International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 2, 2026

Jobscan AI Fake Job Detection System Using Deep Learning And NLP

J Lavanya[1], A.Kranthi[2], M.Mallika Reddy[3], A.Sreeja[4]

[1]Assistant Professor;Department Of Computer Science Engineering(AI&ML) Bhoj Reddy Engineering College For Women Hyderabad India

[2,3,4]B.Tech Students; Department Of Computer Science Engineering(AI&ML) Bhoj Reddy Engineering College For Women Hyderabad India

Mail Id; kranthialikanti@gmail.com[2],reddy-mallikareddymodugu@gmail.com[3], sreejareddyadudodla@gmail.com[4]

Abstract

The rapid expansion of online recruitment platforms has significantly simplified the hiring process for organizations and job seekers. However, this digital transformation has also led to a rise in fraudulent job advertisements, where cybercriminals exploit job portals to deceive applicants and obtain financial or personal information. Consequently, detecting fake job postings has become a critical challenge in the domain of cybercrime and online security. This study proposes a transformer-based approach for identifying fraudulent job advertisements using Bidirectional Encoder Representations from Transformers (BERT) and Robustly Optimized BERT Pretraining Approach (RoBERTa). A novel dataset is constructed by integrating job listings collected from three different sources to address the limitations of existing benchmark datasets, which are often outdated and restricted in diversity. Exploratory Data Analysis (EDA) reveals a significant class imbalance issue, which negatively impacts classification performance. To address this challenge, ten advanced variants of the Synthetic Minority Oversampling Technique (SMOTE) are implemented to balance the dataset. The effectiveness of these sampling techniques is evaluated using the proposed deep learning models. Experimental results demonstrate that all approaches perform competitively, while the combination of BERT with the SMOBD SMOTE variant achieves the best performance with approximately 90% balanced accuracy and recall. The results highlight the effectiveness of transformer-based architectures combined with advanced resampling strategies for detecting fraudulent job postings.

Keywords: *Fake Job Detection, Cybercrime, Online Recruitment Fraud, BERT, RoBERTa, SMOTE, Deep Learning, Natural Language Processing*

Introduction

Rapid developments in digital technology have transformed many everyday activities, including the way organizations recruit employees and how individuals search for jobs. Online recruitment platforms, commonly referred to as e-recruitment systems, enable companies to advertise job vacancies and allow candidates to explore employment opportunities conveniently from anywhere. These platforms provide significant advantages such as reduced recruitment costs, faster hiring processes, and access to a broader pool of applicants. The adoption of online recruitment increased substantially during the COVID-19 pandemic, when unemployment rates rose and organizations relied heavily on digital hiring solutions.Despite these benefits, the widespread use of online job portals has also created opportunities for cybercriminals to exploit job seekers through fraudulent job advertisements. Employment scams have become a growing concern in the digital recruitment ecosystem. Fraudsters often post deceptive job listings to collect sensitive personal information, request upfront payments, or manipulate candidates into financial transactions. Such fraudulent activities may result in privacy violations, financial losses for job seekers, and reputational damage for legitimate organizations. Many job seekers remain unaware of the risks associated with online recruitment fraud (ORF), which increases their vulnerability to these deceptive practices.Several research efforts have attempted to address the problem of detecting fraudulent job postings using computational techniques. Earlier studies primarily focused on traditional machine learning algorithms and ensemble methods to classify job advertisements as legitimate or fraudulent. More recent approaches have explored neural network architectures and feature-based models for improved detection accuracy. However, the potential of advanced transformer-based deep learning models has not been extensively investigated in the context of online recruitment fraud detection.To address these limitations, the present research proposes an approach that leverages modern transformer-based architectures for identifying fake job postings. A new dataset is constructed by integrating legitimate and fraudulent job advertisements obtained from multiple data sources. This helps overcome the limitations of existing benchmark datasets, which are often outdated and limited in scope. Furthermore, Exploratory Data Analysis (EDA) of the collected dataset reveals the presence of a significant class imbalance problem, a common challenge in fraud detection tasks where fraudulent

cases occur far less frequently than legitimate ones. To mitigate this issue and enhance classification performance, oversampling techniques such as the Synthetic Minority Oversampling Technique (SMOTE) are employed to balance the dataset and improve the model's ability to detect fraudulent job postings.

Existing System

A variety of computational techniques have been applied to identify fraudulent job advertisements in online recruitment platforms. Traditional machine learning algorithms have been widely used for this purpose, including Random Forest, Decision Trees, Naïve Bayes, and Support Vector Machines (SVM). These approaches typically depend on feature engineering techniques to transform textual job descriptions into numerical representations. Methods such as Term Frequency–Inverse Document Frequency (TF-IDF) and word embedding models are commonly utilized to extract relevant textual patterns that can assist in distinguishing between genuine and fraudulent job postings.In addition to classical machine learning techniques, deep learning models have also been explored to improve detection performance. Architectures such as Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) have demonstrated the ability to automatically learn complex features from textual data without extensive manual feature engineering. These models capture semantic relationships and contextual information from job descriptions, which enhances the accuracy of fraud detection systems.More recently, transformer-based architectures have emerged as a powerful approach in natural language processing tasks. Models such as Bidirectional Encoder Representations from Transformers (BERT) and Robustly Optimized BERT Pretraining Approach (RoBERTa) provide improved contextual understanding by analyzing words in relation to their surrounding context within a sentence. Due to their superior language representation capabilities, these models have shown promising results in various text classification applications. Consequently, transformer-based models are increasingly being considered as effective tools for identifying fraudulent job postings within online recruitment platforms.

Literature Survey

The rapid expansion of digital technologies has significantly transformed the recruitment landscape, enabling organizations to advertise job vacancies and recruit candidates through online platforms. These online recruitment systems provide advantages such as faster hiring processes, wider access to talent, and reduced operational costs. However, the increasing reliance on digital recruitment platforms has also resulted in a growing number of Online Recruitment Fraud (ORF) cases. In such situations, cybercriminals create fraudulent job advertisements with the intention of misleading job seekers, often to obtain financial payments, steal sensitive personal information, or exploit confidential data. As the number of online employment scams continues to increase, researchers have focused on developing automated systems capable of identifying and filtering fraudulent job postings.One of the earliest contributions in this field was presented by Vidros et al. (2017), who introduced the Employment Scam Aegean Dataset (EMSCAD), a benchmark dataset widely used for detecting fake job advertisements. In their study, several traditional machine learning algorithms, including Naïve Bayes, Logistic Regression, Decision Trees, and Random Forest, were applied to classify job postings as legitimate or fraudulent. Their work provided an important foundation for subsequent research in online recruitment fraud detection. Building upon this work, Dutta and Bandyopadhyay (2020) conducted a comparative analysis of multiple machine learning techniques such as Multi-Layer Perceptron (MLP), K-Nearest Neighbors (KNN), and Decision Trees (DT). They also investigated ensemble learning techniques, including Adaptive Boosting (AdaBoost) and Gradient Boosting (GB). Among the evaluated models, the Random Forest classifier demonstrated the best performance with an accuracy of approximately 98.27%, highlighting the effectiveness of ensemble-based learning methods for fraud detection tasks.Similarly, Lal et al. (2020) explored the application of ensemble voting strategies to improve classification performance in fake job detection systems. Their approach combined voting mechanisms such as Maximum Voting, Majority Voting, and Average Voting with machine learning algorithms including Random Forest, Logistic Regression, and J48 decision trees. The results of their study showed promising outcomes, achieving an overall classification accuracy of 95.5%. In addition to traditional machine learning methods, researchers have also investigated deep learning approaches for detecting fraudulent job postings. For instance, Habiba et al. (2020) utilized deep neural networks (DNN) to analyze textual features of job advertisements and reported an accuracy of nearly 99%. Their findings demonstrated that deep learning models are capable of learning complex patterns and contextual relationships present in textual job data, making them highly effective for classification tasks.Despite the high accuracy achieved by many existing approaches, the problem of class imbalance remains a major challenge in detecting fraudulent job postings. In most recruitment datasets, the number of fraudulent job advertisements is significantly smaller compared to legitimate job postings. This imbalance can cause machine learning models to

become biased toward predicting the majority class, resulting in a higher number of misclassified fraudulent cases. Consequently, although a model may report high overall accuracy, its ability to correctly identify fraudulent job postings may still be limited. To address this issue, researchers often employ oversampling techniques such as the Synthetic Minority Oversampling Technique (SMOTE), which generates synthetic samples for the minority class. By balancing the dataset, SMOTE helps improve the model's ability to detect fraudulent job postings more effectively. Therefore, addressing class imbalance remains a critical factor in developing reliable and accurate online recruitment fraud detection systems.

Requirement Analysis

Requirement analysis is an essential stage in the development of a software system, as it helps identify the functional and operational needs required for the successful implementation of the system. In the proposed fake job detection system, requirement analysis focuses on defining the system's functional capabilities, quality attributes, and computational resources necessary for efficient operation.The functional requirements describe the specific operations that the system must perform in order to detect fraudulent job postings. The system includes a data preparation module responsible for loading the dataset and performing essential preprocessing tasks. These tasks include handling missing values, removing duplicate records, and processing categorical data to ensure data consistency. Feature selection and scaling techniques are applied to enhance the quality of the input data and improve model performance. Since the dataset used in this research contains an imbalance between legitimate and fraudulent job postings, several variants of the Synthetic Minority Oversampling Technique (SMOTE) are implemented to balance the data and improve the model's ability to detect minority class instances.Another important component of the system is the model training module. In this stage, textual job data is processed using tokenization methods compatible with transformer-based models such as BERT and RoBERTa. The tokenized text is then used to train the classification models, enabling them to learn contextual patterns and relationships within the job descriptions. Hyperparameter tuning is performed during the training process to optimize the performance of the models. Various evaluation metrics, including accuracy, precision, recall, and balanced accuracy, are used to assess the effectiveness of the trained models in identifying fraudulent job postings.The system also includes a prediction module that provides a user-friendly web interface for interacting with the trained model. Through this interface, users can input job descriptions or job-related information. The system processes the input text and sends it to the trained classification model, which predicts whether the job advertisement is legitimate or fraudulent. The prediction result is then displayed to the user through the interface, enabling users to verify the authenticity of job postings.The successful implementation of the proposed fake job detection system also depends on adequate computational resources. From a hardware perspective, the system requires a processor equivalent to Intel i3 or higher, at least 4 GB of RAM for efficient model training and execution, and a minimum of 500 GB of storage space. In terms of software requirements, the system is implemented using the Python programming language within the Jupyter Notebook development environment. The web interface is developed using frontend technologies such as HTML, CSS, and JavaScript, while the Flask framework is used to integrate the machine learning model with the web application. SQLite is utilized as the database system to store and manage relevant application data.

Design

System Architecture

The system architecture of the proposed Fake Job Detection System illustrates the overall workflow and interaction between different components involved in identifying fraudulent job postings. The architecture begins with the data acquisition stage, where job posting data is collected from multiple sources containing both legitimate and fraudulent advertisements. The collected data then passes through a preprocessing phase where missing values are handled, duplicate records are removed, and categorical attributes are encoded. After preprocessing, the dataset undergoes feature engineering and class imbalance handling using SMOTE-based oversampling techniques to improve the representation of fraudulent job postings.Following data preparation, the processed dataset is used for training transformer-based deep learning models such as BERT and RoBERTa. These models analyze the contextual relationships within job descriptions and learn patterns that distinguish genuine postings from fraudulent ones. Once the models are trained, they are integrated into a prediction system that allows users to input job details. The system processes the input data and provides a prediction indicating whether the job posting is legitimate or fraudulent. The system architecture therefore integrates data processing, model training, and prediction modules into a unified framework for automated fraud detection.

Technical Architecture

The technical architecture describes the technological components used to implement the fake job detection system. The architecture consists of a frontend interface, backend processing layer, machine learning model, and data storage components. The frontend interface is designed

using web technologies such as HTML, CSS, and JavaScript, which enable users to enter job descriptions and view prediction results through an interactive interface. The backend layer is implemented using the Python programming language and the Flask web framework, which facilitates communication between the user interface and the machine learning model.The machine learning component includes natural language processing techniques and transformer-based deep learning models such as BERT and RoBERTa. These models process textual job descriptions and perform classification tasks to determine whether the job advertisement is legitimate or fraudulent. The dataset used for training and evaluation is stored in CSV format, and the SQLite database is used to manage system data. This layered architecture ensures efficient integration between the user interface, data processing modules, and the deep learning model.

Implementation

The implementation of the proposed fake job detection system focuses on identifying fraudulent job advertisements using advanced deep learning techniques. The system is designed to analyze textual job descriptions and determine whether a job posting is legitimate or fake. The implementation process consists of multiple stages, including user interaction, data processing, model training, evaluation, and prediction.Initially, a user interface is developed to allow users to enter job descriptions or upload job posting details. The system then collects job posting data from multiple datasets containing both legitimate and fraudulent advertisements. The collected data undergoes preprocessing to remove missing values, eliminate duplicate records, and encode categorical attributes. These preprocessing steps ensure that the dataset is clean and suitable for model training.After preprocessing, feature engineering techniques are applied to select relevant features and prepare the data for deep learning models. Since fraudulent job postings represent a minority class in most datasets, class imbalance is addressed using SMOTE-based oversampling techniques. These methods generate synthetic samples for the minority class and improve the model's ability to detect fraudulent postings.The processed dataset is then used to train transformer-based deep learning models such as BERT and RoBERTa. These models utilize contextual language understanding to analyze job descriptions and identify patterns associated with fraudulent advertisements. Once the models are trained, they are evaluated using performance metrics such as accuracy, recall, and classification reports.The trained model is integrated into a prediction system that allows users to verify job postings. When a user submits a job description, the system processes the input text, applies tokenization, and sends the data to the trained model. The model then predicts whether the job posting is fake or genuine. The prediction result is displayed to the user through the interface. Additionally, the system records prediction results and model performance metrics for monitoring and analysis.

Technologies Used

The implementation of the fake job detection system relies on several technologies across different layers of the application. The frontend interface is developed using HTML, CSS, and JavaScript to create a responsive and user-friendly interface for entering job details and displaying prediction results. The backend processing is implemented using Python, which provides powerful libraries for machine learning and natural language processing. The Flask framework is used to connect the frontend interface with the backend machine learning model and enable communication between system components.

Testing

Testing is a critical phase in the development of the fake job detection system, as it ensures the reliability, accuracy, and overall performance of the application. The system utilizes deep learning models such as BERT and RoBERTa to classify job postings as either legitimate or fraudulent. The testing process focuses on verifying the functionality of different modules, including data preprocessing, model training, prediction, and system integration.The testing phase involves validating several aspects of the system, including dataset loading and preprocessing operations, handling of missing and duplicate data, and the implementation of class imbalance handling techniques such as SMOTE. Additionally, the performance of the deep learning models is evaluated using metrics such as accuracy, recall, and loss. The system's prediction outputs are also tested to ensure that the model correctly classifies job postings and provides accurate results. Furthermore, testing confirms that the trained model performs consistently when applied to both training data and unseen datasets, ensuring reliability in real-world scenarios.

Dimensions of Testing

Different dimensions of testing are considered to ensure the quality of the system. Functionality testing verifies that the system correctly classifies job postings as fake or genuine based on the trained model. Performance testing evaluates the efficiency and speed of data processing and model prediction. Security testing ensures that the system protects user data and prevents unauthorized access or misuse of system resources.

Stages of Testing

The testing process is conducted in several stages to ensure comprehensive evaluation of the system. Unit testing is performed to examine each module individually, including dataset preprocessing, feature engineering, SMOTE-based oversampling,

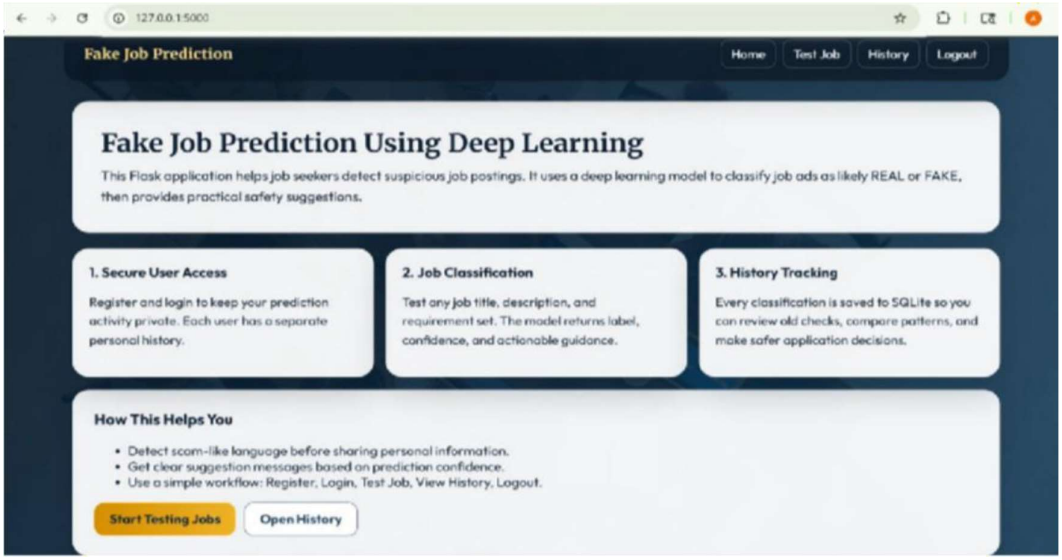
International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

model training, and prediction modules. Integration testing ensures that different modules work together seamlessly, including the interaction between data preprocessing, model training, evaluation metrics, and the prediction interface. System testing evaluates the entire system as a whole, verifying that job datasets are processed correctly, fraudulent postings are accurately detected, and prediction results are displayed appropriately within the application.

Types of Testing

Both white box testing and black box testing are used to evaluate the system. White box testing focuses on verifying the internal logic of the system, including preprocessing steps, feature encoding methods, SMOTE implementation, and deep learning model training procedures. Black box testing evaluates the system based on input-output behavior without examining the internal code. Various scenarios are tested, including job postings with incomplete information, suspicious content, and legitimate job descriptions. The system successfully classifies these inputs and produces accurate prediction results.

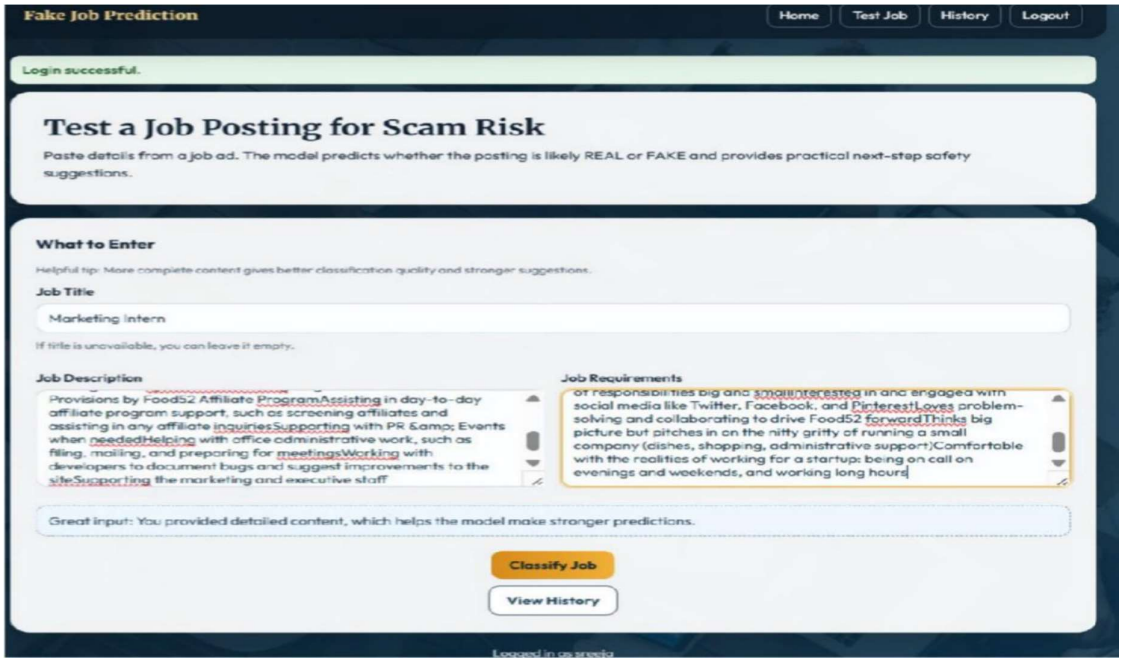
Screenshots



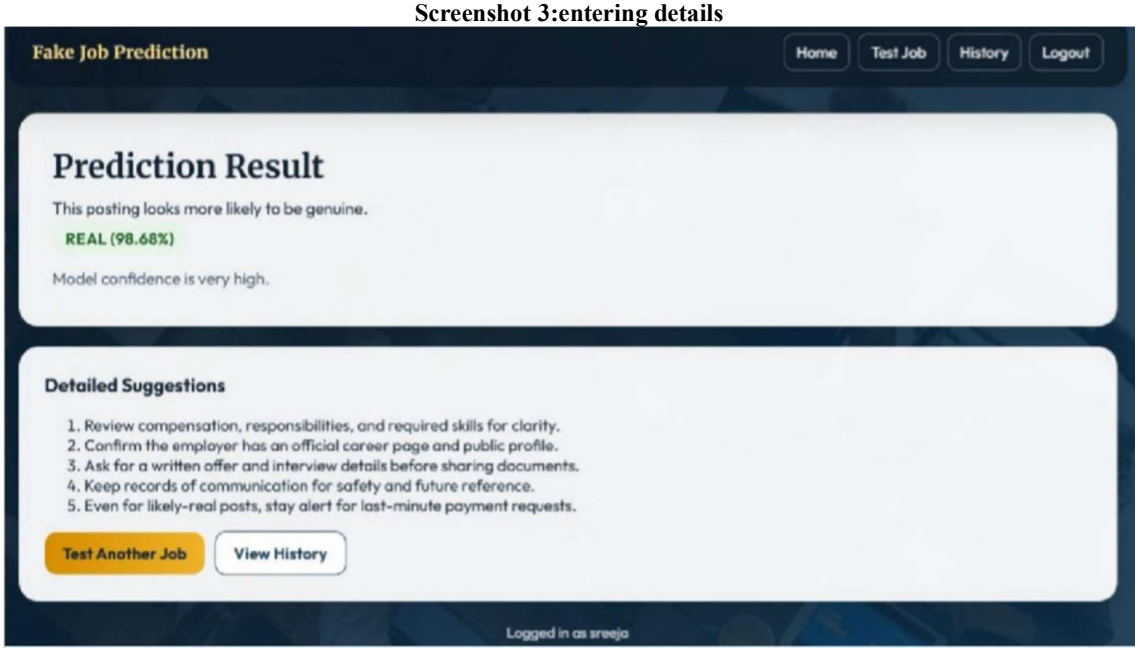
Screenshot 1:Home Page

Screenshot 2:Prediction

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026



Screenshot 3:entering details



Screenshot 4:Result(real)

Conclusion

The increasing prevalence of fraudulent job advertisements on online recruitment platforms has created significant challenges for job seekers and organizations. To address this issue, the proposed system employs advanced transformer-based deep learning models, specifically BERT and RoBERTa, to identify fake job postings. These models provide a strong contextual understanding of textual data, enabling more accurate classification of job descriptions compared to traditional machine learning methods. By leveraging the contextual language representation capabilities of transformer architectures, the system can effectively distinguish between legitimate and fraudulent job advertisements.In addition to the use of transformer-based models, the study addresses the common problem of class imbalance in fraud detection datasets. A combined dataset containing job postings collected from multiple sources was utilized to improve the diversity and relevance of training data. Furthermore, several variants of the Synthetic Minority Oversampling Technique (SMOTE) were applied to balance the dataset and enhance the model's ability to identify minority class instances. The experimental evaluation demonstrated that

applying SMOTE-based balancing techniques significantly improved recall and detection capability for fraudulent job postings.Among the evaluated methods, the combination of the BERT model with the SMOBD oversampling technique achieved the best performance in terms of balanced accuracy and recall. This result indicates that the proposed approach is effective in detecting fraudulent job advertisements while maintaining reliable classification performance. Overall, the developed system contributes to improving the safety and reliability of online recruitment platforms by enabling users to verify the authenticity of job postings. Such systems can assist job seekers in avoiding employment scams and support organizations in maintaining trustworthy digital hiring environments.

Future Scope

Although the proposed system demonstrates promising performance in detecting fraudulent job postings, several improvements can be explored in future research. One potential direction is the development of multilingual fraud detection models. Currently, many fake job detection systems primarily focus on English-language job postings. Expanding the system to support multiple languages would enable detection of fraudulent advertisements across global job platforms and improve its applicability in international recruitment environments.Another potential improvement involves integrating explainable artificial intelligence (XAI) techniques into the model. While transformer-based models provide strong predictive capabilities, they often operate as black-box systems. Incorporating interpretable AI methods would allow the system to provide explanations for its predictions, helping users understand why a particular job posting is classified as fraudulent.Future work may also focus on implementing real-time monitoring systems capable of scanning online job portals continuously. Such systems could automatically detect suspicious job advertisements and flag them before they reach potential victims. Additionally, maintaining and expanding the dataset with newly collected job postings would allow the system to adapt to evolving fraud patterns and emerging scam strategies. Continuous dataset updates would further improve model robustness and ensure long-term effectiveness in detecting recruitment fraud.

References

[1] P. Kaur, “E-recruitment: A conceptual study,” *International Journal of Applied Research*, vol. 1, no. 8, pp. 78–82, 2015.

[2] C. S. Anita, P. Nagarajan, G. A. Sairam, P. Ganesh, and G. Deepakkumar, “Fake job detection and analysis using machine learning and deep learning algorithms,” *Revista Gestão Inovação e Tecnologias*, vol. 11, no. 2, pp. 642–650, 2021.

[3] A. Raza, S. Ubaid, F. Younas, and F. Akhtar, “Fake e-job posting prediction based on advanced machine learning approaches,” *International Journal of Research Publication and Reviews*, vol. 3, no. 2, pp. 689–695, 2022.

[4] Australian Cyber Security Centre, “Online fraud report,” Accessed: Jun. 19, 2022. [Online]. Available: https://www.cyber.gov.au/acsc/report

[5] J. Howington, “Survey: More millennials than seniors victims of job scams,” FlexJobs, Sep. 2015. Accessed: Jan. 2024. [Online]. Available: https://www.flexjobs.com/blog/post/survey-results-millennials-seniors-victims-job-scams