International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Online Recruitment Fraud Detection

Dr. P. S. Gholap[1], Dr. S. S. Khatal[2], Mahima Nanasaheb Nawale[3], Minal Goraksh Tattu[4], Vivek Sanjay Maval[5]

[1,2]Professor, Department of Computer Engineering, Sharadchandra Pawar College of Engineering and Technology, Junnar, Pune, Maharashtra, India
[3,4,5]Student, Department of Computer Engineering, Sharadchandra Pawar College of Engineering and Technology, Junnar, Pune, Maharashtra, India

Abstract
Job seekers and companies may now connect more easily thanks to the fast expansion of online job boards. however, it has also increased the number of fraudulent job postings that exploit applicants by requesting personal information, financial payments, or misleading employment offers. Traditional manual verification methods are not sufficient to detect such scams since there are so many job ads and fraudsters are always coming up with new ways to trick people. To address this problem, this project proposes an Online Recruitment Fraud Detection System that automatically identifies fake job advertisements that use a mix of rule-based filtering and machine learning methods. The system collects job descriptions from recruitment platforms and performs text stages for preprocessing, such as normalization, getting rid of unnecessary characters, and lemmatization to get the data ready for analysis. The TF-IDF (Term Frequency–Inverse Document Frequency) method is used to find relevant text patterns after preprocessing, which converts the textual content into numerical feature vectors suitable for machine learning models. A Logistic Regression classifier is then applied to analyze these features and determine the probability that a job posting is genuine or fraudulent. In addition, a rule-based filtering mechanism checks for suspicious indicators such as unrealistic salary offers, missing company information, unusual email domains, and commonly used scam phrases. The outputs from both the machine learning model and rule-based filtering are combined using hybrid logic to produce the final prediction. This integrated approach improves detection accuracy by identifying both obvious and subtle fraud patterns.
The system ultimately provides a clear result indicating whether the job posting is real or fake along with a confidence level, helping online recruitment platforms reduce manual review efforts, improve security, and protect job seekers from recruitment scams.

Index Terms: Online Recruitment Fraud Detection, Machine Learning, TF-IDF, Logistic Regression, Natural Language Processing, Fraud Detection System, Cybersecurity.

I. INTRODUCTION

The quick growth of internet technologies has significantly transformed the recruitment process by enabling organizations to advertise job opportunities and interact with potential candidates through various online platforms. Job portals, company career pages, and professional networking websites have simplified the employment process by giving instant access to a lot of applicants. However, along with these advantages, the growth of Online job boards have also made it easier for people to create fake job

openings. Cybercriminals exploit these platforms to publish fake job advertisements that promise attractive salaries, easy hiring procedures, or remote work opportunities in order to deceive job seekers and obtain personal or financial information from them. As a result, recruitment fraud has become a major concern for both job seekers and organizations in the digital era [1].

Fraudulent recruitment activities often involve impersonating legitimate companies, creating convincing job descriptions, and communicating with victims through emails or messaging platforms to gain their trust. Victims may be asked to pay application processing fees, training costs, or security deposits before receiving employment confirmation. In many cases, these fraudulent activities lead to a loss of money, identity theft, and the wrong use of personal information. Because so many job listings are made every day on recruitment sites, it is hard to keep up. Verification of each listing becomes difficult and inefficient. Traditional filtering techniques based on simple rules or keyword matching are also limited in their ability to detect complex or well-designed scam advertisements [2].

Recent progress in natural language processing and machine learning has made it possible to automatically detect By looking at text trends and finding odd aspects in job ads, you can find fake job advertising. Machine learning models can examine job descriptions, company information, salary details, and communication patterns to identify anomalies associated with recruitment scams. Several studies have demonstrated that combining text mining techniques with classification algorithms Logistic Regression, Random Forest, and deep learning models, for example, can make it much easier to find fraud in online recruitment systems. [3]. These intelligent systems can assist recruitment platforms in automatically screening job postings, reducing the risk of fraud, and protecting job seekers from potential scams.

In this project, an Online Recruitment Fraud Detection System is proposed to identify fraudulent job postings using a mix of rule-based filtering and machine learning approaches. The system processes job descriptions through text preprocessing, feature extraction utilizing TF-IDF with a Logistic Regression model to sort job postings into real and fake categories. By integrating automated detection mechanisms, the proposed system aims to enhance security in online recruitment platforms, reduce reliance on manual verification, and improve trust among users in digital hiring environments [4].

II. PROBLEM STATEMENT

The increasing use of online recruitment platforms has made job searching more convenient for applicants and employers; however, it has also created opportunities for cybercriminals to post fraudulent job advertisements that deceive job seekers. These fake job postings often promise attractive salaries, quick hiring processes, or work-from-home opportunities to lure applicants into sharing personal information or paying unnecessary fees [5]. Due to the large number of job listings published daily, manually verifying each posting is difficult and time-consuming for recruitment platformsMost current detection methods depend on simple rule-based filtering or user reports., which are not effective in identifying sophisticated fraud patterns. Therefore, there is a need to develop an automated and intelligent system capable of analyzing job postings, detecting suspicious patterns, and accurately identifying fraudulent recruitment advertisements to protect job hunters and keep faith in online job boards [6].

III. RELATED WORK

A. Literature Survey

Dr. S. S. Khatal, Dr. P. S. Gholap, Miss. Tattu Minal Goraksh, Miss. Nawale Mahima Nanasaheb, and Mr. Maval Vivek Sanjay (2025) presented a study on seeing fake job ads on websites that help people find

jobs using machine learning and explainable artificial intelligence techniques, published in the International Journal of Innovative Research in Technology (IJIRT). The study suggests a multi-model approach that incorporates several machine learning algorithms such as Multilayer Perceptron (MLP), Passive Aggressive Classifier, Gradient Boosting, and K-Nearest Neighbors to improve the detection accuracy of fake job advertisements[6]. The system performs comprehensive data preprocessing including text cleaning, normalization, tokenization, and feature encoding to prepare high-quality input data for model training. Important features such as job description, company logo, education requirements, experience details, and email domain are analyzed to identify suspicious patterns in recruitment posts. The framework also introduces a trust score mechanism that evaluates the credibility of each job post and categorizes it as suspicious, doubtful, or verified real based on prediction confidence. Additionally, explainable AI techniques are used to generate reasoning reports that explain why a particular job post is classified as fake or genuine, improving transparency and user trust. The system also supports real-time analysis of job postings and recruitment emails and provides visualization of fraud trends across different platforms and job categories, making it a practical and scalable solution for protecting job seekers from online recruitment scams and enhancing security in digital hiring environments.

Online recruitment fraud has become a big issue with the rapid growth of digital job portals, attracting the attention of many researchers who have proposed intelligent detection systems using machine learning and text mining techniques. Dutta and Bandyopadhyay presented An strategy that uses machine learning to find fake job postings by looking at job advertisement data collected from online recruitment platforms. In their study, different classification algorithms like Random Forest, Decision Tree, K-Nearest Neighbor, and Naïve Bayes were implemented to identify fake job listings. The research highlighted that ensemble learning methods provide better detection accuracy compared to single classifiers and emphasized the importance of data preprocessing and feature extraction for improving classification performance [1].

Alghamdi and Alharby suggested an intelligent approach for finding online recruitment fraud by applying machine learning and feature selection methods. Their approach utilized the Random Forest algorithm combined with Support Vector Machine for feature selection to analyze job advertisement data. The study focused on identifying important attributes such as company profile, job description, salary information, and company logo to detect fraudulent postings. The results showed that the suggested model worked.High prediction accuracy and significantly improved the detection of fraudulent recruitment activities compared to traditional filtering methods [2].

Another important study was conducted by Prasad, Sravya, Kavya, and Kavitha, who introduced a deep learning based approach for identifying fraudulent job advertisements. Their research applied Natural Language Processing techniques to analyze textual patterns in job descriptions and detect suspicious phrases commonly used in scam postings. The system also incorporated metadata analysis to examine additional information such as job location, company details, and how to get in touch. The suggested model has a high rate of detection accuracy and showed that deep learning techniques can effectively identify complex fraud patterns in recruitment platforms [3].

Taneja, Vashishtha, and Ratnoo put forward a model based on transformers, known as Fraud-BERT for detecting online recruitment fraud. Their approach used transfer learning with BERT to understand contextual relationships in job descriptions and improve fraud detection accuracy. Unlike traditional text classification methods, the model was capable of understanding semantic meaning and contextual information within job advertisements. The proposed system was better at finding fake job advertisements

than standard machine learning algorithms including Logistic Regression, Support Vector Machine, and Naïve Bayes, according to experimental results. [4].

Similarly, Anitha, Naga Malleswarao, and Ajay developed a deep learning based framework that utilized Convolutional Neural Networks (CNN) to look at text data from job ads. The technology was made to find fake ads on its own. By identifying hidden patterns in job descriptions and company information. The research demonstrated that deep learning models can effectively capture complex relationships within recruitment data and improve fraud detection performance when compared with traditional machine learning techniques [5].

Overall, previous studies indicate that machine learning and deep learning approaches play an important role in identifying fake job ads on websites that help people find jobs. Natural Language Processing and other methods, feature extraction, and classification algorithms have proven effective in detecting suspicious patterns in job postings. These research contributions highlight the need for intelligent automated systems capable of identifying recruitment fraud and protecting job seekers from online scams.

Comparison Table

Sr. No	Author(s)	Year	Technique Used	Contribution
1	Khatal et al.	2025	MLP, Gradient Boosting, KNN, Explainable AI	Multi-model system with trust score to detect fake job postings.
2	Dutta & Bandyopadhyay	2021	Naïve Bayes, Decision Tree, Random Forest	Machine learning approach for identifying fraudulent job advertisements.
3	Alghamdi & Alharby	2020	Random Forest + SVM	Feature-based model analyzing job details to detect recruitment fraud.
4	Prasad et al.	2022	Deep Learning with NLP	Detects scam job posts by analyzing text patterns in descriptions.
5	Taneja et al.	2023	BERT Transformer	Context-based model improving accuracy in fraud detection.
6	Anitha et al.	2021	CNN	Deep learning model for detecting fraudulent recruitment posts.

IV. PROPOSED SYSTEM

The proposed method is intended to autonomously identify fake job advertisements on online recruitment platforms using a hybrid approach that combines rule-based filtering and machine learning techniques.

The system analyzes the textual content of job advertisements and identifies suspicious patterns that indicate recruitment fraud. The architecture consists of several stages including data input, text preprocessing, feature extraction, machine learning classification, rule-based filtering, hybrid decision logic, and final prediction. This multi-stage pipeline helps Make fraud detection more accurate and dependable while cutting down on manual verification efforts [5].

1. Text Input

The first stage of the system involves collecting job advertisement data from online recruitment platforms. The input may include job title, business name, job description, and pay information, job requirements, and contact information. This textual information is submitted by recruiters or collected from job portals and serves as the primary dataset for analysis. The system accepts this raw text data and prepares it for further processing [6].

2. Text Preprocessing

Before applying machine learning techniques, the input data must be cleaned and standardized. In this stage, the system performs several preprocessing operations such as converting Convert text to lowercase, get rid of punctuation and special characters, and remove stop words, and normalizing whitespace. This step helps remove unnecessary or irrelevant information and ensures that the text data is in a format that is easy to analyze and consistent [7].

3. Lemmatization

Lemmatization is used to change words into their base or root form. For example, words such as “running,” “runs,” and “ran” are converted to their base form “run.” This procedure helps lower the number of dimensions in the data and makes sure that words that are similar are handled the same. term during analysis. Lemmatization improves how well the machine learning model works by providing meaningful and standardized textual features.

4. Feature Extraction

After preprocessing and lemmatization, the system converts textual data using the TF-IDF (Term Frequency–Inverse Document Frequency) method to turn them into numbers. TF-IDF tells you how important a word is in a document compared to the whole dataset. This change lets machine learning algorithms look at textual information effectively and identify patterns associated with fraudulent job postings.

5. Machine Learning Algorithm

The extracted features are provided to a machine learning algorithm for classification. In the proposed system, Logistic Regression is used as the classification model. Logistic Regression is a supervised learning approach that works well for issues with two possible answers. It calculates the probability that a given job posting belongs to either the legitimate or fraudulent category based on the features extracted from the job description.

6. Rule-Based Filter

The system employs both machine learning analysis and a rule-based filtering approach to detect obvious fraud patterns. This filter checks for suspicious indicators such as unrealistic salary offers, missing company details, suspicious email domains, and commonly used scam phrases. If these predefined rules are triggered, the system flags the job posting as potentially fraudulent.

7. Hybrid Logic (Rule + Machine Learning)

To improve accuracy, the outputs from the rule-based filter and machine learning model are combined using hybrid logic. This mechanism prioritizes strong rule-based indicators while also considering

machine learning predictions for complex fraud patterns. By combining both approaches, the system reduces false positives and improves detection reliability.

8. Final Prediction

After analyzing the results from both detection methods, the system generates the final prediction indicating if the job posting is real or fake. The prediction may also include a confidence score showing the probability of fraud [9].

A. Objectives

The main objectives of this undertaking are:

- To create a system that can automatically find fraudulent job postings in real-time.
- To integrate rule-based filtering and machine learning techniques for accurate fraud detection.
- To minimize financial and personal data risks for job seekers by identifying scams before they cause harm.
- To provide confidence-based predictions that allow platforms to implement tiered response strategies.
- To enable continuous learning and adaptation to evolving recruitment fraud patterns.

B. System Architecture

The Online system's architecture. Recruitment Fraud Detection System follows a multi-stage process to analyze job postings and identify whether they are genuine or fraudulent. First, the system receives text input in the form of a job description or recruitment advertisement. This input data is then passed through a text preprocessing stage where unnecessary symbols, stop words, and formatting errors are removed to clean the data. After preprocessing, lemmatization is applied to convert words into their base forms, which helps improve the accuracy of text analysis.

Next, a cleaned text is converted in to number data using feature extraction techniques such as TF-IDF helps the machine figure out how important the words in the job description. Then, these traits are processed by a machine learning algorithm, specifically Logistic Regression, to predict the probability that a job posting is fake At the same time, the system also applies a rule-based filter that checks for suspicious patterns such as unrealistic salary offers, missing company information, or suspicious email domains [11].

The outputs from the machine learning model and rule-based filter are combined using hybrid logic, which improves the accuracy of fraud detection. Finally, the system generates a final prediction indicating whether the job advertising is real or false, and the system shows the outcome as output to help protect job seekers from recruitment fraud.

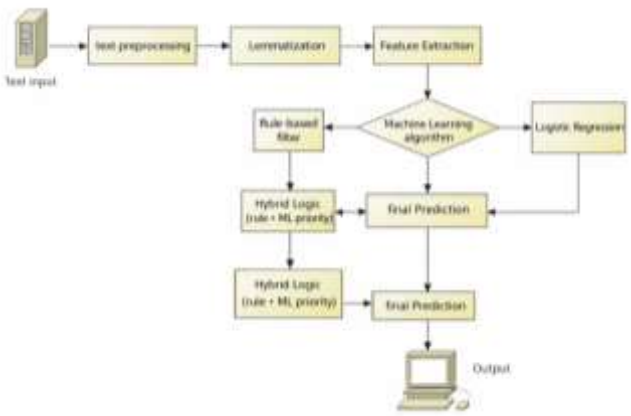

Fig. 1 System Diagram

C. Module Descriptions

1. Data Input Module

The Data Input Module is responsible for collecting job posting information from recruitment platforms or system users. The input data may include job title, company details, job description, salary information, location, and contact details. This module acts as the entry point of the system where job advertisements are submitted for analysis. The collected data is stored and forwarded to the preprocessing module for further processing and fraud detection analysis [8].

2. Text Preprocessing Module

The Text Preprocessing Module prepares the raw textual data for analysis by cleaning and standardizing the content. This module performs operations such as converting text into lowercase, removing punctuation marks, eliminating stop words, and removing unnecessary characters or HTML tags. These steps ensure that the text data becomes consistent and suitable for machine learning processing, thereby improving the efficiency and accuracy of fraud detection [9].

3. Lemmatization Module

The Lemmatization Module converts words into their root or base forms to reduce variations in the dataset. For example, words such as "running," "runs," and "ran" are converted into the base word "run." This process helps reduce the complexity of textual data ,it allows a machine learning model to recognize similar words as the same feature, which improves classification performance [10].

4. Feature Extraction Module

A Feature Extraction Module transforms the processed transforming text data into numbers using methods like TF-IDF (Term Frequency–Inverse Document Frequency). TF-IDF tells you how important terms in a job description are compared to the rest of the dataset. This step enables the system to convert textual content into structured numerical characteristics applicable in machine learning algorithms for classification tasks [11].

5. Machine Learning Classification Module

The Machine Learning Classification Module applies the Logistic Regression algorithm to analyze the extracted features and predict whether a job posting is genuine or fraudulent. Logistic Regression is a supervised learning method that is used to solve issues with two options. The model calculates a probability score based on the input features and classifies the job advertisement into either legitimate or fraudulent categories [12].

6. Rule-Based Filtering Module

The Rule-Based Filtering Module identifies obvious signs of fraud by applying predefined rules and conditions. This module checks for suspicious keywords, unrealistic salary offers, missing company information, unusual email domains, or requests for payment from applicants. If any suspicious pattern is detected, the system flags the job posting as potentially fraudulent. This rule-based mechanism acts as the first line of defense against simple recruitment scams [13].

V. METHODOLOGY

The methodology of the Online Recruitment Fraud Detection System focuses on developing an automated framework capable of identifying fraudulent job postings using a mix of text processing techniques and the machine learning algorithms. A proposed approach follows a systematic workflow that begins with collecting job advertisement data and ends with generating a prediction that decides if the job posting is real or fake. A system is designed to improve the reliability of online recruitment platforms Help keep job

seekers safe from potential scams.

Initially, the system collects job advertisement data that contains information such the job title, business name, job description, and pay information, job requirements, and contact information. This data serves as a primary input for a fraud detection system. Since the collected information is in textual form and may contain irrelevant characters or inconsistent formatting, the next step involves text preprocessing. During this stage, the textual data is cleaned by turning all words into lowercase, taking off punctuation marks, and getting rid of stop words, and removing unnecessary symbols or HTML tags. These preprocessing operations help standardize the data and prepare it for further analysis.

After preprocessing, the system performs lemmatization to convert words into their base or root forms. This step reduces variations in words and ensures that words with similar meanings are treated as the same feature during analysis. For example, words such as “running,” “runs,” "ran" and "run" are both changed to the root word "run." Lemmatization helps make the dataset smaller and speeds up the process of extracting features.

Once the text has been cleaned and normalized, the system performs feature extraction using the TF-IDF (Term Frequency–Inverse Document Frequency) technique. TF-IDF converts the textual data into numerical vectors by figuring out how important words are in a document compared to the whole dataset. Words that show up a lot in one job description but not in others get more weight. This step lets the machine learning algorithm to identify important keywords and patterns associated with fraudulent job postings.

The extracted features are then provided to a machine learning classification model, specifically Logistic Regression, which is used to classify job advertisements into two categories: genuine or fraudulent. Logistic Regression is good for issues with two possible outcomes. It finds the chance that a job ad belongs to a certain group class based on the weighted features generated during the feature extraction stage. The model is trained using labeled datasets so that it can learn patterns that tell the difference between real job postings and fake ones.

In addition to machine learning analysis, the system also applies a rule-based filtering mechanism to detect obvious signs of recruitment fraud. This module checks for suspicious keywords, unrealistic salary offers, missing company information, unusual email domains, or requests for payment from applicants. These predefined rules help the system quickly identify common scam indicators and flag suspicious job postings.

Finally, the outputs from both the machine learning classifier and the rule-based filter are combined using a hybrid decision approach. This integration improves the accuracy of fraud detection by capturing both simple and complex fraud patterns. The system then produces the final prediction indicating whether a job advertisement is real or fake. The system shows the user the outcome. interface, helping administrators and job seekers identify suspicious job postings and maintain a safer online recruitment environment.

A. Technology Stack

- **Coding Language – Python 3.12.0:**
  Python is used as the main programming language for developing the system. It is widely used for machine learning, data processing, and text analysis because of its powerful libraries and simplicity.
- **Web Framework – Flask:**
  Flask is used to build the backend of the application. It helps connect the machine learning model with the web interface and handles requests, responses, and data processing.
- **Frontend – HTML, CSS, JavaScript:**

Use HTML, CSS, and JavaScript to design the user interface. These technologies allow users to enter job descriptions and view the fraud detection results in an interactive and user-friendly web page.

B. Implementation and Training

- **Data Collection:** Job posting data is collected from recruitment datasets containing both genuine and fraudulent job advertisements. This dataset is used to train and evaluate the fraud detection system.
- **Data Preprocessing:** The collected text data is cleaned by converting it to lowercase, removing punctuation, stop words, and unnecessary characters to make the dataset suitable for analysis.
- **Text Normalization and Lemmatization:** Words in the dataset are converted into their root form using lemmatization to reduce word variations and improve the accuracy of text analysis.
- **Feature Extraction:** The TF-IDF (Term Frequency–Inverse Document Frequency) method changes the preprocessed text into numbers so that machine learning algorithms can work with it..
- **Model Training:** The retrieved features are utilized to train the Logistic Regression machine learning model for the classification of job ads as authentic or fake..
- **Model Evaluation:** The trained model is tested using evaluation metrics such as accuracy and prediction results to ensure the system can correctly identify fraudulent job advertisements.
- **System Integration:** The Flask-based web app has the trained machine learning model built into it. This lets users enter job descriptions and get fraud detection results using the web interface.

VI. EVALUATION AND OUTCOMES

1. System Initialization Interface

Fig 2: Interface

The system successfully initializes the CYBERGUARD Threat Detection System, which serves as the main interface for detecting fraudulent job posts, scam emails, and suspicious URLs. The interface confirms that the AI model has been loaded and the system is ready to receive user input. This dashboard provides the main analysis hub where users can select different detection options such as job analysis, email scanning, or URL verification.

2. Fake Job Detection Result

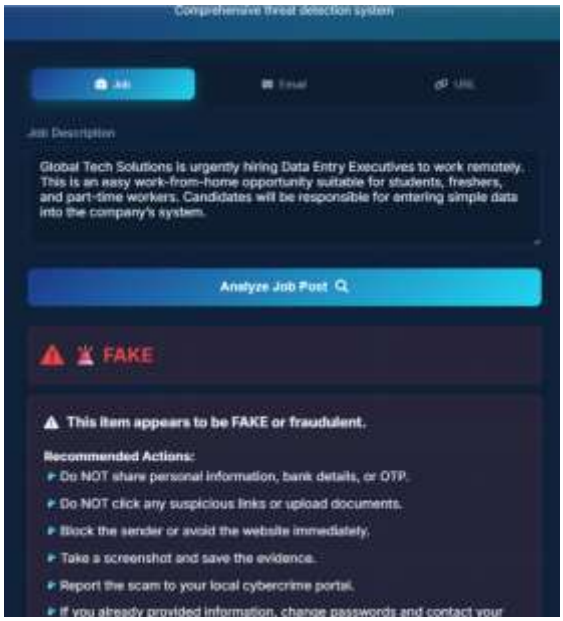

Fig 3: Analysis

The system analyzes the job description entered by the user and processes the text using preprocessing, feature extraction, and the trained machine learning model. After analysis, the system identifies the job posting as FAKE, indicating that the advertisement contains suspicious patterns such as unrealistic salary offers, vague job descriptions, or suspicious contact details. The system also provides safety recommendations, such as avoiding sharing personal information, not clicking suspicious links, and reporting the scam to cybercrime authorities.

3. Threat Monitoring Dashboard

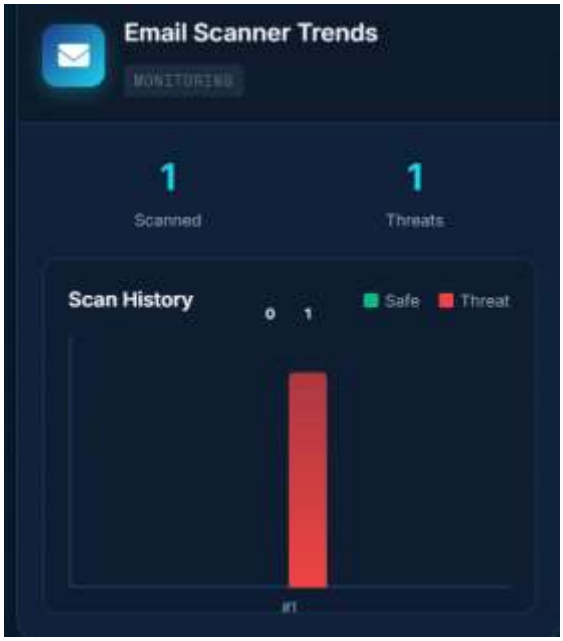

Fig 4: Email_Scanner

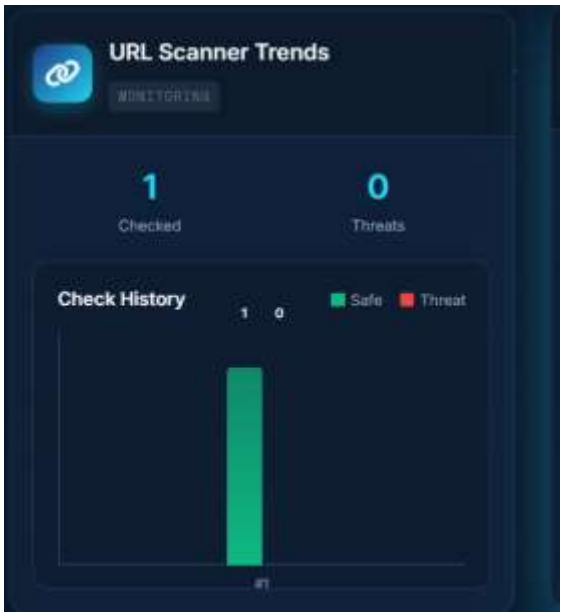

Fig 5: URL_Scanner_Trends

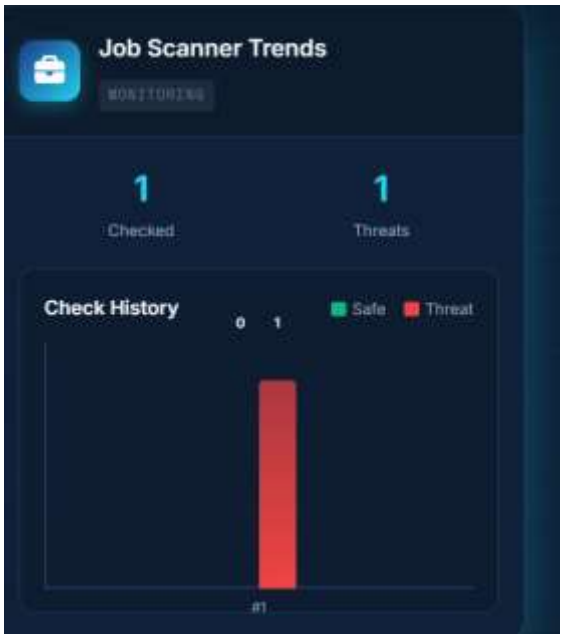

Fig 6: Job_Scanner_Trends

The system also displays a monitoring dashboard that tracks scanning activity for different categories such as Email Scanner Trends, URL Scanner Trends, and Job Scanner Trends. This dashboard shows the number of scanned items and detected threats, helping administrators monitor system performance and identify suspicious activities over time. The visual charts provide a quick overview of safe and malicious detections within the system.

4. Legitimate URL Detection Result

Fig 7: Detections

The system analyzes a provided job-related URL and classifies it as REAL, indicating that the link appears to be legitimate and safe. The result section also provides precautionary suggestions to users, such as verifying the company's official website, avoiding payments for job applications, and checking the recruiter's email domain. This feature helps users confirm whether a recruitment website or job link is trustworthy before interacting with it.

5. System Performance Outcome

The experimental findings indicate that the proposed system can successfully detect fraudulent job advertisements and distinguish them from legitimate recruitment content. By combining machine learning analysis with rule-based filtering, the system provides reliable predictions and enhances security in online recruitment platforms. The results show that the system can effectively assist users in identifying scams and reducing the risk of recruitment fraud.

VII. CONCLUSION AND FUTURE ENHANCEMENTS

Conclusion

b. The system employs a mix of rule-based filtering and machine learning to look for strange patterns in job descriptions, emails, and URLs. The system can find bogus job ads more accurately by employing text preprocessing, TF-IDF to extract features, and Logistic Regression to classify them. The web-based interface that was created makes it easy for users to send in job descriptions or URLs and get fast analysis results. The trial results show that the suggested system can tell the difference between real and fake job postings and also give users safety tips. In general, the method helps cut down on recruitment fraud, keeps job seekers safe from online frauds, and makes digital recruitment platforms more trustworthy and secure..

Future Enhancements

- **Integration of Advanced Machine Learning Models:** Future research may incorporate sophisticated algorithms, including Random Forest, Support Vector Machine, or deep learning models, to enhance detection precision.
- **Real-Time Data Integration:** The system can be enhanced to automatically collect job postings from online job portals and social media platforms for real-time fraud detection.

- **Mobile Application Development:** The mobile application can be developed to allow users to quickly check suspicious job postings directly from their smartphones.
- **Improved Dataset Expansion:** A bigger and more varied dataset can help. the machine learning model learn more complex fraud patterns and improve prediction performance.

REFERENCES

1. S. Vidros, C. Kolias, G. Kambourakis, and L. Akoglu, "Automatic Detection of Online Recruitment Frauds: Characteristics, Methods, and a Public Dataset," Future Internet, vol. 9, no. 1, pp. 1–19, 2017.
2. B. Alghamdi and F. Alharby, "An Intelligent Model for Online Recruitment Fraud Detection," Journal of Information Security, vol. 10, no. 2, pp. 1–12, 2019.
3. S. Dutta and S. K. Bandyopadhyay, "Fake Job Recruitment Detection Using Machine Learning Approach," International Journal of Academic Research in Business and Social Sciences, vol. 10, no. 6, pp. 1–12, 2020.
4. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," SN Computer Science, vol. 2, no. 3, pp. 1–21, 2021.
5. H. Tabassum, G. Ghosh, A. Atika, and A. Chakrabarty, "Detecting Online Recruitment Fraud Using Machine Learning," Proceedings of the International Conference on Information and Communication Technology, pp. 472–477, 2021.
6. S. Mahbub and E. Pardede, "Using Contextual Features for Online Recruitment Fraud Detection," International Conference on Information Systems Development, pp. 1–10, 2022.
7. Nessa, B. Zabin, K. Faruk, A. Rahman, and K. Nahar, "Recruitment Scam Detection Using Gated Recurrent Unit," IEEE Region 10 Humanitarian Technology Conference, pp. 445–449, 2022.
8. Pillai, "Detecting Fake Job Postings Using Bidirectional LSTM," arXiv Preprint, pp. 1–12, 2023.
9. H. Tabassum, G. Ghosh, and A. Chakrabarty, "Machine Learning Approaches for Detecting Fraudulent Job Advertisements," International Journal of Data Science, vol. 11, no. 2, pp. 55–63, 2023.
10. S. Rekha, A. Tyagi, and N. Sreenath, "Class Imbalanced Data: Open Issues and Future Research Directions," International Conference on Computer Communication and Informatics, pp. 1–6, 2023.
11. T. N. Goud and N. R. Reddy, "A Machine Learning Approach for Detecting Fraudulent Job Postings in Online Recruitment Platforms," Journal of Sensors, IoT & Health Sciences, vol. 3, no. 3, pp. 14–28, 2025.
12. K. Taneja, J. Vashishtha, and S. Ratnoo, "Fraud-BERT: Transformer-Based Context Aware Online Recruitment Fraud Detection," Information Systems Frontiers, 2025.
13. M. Anitha, Y. N. Malleswarao, and P. Ajay, "Online Recruitment Fraud Detection Using Deep Learning Approach," International Journal of Computer Applications, vol. 185, no. 6, pp. 1–8, 2025.
14. H. Tabassum, G. Ghosh, and A. Chakrabarty, "Deep Learning Based Online Recruitment Fraud Detection," International Journal of Creative Research Thoughts, vol. 13, no. 4, pp. 1–8, 2025.
15. T. C. Tran and T. K. Dang, "Machine Learning for Prediction of Imbalanced Data: Credit Fraud Detection," International Conference on Ubiquitous Information Management and Communication, pp. 1–7, 2021.
16. S. Ravenelle, E. Janko, and K. Kowalski, "Good Jobs, Scam Jobs: Detecting Online Job Scams During the COVID-19 Pandemic," New Media & Society, vol. 24, no. 7, pp. 1591–1610, 2022.
17. T. Namdev Goud and N. Ramana Reddy, "Machine Learning Based Fake Job Detection System," International Journal of Engineering Research and Technology, vol. 14, no. 5, pp. 1–6, 2024.

18. H. Tabassum et al., "Predicting Fraudulent Job Advertisements Using Machine Learning Models," International Journal of Artificial Intelligence Research, vol. 7, no. 1, pp. 1–10, 2024.
19. M. Singh, P. Sharma, and R. Gupta, "Hybrid Model for Detection of Fake Job Postings on Online Platforms," International Journal of Data Science and Analytics, vol. 12, no. 2, pp. 88–101, 2024.
20. Kumar and S. Verma, "Online Recruitment Fraud Detection Using NLP and Machine Learning Techniques," Journal of Cybersecurity and Data Protection, vol. 9, no. 1, pp. 1–12, 2023.