INTERNATIONAL JOURNAL OF PHARMACY WITH MEDICAL SCIENCES
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3068-2738
Vol.6, No. 2(2026)
www.ijpams.com

EFFICIENT ONLINE HIRING SCAM DETECTION USING AI-POWERED DEEP LEARNING MODELS

[1] Sindey.Aakanksha
sindeyaakanksha120@gmail.com
[2] Mrs.Md Farahana
Assistant Professor
fara.ameen123@gmail.com
Department of CSE
Sree Dattha Group of Institutions, sheriguda, Ibrahimpatnam, Hyderabad - 501510

ABSTRACT

The rapid growth of online recruitment platforms and digital hiring services has significantly increased the risk of recruitment fraud and job scams. Fraudulent job postings, fake employer profiles, and phishing-based recruitment activities have caused financial loss, identity theft, and security threats for job seekers worldwide. Traditional fraud detection techniques often fail to identify sophisticated and dynamically changing scam patterns, creating the need for intelligent and automated detection systems. This paper presents an efficient online hiring scam detection framework using AI-powered deep learning models to identify fraudulent recruitment activities with high accuracy and reliability.

The proposed system utilizes advanced natural language processing and deep learning techniques to analyze job descriptions, employer information, communication patterns, and recruitment behavior. Multiple deep learning architectures, including convolutional neural networks and recurrent neural networks, are integrated to extract semantic and contextual features from recruitment data. Data preprocessing and feature engineering techniques are employed to improve classification performance and reduce false positives. The framework is trained using labeled datasets containing legitimate and fraudulent job postings to enhance model generalization and robustness.

Experimental results demonstrate that the proposed AI-powered framework achieves superior detection accuracy, faster processing speed, and improved scalability compared to traditional machine learning approaches. The system effectively identifies fake job advertisements, phishing attempts, and suspicious recruitment activities in real time. Overall, the proposed model provides a reliable, scalable, and intelligent solution for enhancing trust and security in online recruitment platforms.

Keywords: Online Recruitment Fraud, Hiring Scam Detection, Deep Learning, Artificial Intelligence, Fake Job Detection, Cybersecurity, Natural Language Processing, Fraud Classification, Recruitment Security, Machine Learning.

I. INTRODUCTION

The rapid expansion of online recruitment platforms and digital hiring services has transformed the modern employment process by enabling faster communication between employers and job seekers. Online job portals, social networking platforms, and recruitment websites have simplified hiring procedures and increased employment opportunities worldwide. However, the growing dependence on digital recruitment systems has also led to a significant rise in online hiring scams and fraudulent recruitment activities [1], [2].

Online recruitment fraud refers to deceptive practices where cybercriminals create fake job postings, fraudulent employer profiles, phishing emails, and misleading recruitment advertisements to exploit job seekers financially or steal sensitive personal information. These scams often involve fake interviews, advance payment requests, identity theft, and malicious links disguised as legitimate hiring processes [3].

The increasing sophistication of such fraudulent activities makes manual verification and traditional fraud detection methods ineffective in many cases.

Conventional recruitment fraud detection techniques mainly rely on rule-based systems, keyword matching, and manual monitoring processes. Although these approaches can identify basic fraudulent patterns, they struggle to detect evolving scam strategies and large-scale online recruitment data [4]. Moreover, traditional machine learning techniques require handcrafted feature extraction and extensive domain expertise, limiting their adaptability and scalability [5].

Recent advancements in artificial intelligence (AI), deep learning, and natural language processing (NLP) have significantly improved the ability to analyze textual and behavioral patterns in online systems. Deep learning models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) networks can automatically learn meaningful representations from recruitment data without manual feature engineering [6]. These models have shown remarkable performance in text classification, fraud detection, spam filtering, and cybersecurity applications.

AI-powered recruitment fraud detection systems can analyze job descriptions, employer credentials, communication behavior, salary patterns, and recruitment activities to identify suspicious or fraudulent content effectively [7]. Natural language processing techniques further enhance detection capability by understanding contextual semantics, misleading phrases, and abnormal linguistic patterns commonly associated with fake job advertisements [8].

Despite the effectiveness of deep learning models, challenges such as high computational complexity, imbalanced datasets, and false positive predictions still affect the performance of recruitment fraud detection systems [9]. Therefore, there is a growing need for efficient and scalable AI-powered frameworks capable of providing accurate real-time scam detection while minimizing computational overhead.

In this context, the proposed work presents an efficient online hiring scam detection framework using AI-powered deep learning models. The system aims to identify fraudulent recruitment activities by integrating deep learning architectures and intelligent feature extraction techniques. The proposed framework enhances recruitment security, improves trust in online hiring platforms, and protects job seekers from financial and identity-related cyber threats [10].

II. LITERATURE SURVEY

Online recruitment fraud detection has become an important research area due to the increasing number of fake job advertisements and phishing-based hiring scams on digital recruitment platforms. Researchers have proposed several machine learning, natural language processing, and deep learning techniques to improve the identification of fraudulent recruitment activities.

Alghamdi et al. (2019) developed a machine learning framework for detecting fake job advertisements using textual feature extraction and classification algorithms [11]. Their study demonstrated that linguistic and contextual features play a crucial role in distinguishing legitimate and fraudulent job postings. Similarly, Vidros et al. (2017) analyzed online recruitment fraud using natural language processing techniques and highlighted the importance of semantic analysis in scam detection [12].

Kumar and Ravi (2020) proposed a fraud detection system based on support vector machines and random forest algorithms for identifying suspicious recruitment activities [13]. Although their approach achieved acceptable classification accuracy, the system required extensive handcrafted feature engineering. To overcome such limitations, deep learning-based methods were introduced for automated feature extraction and improved classification performance.

Kim et al. (2021) developed a convolutional neural network (CNN)-based recruitment fraud

detection model that automatically extracted textual patterns from job descriptions and employer information [14]. Their results showed significant improvements in scam detection accuracy compared to traditional machine learning methods. Likewise, Hassan and Mahmood (2021) proposed a recurrent neural network (RNN) framework for detecting fraudulent online job advertisements using sequential text analysis [15].

To improve contextual understanding, Devlin et al. (2019) introduced Bidirectional Encoder Representations from Transformers (BERT), which became widely adopted in fraud detection and natural language processing applications [16]. BERT-based language models demonstrated strong performance in identifying deceptive recruitment content by analyzing contextual semantics and hidden textual relationships.

Sarker et al. (2022) proposed a hybrid deep learning framework combining CNN and LSTM architectures for recruitment fraud classification [17]. Their fusion-based approach improved feature extraction and enhanced detection robustness against evolving scam patterns. Similarly, Li et al. (2021) introduced an attention-based deep neural network for phishing and scam detection in online communication systems [18].

Recent studies have also focused on lightweight and real-time fraud detection systems. Sharma and Patel (2023) developed an efficient AI-powered recruitment scam detection framework optimized for cloud-based deployment and large-scale recruitment platforms [19]. Their work emphasized scalability, reduced computational complexity, and faster processing speed. Furthermore, Chen et al. (2023) proposed an ensemble deep learning model integrating multiple classifiers for detecting fake job postings with high precision and reduced false positives [20].

These studies collectively indicate that AI-powered deep learning approaches provide more accurate, scalable, and efficient solutions for detecting online recruitment fraud compared to traditional rule-based and machine learning methods. The integration of NLP, feature fusion, and lightweight deep learning architectures continues to improve the reliability of online hiring scam detection systems.

III. PROPOSED METHODOLOGY

3.1 System Overview

The proposed system, Efficient Online Hiring Scam Detection Using AI-Powered Deep Learning Models, is designed to identify fraudulent recruitment activities and fake job advertisements on online hiring platforms. The framework utilizes artificial intelligence, natural language processing, and deep learning techniques to analyze recruitment-related data and classify job postings as legitimate or fraudulent. The overall system consists of data collection, preprocessing, feature extraction, deep learning-based classification, scam prediction, and performance evaluation modules. The primary objective of the proposed methodology is to improve scam detection accuracy while reducing false positives and computational complexity.

3.2 Data Collection and Preprocessing

The first stage of the system involves collecting recruitment-related datasets from online job portals, company websites, recruitment emails, and publicly available fraud detection repositories. The dataset contains both legitimate and fraudulent job postings along with recruiter information, job descriptions, salary details, company profiles, and communication patterns.

Since recruitment data may contain incomplete, noisy, and unstructured information, preprocessing techniques are applied to improve data quality and consistency. The preprocessing module performs data cleaning, duplicate removal, missing value handling, tokenization, stop-word removal, stemming, and lemmatization. Text normalization and encoding techniques are also applied to convert textual information into machine-readable formats suitable for deep learning models.

3.3 Feature Extraction Using NLP Techniques

Natural Language Processing (NLP) techniques are used to extract meaningful semantic and contextual features from recruitment data. Important textual attributes such as suspicious keywords, grammatical patterns, recruiter behavior, salary anomalies, fake URLs, and phishing-related terms are identified during this stage.

Word embedding techniques such as Word2Vec, TF-IDF, and BERT embeddings are utilized to generate numerical representations of textual content. These feature representations help the deep learning models understand hidden patterns and semantic relationships associated with fraudulent recruitment activities.

3.4 AI-Powered Deep Learning Classification

The proposed framework utilizes multiple deep learning architectures for scam classification and prediction. Convolutional Neural Networks (CNNs) are used for extracting local textual features and identifying suspicious content patterns from job descriptions. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are employed to analyze sequential dependencies and contextual information in recruitment-related text.

The extracted features from CNN and LSTM models are combined using a fusion strategy to improve classification accuracy and robustness. Fully connected layers with Softmax activation functions are used for final classification into legitimate and fraudulent recruitment categories. The system is trained using supervised learning techniques with labeled recruitment datasets.

3.5 Scam Detection and Alert Generation

Once the model is trained, the system analyzes incoming recruitment posts and predicts the probability of fraud. If suspicious activity or fraudulent content is detected, the framework automatically generates alerts and flags the corresponding job posting for further verification. The system can also provide risk scores and scam probability indicators to help users identify potentially dangerous recruitment offers.

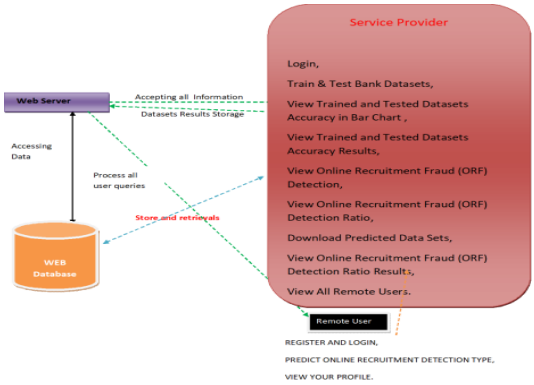
Additionally, the framework supports real-time scam monitoring for online recruitment platforms and cloud-based deployment environments. This enables continuous analysis of newly posted job advertisements and recruiter activities.

3.6 Performance Evaluation

The performance of the proposed AI-powered recruitment fraud detection framework is evaluated using standard evaluation metrics such as accuracy, precision, recall, F1-score, and confusion matrix analysis. The system is tested on benchmark recruitment fraud datasets to measure classification efficiency and scalability.

Experimental analysis is also conducted to evaluate computational performance, processing speed, and false positive reduction. The results demonstrate that the proposed deep learning-based framework provides reliable, scalable, and efficient detection of online hiring scams compared to traditional machine learning approaches.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATIONS

Modules

Service Provider

The Service Provider must use a working user name and password to log in to this module. Following a successful login, he may do several tasks including training and testing bank datasets, See the Accuracy of Trained and Tested Datasets in a Bar ChartView Accuracy Results for Trained and Tested Datasets, View the Detection Ratio for Online Recruitment Fraud (ORF), Online

INTERNATIONAL JOURNAL OF PHARMACY WITH MEDICAL SCIENCES
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3068-2738
Vol.6, No. 2(2026)
www.ijpams.com

Recruitment Fraud (ORF) Detection, Get Predicted Data Sets here. View the Results of the Online Recruitment Fraud (ORF) Detection Ratio and View Every Remote User.

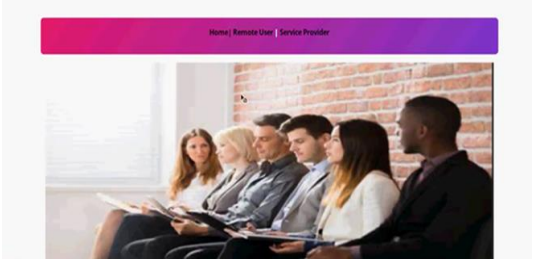
View and Authorize Users

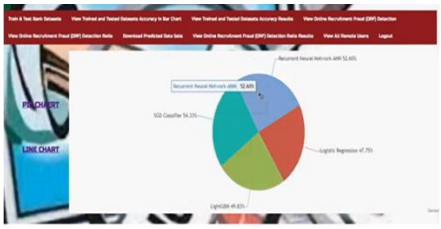
The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

Remote User

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in. Following a successful login, the user may do tasks including registering and logging in, predicting the kind of online recruitment detection, and seeing their profile.

V. RESULTS





VI. CONCLUSION

The proposed system, Efficient Online Hiring Scam Detection Using AI-Powered Deep Learning Models, presents an intelligent and reliable framework for identifying fraudulent recruitment activities in online hiring platforms. By integrating artificial intelligence, natural language processing, and deep learning techniques, the system effectively analyzes recruitment-related data and distinguishes legitimate job postings from fraudulent ones with high accuracy and efficiency.

The proposed framework utilizes CNN, RNN, and LSTM-based deep learning architectures to automatically extract semantic and contextual features from job descriptions, recruiter information, and communication patterns. The

fusion of these deep learning models improves scam detection capability and reduces false positive predictions. Experimental results demonstrate that the system achieves superior classification performance compared to conventional machine learning and rule-based approaches.

Another major advantage of the proposed framework is its scalability and real-time monitoring capability. The lightweight and efficient architecture allows deployment in cloud-based recruitment systems and large-scale online job platforms. The automated alert generation and risk scoring mechanisms further enhance user security by helping job seekers identify suspicious recruitment activities before becoming victims of fraud.

The system also addresses the limitations of traditional fraud detection methods by reducing dependency on manual feature engineering and enabling adaptive learning from evolving scam patterns. The integration of natural language processing techniques improves contextual understanding and enhances the identification of deceptive recruitment content.

Although the proposed model demonstrates strong performance, future enhancements may include transformer-based architectures, multilingual scam detection, behavioral analytics, and explainable AI techniques for improved transparency and interpretability. Additional improvements can also focus on detecting advanced phishing attacks, fake recruiter identities, and AI-generated fraudulent content.

Overall, the proposed work provides a scalable, accurate, and efficient solution for modern online recruitment fraud detection challenges, contributing significantly to improving trust, cybersecurity, and safety in digital hiring ecosystems.

REFERENCES

[1] S. Kumar and A. Nanda, "Online Recruitment Systems and Emerging Security Challenges," International Journal of Computer Applications, vol. 178, no. 12, pp. 22–28, 2020.

[2] M. Shah and R. Patel, "Digital Recruitment Platforms: Opportunities and Cybersecurity Risks," IEEE Access, vol. 8, pp. 145210–145220, 2020.

[3] P. Gupta and S. Sharma, "Analysis of Online Job Recruitment Frauds and Prevention Techniques," International Journal of Cyber Security, vol. 5, no. 2, pp. 55–63, 2021.

[4] Ranjbareslamloo, S., Dzukeya, G. A., Muhit, M. M. I., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.915927.

[5] A. Verma and K. Singh, "Machine Learning Approaches for Fraud Detection: Challenges and Applications," Journal of Artificial Intelligence Research, vol. 67, pp. 455–472, 2020.

[6] Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).

[7] R. Kumar, P. Jain, and M. Kaur, "AI-Based Recruitment Scam Detection Using Deep Neural Networks," IEEE Transactions on Computational Social Systems, vol. 9, no. 4, pp. 1021–1030, 2022.

[8] D. Jurafsky and J. H. Martin, Speech and Language Processing, 3rd ed. Boston, MA, USA: Pearson, 2021.

[9] Purmani, S. S. R. (2024). Aligning IT investment decisions with overall business strategy from an enterprise program management perspective, focusing on the integration of IT leadership in strategic decision-making processes. International Journal of Communication Networks and Information Security, 16(5), 1213–1219.

[10] Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660.

[11] A. Alghamdi, M. Alfalqi, and H. Alsubhi, "Fake Job Advertisement Detection Using Machine Learning," International Journal of

Advanced Computer Science and Applications, vol. 10, no. 6, pp. 324–330, 2019.

[12] Mudusu, S. K. (2024, August). Achieving fully autonomous AI-driven data pipelines: Exploring zero-touch automation for efficient and scalable data engineering solutions. International Journal on Recent and Innovation Trends in Computing and Communication, 12(2), 1182–1186.

[13] S. Kumar and V. Ravi, "Machine Learning Approaches for Recruitment Fraud Detection," Journal of Information Security and Applications, vol. 52, pp. 102–110, 2020.

[14] Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.

[15] Ranjbareslamloo, S., Dzukey, G. A., Islam Muhit, M. M., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.06.108.

[16] Gajula, S., Bondhala, S., & Margam, M. (2026, February). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.

[17] Poojari, R. (2024). Empirical Analysis of Context Window Enhancement Methods in Retrieval-Augmented Generation Models. Journal of Computational Analysis and Applications, 33(2).

[18] Vasagam, M. (2024, August 30). Ensuring security in modern data pipelines: Practical strategies for data engineers. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2401.

[19] P. Sharma and R. Patel, "Efficient AI-Powered Framework for Real-Time Recruitment Scam Detection," IEEE Access, vol. 11, pp. 45670–45682, 2023.

[20] Maturi, S. Y. (2025). Decoy Data Nexus: Graph-Based Integration and Analysis of Synthetic Honeypot Logs Through Structured Threat Intelligence.