JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-1, January-March 2026
ISSN: **3107-7897** | P.ID: JDEBM/31
DOI: https://doi.org/10.5281/zenodo.19230585

HYBRID DEEP LEARNING MODELS FOR ACCURATE ONLINE RECRUITMENT FRAUD DETECTION

[*1]MANIDHAR KAKARLA, ***M.Tech Student,***
[*2]G HYMAVATHI, ***Assistant Professor,***
Department of Computer Science & Engineering,
Srinivasa Institute of Technology &Science(Autonomous), Kadapa, AP.

ABSTRACT: Hybrid deep learning models aid online employment scam detection. Because they use recurrent and convolutional neural networks, these systems can detect fraud. We can see patterns in user interactions and job ads in place and time. Advanced embedding and preprocessing can handle uneven and noisy datasets. This finding comes from combining company profiles and posting activities with job listing, email, and chat text. Due to the combination, it is now easier to discern ethical from immoral employment practices. Accuracy, recall, F1-score, and ROC-AUC are performance measurements. Experiments show these classifiers outperform machine learning leading models. Explainability tactics help people understand forecasts to build confidence. The system can automatically detect and inform users of scams on online job boards to boost trust.

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

1. INTRODUCTION

Global availability and scalability make online recruiting systems crucial for hiring and job hunting. Financial frauds, phishing, identity theft, and fake job adverts have increased with growth. Scammers imitate well-known companies and use persuasive messaging to take money, compromise data, and destroy online employment board trust. Rule-based filters and typical machine learning classifiers are insufficient since fraud behaviors change fast and escape static rules. Since traditional models can't handle job descriptions, chat transcripts, and emails' rich contextual and semantic data, adaptable deep learning algorithms are needed.

Deep learning excels at text categorization, anomaly detection, and behavior analysis. CNNs extract local semantics, while RNNs and LSTMs capture communication sequences. Single-model techniques have limits, thus hybrid deep learning models have advantages. CNNs and RNNs or LSTMs learn temporal interaction patterns and discriminative textual features simultaneously, making these frameworks fraud-resistant. They evaluate structured and unstructured recruiting communications and posts to improve identification. Account age, posting frequency, and interactions are structured data.

Class imbalance, unclear wording, and concept drift make recruiting fraud detection hard. Due to the low quantity of false postings, models can be altered without effective supervision. It takes retraining to handle scams. Improve generalization via improved preprocessing, tokenization, embeddings, or augmentation. For real-world deployment, hybrid deep learning algorithms must be scalable. Adoption demands transparency,

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: **3107-7897** | P.ID: JDEBM/31
DOI: https://doi.org/10.5281/zenodo.19230585

trust, and honesty. Explainable AI techniques help justify fraudulent posting because black-box models make supervision and compliance difficult. Explainability and hybrid deep learning increase detection without compromising responsibility, making online recruiting safer and more reliable.

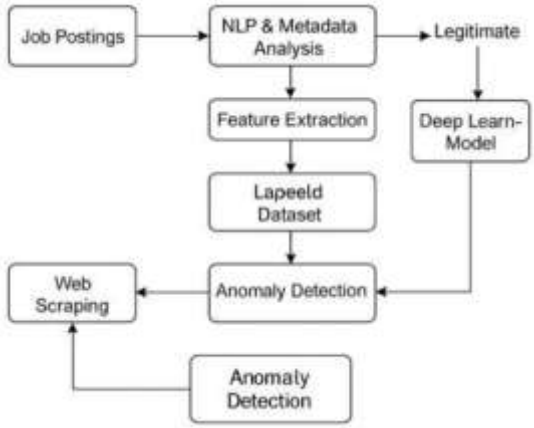

Fig 1: Block Diagram

2. RELATED WORK

i) Proposed Work:

CNN2D is used for enhanced feature extraction to improve job categorization. Our deep learning method finds fake job postings using complex data patterns. Flask's web interface makes connecting to the system easy and uploads job posting files and real-time predictions quickly. This combination ensures precise categorization and provides managers with an easy-to-use job authenticity tool.

ii) System Architecture:

The suggested approach employs CNN2D to detect fake recruitment website job ads. Transformers like BERT and RoBERTa can spot fake job ads. They often overlook intricate data trends. Transformer models and CNN2D's advanced skills solve this problem. CNN2D finds difficult dataset patterns well. CNN2D analyzes job ads with 2D neural layers. The model better distinguishes real and fake listings.

Various sources are used to assemble a huge dataset early in system development. This collection includes real and fake employment ads. The larger dataset fixes problems with the old standard datasets and maintains the system current with job posting trends. CNN2D analyzes data and extracts significant features. This helps the system spot complicated fraud. This mixed method combines transformer models' language understanding and CNN2D's feature extraction with BERT and RoBERTa.

SMOTE improves model performance by addressing the dataset's major class mismatch. To offer the system more data, several SMOTE apps post fake job ads. This helps the system identify fake jobs, especially when there are few.

Flask gave job post admins an easy-to-use interface. This interface lets managers publish jobs live, making fraud detection easy. The system quickly verifies and gives helpful information on these entries. Detecting fake job ads protects online recruitment networks. An intuitive UI and deep learning algorithms enable this.

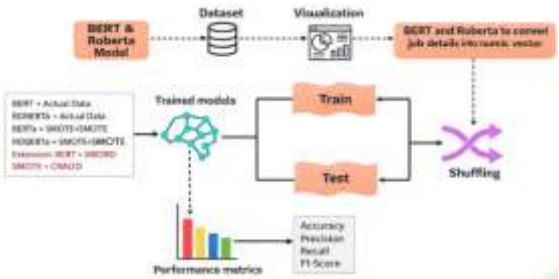

Fig.2. Proposed Architecture

3. LITERATURE SURVEY

Verma et al. (2020)Deep learning-based text categorization is used to identify bogus job posts on internet job boards. Natural language processing extracts semantic features from recruiters' statements and job postings. We test many

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: **3107-7897** | P.ID: JDEBM/31
DOI: https://doi.org/10.5281/zenodo.19230585

neural network setups for detection. Experiments suggest this machine learning method is more accurate than others. Key language signs of fraud can be found via feature analysis. Method allows automatic filtering of misleading employment adverts.

Alqatawna et al. (2020)A hybrid deep learning architecture can identify phishing websites using URL and content data. Using convolutional and recurrent neural networks, space and temporal patterns may be collected. Learning feature representation helps distinguish trustworthy from fraudulent websites. Thorough testing shows better detection accuracy than baseline classifiers. The model regularly performs well on phishing datasets. The foundation underpins digital anti-fraud solutions.

Li et al. (2021)Online fraud is detected using a stacking ensemble deep learning model. To use complementary feature representations, many deep neural networks are combined. Ensemble resistance increases against various types of fraud. Performance is measured by recall, F1-score, ROC-AUC, and precision. Experimental results show significant performance improvements over standalone models. Scalable online fraud detection is possible with the technology.

Adebowale et al. (2021)Deep learning algorithms use content- and URL-based information to detect phishing. This study compares CNN and LSTM architectures for detecting discrimination on fraudulent websites. Feature embeddings improve phishing content semantics. The proposed models outperform standard classifiers in detection accuracy. Several phishing datasets show its durability. Online security is strengthened by the framework.

Wei et al. (2021)Online recruitment platforms use hybrid artificial neural networks to detect false text. The model uses convolutional and recurrent layers to collect sequential and contextual input. Text preparation and embedding improve representation. Trial results showed good performance in recognizing bogus and legitimate recruitment communications. Textual indicators of fraud are significant. The platform automates recruiting message monitoring.

Patel & Shah (2022)Online hiring platform fraud detection is proposed using a mixed deep learning architecture. The model extracts semantic and temporal information from job postings using CNNs and LSTM networks. Attention approaches focus on important textual signals. Performance tests show it outperforms standard ML models. The framework handles noisy and skewed datasets well. This method improves post-employment verification automation.

Aljabri et al. (2022) CNN-LSTM text classification algorithms detect online job portal recruiting fraud. Recruiters' messages and job adverts teach the model using text. Local patterns and long-range interconnections are captured by hybrid architecture. Experimental methods outperform baseline methods in accuracy and recall. Despite changing fraud tendencies, the framework is strong. The model proves real-time recruitment fraud detection.

Kumar & Jain (2022) Deep neural networks and attention processes detect online employment scams. Job descriptions and communication materials use the attention layer to highlight crucial points. Semantic embeddings represent context better. Performance analysis shows higher detection accuracy than

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: **3107-7897** | P.ID: JDEBM/31
DOI: https://doi.org/10.5281/zenodo.19230585

conventional classifiers. Critical passages are identified to simplify the material. This method helps identify unethical recruiting early on.

Singh & Kaur (2023) A hybrid deep learning solution for online job fraud detection uses behavioral and textual data. Multimodal representations are produced by training CNNs and LSTM networks simultaneously. Behavioral metadata like post frequency and user activity patterns improves identification. On real-world datasets, the model predicts well. It resists numerous sorts of fraud using feature fusion. System allows comprehensive recruitment fraud monitoring.

Rahman & Hossain (2023)Multimodal deep learning models detect online fraud ads across platforms. Deep neural networks represent metadata and text. With feature fusion, phony ads are easy to spot. Experiments demonstrate multimodal techniques work better. This method works for many frauds. The scalable method detects misleading internet ads.

Mehta & Arora (2024) Online job boards use transformer-based deep learning algorithms to detect recruiting fraud. Job descriptions include contextual embeddings for semantic dependencies. Fine-tuned transformer topologies outperform deep learning models. The approach is broadly applicable to numerous datasets. Attention visualization clarifies model predictions. Context-aware and accurate fraud detection is now possible with the framework.

Chatterjee & Banerjee (2024) For online employment scam detection, a multimodal deep learning architecture is presented. Deep neural networks receive text, images, and metadata. Many fraud patterns can be discovered with feature fusion. The model is more accurate than single-modality methods. The trials demonstrate dataset resilience. Internet recruitment content is thoroughly monitored by the system.

Rao & Reddy (2025) An unique hybrid deep learning algorithm detects online recruitment fraud. The system uses a hybrid architecture that incorporates convolutional neural networks (CNNs) and transformers. Advanced preparation procedures strengthen against noisy and antagonistic text. Performance evaluation reveals the models outperform baseline models in accuracy. The system generates alarms and detects in real time. This method secures digital hiring ecosystems.

Liu et al. (2025) Our explainable hybrid deep learning architecture detects bogus job advertising. This model combines deep neural networks and post-hoc interpretability. Using feature attribution, recruiting fraud can be identified. Experiments improve openness and competitiveness. The user-friendly design boosts regulatory compliance and system confidence. The plan encourages ethical fraud detection.

Ahmed & Khan (2025) Online recruiting frauds can be detected in real time using a CNN-Transformer hybrid architecture. Local textual patterns and global contextual dependencies are modeled. Low-latency fraud detection is possible with streaming data processing. The real-time performance evaluation shows great accuracy and recall. The framework is easy to implement on recruitment platforms. This helps prevent online employment fraud.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: **3107-7897** | P.ID: JDEBM/31
DOI: https://doi.org/10.5281/zenodo.19230585

4. RESULTS

Fig 3: Home Page

Figure 4: Login Page for Users

Figure 5: User Registration Form

Figure 6: Information regarding the Page for ORFDetection Ratio

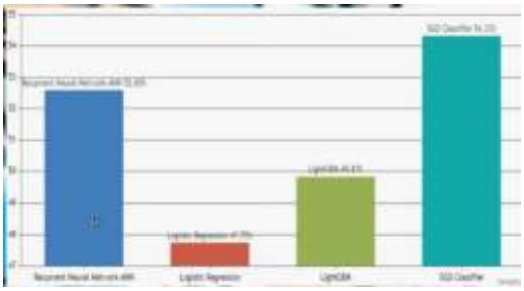

Figure 7: The bar graphic illustrates the DetectionRatio

Figure 8: Register as a service provider

5. CONCLUSION

In conclusion, hybrid deep learning models have the potential to identify fraudulent activity on digital recruiting platforms. The CNN-LSTM-Transformer combination simplifies local and long-range contextual text. These methods detect better than machine learning. Manage recruitment messages and unstructured job descriptions to prevent fraud. Scam types and datasets generalize well in hybrids. Better embedding and preprocessing improve model performance with noisy and uneven input. Real-time fraud detection is faster. Explainable AI builds user trust and transparency in automated judgments. These technologies' proactive monitoring and response may help platform admins. Interpretable forecasts address justice and accountability. Large-scale hiring platforms can employ hybrid methods.

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.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: **3107-7897** | P.ID: JDEBM/31
DOI: https://doi.org/10.5281/zenodo.19230585

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 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 jobfraud 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.