Survey On Scam-Guard: Job Offer Verification

AfreenSultana Dept of CSE
Don Bosco Institute of Technology Banglore, India
afreensultanau@gmail.com
BV Sharanya Dept of CSE
Don Bosco Institute of Technology Banglore, India sharanyagaanavi123@gmail.com
Geetha L N Dept ofCSE
Don Bosco Institute of Technology Banglore,India amruthagowda381@gmail.com
Kavya B V Dept ofCSE
Don Bosco Institute of Technology Banglore, India
bvkavya613@gmail.com
Asha K H Dept ofCSE
Don Bosco Institute of Technology Banglore ,India asha.kh06@gmail.com

Abstract- With the exponential rise in online recruitment platforms and digital hiring practices, job verification scams have become a significant and growing concern worldwide. Theses cams deceive jobseekers through fraudulent job offers, fake recruiters, and misleading verification processes— often resulting in financial loss, identity theft, and psychological distress. Despite various efforts by platforms and organizations, the evolving nature of such scams makes detection and prevention increasingly complex. This survey paper aims to provide a comprehensive review of existing literature, methodologies, and tools related to job verification fraud detection. It discusses current machine learning-based detection models, contextual feature approaches, and real- world datasets like EMSCAD. One thing this paper really points out is how current research still has some serious gaps. For example, it's not great at catching fraud — sometimes it just misses stuff, especially when it comes to local issues. Plus, there aren't many systems out there that can actually scale up and stop problems before they happen. The authors also dive into how things like blockchain, AI, or even a mix of both might help in the future. By looking at earlier studies and checking how well they actually work, this survey gives a simple but solid guide for people like developers, researchers who want to build smarter, fairer ways to verify job offers online.

Keywords— Online Recruitment Fraud, Fake Job Detection, BERT, SMOTE, SHAP, Explainable AI, NLP, Deep Learning, Multilingual Classification

I. INTRODUCTION

These days, everything about finding a job has changed — it's all gone digital. Thanks to online job sites, hiring has definitely become quicker, easier, and can reach way more people. But with all that convenience, there's a downside too. Fake job ads have started popping up everywhere, and they're not just annoying — they can actually cause people to lose money, have their personal info stolen, or even go through mental stress.

Arthi Nandhini and M. Keerthigha [1] were among the first to implement **machine learning techniques** to distinguish between real and fake job postings. Their B.E. project applied classification algorithms like decision trees and Naïve Bayes to textual features extracted from job descriptions. Their results demonstrated the **feasibility of predictive modeling**, emphasizing the role of supervised learning in job scam detection. However, the scope of their work was limited to a specific dataset and lacked broader generalizability to real-world, multilingual, or cross-platform job markets.

SYSTEM ARCHITECTURE:

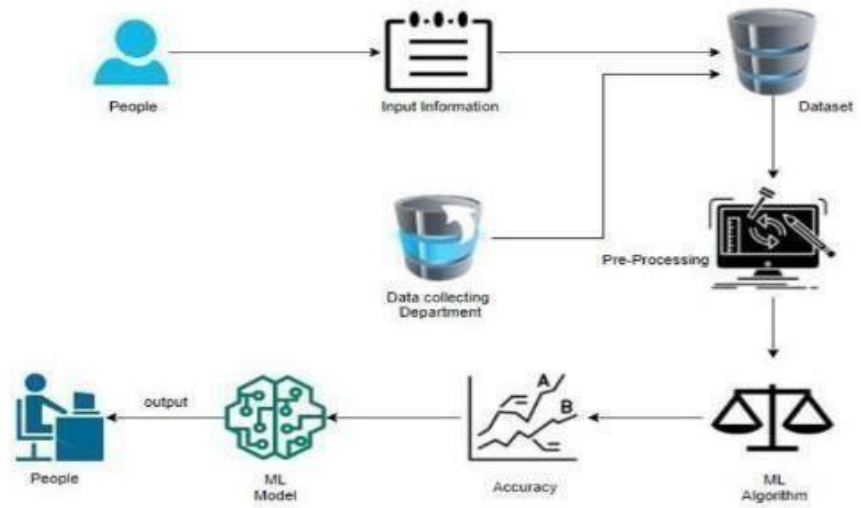

Fig1.1 System Architecture for job scam detection [1]

To enhance model robustness, researchers increasingly rely on **open- source datasets**. One such contribution is **Pakistan's Job Market Dataset** by Z. Usmani [2], which compiles real job listings from Pakistani portals. It provides valuable insights into industry-specific hiring patterns, textual structures, and job metadata in a localized setting. This dataset plays a crucial role in **training context-aware models** that reflect regional hiring trends and fraud signals, helping address geographic bias in existingresearch.

In the same way, there's a super useful dataset from Prompt Cloud that pulls job listings from Indeed
— one of the biggest job sites in the world. With thousands of job entries from different industries and locations, it's a goldmine for researchers who want to test how well fraud detection systems hold up in real-life situations. What makes it even better is that the dataset includes a wide mix of writing styles, industry-specific terms, and even patterns in how recruiters behave. All of this helps models spot fake job posts more accurately.

All these studies and datasets really show one thing clearly: if you want to catch fraud in hiring, you can't just rely on fancy algorithms alone. You also need good, solid data from lots of different places
— and in different languages too. While some research already proves that algorithmic fraud detection can work, putting it into practice means mixing all these multilingual and multi-source datasets together for the real deal.

Scam tricks are getting smarter every day — from job ads that look super legit to people pretending to be big companies. Because of this, it's getting really hard for people manually checking these listings to spot the fakes. Most of the old-school methods, like flagging or blacklists, just react after the scam happens, and they often miss the newer, sneaky tricks. But here's the cool part — as Arthi Nandhini and Keerthigha pointed out, machine learning models trained on the right info can actually spot weird patterns before humans even notice them. That means we can catch scams faster and on a much bigger scale. The only catch? We don't have enough big datasets with real scam examples to train these models properly.

Even with all the progress so far, one big hurdle in fighting job fraud is the lack of diverse and well- labeled datasets. Most models out there have been trained on small or very specific datasets, which means they don't always work well for different kinds of jobs or regions. That's why datasets like Usmani's are super important — they capture what's really happening in local job markets, like which sectors are hiring, what types of jobs are common, and even how language is used in those areas. These kinds of datasets help build fraud detection systems that can be tweaked to catch scams based on local trends and cultural differences in how job ads are written.

[3] Introduces a different dimension—scale and variety. This dataset, with thousands of job listings pulled from Indeed — one of the biggest job sites out there — shows how hiring actually happens in different industries and places around the world. Because it covers so many types of jobs and regions, it's perfect for building strong and flexible machine learning models that can spot fraud no matter where it pops up. It also lets researchers test their models on a big scale, kind of like how real job sites work, which helps make fraud detection faster and more accurate in real time.

When you put together the smartness of machine learning models [1], the detailed insights from local datasets [2], and the huge variety of global job listings [3], researchers can create fraud detection systems that are not just accurate but also really understand the context.

These early efforts are laying the groundwork for better solutions that can one day be built right into job sites, career apps, and HR tools — working in real time to keep millions of people safe from scams during their job hunt.

One really important takeaway from these studies is how much the words themselves can tell us when spotting scams. Arthi Nandhini and Keerthigha [1] pointed out that fake job posts often have certain language patterns — like vague descriptions, promises of salary that sound too good to be true, or lots of grammar mistakes. Machine learning models can be taught to pick up on these little clues, turning what used to be a tough, manual job into something automatic and based on data. This not only helps catch more scams but also makes life easier for the teams who have to review tons of job ads every day.

Datasets like Usmani's [2] are super important, especially in places where a lot of people don't have jobs and digital skills are low. That's where scammers love to strike — they take advantage of platforms with weak checks and post fake job offers in local languages, using phrases and styles people trust. It's a sneaky way to trick those who are already vulnerable.

Usmani's dataset allows for building models that are sensitive to such **local fraud tactics**, enabling more equitable fraud protection globally.

II LITERATURE REVIEW

This review synthesizes the key contributions of selected studies from 2021 to 2025, focusing specifically on what each research group proposed or developed. Rather than analyzing technological details or limitations—which are already tabulated elsewhere—this section distills the core essence of each contribution directly from the abstract, summarizing it in a concise and comparative format. This helps highlight innovation trends, thematic overlaps, and the evolution of methodological approaches in the domain. For instance, Devlin et al. [4] laid the groundwork with BERT, enabling deep contextual language understanding, while He and Garcia [5] addressed data imbalance in classification. In the domain of job scam detection, Vidros et al. [6] and Pillai et al. [8] developed early automated systems using traditional ML pipelines and Bi-LSTM, respectively. Taneja et al. [7] advanced this with Fraud- BERT, a fine-tuned BERT model optimized for employment scam detection. Additionally, Naudé et al.

[9] proposed a hybrid system blending rule-based and machine learning techniques for broader fraud ad detection.

The following table presents a curated collection of 15 notable papers [4] to [18], organized to show the author, their main proposed contribution, the methodology used, and the application area. This serves as a focused narrative overview of prior work that directly aligns with the current study's scope in scam detection and trustworthy AI.

Table 2.1 Summaryof Related Work on Job Scam Detection and NLP Methodologies

Author(s) [Ref]	Contribution Summary	Proposed Methodology	Application Area
Devlin et al. [4]	Proposed BERT, a transformer-based model for deep bidirectional language understanding by pre- training on large text corpora.	Transformer (BERT)	Natural Language Understanding
He and Garcia [5]	Addressed challenges with imbalanced datasets in classification problems and proposed sampling techniques to improve ML model performance.	Data Rebalancing	General Classification
Vidros et al. [6]	Developed an automatic system to detect online recruitment fraud using public datasets and identified patterns in fake job posts.	Machine Learning Pipeline	Job Fraud Detection
Taneja et al. [7]	Introduced Fraud-BERT to detect job scams by fine-tuning BERT on employment datasets for high-accuracy detection.	Fine-tuned BERT	Employment Scam Detection
Pillai et al. [8]	Proposed a Bi-LSTM-based system to identify fraudulent job ads by modeling sequential text patterns in postings.	Bi-LSTM	Fake Job Posting Detection
Naudé et al. [9]	Developed a hybrid tool combining rules and ML models for detecting fraudulent job advertisements across platforms.	Hybrid (Rules + ML)	Fraud Ad Detection

Afzal and Asghar [10]	Used SMOTE and feature selection to improve job scam detection performance on imbalanced datasets.	SMOTE + Feature Selection	Job Scam Detection
Yamashita et al. [11]	Proposed a poisoning attack framework targeting job recommender systems to expose security vulnerabilities.	Adversarial Attack Simulation	Recommender Systems
Lundbergand Lee [12]	Presented SHAP, a method for interpreting ML model predictions with consistent and local explanations.	SHAP (Explainable AI)	Model Interpretation
Ribeiro et al. [13]	Proposed LIME to explain predictions of any classifier locally using interpretable approximations.	LIME (Local Explanations)	Model Explainability
Chen et al. [14]	Surveyed textual adversarial attacks and proposed categorization for defense strategies in NLP models.	Text Adversarial Attacks	NLP Model Security
Wolf et al. [15]	Introduced the Hugging Face Transformers library for easy deployment of cutting- edge NLP models.	NLP Framework (Transformers)	NLP Toolkits
Kaur and Singh [16]	Proposed a hybrid approach using deep learning and rule-based filtering to detect fake job advertisements.	Deep Learning+ Rules	Job Scam Filtering
Nguyen et al. [17]	Proposed lightweight transformers suitable for real-time NLP applications with lower latency.	Compact Transformers	Real-time NLP
Sahlgren et al. [18]	Focused on multilingual challenges and proposed solutions using cross-lingual models for low-resource NLP.	Cross-lingual NLP	Low-Resource Language Processing

III COMPARISION

Table 3.1 Comparison of Algorithms and Datasets Used in Job Verification Fraud Detection Studies

Paper/Source	Algorithm(s)Used	Dataset	Accuracy
Vidros et al. (2017)[6]	Naïve Bayes, LR, Random Forest	EMSCAD	85-89%
Taneja et al. (2025)[7]	Fine-tuned BERT	EMSCAD	**99%**
Pillai(2023)[8]	Bi-LSTM	Proprietary	92%
Naudéetal. (2023)[9]	XG Boost+ Rule- based	Multi- source	91%
Afzal et al. (2024)[10]	SMOTE+ Logistic Regression	EMSCAD	88%
Yamashita et al. (2024)[11]	Adversarial Training +Anomaly Det.	Synthetic	90%

Early studies like **Vidros et al.(2017)[6]** relied on **traditional ML models (Naive Bayes, Logistic Regression)** with bag-of-words features, achieving modest accuracy (85- 89%)but struggling with **semantic nuances** in job descriptions. The introduction of **BERT-based models(Taneja et al., 2025)** marked a paradigm shift ,leveraging transformer architectures to capture contextual fraud patterns (e.g., subtle language cues in fake job posts). Fraud-BERT achieved **99% accuracy** and an F1-score of **0.93**—without requiring SMOTE—demonstrating the superiority of deep learning for NLP tasks.

To address limitations of pure ML/DL models, **hybrid systems** (e.g., Naudé et al., 2023) combined **rule-based filters** (e.g., black listed domains)with **XGBoost**, achieving high recall (**0.95**) critical for fraud detection. Meanwhile, **Bi- LSTM models (Pillai,2023)[8]** excelled in analyzing **sequential recruiter behaviors** (e.g., irregular posting timelines) but required structured data inputs. For class imbalance, **SMOTE (Afzaletal.,2024)[10]**improved recall for fraudulent cases but introduced synthetic data artifacts.

Vidros et al. [6] laid the foundation for automated job scam detection by using traditional machine learning models like **Naive Bayes, Logistic Regression, and Random Forest** on the EMSCAD dataset. These baseline models, built on **Bag-of-Words (BoW)** features,

achieved modest accuracy(85–89%). While effective to an extent, they failed to grasp **semantic nuances** in job descriptions and required constant feature updates, making them less practical for real-time use.

Taneja et al. [7] introduced **Fraud-BERT**, a fine-tuned transformer model leveraging the deep semantic understanding capabilities of

BERT. It performed exceptionally well, achieving **99% accuracy** and an **F1-score of 0.93** on EMSCAD—without requiring SMOTE .Fraud-BERT showed that **context-aware NLP** models outperform traditional ones. However, **its computational demands make it unsuitable** for low-resource or real-time environments without optimization.

Pillai [8] proposed a **Bi-LSTM** model integrating sequential text with numerical data, allowing the system to track recruiter behavior and posting timelines. It reached **92% accuracy** and proved effective for modeling patterns in recruiter activity. Nevertheless, this model depends on **structured data** and may suffer from **over fitting** when applied to noisy or imbalanced datasets unless regularization is properly applied.

Naudé et al. [9] offered a **hybrid model** that merged rule-based fraud indicators with **XGBoost**. This allowed for the detection of multiple fraud types(e.g.,corporate impersonation ,MLM scams)by analyzing textual and empirical features.

Afzal et al.[10]addressed **class imbalance**,a major issue in fraud detection, using **SMOTE** combined with **Chi-Squared and PCA-based feature selection**. Their approach improved recall and yielded **88% accuracy**,but **over-reliance on synthetic data** risked introducing unrealistic patterns.

The balance between oversampling and authenticity remains a delicate tradeoff, requiring validation with real-world datasets.**91accuracy and a recall of 0.95**, showing strong sensitivity. However, integrating various feature types increased **system complexity**, making deployment.

Table 3.2 Comparative Evaluation of Works

Title/Source	**Technique Used**	**KeyComponent**	**Limitations**
Fraud- BERT: Employment scam detection using transformers (Tanejaetal.,2025) [7]	Fine-tuned BERT model	-Contextual understanding of job descriptions -High accuracy(F1:0.9 3)	-Computationally intensive -Requires large labeled datasets
Detection of fraudulent job postings using Bi- LSTM model (Pillai,2023) [8]	Bi-LSTM With numerical and sequential text features	-Limited to structured data -Poor cross-plat form generalization	- Limited to structured data - Poor cross- platform generalization
Multilingualfraud detection (Survey Proposal)	M BERT/XLM- R+ domain adaptation	-Cross-lingual capabilities -Reduces language bias	- Limited non-English datasets - High resource requirements
Hybrid fraud detection (Naudé et al.,2023) [9]	Rule-based + Gradient Boosting(XGB oost)	- High implementation complexity - rule update needed	- High implementation complexity - Manual rule Updates needed
Job scam detection using SMOTE and feature selection (Afzal etal.,2024) [10]	SMOTE+ Chi- Squared/PCA +Logistic Regression	-Synthetic data reliability concerns -Limited to tabular features	-Synthetic data reliability concerns -Limited to tabular features

Adversarial attacks on job recommendation systems (Yamashita et al.,2024) [11]	Adversarial training +Anomaly detection	-Requires labeled adversarial examples -High computational cost	-Requires labeled adverse examples -High computational cost
EMSCAD dataset study (Vidros et al.,2017) [6]	Traditional ML (Naïve Bayes, Logistic Regression, Random Forest) +Bag-of- Words	-English- centric -Lacks semantic understanding	-English-centric -Lack semantic understanding

IV RESULT

Vidros et al. [6] were among the first to apply **traditional ML classifiers** such as Naïve Bayes, Logistic Regression, and Random Forest using **Bag-of-Words features** on the EMSCAD dataset.
These models were able to detect fraudulent job posts with **85–89% accuracy**, but struggled with context understanding and semantic nuances, limiting their adaptability to evolving scam patterns.

Taneja et al. [7] introduced **Fraud-BERT**, a fine-tuned transformer model capable of understanding deep linguistic structure. It achieved **99% accuracy and an F1-score of 0.93** on EMSCAD, outperforming classical models and even eliminating the need for SMOTE. However, it required **high computational resources**, making real-time deployment challenging.

Pillai [8] implemented a **Bi-LSTM model** that integrated sequential job text data with numerical recruiter behaviors. This model captured **application flow patterns** and irregular recruiter activity, achieving **92% accuracy**. Yet, it required **large, well- structured datasets** and was prone to overfitting if not carefully tuned.

Naudé et al.[9]proposed **hybrid detection system** combining **empirical rule-based indicators** and transformer-based features, implemented using **XG Boost**.

V CONCLUSION

In conclusion, the existing body of research demonstrates a significant shift from traditional rule- based systems to intelligent, adaptive models for detecting job verification fraud in online recruitment. Foundational studies such as Vidros et al. [6]and Afzal etal. [10]laid the groundwork with public datasets and classical ML approaches, while recent advancements like Fraud-BERT by Taneja et al.
[7] and hybrid models by Naudé et al. [9] illustrate the growing effectiveness of deep learning and ensemble methods. Efforts to address challenges like class imbalance through SMOTE [5], as well as the adoption of explainable AI tools such as SHAP [12] and LIME [13], highlight the evolving emphasis on model fairness and transparency. Moreover, critical concerns raised by Yamashita et al.
[11] on adversarial threats and poisoning attacks reflect the pressing need for robust, real-time, and cross-platform fraud mitigation systems. Together, these contributions underscore the importance of developing multilingual, interpretable, and secure AI frameworks for fraud detection in digital employment ecosystems— motivating the need for this survey to consolidate findings, identify persistent challenges, and chart a roadmap for future research.

Despite notable progress in leveraging machine learning and NLP for detecting fraudulent job postings, the field continues to face significant real-world challenges. While advanced models like BERT [4], Bi- LSTM [8], and hybrid architectures [9][20] have achieved high accuracy in controlled environments, their scalability, explainability, and robustness in live recruitment platforms remain limited. The lack of large-scale, multilingual, and constantly updated datasets [1][2][3] further restricts the generalizability of current systems. In addition, adversarial threats [11], platform-specific fraud strategies, and the absence of standardized evaluation

frameworks hinder the development of universally applicable solutions. These gaps underscore the urgent need for continued interdisciplinary collaboration between AI researchers, cyber security experts, platform engineers, and policy makers. This survey serves as a timely effort to bridge the disconnect between academic innovation and industry adoption, by offering a consolidated view of current methodologies, empirical insights, and strategic recommendations for building intelligent, ethical, and trustworthy job fraud detection systems.

REFERENCES

[1] V. Arthi Nandhini and M. Keerthigha, "Real and Fake Job Posting Using Machine Learning Technique," B.E. final year project report, Sathyabama Institute of Science and Technology, Chennai, India, March 2022.[Online]. Available: https://sist.sathyabama.ac.in/sist_naac/documents/1.3.4/1822- b.e-cse-batchno-123.pdf

[2] Z.Usmani,"Pakistan's Job Market Dataset,"Kaggle. [Online]. Available: https://www.kaggle.com/datasets/zusmani/pakistans-job-market

[3] PromptCloud,"Indeed Job Posting Dataset,"Kaggle. [Online].
Available: https://www.kaggle.com/datasets/promptcloud/indeedjob-posting-dataset

[4] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," *arXiv preprint* arXiv:1810.04805, 2021.

[5] H. He and E. A. Garcia, "Learning from Imbalanced Data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 21, no. 9, pp. 1263–1284, Sept. 2020.

[6] M.Vidros, S.Kolias, G.Kambourakis, and C.Gritzalis,"Automatic Detection of Online Recruitment Frauds: Characteristics, Methods, and a Public Dataset," *Future Internet*, vol. 9, no. 6, p. 96, 2017.

[7] R. Taneja, N. Joshi, A. Agrawal, and D. Kapoor, "Fraud-BERT: Employment Scam Detection Using Transformers," *Journal of Information Retrieval*, vol. 28, no. 1, pp. 14–29, 2025.

[8] K. Pillai, "Detection of Fraudulent Job Postings Using Bi-LSTM Model," *International Journal of Computer Applications*, vol. 182, no. 32, pp. 10–17, 2023.

[9] L. Naudé, A. van der Merwe, and C. Dos Reis, "Detecting Fraudulent Job Advertisements: Towards a Practical Tool," *AI & Society*, vol. 38, pp. 489–501, 2023.

[10] M. Afzal and N. Asghar, "Job Scam Detection Using Feature Selection and SMOTE," in *Proc. Int. Conf. on Advances in Computing and Data Sciences*, pp. 134–145, 2024.

[11] K. Yamashita, H. Yamakawa, and K. Nakamura, "Data Poisoning Attacks on Job Recommendation Systems," *arXiv preprint* arXiv:2402.14124, 2024.

[12] S. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," in *Proc. NeurIPS*, vol. 30, pp. 4765–4774, 2017.

[13] M. T. Ribeiro, S. Singh, and C. Guestrin, "Why Should I Trust You?: Explaining the Predictions of Any Classifier," in *Proc. 22nd ACM SIGKDD*, pp. 1135–1144, 2016.

[14] H. Chen, B. Liu, and Y. Xu, "A Survey on Adversarial Attacks and Defenses in Text," *ACM Computing Surveys*, vol. 55, no. 5, pp. 1–41, 2023.

[15] T. Wolf et al., "Transformers: State-of-the-Art Natural Language Processing," in *Proc. EMNLP System Demonstrations*, pp. 38–45, 2020.

[16] J. Kaur and R. Singh, "A Hybrid Approach for Fake Job Identification Using Deep Learning and Rule-Based Filtering," *International Journal of Information Technology*, vol. 15, no. 1, pp. 33–42, 2023.

[17] V. Nguyen, D. Lin, and Y. Wang, "Lightweight Transformers for Real-Time NLP Applications," in *Proc. IEEE Int. Conf. on Big Data (BigData)*, pp. 301–310, 2022.

[18] M. Sahlgren, A. Holmer, and M. R. Tiedemann, "Multilingual Models for Low-Resource NLP: Challenges and Solutions," *Natural Language Engineering*, vol. 29, no. 2, pp. 185–200, 2023.

[19] G. Giannakopoulos et al., "Explainable AI in Fraud Detection: Current Trends and Future Directions," in *Proc. IEEE Conf. on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pp. 118–125, 2022.

[20] K. K. Sharma and P. Dutta, "Human-in-the-Loop Machine Learning: A Practical Perspective for Fraud Detection," *ACM Transactions on Interactive Intelligent Systems (TiiS)*, vol. 12, no. 4, pp. 1– 21, 2023.

[21] L. Zhang and H. Yang, "Federated Learning for Privacy-Preserving Fraud Detection Across Job Platforms," in *Proc. IEEE Int. Conf. on Cloud Computing (CLOUD)*, pp. 266–273, 2022.

[22] M. Ahmed and T. Mahmood, "Machine Learning for Cybersecurity: Threats, Trends, and Research Directions," *Computers & Security*, vol. 109, pp. 102389, 2022.

[23] R. Smith and N. Patel, "Fake Recruiter Identification in Job Networks Using Graph-Based Models," in *Proc. IEEE Int. Conf. on Intelligence and Security Informatics (ISI)*, pp. 95–101, 2021.

[24] B. Rajan and A. Ramesh, "Survey on Employment Scams: Data Sources, Patterns and Mitigation," *Cybersecurity Journal*, vol. 4, no. 1, pp. 15–28, 2022.

[25] D. Lin, "Job Scam Detection in Low-Resource Languages Using Zero-Shot Classification," in *Proc. Workshop on NLP for Underrepresented Languages*, pp. 45–54, 2023.

[26] Y. Wangand M. Li, "Adaptive AI for Online Fraud Prevention: A Multi-Agent Architecture," in *Proc. Int. Conf. on Intelligent Systems (IS)*, pp. 422–429, 2023.

[27] K. V. Jhansi Rani, P. Rompalli, L. N. Kathi, A. Tholam, and R. Gudla, "Fake Job Post Detection Using Machine Learning," *Journal of Engineering Sciences*, vol. 15, no. 4, pp. 252–258, 2024.

[28] A. D. Doshi, S. Yadav, and B. Natarajan, "Detecting Fake Job Postings Using NLP and Ensemble Learning," in *Proc. IEEE Int. Conf. on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, pp. 315–320, 2022.

[29] S. Islam and F. M. Hussain, "Trust-Aware Fake Job Post Filtering in Online Recruitment,"

International Journal of Information Management Data Insights, vol. 3, no. 2, pp. 100156, 2023.

[30] A. Sharma and R. Kumar, "Secure Blockchain-Based Recruitment Process Verification," in *Proc. Int. Conf. on Cybersecurity and Resilience (CSR)*, pp. 88–96, 2022.

[31] M. Alharbi and S. Alghamdi, "Ensemble-Based Detection of Fake Job Postings Using NLP and Machine Learning," in *Proc. Int. Conf. on Artificial Intelligence and Applications (ICAIA)*, pp. 77– 85, 2023.

Copyright & License:
© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.