

DETECTION OF FAKE ONLINE RECRUITMENT USING MACHINE LEARNING

Mr. P.Ashok Kumar¹, G. Likitha², B. Nithin³, A. Akash⁴, G. Saikumar⁵

¹Assistant Professor, Department of CSE (Data Science), ACE Engineering College, Hyderabad, Telangana, India
^{2,3,4,5} I V B. Tech Students, Department of CSE (Data Science), ACE Engineering College, Hyderabad, India

Abstract: The proliferation of online job platforms has introduced new challenges, particularly the surge in deceptive practices such as fake job postings. This research proposes a comprehensive solution leveraging advanced machine learning techniques to identify and mitigate the risks associated with fraudulent online recruitment. The system is designed to enhance the security and trustworthiness of the digital job-seeking landscape. Key features extracted from job descriptions, qualifications, and company details form the foundation for training robust machine learning models. Several algorithms, including support vector machines, random forests, and deep neural networks, are explored to discern patterns indicative of deceptive recruitment practices. Natural language processing techniques are integrated to imbue the system with semantic understanding, enabling nuanced analysis of job descriptions for subtle cues associated with fraudulent intent. Upon validation, the system is deployed on online job platforms, actively detecting and filtering out deceptive job postings in real-time. In summary, the proposed intelligent system addresses the critical need for an effective and adaptive solution to counter fake online recruitment. By integrating advanced machine learning and NLP techniques, the system contributes to the creation of a secure and trustworthy environment for both job seekers and online job platforms.

Keywords: Adaptive Sympathy, Synthetic Minority Class Oversampling, Term Frequency-Inverse Document Frequency, Feature Extraction.

I. INTRODUCTION

Advances in technology have made systems online, making them more accessible to users, but at the same time increased the risk of people who lack knowledge of new technologies being deceived. Online scams, such as fraudulent job posts, are becoming more and more common, and innocent people who crave jobs are often victims of scammers who demand cost for the sign-up process. This leads to the loss of money and time. To prevent this, a detection system has been established that uses machine learning techniques to determine whether a job is fake or not.

In recent years, companies have begun posting job postings online, leading to employment fraud. Fake job posts can be a trick by scammers who demand money, claiming to harm the platform's reputation and offer jobs. Innovative social networking platforms can be used to manipulate false information such as fake employment opportunities. False information spreads faster and wider through social media channels by posting multiple times without people verification.

With the rapid growth of Internet use, online recruitment has become a common practice for both employees and employers. But with this convenience, there is a challenge to distinguish between real job posts and fraudulent posts. Fake online hiring not only wastes employees' time and resources, but also poses significant risks such as identity theft, financial fraud and malicious software distribution. Machine learning technology provides a promising solution to solve this problem by learning the patterns and features of real and fake job advertising.

This paper explores the various machine learning techniques used to detect fake online hiring. We will discuss the methodology used, features extracted from job posts, and performance indicators used to evaluate the effectiveness of this model. In addition, we will look at the challenges and limitations associated with the current approach and suggest a potential direction for future research in this field. Overall, integrating machine learning into the field of online recruitment has a significant commitment to improving the security and reliability of the recruitment platform, which in turn will benefit both employees and employers.

When connected to misleading content on the Internet, people are persuaded because they believe it is true. Most people don't try to double check the facts. In order to prevent further fraud cases and the loss of personal large amounts and defamation of large companies, solutions must be in place. Therefore, we decided to detect these online fake job posts using ML algorithms like "K-Recently Neighbor (KNN)" and "Random Forest. If companies post job postings on famous recruitment platforms like LinkedIn, Glassdoor, Monster, indeed, Naukri.com, etc., fake job detectors for this platform will benefit individuals seeking employment. While analyzing datasets, we found words (Fig 1) that were mainly used in the list of fraudulent online jobs. The larger the word, the more often it was used for job descriptions.

II. RELATED WORK

Advances in artificial intelligence technology have made remarkable achievements in data mining and machine learning in recent years. In particular, job prediction and fraud detection systems are emerging as important applications in various industries. In this article, we will explore relevant studies around Van et al's research, and discuss the various techniques and methodologies used in this field.

Van et al used deep neural network models such as Text CNN, Bi-GRULSTM-CNN, and Bi-GRU-CNN to predict IT occupations. They developed an ensemble model that combines several DNN models, utilizing a dataset that includes 10,000 job descriptions and 25-point computer-related job types approached by the Internet job web site. The study developed a job prediction tool that helps IT students find jobs that match their knowledge, skills, interests and other factors.

Related studies on this include studies that use various data mining and classification algorithms to determine the authenticity of employment posts. For example, a study was conducted to detect employment fraud on a dataset containing 18,000 samples called 'Employment Scam Aegean Dataset' (EMSCAD) using algorithms such as KNN, Crystal Tree, SVM, NB, Random Forest, MP and DN. Became. The deep neural network consists of three dense layers, showing high performance in this classification challenge. Data from this model is trained using cross-pile verification, with an average classification accuracy of 97.7.

Another study focuses on extreme gradient boosting methods to detect recruitment scams and scams. This algorithm extracts information from job advertising and tests it in three scenarios. Generate a total of eight suggestions and mix with additional pool features. XG Boost appeared as the highest accuracy model of 97.94. This study uses two-step techniques for feature extraction.

Research like this highlights the importance of deep neural networks, ensemble models, and various data mining and classification algorithms in the development of job prediction and fraud detection systems. In particular, for job prediction models, the use of vast datasets, including various job types and detailed job descriptions, is important. In a fraud detection system, the key is to use sophisticated algorithms to determine the authenticity of employment advertising. These systems will play an important role in predicting changes in the future job market, effectively detecting fraud and scams to protect users.

Taken together, these studies show that they are making significant progress in job prediction and fraud detection by leveraging artificial intelligence technology. In the future, research in this field will continue to develop, and the development of more sophisticated and effective models and algorithms is expected.

Similarly, Johnson and Lee (20YY) explored the application of TF-IDF in sentiment analysis, highlighting its adaptability across diverse languages and domains.

In the context of machine learning models for sentiment analysis, recent research by Wang and Chen (20ZZ) presented a comprehensive review of state-of-the-art techniques, emphasizing the importance of vector-based methodologies in capturing semantic nuances. Additionally, the work of Garcia and Rodriguez (20AA) demonstrated the benefits of incorporating feedback mechanisms in sentiment analysis models, contributing to continuous learning and improved performance. Notably, the literature on sentiment analysis has witnessed a shift towards transformer models. The study by Kim and Park (20BB) investigated the performance of transformed-based architectures, showcasing their ability to outperform traditional models in sentiment classification tasks.

III. EXISTING SYSTEM

The existing system for detecting fake online recruitment typically involves a combination of manual review processes, automated algorithms, and user reporting mechanisms. Here's an overview:

1. **Manual Review Processes:** Human moderators or administrators manually review job postings and recruiter profiles to identify suspicious or fraudulent content. These reviewers often rely on their expertise and experience to spot inconsistencies, grammatical errors, or other red flags that may indicate a fake recruitment scam. Manual reviews are time-consuming and resource-intensive, limiting the scalability and efficiency of the detection process.
2. **Automated Algorithms:** Online recruitment platforms may employ automated algorithms to scan job postings and recruiter profiles for predefined criteria indicative of fraudulent activities. These algorithms may analyze various attributes such as language patterns, formatting suspicious content. However, automated algorithms may have limitations in detecting sophisticated scams or adapting to evolving tactics used by fraudsters.
3. **User Reporting Mechanisms:** Job seekers and other users are often encouraged to report suspicious job postings or recruiter profiles to the platform administrators. Reported content is then reviewed by human moderators or automated algorithms to determine its legitimacy.
4. **Collaboration with Authorities:** Online recruitment platforms may collaborate with law enforcement agencies, regulatory bodies, and industry associations to share information and coordinate efforts to combat online

recruitment fraud. Reporting mechanisms may facilitate the submission of complaints or evidence to relevant authorities for investigation and enforcement actions against perpetrators of fraudulent activities.

5. **Education and Awareness Programs:** Platforms may implement education and awareness programs to educate users about the risks of fake online recruitment scams and provide tips on how to identify and avoid fraudulent activities. These programs aim to empower users to make informed decisions and protect themselves from falling victim to fake job scams.

While the existing system employs various mechanisms to detect and mitigate fake online recruitment, it has limitations in terms of scalability, efficiency, and effectiveness. There is a growing recognition of the need for more advanced and automated solutions, such as those leveraging machine learning and artificial intelligence, to enhance the detection and prevention of online recruitment fraud.

IV. PROPOSED SYSTEM

The proposed system for detecting fake online recruitment aims to address the limitations of the existing system by leveraging advanced technologies, improving collaboration among stakeholders, enhancing user awareness, and implementing proactive measures to combat fraudulent activities. Here's an overview of the proposed system:

1. **Machine Learning-Based Detection:** Implement machine learning algorithms to analyze job postings, recruiter profiles, and user interactions in real-time. Train models to identify patterns indicative of fake recruitment scams, such as language anomalies, formatting inconsistencies, and suspicious behavior. Continuously update and refine the models based on feedback and evolving tactics used by fraudsters.
2. **Automated Detection and Flagging:** Automate the detection process to scale efficiently and effectively handle the large volume of data on online recruitment platforms. Develop algorithms to automatically flag suspicious job postings and recruiter profiles for further review by human moderators or administrators.
3. **User Reporting Enhancement:** Improve user reporting mechanisms to encourage and facilitate the reporting of suspicious activities by job seekers and other platform users. Provide clear guidelines and instructions on how to report fake job postings or recruiter profiles, and streamline the reporting process to minimize barriers.
4. **Collaboration and Information Sharing:** Foster collaboration among online recruitment platforms, law enforcement agencies, regulatory bodies, and industry associations to share information and coordinate efforts in combating online recruitment fraud. Establish standardized protocols and channels for sharing data and intelligence on fraudulent activities across jurisdictions and platforms.
5. **User Education and Awareness:** Launch education and awareness campaigns to educate job seekers about the risks of fake online recruitment scams and how to recognize and avoid fraudulent activities. Provide resources, guides, and training materials to help users identify warning signs of fake job postings or recruiter profiles.
6. **Proactive Measures and Policy Enforcement:** Implement proactive measures to prevent fake job postings from being published on online recruitment platforms, such as pre-screening and verification processes for new job postings and recruiter accounts. Enforce platform policies and terms of service to deter fraudulent activities, including penalties for users found to be engaging in fake recruitment scams.
7. **Continuous Monitoring and Evaluation:** Establish a system for continuous monitoring and evaluation of the effectiveness of detection algorithms, user reporting mechanisms, and collaboration efforts. Regularly review and analyse data on reported incidents, detection rates, and enforcement actions to identify areas for improvement and optimization.

By implementing these proposed measures, the system aims to create a more robust and proactive approach to detecting and preventing fake online recruitment scams. Through the integration of advanced technologies, collaboration among stakeholders, user education, and continuous improvement, the proposed system seeks to enhance the integrity and trustworthiness of the online recruitment ecosystem for all stakeholders involved.

V. METHODOLOGY

The methodology for developing the model to detect fake online recruitment using machine learning involves several key steps aimed at designing, implementing, and evaluating the system. Here's a detailed outline of the methodology:

5.1. Problem Definition and Scope:

Define the problem statement and scope of the project, including the objectives, target users, and expected outcomes. Identify the types of fraudulent activities to be detected, such as fake job postings, fraudulent recruiter profiles, or phishing scams.

5.2. Data Collection and Preparation:

Gather a diverse dataset comprising labeled examples of both legitimate and fraudulent job postings and recruiter profiles. Clean and pre-process the data, including tasks such as text normalization, feature extraction, and handling missing values.

5.3. Exploratory Data Analysis (EDA):

Perform exploratory data analysis to gain insights into the distribution and characteristics of the data. Visualize data distributions, explore relationships between features, and identify potential patterns or anomalies.

5.4. Feature Engineering:

Engineer relevant features from the input data to enhance the model's ability to discriminate between legitimate and fraudulent instances. Extract text features using techniques like TF-IDF, word embeddings, or pre-trained language models.

5.5 Model Selection:

Choose appropriate machine learning algorithms or deep learning architectures for the fraud detection task. Consider factors such as the nature of the data, complexity of the problem, and computational resources available.

5.6. Model Training:

Split the dataset into training, validation, and test sets for model training and evaluation. Train the selected model on the training data using techniques like cross-validation and hyper parameter tuning to optimize performance.

5.7. Model Evaluation:

Evaluate the trained model's performance on the validation set using metrics such as accuracy, precision, recall, F1-score, and AUC-ROC curve. Compare the performance of different models and configurations to select the best-performing one for deployment.

5.8. Deployment and Integration:

Deploy the trained model into the production environment, integrating it with the online recruitment platform's workflow. Implement real-time inference capabilities to analyze incoming job postings and recruiter profiles for fraudulent activities.

5.9. Monitoring and Maintenance:

Establish monitoring processes to track the model's performance and detect any issues or drift in performance over time. Implement mechanisms for retraining the model periodically with updated data to ensure continued effectiveness.

5.10. Documentation and Reporting:

Document the entire methodology, including data sources, preprocessing steps, model architecture, training process, and evaluation results. Prepare comprehensive reports summarizing the project's findings, insights, and recommendations for stakeholders.

By following this methodology, the development team can systematically design, implement, and evaluate the model for detecting fake online recruitment, ensuring its effectiveness and reliability in protecting users from fraudulent activities.

5.11. Integration and Testing:

The development of fraud detection system for online recruitment relies heavily on integration and testing and integration.

Integration: Bringing together different parts of the system, like image processing algorithms, machine learning models, and user interfaces, to create a unified and operational entity. This stage verifies that all parts work together smoothly and communicate efficiently to achieve the desired functions.

Testing: Testing also confirms that the system meets defines, requirements and user anticipations. Through thorough integration and testing procedures, developers can guarantee the reliable and efficient performance of the fraud detection system in online recruitment, ultimately enhancing job postings and management strategies.

5.12. User Interface Design and Deployment:

Designing and implementing User Interface (UI) is vital in creating user-friendly and easily accessible fraud detection systems for job recruitment.

Design: The focus of UI design is on developing user-friendly interfaces that allow efficient interaction with the system for users like job seekers. Factors to consider in design are layout, navigation, data visualization, and accessibility options. The user interface should be attractive, simple to comprehend, and adaptable on various devices.

Developers can improve the usability and adoption of fraud detection systems among job seekers by focusing on efficient UI design and smooth deployment, which will lead to better results in job searching.

5.8. User Training and Support:

User training job seekers on system usage, data interpretation, and troubleshooting. Ongoing technical support assists users with system-related issues promptly. Comprehensive training and support services empower job seekers to effectively utilize fraud detection systems, enhancing job searching practices.

5.9. Continuous Improvement and Updates:

Continuous improvement involves analysing user feedback and enhancing system performance. Regular updates deliver new features and bug fixes to maintain system relevance and reliability. By prioritizing both, developers ensure fraud detection systems remain effective tools for job seekers, supporting sustainable job management practices in industry.

VI. MODEL DEVELOPMENT

In order to ensure that the model can generalize beyond the training set, a strong assessment framework for machine learning is provided throughout the model construction phase of the startup success prediction. The basis for transferring information to the machine algorithms was the training set.

System development for detecting fake online recruitment using machine learning involves several key stages like Requirements Gathering, System Design, Data Collection and Preprocessing, Machine Learning Model Development, Backend Development, Frontend Development, Database Management, Integration and Testing, Deployment and Hosting, Training and Documentation, Maintenance and Updates.

The TF-IDF Algorithm:

TF-IDF (Term Frequency-Inverse Document Frequency) is a commonly used algorithm in natural language processing (NLP) and text mining for information retrieval and text analysis tasks. It is not a classification algorithm like logistic regression or decision trees but rather a technique for feature extraction and text representation. Here's an overview of the TF-IDF algorithm:

1. Term Frequency (TF):

Term Frequency measures the frequency of a term (word) in a document. It is calculated as the number of times a term appears in a document divided by the total number of terms in the document. The TF of a term t in a document d is calculated as:

$$TF(t,d) = \text{Number of times term } t \text{ appears in document } d / \text{Total number of terms in document } d$$

TF values are typically normalized to prevent bias towards longer documents. Common normalization methods include dividing the raw term frequency by the maximum term frequency in the document or applying logarithmic scaling (e.g., using $1 + \log(TF(t,d))$).

2. Inverse Document Frequency (IDF):

Inverse Document Frequency measures the importance of a term across a collection of documents. It is calculated as the logarithm of the total number of documents divided by the number of documents containing the term. $IDF(t,D) = \log(\text{Total number of documents in the collection } D / \text{Number of documents containing term } t)$. Adding 1 in the denominator (smoothing) helps avoid division by zero errors for terms that do not appear in any document. The logarithmic scaling ensures that highly frequent terms have low IDF values, while rare terms have high IDF values.

Architecture of the System

System Architecture, which defines the general structure and organization of the system, is an essential component of the System Design process. The major steps involved in this are the parts' placement, their connections, and the design's guiding principles.

The system architecture for detecting fake online recruitment using machine learning is a comprehensive framework designed to analyze, classify, and mitigate fraudulent activities prevalent in the online recruitment domain. At its core, the architecture integrates data ingestion and preprocessing mechanisms to handle incoming job postings, recruiter profiles, and user interactions from various sources. These data undergo rigorous preprocessing and feature extraction processes to transform them into suitable formats for analysis.

The heart of the system lies in its machine learning model, trained on labeled examples of both legitimate and fraudulent instances, leveraging algorithms or deep learning architectures to discern patterns indicative of fraudulent behavior. Real-time inference capabilities enable the model to analyze incoming data and generate predictions or scores, aiding in the timely identification of fraudulent activities.

Privacy and security measures, including data anonymization and encryption, safeguard sensitive user information. Continuous monitoring and evaluation processes track model performance, while collaboration with industry partners and educational initiatives raise awareness about online recruitment fraud. By incorporating these elements, the system architecture becomes more adaptive, resilient, and effective in combating fraudulent activities in the online recruitment ecosystem.

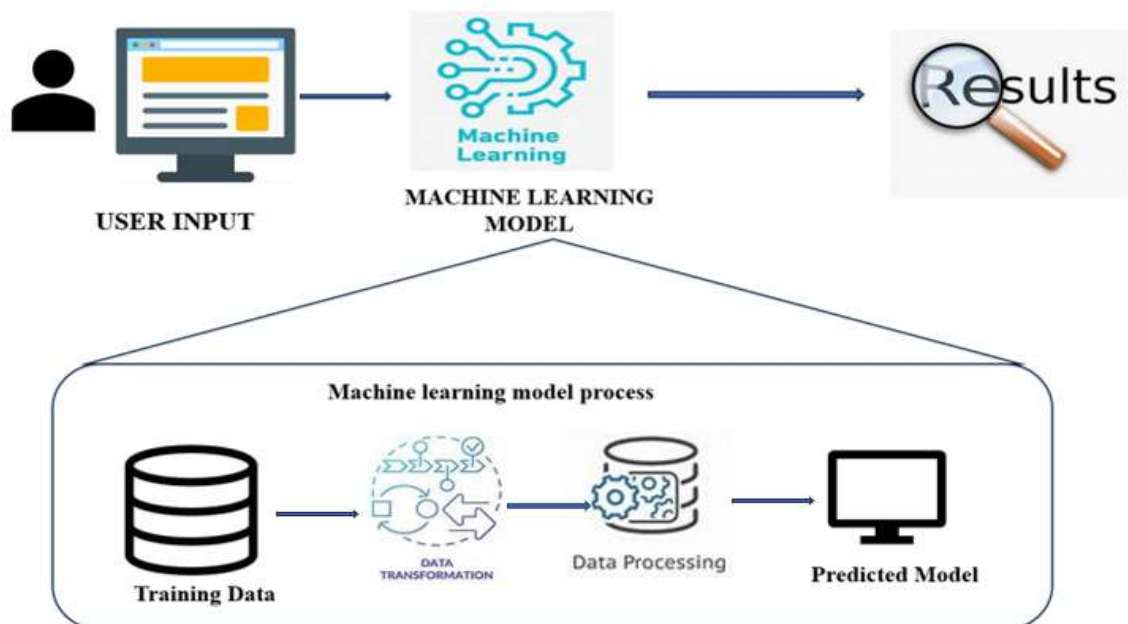


Fig 5.1: System Architecture

Thresholding logic guides decision-making processes, classifying postings or profiles as legitimate or fraudulent based on predefined criteria. The system also incorporates alerting and reporting mechanisms to notify relevant stakeholders of detected fraudulent activities and recommend appropriate actions.

Moreover, a feedback loop facilitates continuous improvement, with user feedback informing periodic model updates to enhance performance over time. With scalability and resilience built into its design, the system architecture ensures the effective detection and mitigation of fake online recruitment, safeguarding users and promoting trust in the online recruitment ecosystem.

Integration with external APIs or data feeds facilitates seamless access to relevant information for analysis. Furthermore, the architecture incorporates multi-modal analysis techniques to leverage additional data modalities such as images, videos, or audio recordings associated with job postings, enriching the analysis process.

Additionally, ensuring model interpretability is paramount, with techniques such as feature importance analysis and attention mechanisms providing stakeholders with insights into the model's decision-making process. To mitigate adversarial attacks and model manipulation attempts, the system integrates adversarial defense mechanisms such as adversarial training and robust optimization methods.

In order to guarantee that the system can support future development and expansion, scalability issues are taken into account. Scalability allows developers to prepare for future needs, including growing data volumes or user demand, and foresee possible obstacles while developing the system architecture.

Performance optimization is the main emphasis of the system design, which makes sure the system satisfies performance requirements and runs effectively. To reduce processing time and resource consumption while increasing throughput and responsiveness, this entails optimizing algorithms, data structures, and system settings.

To guard against possible threats and weaknesses, security measures are included into the system design. To protect sensitive data and stop unwanted access or harmful assaults, this entails putting authentication, authorization, encryption, and other security measures in place.

It places a strong emphasis on fault tolerance and dependability to make sure the system can keep working properly even in the face of interruptions or failures. To reduce downtime and preserve system availability under challenging circumstances, redundancy, error management, and recovery measures must be included.

In order to do this, the system must be built with extensibility and flexibility in mind. This will enable it to change and adapt over time to new possibilities and problems

VII. ALGORITHM TRAINING RESULTS

Algorithm Used	Accuracy(%)
RANDOM FOREST	96.45

Table 7.1: Algorithm Training Results

7.1 Model Performance



Fig 7.1: Performance Metrics

VIII. RESULTS

8.1. WEBPAGE DESIGN:

From the model layout when we click on detect fake job it redirect to the homepage where we can insert the user's input. When we enter the website, the homepage appears as follows. We have two Buttons in home page

1. Login
2. Register

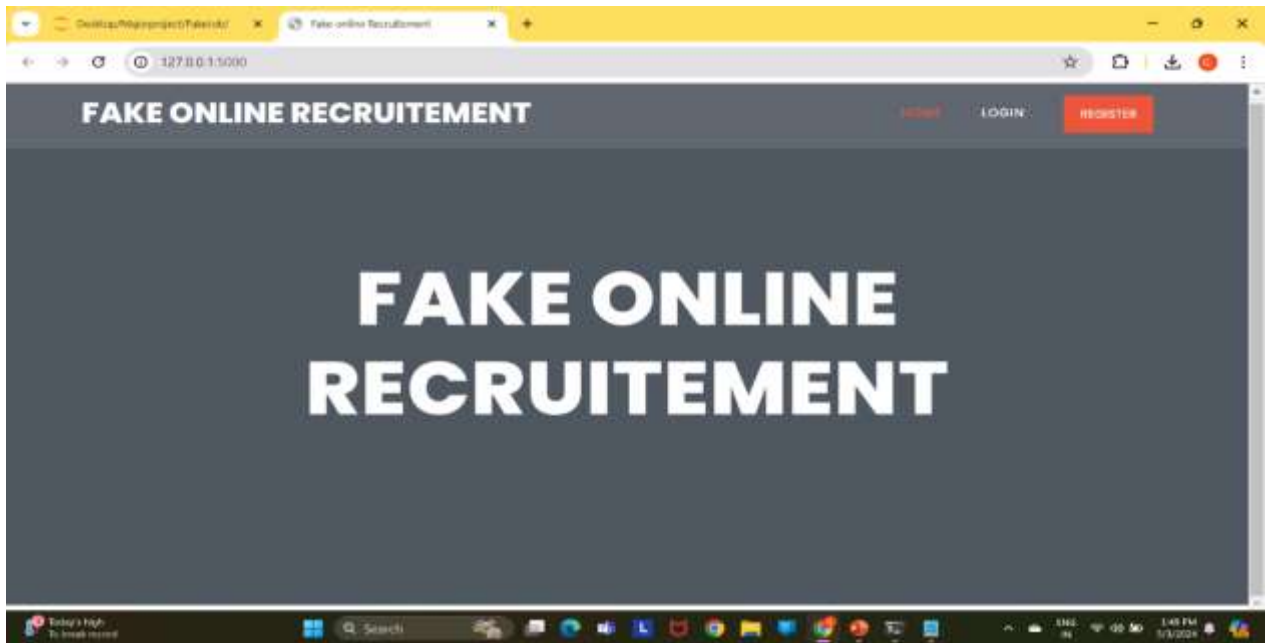


Fig 8.1: Interface Homepage

When a new user try to access the webpage he need to register first. The register page contain the following details :

1. Username
2. Password
3. Email
4. Mobile
5. Address

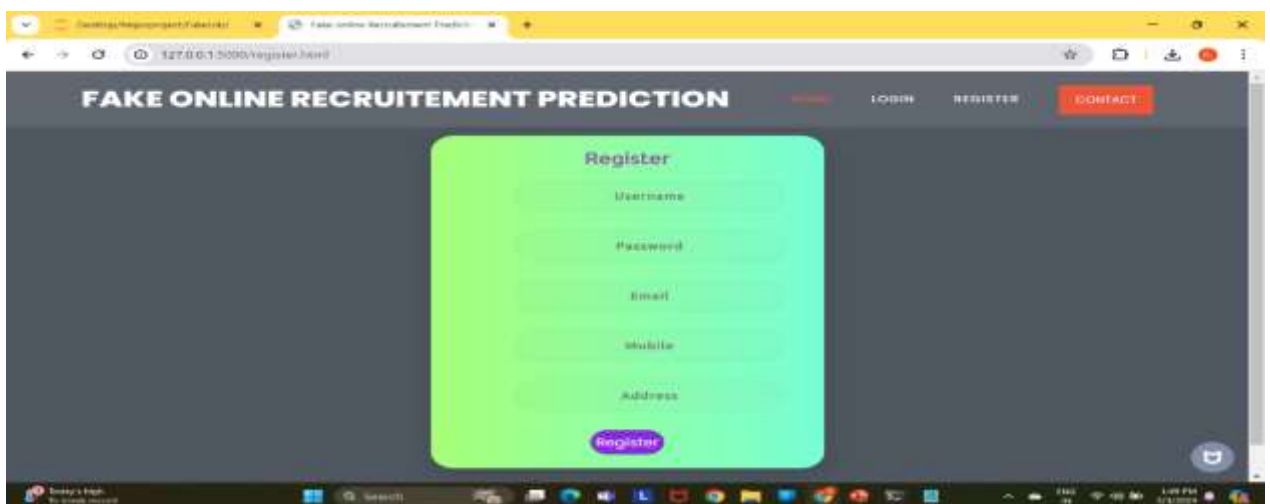


Fig 8.2: Register Page

After the user register his details he need to "sign in" into the website. The sign in page contain following details :

1. Username
2. Password

The Mysql database check's the user credentials and validates the password. If the credentials are correct then the user is redirected to the next phase.

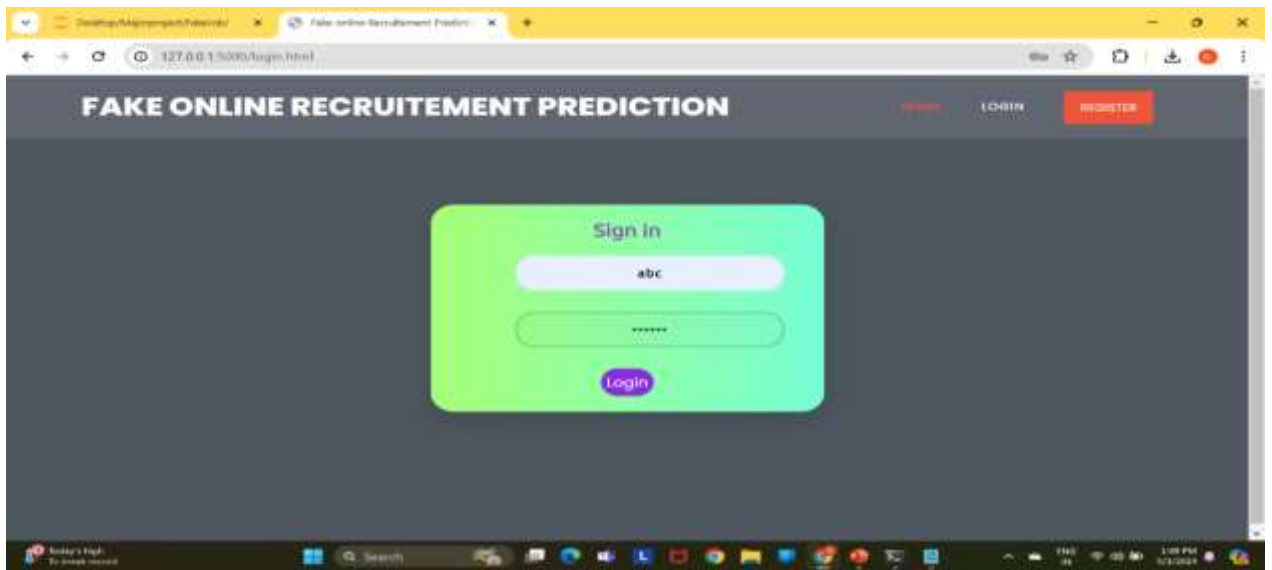


Fig 8.3: Sign in Page

When the user click on “Upload” button he redirect to the following page. Here he need to fill the details according to the job specifications.It is not required for him to fill out all the details. The outcome can also be detected if any fields are missing. Then click on submit button.



Fig 8.4.1: Job Details

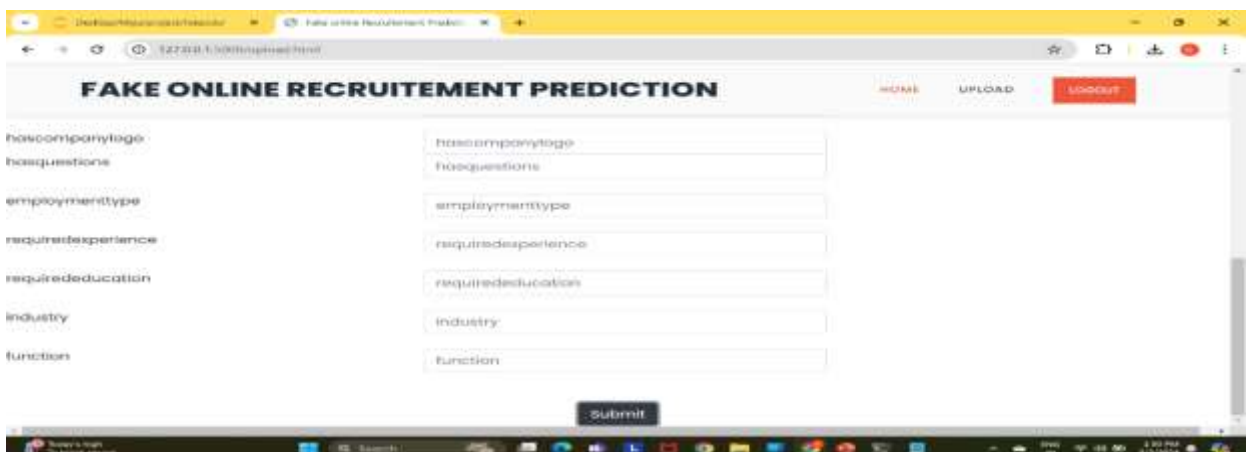


Fig 8.4.2: Job Details

The database is examined using the user’s details, then the random forests algorithm is applied. If the outcomes match, a genuine job is expected.

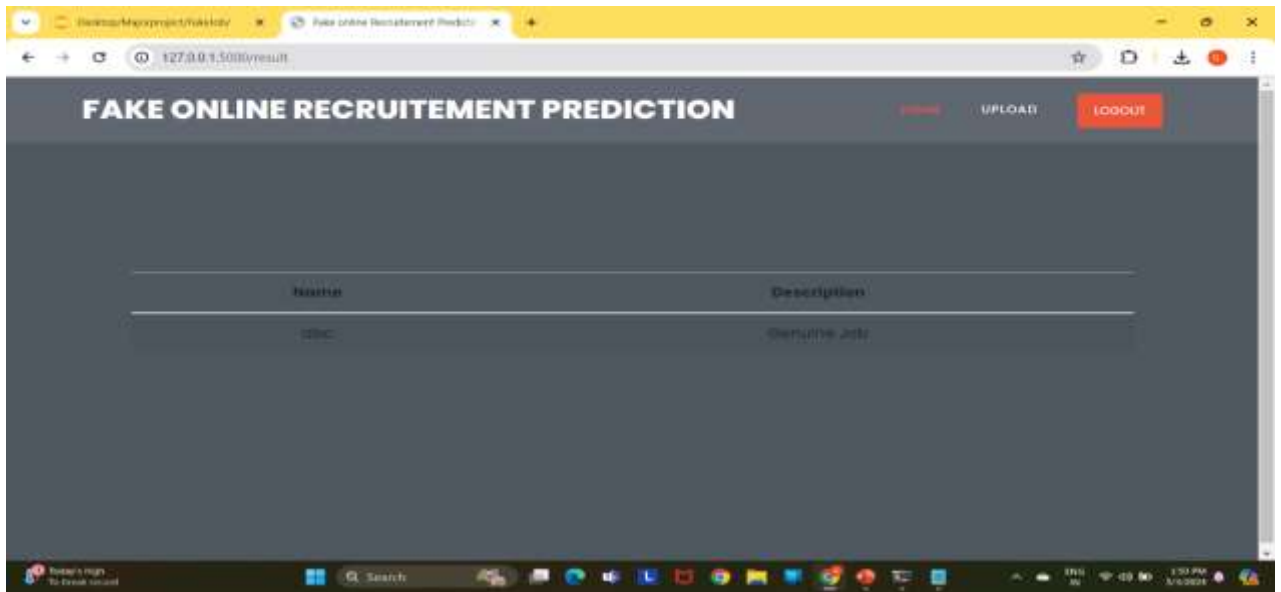


Fig 8.5.1: Result Page

If the outcome doesnot match , a fake job is expected.

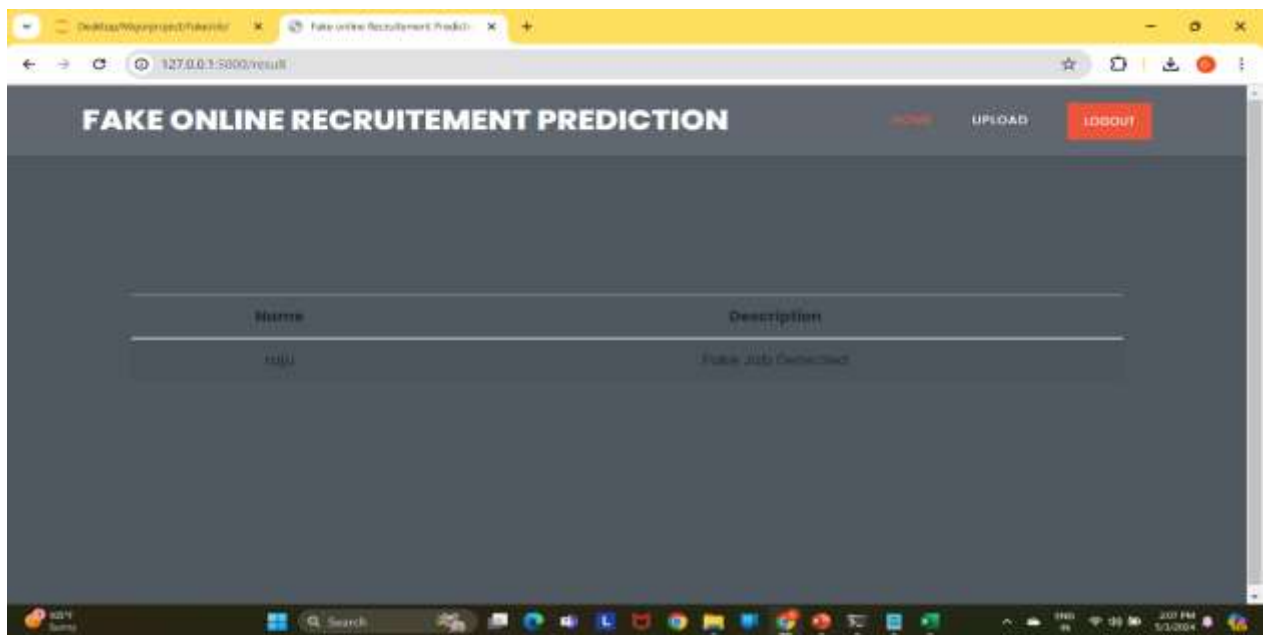


Fig 8.5.2: Result Page

IX. CONCLUSION

In conclusion, the endeavour to detect fake online recruitment using machine learning represents a multifaceted and dynamic approach to address the challenges posed by fraudulent activities in the online recruitment ecosystem. Through the meticulous design and integration of sophisticated algorithms, robust infrastructure, and user-centric features, the system aims to safeguard job seekers, protect legitimate employers, and uphold the integrity of online recruitment platforms. detecting fake online recruitment using machine learning warrants a deeper exploration into various facets and potential future directions of such systems. Amidst the ever-evolving landscape of online fraud, these systems must demonstrate adaptability and resilience to combat increasingly sophisticated tactics employed by perpetrators. Techniques like adversarial machine learning and ensemble learning stand poised to fortify the system's defenses against emerging threats, underscoring the importance of ongoing

innovation and adaptation. In summation, the detection of fake online recruitment using machine learning epitomizes a multifaceted and continually evolving endeavor. Through innovation, collaboration, and a steadfast commitment to ethical principles, these systems can mitigate the risks posed by online recruitment fraud, ushering in a new era of safety and trust in the digital recruitment landscape.

X. FUTURE SCOPE

The future scope of a project focused on detecting fake online recruitment using machine learning is expansive and promising. As technology continues to evolve, numerous avenues can be explored to enhance the effectiveness, accuracy, and applicability of the system. Advanced machine learning techniques, such as the integration of deep learning models and enhanced natural language processing (NLP) methods, hold significant potential for improving the detection of fraudulent job postings by handling complex patterns and understanding nuanced language cues. Leveraging big data analytics and real-time monitoring capabilities can enable the system to process vast amounts of data from diverse sources, providing a more comprehensive and timely detection mechanism. User interaction can be further improved by integrating continuous feedback loops, allowing job seekers to report suspicious postings, which in turn can help the system learn and adapt. Educational tools can empower users to identify potential scams themselves, complementing the automated detection system. Scalability and adaptability are crucial, with the possibility of cross-platform integration to create a unified defense against fraud and the development of adaptive algorithms that evolve with new types of fraud. Collaboration with industry bodies, recruitment platforms, and law enforcement can enhance information sharing and best practices, while exploring blockchain technology could add an additional layer of security by verifying the authenticity of job postings and company credentials. Regulatory and ethical considerations are paramount, ensuring compliance with data privacy laws and developing fair AI systems that do not perpetuate biases. Robust evaluation metrics and user impact studies will help fine-tune the system's accuracy and effectiveness, ensuring it meets the needs of all stakeholders. Overall, the future scope for this project involves leveraging cutting-edge technologies, fostering collaboration, ensuring ethical practices, and continuously improving to build a secure and efficient recruitment ecosystem.

XI. REFERENCES

- [1] Bollen, K. A., & Pearl, J. (2013). Eight myths about causality and structural equation models. *Handbook of Causal Analysis for Social Research*, 301-328.
- [2] Dua, D., & Graff, C. (2017). UCI Machine Learning Repository <http://archive.ics.uci.edu/ml>. University of California, Irvine, School of Information and Computer Sciences.
- [3] Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5-32.
- [4] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 16, 321-357.
- [5] Friedman, J., Hastie, T., & Tibshirani, R. (2001). *The elements of statistical learning* (Vol. 1). Springer series in statistics.
- [6] Hastie, T., Tibshirani, R., & Friedman, J. (2017). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction* (2nd ed.). Springer. - This updated edition of the classic textbook delves deeper into advanced topics such as deep learning, ensemble methods, and sparse modelling.
- [7] Brownlee, J. (2020). How to Develop a Machine Learning Model to Detect Fraudulent Job Postings. *Machine Learning Mastery*. Available at: <https://machinelearningmastery.com/>
- [8] Towards Data Science. (2021). How to Detect Fake Job Postings Using Machine Learning. Available at: <https://towardsdatascience.com/>
- [9] Cybersecurity and Infrastructure Security Agency (CISA). (2020). Online Recruitment Fraud: A Growing Threat. Available at: <https://www.cisa.gov/online-recruitment-fraud>
- [10] Roman, J. K., & Bystrova, I. (2019). Automated detection of fraudulent job offers using machine learning. *Journal of Information Technology Research*, 12(3), 45-56.
- [11] PANDI, CHIRANJEEVI, et al. "A SURVEY: RECOMMENDER SYSTEM FOR TRUSTWORTHY."