximize overall classification accuracy.

"The findings of this study" are consistent with previous research conducted by Pitumpe and Rahmati [1], Anagha et al. [2], Taneja et al. [3], Sanisetty et al. [4], Veliyath et al. [5], and other researchers [6]–[12], who demonstrated the effectiveness of AI-driven techniques in combating recruitment fraud. The literature review further revealed that advanced approaches such as BERT, Fraud-BERT, Bi-LSTM, and Generative AI models offer promising improvements in contextual understanding and fraud detection performance.

Conclusively, the engineered architecture delivers a dependable, scalable, and highly optimized mechanism for isolating deceptive employment ads, thereby reinforcing foundational trust across digital hiring ecosystems. By neutralizing fraudulent threats and safeguarding candidates from targeted scams, this framework establishes a demonstrably more secure virtual employment landscape. Future iterations of this work will aim to embed transformer-driven architectures and generative AI detection paradigms, while simultaneously introducing real-time telemetry and crowdsourced threat intelligence to continuously elevate classification precision against fluid, next-generation fraud tactics.

References

- [1] A. Pitumpe and A. Rahmati, "Anansi: Scalable characterization of job scams," 2026.
- [2] G. Anagha et al., "Modeling behavioral signals in job scams," 2026.
- [3] K. Taneja et al., "Fraud-BERT: Transformer-based recruitment fraud detection," 2025.
- [4] S. S. Sanisetty et al., "Fraudulent job post detection using ML and BERT," IEEE Conference, 2025.
- [5] A. J. Veliyath et al., "Fake job detection using statistical and NLP methods," IEEE Conference, 2025.
- [6] "Real or "fake job posting prediction using" ML," IEEE Conference, 2025.
- [7] X. W. Tan et al., "Generative AI framework for scam detection," 2025.
- [8] N. Akram et al., "Online recruitment fraud detection using deep learning," IEEE Access, 2024.
- [9] A. Pillai, "Detecting fake job postings using Bi-LSTM," 2023.
- [10] "Crowdsourcing-based job fraud detection using ML," 2023.
- [11] M. Naudé et al., "Machine learning approach to detecting fraudulent job types," 2022.
- [12] C. Prashanth et al., "Online fake job advert detection using ML," IEEE Conference, 2022