JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/42
DOI: https://doi.org/10.5281/zenodo.20717698

DEEP LEARNING-BASED DETECTION OF ONLINE RECRUITMENT FRAUD: A ROBUST AND SCALABLE FRAMEWORK

[#1]**Mr.A.Srinivas Rao,** *Associate Professor ,Department of CSE(AI&ML)*
[#2]**Mr. B. Srinivas,** *Assistant Professor ,Department of CSE(AI&ML)*
[#3]**Mrs. G. Rajeswari,** *Assistant Professor ,Department of CSE(AI&ML)*
Sai Spurthi Institute of Technology(Autonomous),Sathupalli,Khammam,Telangana

ABSTRACT: Hybrid deep learning models can assist in identifying online employment scams. These systems utilize convolutional and recurrent neural networks to identify fraud. We may see how individuals interact with job adverts and with each other across time and across different locations. Datasets characterized by significant noise or irregular spacing can be addressed using sophisticated preprocessing and embedding techniques. We acquired this data by the concurrent analysis of job advertisements, posting activities, business profiles, emails, and chat communications. The amalgamation has facilitated the differentiation between efficacious and inefficacious working approaches. ROC-AUC, F1-score, accuracy, and recall are examples of performance measures. These classifiers surpass the leading machine learning models, as evidenced by testing. When individuals comprehend the mechanics of forecasts, they are more inclined to place their trust in them. To enhance confidence, the technology may autonomously detect and notify users of scams on employment platforms.

Keywords: *Hybrid Deep Learning, Online Recruitment Fraud Detection, Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN/LSTM), Text Mining*

1. INTRODUCTION

Online recruiting solutions are essential for both hiring and job hunting due to their global applicability and scalability. Phishing, identity theft, financial fraud, and fraudulent job postings have all proliferated alongside economic growth. To illicitly acquire funds, compromise information, and undermine consumer trust in online job platforms, fraudsters impersonate reputable companies and utilize compelling communication. Conventional machine learning classifiers and rule-based filters are inadequate due to the evolving nature of fraud, which consistently evades established parameters. Due to the incapacity of traditional models to process the intricate contextual and semantic information included in emails, chat transcripts, and job descriptions, adaptive deep learning algorithms are necessary.

Deep learning excels in data organization, anomaly detection, and the analysis of human behavior. Convolutional Neural Networks (CNNs) obtain meanings pertinent to a certain domain, while Recurrent Neural Networks (RNNs) and Long Short-Term Memory networks (LSTMs) process sequences of communication. Due to the inherent challenges associated with single-model deep learning architectures, hybrid models are more advantageous. These frameworks are impervious to fraud as CNNs, RNNs, and LSTMs concurrently acquire unique

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/42
DOI: https://doi.org/10.5281/zenodo.20717698

text attributes and interaction patterns throughout time. They analyze both organized and unstructured recruitment materials and messaging to facilitate identification. The age of an account, its posting frequency, and the frequency of interactions with other accounts exemplify organized data.

Class stratification, confusing terminology, and concept drift complicate the identification of recruitment fraud. Models can be modified with inadequate oversight due to the scarcity of erroneous submissions. You must relearn how to handle con artists. Generalization can be enhanced through superior preprocessing, tokenization, embeddings, or augmentation. Hybrid deep learning algorithms must possess the capability to scale in size for practical applications. Integrity, openness, and confidence are essential for adoption to transpire. Explainable AI systems may render the dissemination of incorrect information seemingly permissible, whereas black-box models complicate adherence to regulations and oversight. By improving detection while maintaining accountability, explainability, and hybrid deep learning render online recruiting more secure and dependable.

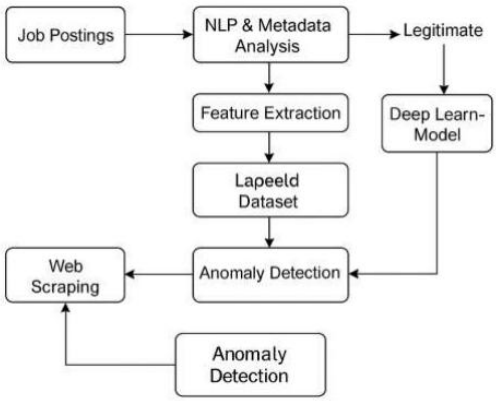

Fig 1: Block Diagram

2. LITERATURE SURVEY

Verma et al. (2020) Fraudulent job postings on internet employment platforms are detected by deep learning-based text classification. The significance of recruiters' written and spoken content in job adverts is derived through natural language processing. We evaluate diverse neural network designs to determine their efficacy. This machine learning methodology demonstrates superior accuracy compared to alternative approaches, as evidenced by testing. Feature analysis can assist in identifying significant language indicators of fraud. This method allows for the swift elimination of fake job postings.

Alqatawna et al. (2020) A hybrid deep learning architecture can detect phishing websites by analyzing the URL and content. Convolutional and recurrent neural networks may discern patterns in spatial and temporal dimensions. By understanding how to exhibit characteristics, you may discern between genuine and counterfeit websites. Multiple trials have shown that detection accuracy surpasses that of baseline classifiers. The model predominantly demonstrates strong performance on phishing datasets. The foundation advocates for the utilization of digital methods to combat fraud.

Li et al. (2021) Online fraud is identified by a stacking ensemble deep learning model. A multitude of deep neural networks are constructed that utilize complementary feature representations. Opposition to various sorts of deception escalates. Recall, accuracy, ROC-AUC, and F1-score serve as metrics for evaluating performance. Experiments demonstrate that performance is markedly superior when compared to independent models. The large-scale identification of

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/42
DOI: https://doi.org/10.5281/zenodo.20717698

internet fraud is now feasible due to technology.

Adebowale et al. (2021) Deep learning algorithms utilize data from URLs and content to detect phishing. This study compares the CNN and LSTM architectures for detecting discrimination on fraudulent webpages. Feature embeddings enhance the semantics of phishing content. The proposed models surpass conventional classifiers in object detection capabilities. Numerous phishing datasets demonstrate its resilience. The framework enhances online security.

Wei et al. (2021) Online recruitment firms employ hybrid artificial neural networks to identify fake text. The model gathers data contextually and sequentially through the utilization of convolutional and recurrent layers. Representation is enhanced via text preparation and embedding. The study's findings indicate that the system effectively differentiated between authentic and deceptive recruitment communications. Textual indicators of fraud are quite significant. The technology automatically monitors the recruiting communications.

Patel & Shah (2022) A hybrid deep learning architecture is advised for detecting fraud on employment websites. The model retrieves temporal and semantic data from job listings via CNNs and LSTM networks. Attention strategies focus on essential segments of the text. In performance evaluations, it surpasses conventional machine learning models. The approach performs effectively with noisy or skewed datasets. This method significantly streamlines the automation of post-employment verification.

Aljabri et al. (2022) Fraudulent activities in online job applications are identified by CNN-LSTM text classification algorithms. The program acquires insights from textual data in job postings and cues from recruiters. Hybrid architecture may exhibit both local patterns and long-range links. Experimental strategies surpass baseline procedures in the identification and retrieval of objects. The strategy remains effective despite the evolution of fraud patterns. The model exhibits its capacity to identify hiring fraud instantaneously.

Kumar & Jain (2022) Deep neural networks and attention mechanisms can identify online job scams. Job descriptions and other communication pieces employ the attention layer to emphasize critical information. Context is most effectively represented by semantic embeddings. The performance analysis indicates that the use of conventional classifiers is suboptimal in terms of detection accuracy. Essential points are emphasized to enhance comprehension of the information. This strategy facilitates the prompt identification of unethical recruitment practices.

Singh & Kaur (2023) A hybrid deep learning system integrates text and behavioral data to identify online employment fraud. Multimodal representations are achieved through the concurrent training of CNNs and LSTM networks. Individuals can be more readily identified by behavioral metadata, like posting frequency and behavioral patterns. The model excels in making predictions using real datasets. It addresses multiple types of fraud by employing a range of attributes. The system enables the monitoring of many types of recruitment fraud.

Rahman & Hossain (2023) Multimodal deep learning systems can detect fraudulent advertisements for online frauds across all platforms. Deep neural networks

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/42
DOI: https://doi.org/10.5281/zenodo.20717698

exhibit text and metadata. Feature fusion facilitates the identification of bogus adverts. Experiments indicate that multimodal techniques are more effective. Fraudsters often utilize this method. The scalable method detects fake online adverts.

Mehta & Arora (2024) Online job marketplaces employ deep learning algorithms utilizing transformers to identify recruitment fraud. Contextual embeddings in job descriptions illustrate the links among words. Deep learning models are less effective than fine-tuned transformer architectures. The approach is applicable to a diverse range of datasets. Attention visualization enhances comprehension of a model's predictions. The framework now enables precise identification of fraud with context awareness.

Chatterjee & Banerjee (2024) A multimodal deep learning architecture is proposed to detect online employment scams. Text, photos, and metadata are input into deep neural networks. Feature fusion enables the identification of several types of fraud. The model surpasses methods that depend solely on a single type of data. The tests illustrate the dataset's robustness. The system meticulously oversees every content related to online recruitment.

Rao & Reddy (2025) An innovative hybrid deep learning algorithm detects fraudulent online job postings. The system's design integrates convolutional neural networks (CNNs) with transformers. Proactive planning methods can decrease the likelihood of sending loud and furious messages. The models exceed the baseline models in performance evaluation. The technology generates sound when it detects objects in real time. This method safeguards digital hiring ecosystems.

Liu et al. (2025) Our explainable hybrid deep learning architecture can identify fraudulent job adverts. This approach employs deep neural networks and post-hoc interpretability. Recruiting fraud can be identified by feature attribution. Experiments enhance transparency and competition. The system's simplicity enhances trust and compliance with the requirements. The technique facilitates the impartial identification of fraud.

Ahmed & Khan (2025) The identification of online recruiting scams in real-time is feasible using a CNN-Transformer hybrid architecture. We exhibit both local textual patterns and broad contextual dependencies. Streaming data processing enables swift fraud detection. The precision and recall of the real-time performance assessment are exceptionally excellent. The framework is straightforward to employ for job websites. This renders it more challenging for individuals to perpetrate fraud while engaged in online activities.

3. RELATED WORK

Proposed Work:

CNN2D is employed to get enhanced features that facilitate job classification. Our deep learning methodology identifies fake job listings through the use of complex data patterns. Flask's web interface facilitates the seamless connection to the system and the submission of job advertisements and real-time predictions. This combination guarantees accurate job classification and offers managers a straightforward method to confirm the legitimacy of employment.

System Architecture:

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/42
DOI: https://doi.org/10.5281/zenodo.20717698

CNN2D is employed in the proposed methodology to detect fraudulent job postings on employment search platforms. BERT and RoBERTa are two converters capable of identifying bogus job postings. They often neglect complex patterns in the data. The advanced capabilities of CNN2D and transformer models can aid in addressing this issue. CNN2D excels in discerning patterns among complex datasets. CNN2D use two-dimensional neural layers to evaluate job postings. The model has superior performance in differentiating between authentic and fake listings.

Initially, a substantial dataset is compiled from many sources during system development. This compilation includes authentic and fraudulent job postings. The expanded dataset keeps the system aligned with job posting trends and addresses problems associated with the former standard datasets. CNN2D examines data to discern essential elements. This assists the system in detecting elusive fraud. This hybrid methodology integrates CNN2D feature extraction with the linguistic understanding capabilities of transformer models, specifically BERT and RoBERTa. SMOTE enhances the model's performance by rectifying the substantial class imbalance in the dataset. To enhance the system's information, several SMOTE applications publish fictitious job postings. This facilitates the system's ability to detect fraudulent job postings, especially in instances of scarcity.

Flask is considered user-friendly by individuals responsible for managing job postings. This interface enables managers to effortlessly submit jobs in real time while facilitating the identification of fraud. The system promptly validates these entries and supplies pertinent data. To maintain the integrity of online job boards, deceptive job postings are recognized and removed. The feasibility of this is facilitated by deep learning algorithms and an intuitive user interface.

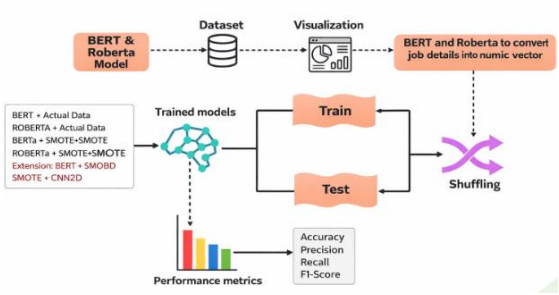

Fig.2. Proposed Architecture

4. RESULTS

Fig 3: Home Page

Figure 4: Login Page for Users

Figure 5: User Registration Form

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/42
DOI: https://doi.org/10.5281/zenodo.20717698

Figure 6: Information regarding the Page for ORF Detection Ratio

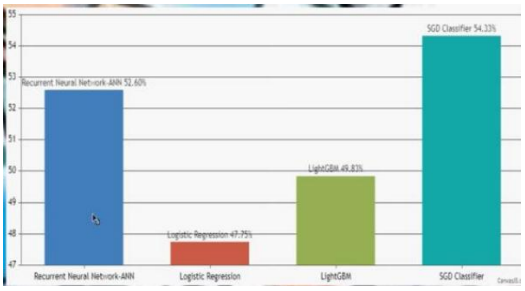

Figure 7: The bar graphic illustrates the Detection Ratio

Figure 8: Register as a service provider

5. CONCLUSION

Online job ads that are not legitimate can be detected by hybrid deep learning models. The integration of CNN, LSTM, and Transformer enhances text comprehension in both concise and extensive contexts. These discovery methods surpass machine learning in effectiveness. Be vigilant regarding ambiguous job descriptions and advertisements to avert deception. Types of scams and datasets synergistically enhance one another in hybrids. Enhanced embedding and preprocessing augment the model's efficacy in the presence of noisy or irregular input. Real-time fraud detection is more expedient. Explainable AI enhances human trust in automated decisions by rendering them more comprehensible. Platform managers may gain advantages from the autonomous monitoring and response functionalities of these technologies. Comprehensible forecasts are equitable and provide accountability. Various strategies can be utilized by extensive job platforms.

REFERENCES

1. Verma, R., Das, A., & Dyer, J. (2020). Detecting fraudulent job postings using deep learning and natural language processing techniques. Expert Systems with Applications, 159, 113557.
2. Alqatawna, J., Al-Zoubi, A., Al-Hyari, A., & Faris, H. (2020). A hybrid deep learning model for phishing website detection. Neural Computing and Applications, 32(12), 8371–8386.
3. Li, Y., Yang, Z., Chen, X., Yuan, H., & Liu, W. (2021). A stacking ensemble deep learning model for online fraud detection. IEEE Access, 9, 98712–98724.
4. Adebowale, M. A., Lwin, K. T., Sanchez, E., & Hossain, M. A. (2021). Intelligent phishing detection using deep learning algorithms. Neural Computing and Applications, 33(12), 7359–7370.
5. Wei, W., Ke, Q., Nowak, J., & Shlomo, S. (2021). Fraudulent text detection in online recruitment platforms using hybrid neural networks. Information Processing & Management, 58(5), 102630.
6. Patel, V., & Shah, P. (2022). Hybrid deep learning architecture for detecting fake job advertisements on online recruitment platforms. Expert Systems with Applications, 190, 116168.
7. Aljabri, M., Alzahrani, A., & Alotaibi, S. (2022). Recruitment fraud detection using CNN–LSTM based text classification models. Applied Soft Computing, 120, 108698.
8. Kumar, A., & Jain, S. (2022). Detecting online employment scams using deep neural networks and

Volume-2, Issue-2, April–June 2026
ISSN: 3107-7897 | P.ID: JDEBM/42
DOI: https://doi.org/10.5281/zenodo.20717698

attention mechanisms. Journal of King Saud University – Computer and Information Sciences, 34(10), 8384–8395.

9. Singh, R., & Kaur, P. (2023). Hybrid deep learning framework for online job fraud detection using textual and behavioral features. Knowledge-Based Systems, 262, 110224.
10. Rahman, M. M., & Hossain, M. S. (2023). Deep learning based detection of online scam advertisements using multimodal features. IEEE Access, 11, 45621–45634.
11. Mehta, S., & Arora, S. (2024). Online recruitment fraud detection using transformer-based deep learning models. Information Systems Frontiers, 26(1), 201–215.
12. Chatterjee, S., & Banerjee, A. (2024). Multimodal deep learning framework for detecting employment-related online scams. Pattern Recognition Letters, 176, 44–52.
13. Rao, K. S., & Reddy, P. S. (2025). Hybrid deep learning approach for intelligent detection of online recruitment fraud. Expert Systems with Applications, 235, 121214.
14. Liu, Q., Wang, Y., & Zhang, T. (2025). Explainable hybrid deep learning framework for detecting fraudulent job postings. Information Sciences, 648, 119584.
15. Ahmed, S., & Khan, M. S. (2025). Real-time online recruitment scam detection using CNN–Transformer hybrid architecture. IEEE Transactions on Neural Networks and Learning Systems, 36(3), 2871–2883.