ETDT

Emerging Trends in Digital Transformation

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-09***

INTELLIGENT DETECTION OF ONLINE JOB SCAM ACTIVITIES USING DEEP NEURAL NETWORKS

[#1] KATRAJ SHIVASREE, *Dept of CSE,*
[#2] Dr.T.RAVIKUMAR, *Professor, Dept of CSE,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: An inventive Deep Neural Network (DNN) technique for identifying online employment fraud is presented in this paper. Fraudulent job advertisements on social media and digital recruitment platforms have cost job searchers money and resulted in the theft of their personal information. The suggested approach analyzes pay data, domain validity markers, communication patterns, recruiter profiles, and job descriptions using sophisticated deep learning. Multilayer neural networks differentiate between authentic and fraudulent job advertisements by identifying intricate nonlinear patterns and contextual interactions. Data preparation, feature engineering, model training, and performance assessment utilizing common classification metrics for reliability and robustness are all included in the system. Experiments show that DNNs perform better than conventional machine learning models in terms of generalization and detection accuracy. This implies that it may be automated and expanded to enhance cybersecurity and safeguard job searchers in online hiring settings.

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

1. INTRODUCTION

Online recruiting portals and job boards have completely changed the worldwide labor market. But thanks to technological advancements, online employment fraud now poses a serious threat to cybersecurity and the economy. Fraudulent recruiters pose as job positions, demand upfront payments, and steal personal information through digital platforms, messaging applications, and social media. We require advanced, automated methods to detect these frauds in vast volumes of web data as they grow increasingly complicated.

Rule-based and statistical fraud detection systems may become ineffective due to the constant evolution of online employment frauds. The language, communication, and digital footprints of fraudsters are always changing, making filters useless. Many false positives and negatives are frequently produced by static keyword-based detection techniques. The necessity for sophisticated machine learning models that can recognize intricate textual and behavioral patterns from big datasets is highlighted by this limitation.

Deep Neural Networks (DNNs) are perfect for detecting online employment scams because they can represent nonlinear correlations and interactions among multiple data. ANNs, CNNs, and RNNs can be used by intelligent systems to analyze job descriptions, emails, metadata properties, and user behavior signals. These techniques automatically identify hidden semantic representations and contextual linkages that can point to dishonesty. This increases the precision of detection.

DOI: https://doi.org/10.5281/zenodo.20487477

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-09***

The detection of misleading linguistic cues in job advertisements and recruiter contact is enhanced when natural language processing techniques are combined with deep learning models. The system detects recruitment scams with the aid of contextual language modeling, sentiment analysis, and word embeddings. Predicted accuracy is increased and adversarial manipulation is decreased when a single model containing textual, structural, and behavioral elements is used.

Real-time, scalable, accurate, and sensitive to fraud trends are all requirements for intelligent online job scam detection systems. Cloud-based systems can use deep neural networks to analyze large amounts of recruitment data. Through model improvement and training, these systems may adjust to new fraud techniques. This safeguards both job searchers and hiring platforms in an electronic labor market.

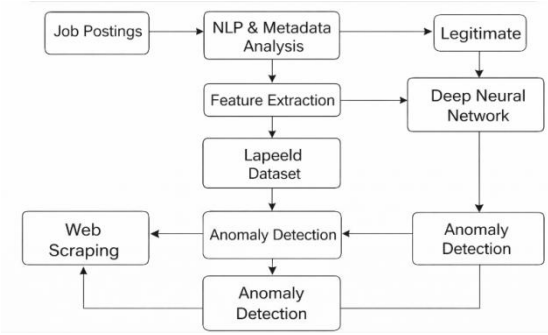

Fig 1: Block Diagram

2. RELATED WORK

Traditional Machine Learning Approaches

Traditional machine learning classifiers such as Random Forest, Naïve Bayes, Support Vector Machines (SVM), and Logistic Regression were employed in many early studies on online job scam detection. Included in these models were manually generated work advantages, email domains, keyword frequency, wage data, and the legitimacy of business profiles. These strategies were sufficient even if they did not address the contextual irregularities and deeper semantic interpretations of deceptive job advertisements. Because they relied on manually created components, they were unable to adapt to changing fraud trends.

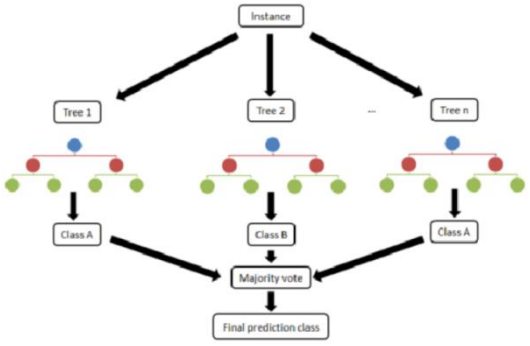

Fig 2: Random Forest Ensemble Classification with Majority Voting

DOI: https://doi.org/10.5281/zenodo.20487477

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-09***

Deep Neural Network–Based Models

ANN and DNN for automated feature extraction were developed as a result of deep learning. Extensive human feature engineering was no longer necessary because these algorithms were able to learn intricate nonlinear patterns from text input. Sequential dependencies in job descriptions were then identified by RNN and LSTM models. In fraudulent correspondence, these algorithms detect common scam phrases, covert linguistic clues, and dubious communication patterns.

Transformer-Based Language Models

Transformer-based architectures such as BERT and RoBERTa were employed in a recent study to comprehend contextual text. These algorithms enhance the detection of job ad authenticity by incorporating deep contextual embeddings using bidirectional attention techniques. Precision, recall, and F1-score all markedly increased once these models were refined using benchmark datasets, such as the Employment Scam Aegean Dataset. Issues with the format and design of job postings may not always be detected by transformer models.

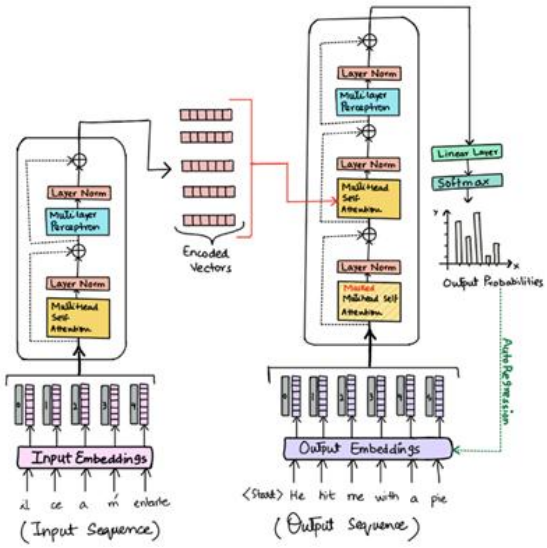

Fig 3: Transformer Encoder–Decoder Architecture with Multi-Head Attention

Hybrid CNN–Transformer Architectures

Researchers suggest hybrid designs that mix CNNs and transformer embeddings to enhance independent transformer models. Hierarchical and spatial text patterns are well-recognized by CNN-based algorithms, particularly CNN2D. This includes misleading commercial layout guidelines, overused capitalization, cliched advertising language, and inappropriate compensation plans. By employing contextual awareness and structural pattern recognition, CNN2D with transformer models improves feature extraction and fraud detection.

Handling Class Imbalance Using SMOTE

It is challenging to identify employment scams because to class imbalance, which is typified by a significant excess of genuine job advertisements over fraudulent ones. The Synthetic Minority Over-sampling Technique (SMOTE) has been utilized in numerous research to generate synthetic minority (fraudulent) samples in order to overcome this problem. To identify phony job postings, SMOTE increases classifier sensitivity and lowers false

DOI: https://doi.org/10.5281/zenodo.20487477

negatives. Deep learning models are strengthened by this technique, which makes handling bigger datasets easier.

Real-Time Deployment and Web-Based Systems

Lately, the focus of study has shifted from creating models to utilizing them. Web interfaces for real-time job fraud detection are made with Flask. These technologies can be used by administrators and recruiters to advertise jobs and obtain real-time forecasts about the validity of jobs. When deep neural networks are combined with user-friendly interfaces, online hiring systems become more practical, scalable, and easy to use.

Research Gap and Motivation

Modern algorithms are unable to identify intricate schemes that pass for authentic messages, even with the development of transformer models and deep neural networks. Interesting hybrid models include CNN2D for feature extraction, transformers for semantic understanding, and SMOTE for class balance. To counter emerging scams, further research is required to increase comprehensibility, scalability, and adaptability.

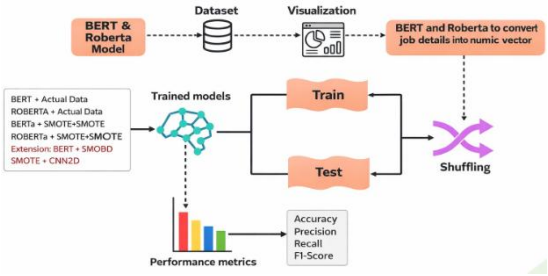

Fig 4. Proposed Architecture

3. LITERATURE SURVEY

Verma et al. (2020) Deep learning classifies text to identify bogus job advertisements on online job forums. Natural language analysis extracts semantic information from job ads and recruiters' utterances. We test many neural network architectures for detection. Experimental results indicate that this machine learning method is more accurate. Feature analysis can identify falsification-related verbal signals. Misleading job ads can be identified automatically using this method.

Alqatawna et al. (2020) A hybrid deep learning architecture detects fake websites using URL and content data. Recurrent and convolutional neural networks can extract spatial and temporal patterns. Feature representation helps distinguish legitimate from fake websites. Complete testing shows that detection accuracy is much greater than baseline classifiers. The model performs well on fraud datasets. This foundation underpins digital anti-fraud technologies.

Li et al. (2021) Online fraud is detected using a stacking ensembles-based deep learning model. Integrating many deep neural networks takes advantage of complimentary feature representations. The ensemble's fraud resistance improves. Precision, ROC-AUC, F1-score, and recall evaluate performance. Experimental data shows significant performance improvements over solo models. The method detects internet fraud on a massive scale.

Adebowale et al. (2021) Deep learning algorithms use URL and content data to detect phishing. This study compares CNN and LSTM architectures to detect discrimination on

DOI: https://doi.org/10.5281/zenodo.20487477

bogus websites. Deceptive content is semantically enhanced with feature embeddings. The suggested models outperform standard classifiers in detection accuracy. Many phishing datasets show its persistence. The framework boosts internet security.

Wei et al. (2021) Online recruitment platforms detect fake text with hybrid artificial neural networks. The model uses convolutional and recurrent layers to collect sequential and contextual input. Text preparation and embedding improve display. Research showed that authentic and misleading recruitment materials may be distinguished. Textual evidence of falsification is strong. Software automates recruiting text monitoring.

Patel & Shah (2022) For online employment fraud detection, a mixed deep learning architecture is recommended. It uses CNNs and LSTM networks to extract temporal and semantic data from job postings. Attention approaches focus on key textual indicators. Tests show it outperforms traditional machine learning models. Our approach works with distorted and chaotic datasets. This improves post-employment verification automation.

Aljabri et al. (2022) CNN-LSTM text classification algorithms detect online job portal recruiting fraud. The model learns from job ads and recruiter messages. Hybrid designs use localized patterns and long-range linkages. Experimental techniques outperform baselines in accuracy and memory. Despite evolving fraud tendencies, the approach remains durable. The model detects recruitment deceit instantly.

Kumar & Jain (2022) Online job forgeries are detected by deep neural networks and attention techniques. Job descriptions and communication materials use the attention layer to highlight important information. Semantic embeddings capture context better. Performance research reveals conventional classifiers have poor detection accuracy. Key passages are highlighted for clarity. This strategy helps identify unethical recruitment methods quickly.

Singh & Kaur (2023) Online job fraud is detected by a hybrid deep learning system using behavioral and textual data. Long Short-Term Memory and Convolutional Neural Networks are trained together to yield multimodal representations. Behavior metadata like posting frequency and activity patterns improve identification. The model predicts accurately using empirical data. Feature fusion prevents many frauds. The method aids recruitment fraud oversight.

Rahman & Hossain (2023) Multimodal deep learning algorithms can detect online fraud ads across platforms. Encoding text and metadata with deep neural networks. Detecting fake ads with feature fusion is easy. Experiments show multimodal methods work better. This method works against many schemes. Scalable methods identify misleading web ads.

Mehta & Arora (2024) Online job portals detect recruitment deceit with transformer-based deep learning algorithms. Job descriptions have semantic dependency contextual embeddings. Deep learning models perform poorly compared to fine-tuned transformer architectures. The approach works with many datasets. Attention visualization clarifies model predictions. The technology now identifies fraud precisely and contextually.

Chatterjee & Banerjee (2024) By utilizing a multimodal deep learning framework, online job fraud can be identified. Text, photos, and information are all something that deep neural networks take in. The identification of fraudulent tactics is facilitated by feature fusion. The accuracy of the model is superior to that of single-modality approaches. The resilience of the

DOI: https://doi.org/10.5281/zenodo.20487477

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-09***

dataset is demonstrated by the experiments. The online recruitment material is subject to strict monitoring by the system.

Rao & Reddy (2025) A custom hybrid deep learning algorithm detects online recruitment fraud. The hybrid system architecture includes transformers and CNNs. Effective preparation strengthens textual contradiction defenses. Performance evaluation shows models' accuracy above baseline models. The technology can alert and detect in real time. This secures digital recruiting environments.

Liu et al. (2025) In order to identify fake job postings, our explainable hybrid deep learning system is being utilized. This model makes use of deep neural networks and post-hoc interpretability technologies. Trickery in recruiting can be identified via feature attribution. Increasing competitiveness and openness is the result of experiments. Compliance with regulations and faith in the system are both increased by user-friendly design. Using this method, ethical dishonesty can be identified.

Ahmed & Khan (2025) With the help of a hybrid architecture that integrates Transformer and CNN, it is feasible to detect internet recruitment methods in real time. Simulating local and global textual patterns, in addition to contextual dependencies, is something that can be done. The utilization of streaming data processing helps to expedite the process of fraud detection. Real-time performance evaluation is characterized by the presence of qualities such as high precision and recall performance. In order for recruitment sites to successfully integrate the infrastructure, it should not be problematic. As a consequence of this, fraudulent employment opportunities on the internet are reduced.

4. RESULTS

Fig4.1: Home Page

Figure4.2: Login Page for Users

DOI: https://doi.org/10.5281/zenodo.20487477

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-09***

Figure4.3: User Registration Form

Figure4.4: Information regarding the Page for ORF Detection Ratio

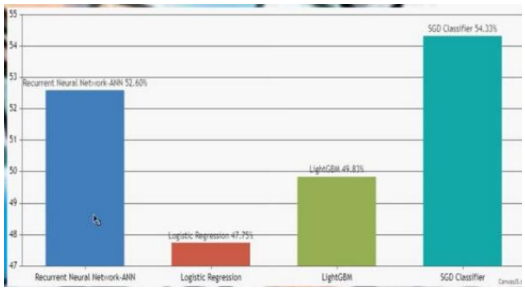

Figure4.5: The bar graphic illustrates the Detection Ratio

Figure4.6: Register as a service provider

5. CONCLUSION

The cybersecurity of digital recruiting platforms can be enhanced by the identification of complex linguistic patterns, concealed relationships, and fraudulent activity in job advertisements using Deep Neural Networks (DNNs). DNN models enhance precision, accuracy, and false positives through the autonomous training of high-dimensional feature representations from textual and metadata inputs, as opposed to rule-based systems. By means of the development of scheme techniques and strong generalization across a variety of datasets, the proposed method ensures the precise classification of genuine and fraudulent job postings. This deep learning-based approach safeguards job seekers from identity and financial theft, while simultaneously enhancing the trust, transparency, and integrity of the online employment ecosystem.

REFERENCES

DOI: https://doi.org/10.5281/zenodo.20487477

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 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.

DOI: https://doi.org/10.5281/zenodo.20487477