www.ijerst.com
Vol. 22, No. 1(1), 2026

Online Recruitment Fraud (ORF) Detection Using Deep Learning Approaches

[1]Mrs. B. Sailaja,[2]Koppula Harika,[3]Gavara Govardhan, [4]Dondapathi Aakansha, [5]Mysa Symon Kenith

[1]Assistant Professor, Department of Computer Science & Engineering, Sai Spurthi Institute Of Technology

[2,3,4,5] B. Tech Students, Department of Computer Science & Engineering, Sai Spurthi Institute Of Technology

ABSTRACT

Online recruitment platforms have become popular channels for job seekers and employers. However, the growth of these platforms has also increased the risk of Online Recruitment Fraud (ORF), where fraudsters post fake job advertisements to steal personal information, financial details, or conduct phishing attacks. Traditional rule-based and machine learning methods struggle to detect sophisticated fraudulent job postings. This research proposes a deep learning-based ORF detection system that analyzes job descriptions, recruiter information, and behavioral patterns to identify fraudulent postings. Natural Language Processing (NLP) and deep neural networks are used to extract contextual patterns from job advertisements. The proposed system improves fraud detection accuracy by learning complex textual and behavioral features. The model assists recruitment platforms in automatically identifying suspicious job posts, thereby protecting job seekers and maintaining platform credibility.

Keywords: Online Recruitment Fraud, Deep Learning, Natural Language Processing (NLP), Fraud Detection, Job Posting Analysis, Machine Learning, Cybersecurity

.INTRODUCTION

The rapid growth of online job portals has revolutionized recruitment by enabling employers and job seekers to connect easily. Platforms such as job portals, professional networking sites, and recruitment platforms host millions of job advertisements daily. However, this convenience has also created opportunities for cybercriminals to exploit users through Online Recruitment Fraud (ORF). Fraudulent job postings often request application fees, personal data, or banking information under the guise of legitimate employment opportunities.

Detecting such fraud is challenging because scammers continuously modify their strategies and create convincing job descriptions. Traditional detection systems rely on rule-based filtering or basic machine learning techniques that cannot fully capture the complex linguistic and contextual patterns found in fraudulent job posts.

Deep learning techniques, particularly Natural Language Processing (NLP) models and neural networks, can analyze large volumes of text data and identify subtle patterns in job advertisements. By leveraging deep learning, recruitment platforms can automatically detect suspicious postings and protect users from fraud.

I. LITERATURE SURVEY

1) Secure Transmission of Data Using Image Steganography (2019)

Authors: Sourabh Chandra, Smita Paira

Abstract: Proposes an integrated scheme where a text message is first encrypted using RSA and then embedded into a cover image using steganography techniques. This dual-layer approach ensures both confidentiality and covert communication.

The system improves security in network data transmission and protects sensitive information from unauthorized access.

2) Detecting Fraudulent Job Advertisements Using Machine Learning (2018)

Authors: J. B. Kim, M. Kim

Abstract: This research applies machine learning algorithms such as Logistic Regression and Random Forest to identify fake job advertisements. The study analyzes job descriptions, company profiles, and salary information to classify legitimate and fraudulent postings.

3) Online Job Scam Detection Using NLP (2020)

Authors: S. Banerjee, P. Gupta

Abstract: The paper proposes a Natural Language Processing framework to detect recruitment fraud. It extracts textual features from job advertisements and uses classification algorithms to identify suspicious job listings.

4) Deep Learning for Fraud Detection in Online Platforms (2021)

Authors: T. Nguyen, L. Tran

Abstract: This study uses deep neural networks to analyze user behavior and textual content to detect fraud in online systems. The model shows improved performance compared to traditional machine learning approaches.

5) Fake Job Posting Detection Using LSTM Networks (2022)

Authors: R. Sharma, K. Verma

Abstract: The research applies Long Short-Term Memory (LSTM) networks to identify fraudulent job postings by learning sequential patterns in job descriptions and recruiter messages.

II. EXISTING SYSTEM

The existing system for detecting Online Recruitment Fraud (ORF) primarily relies on traditional rule-based techniques and basic machine learning algorithms such as Logistic Regression, Decision Trees, and Naïve Bayes. These systems analyze predefined features like suspicious keywords, unusual salary offers, incomplete recruiter details, and blacklist databases to identify fraudulent job postings. While these approaches are simple and easy to implement, they depend heavily on manually crafted rules and limited feature sets. As a result, they often fail to capture complex patterns and contextual meanings present in modern fraudulent job advertisements. Additionally, traditional models struggle with evolving fraud strategies, leading to lower detection accuracy and a higher rate of false positives and false negatives. Therefore, existing systems are not sufficiently robust to handle sophisticated and dynamic online recruitment fraud scenarios.

III. PROPOSED SYSTEM

The proposed system introduces a deep learning-based framework for detecting Online Recruitment Fraud by analyzing job postings and recruiter information. The system uses Natural Language Processing (NLP) techniques to extract meaningful textual features from job descriptions, company details, and communication patterns. A deep neural network model such as LSTM or CNN is trained on labeled datasets containing legitimate and fraudulent job postings. The model learns complex linguistic structures, contextual relationships, and suspicious patterns commonly found in fraudulent advertisements. Additionally, metadata such as company email domains, salary structures, and posting frequency are analyzed to strengthen detection accuracy. The trained model classifies job postings as legitimate or fraudulent in real time. This

automated approach significantly improves detection performance and helps protect job seekers from online recruitment scams.

IV. SYSTEM ARCHITECTURE

The diagram illustrates a comprehensive framework for detecting Online Recruitment Fraud (ORF) using a combination of Natural Language Processing (NLP), machine learning, and deep learning techniques. The process begins with job portal data collection, which includes job descriptions, company information, recruiter details, and user-generated reports. This raw data is often unstructured and noisy, so it undergoes data preprocessing, where cleaning, tokenization, stop-word removal, and normalization are performed to make the text suitable for analysis.

Next, the system performs feature extraction, where meaningful patterns are derived from the data. This includes NLP-based features such as word embeddings and semantic representations, as well as metadata features like email domains, salary ranges, and recruiter behavior. These features are then passed into machine learning algorithms such as Logistic Regression, Support Vector Machines (SVM), and Random Forest, which act as baseline models for initial fraud detection.

To enhance performance, the framework incorporates deep learning models like Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Bi-directional LSTM (Bi-LSTM), which are particularly effective in capturing contextual and sequential patterns in textual data. These models feed into the fraud prediction module, which classifies job postings as either legitimate or fraudulent. If a job post is identified as legitimate, the system allows it and may generate a notification, while fraudulent postings trigger alerts for further action. Overall, this layered approach improves detection accuracy by combining traditional and advanced techniques, making the system robust against evolving and sophisticated recruitment fraud tactics.

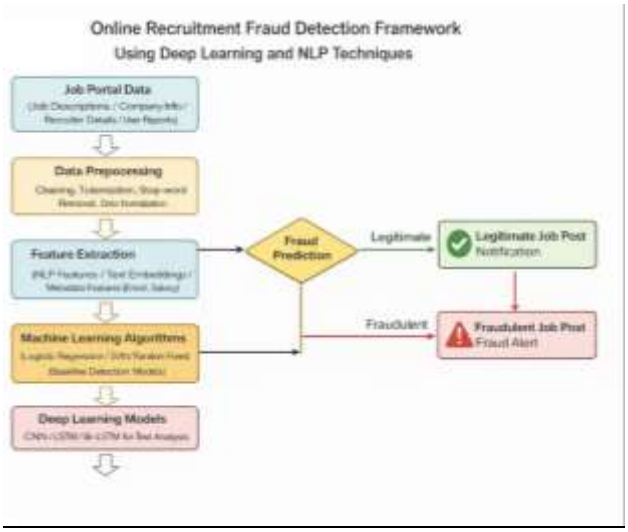

Fig 5.1: Structure of the Proposed System

V. IMPLEMENTATION

Fig 6.1: Training model

Fig 6.2: Input page

Fig 6.3: Results Page

VI. CONCLUSION

Online Recruitment Fraud has become a serious issue with the widespread use of online job portals. Fraudulent job advertisements exploit job seekers by requesting sensitive information or financial payments. Traditional rule-based and machine learning methods are not sufficient to detect complex and evolving fraud patterns. This research proposes a deep learning-based detection system that analyzes textual and contextual features from job postings to identify fraudulent advertisements effectively. By integrating Natural Language Processing techniques with deep neural networks, the system can automatically detect suspicious job postings with higher accuracy compared to conventional approaches. The architecture includes modules for data collection, preprocessing, feature extraction, deep learning classification, and alert generation. The proposed approach reduces manual monitoring and helps recruitment platforms maintain trust and credibility. Overall, the system contributes to improving online job portal security and protecting job seekers from recruitment scams.

VII. FUTURE SCOPE

The proposed Online Recruitment Fraud detection system can be further improved by incorporating advanced deep learning and artificial intelligence techniques. Future work can focus on integrating transformer-based models such as BERT or GPT-based architectures to enhance the understanding of contextual language patterns in job advertisements. These models can significantly improve the accuracy of fraud detection by analyzing semantic relationships within job descriptions. Another possible extension is the integration of real-time monitoring systems that continuously analyze newly posted job advertisements on recruitment platforms. Behavioral analysis of recruiters, including posting frequency and communication patterns, can also be incorporated to strengthen fraud detection. Additionally, the system can be expanded to include multi-modal data analysis such as images, documents, and email communications used in recruitment processes. Integration with large job portals and government employment platforms can further enhance the system's effectiveness in preventing recruitment scams and ensuring safer online job search environments.

VIII. REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson Education, 2017.
[2] C. Bishop, Pattern Recognition and Machine Learning, Springer, 2016.
[3] I. Goodfellow, Deep Learning, MIT Press, 2016.
[4] T. Mikolov, Efficient Estimation of Word Representations in Vector Space, Google Research, 2013.
[5] Y. Goldberg, Neural Network Methods for NLP, Morgan & Claypool, 2017.
[6] S. Banerjee, Online Job Scam Detection Using NLP Techniques, IEEE, 2020.
[7] J. Kim, Fraudulent Job Posting Detection Using Machine Learning, ACM, 2018.
[8] T. Nguyen, Deep Learning Approaches for Fraud Detection, IEEE, 2021.
[9] R. Sharma, Fake Job Posting Detection

Using LSTM Networks, Springer, 2022.
[10] A. Ng, Machine Learning Yearning, DeepLearning.ai, 2019.
[11] D. Jurafsky, Speech and Language Processing, Pearson, 2021.
[12] K. Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012.
[13] F. Chollet, Deep Learning with Python, Manning Publications, 2018.
[14] P. Domingos, The Master Algorithm, Basic Books, 2015.
[15] S. Russell, Artificial Intelligence: A Modern Approach, Pearson, 2020.