IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 6, Issue 7, March 2026

Impact Factor: 8.2

JobShield AI Detecting Fake Recruiters and Scam Offers

Ms. Hemamalini S, Ms. Kanaga T, Ms. Meera P, Ms. Santhiya M, Mr. Alex Giftson R
Department of Computer Science and Engineering
N.S.N. College of Engineering and Technology , Karur , Tamil Nadu , India
ssmalini253@gmail.com, kanaga13122004@gmail.com, meeraprabhu076@gmail.com
msanthiyacse24@gmail.com, arcanoalexis@gmail.com

Abstract: *Online job and internship portals have become a major platform for job seekers. However, the rapid growth of these platforms has also increased fake recruiters and fraudulent job postings. Many job seekers are misled by scam offers and lose money or personal information. To solve this problem, the proposed system Job Shield AI is developed to detect fake recruiters and scam job offers. The system uses Artificial Intelligence (AI), Natural Language Processing (NLP), and Machine Learning (ML) techniques to Analyse job postings and recruiter details. It identifies suspicious patterns such as unrealistic salary offers, unknown email domains, and misleading job descriptions. The system classifies job postings as real or fake based on the trained machine learning model. Users can safely browse verified job opportunities through the platform. The system also alerts users about suspicious job postings. This solution helps job seekers avoid scams and creates a safer online job search environment.*

Keywords*:* Job Scam Detection, Machine Learning, Online Job Portals, Recruitment Fraud Detection

I. INTRODUCTION

The rapid growth of online job portals and digital recruitment platforms has made job searching easier for people around the world. However, along with these advantages, the number of fake recruiters and job-related scams has also increased significantly. Many fraudsters create fake job postings, send misleading emails, or contact job seekers through social media platforms pretending to represent well-known companies. As a result, many individuals lose money, personal information, and sometimes even their confidence in online recruitment systems expenses, and a decline in mental and physical health. Therefore, creating intelligent systems for injury prevention, fall detection, and on going health monitoring has emerged as a top goal in contemporary healthcare research. To address this problem, the AI-Based Fake Recruiter & Job

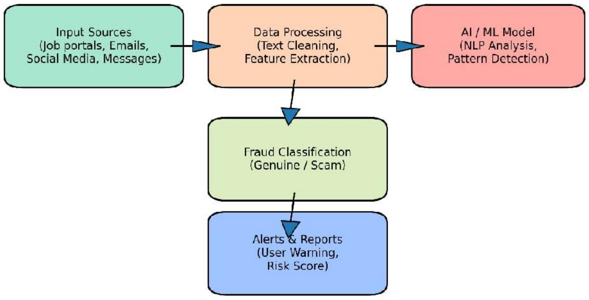


Fig 1 : Block Diagram

Scam Detection System is designed to identify suspicious recruitment activities using modern technologies. The system analyzes job postings, recruiter messages, and communication patterns to determine whether they are genuine or potentially fraudulent. By examining language patterns, contact information, and behavioral indicators, the system can detect warning signs that may not be easily recognized by users

Artificial Intelligence and Machine Learning techniques play a crucial role in improving the accuracy of the system. With the help of Natural Language Processing (NLP), the system can understand the text used in job advertisements, emails, and recruiter conversations. It then compares these patterns with known scam behaviors stored in its dataset. Based on this analysis, the system classifies the recruitment activity as either genuine or suspicious and provides appropriate alerts to users.

Overall, this system aims to create a safer digital recruitment environment by protecting job seekers from fraudulent activities. It not only helps individuals verify job opportunities but also supports job portals and organizations in maintaining trust and transparency in their hiring processes. By continuously learning from new scam patterns, the system becomes more effective over time and contributes to reducing online job fraud.

II. LITERATURE SURVEY

The rise of digital recruitment platforms has fundamentally changed the way employers and job seekers connect across the world. As online job portals became mainstream, they brought with them not only opportunities but also serious vulnerabilities that bad actors have learned to exploit efficiently. Recruitment fraud, a phenomenon rooted in deception and financial manipulation, has grown proportionally alongside the expansion of internet access and remote work culture. Researchers in the early 2000s began documenting patterns of fake job advertisements that promised high salaries, relocation benefits, and prestigious roles to lure unsuspecting candidates. These fraudulent listings were often indistinguishable from legitimate postings, making it difficult for even experienced job seekers to identify the threat. Studies conducted by cybersecurity institutes noted that job-related scams ranked among the top five categories of online fraud reported annually. The psychological profile of victims indicated that individuals under financial stress, recent graduates, and those re-entering the workforce were disproportionately targeted. The monetary losses associated with recruitment scams were found to be secondary to the psychological damage, which included damaged trust and prolonged career disruption. Early literature in this space concentrated heavily on qualitative analysis of complaint reports filed with consumer protection agencies. These foundational studies established the groundwork for building automated detection systems capable of identifying patterns consistent with fraudulent recruitment behavior.

Natural Language Processing has emerged as one of the most promising technological avenues for the automated detection of scam-related content in job postings and recruiter communications. Scholars working in computational linguistics observed that fraudulent job advertisements tend to exhibit distinct textual features, including exaggerated salary claims, vague job descriptions, and an unusual urgency in the language used by the poster. Initial NLP models applied to this domain relied on bag-of-words approaches and term frequency-inverse document frequency metrics to classify job listings as genuine or deceptive. These early classifiers achieved moderate accuracy but suffered when confronted with increasingly sophisticated scams that mimicked the structure and tone of authentic postings. The development of transformer-based architectures such as BERT and Robert a marked a pivotal shift in this research, enabling models to understand contextual meaning rather than relying purely on surface-level vocabulary patterns. Researchers fine-tuned these large language models on curated datasets of labelled job advertisements, reporting substantial gains in precision and recall over previous methods. Linguistic patterns associated with high-risk postings were systematically catalogued, including overuse of superlatives, absence of verifiable employer details, and requests for sensitive personal information early in the application process. Sentiment analysis components were incorporated to evaluate the emotional tone of job descriptions, as scam postings often employed excessively positive or persuasive language designed to bypass rational evaluation. Named entity recognition pipelines were further utilized to flag postings that failed to mention identifiable company names, addresses, or registration numbers. The convergence of

DOI: 10.48175/IJARSCT-32262

these NLP techniques laid the theoretical basis for modern AI-powered systems such as Job Shield, which integrate multiple language-based signals to produce a composite risk assessment for each posting.

Machine learning classification algorithms have played a central role in building scalable fraud detection pipelines applicable to the recruitment domain. Research teams from various universities and industry labs explored the suitability of decision trees, support vector machines, random forests, and gradient boosting classifiers for distinguishing fraudulent from genuine job advertisements. The Employment Scam Aegean Dataset, published by the University of the Aegean, became a widely used benchmark in this field and enabled comparative evaluation of competing approaches. Studies leveraging this dataset found that ensemble methods consistently outperformed individual classifiers, particularly when feature engineering incorporated both textual and structural signals from the posting. Beyond the content of job advertisements themselves, behavioural features of recruiter accounts were identified as powerful discriminating factors, including posting frequency, account age, response patterns, and degree of profile completeness. Graph-based models were applied to map relationships between recruiter accounts and job postings, identifying coordinated fraud networks operating across multiple platforms simultaneously. Anomaly detection techniques were deployed to surface recruiters whose behavioural signatures deviated significantly from established norms for verified employers on major job boards. Researchers also explored semi-supervised learning approaches to address the challenge of limited labelled data, given that many scam postings are removed before they can be formally documented and annotated. The integration of real-time data streams from job platforms allowed for dynamic model updating, ensuring that classifiers could adapt to the evolving tactics employed by fraudulent recruiters. This body of machine learning research provided the algorithmic backbone upon which intelligent anti-scam systems in the recruitment sector have been designed and deployed.

The domain of digital identity verification has contributed significantly to the challenge of authenticating recruiter credentials and company legitimacy in online hiring environments. Research in this area recognized that fraudulent recruiters routinely fabricated corporate identities, forged registration documents, and impersonated representatives of well-known organizations to lend their scam operations an air of credibility. Identity verification frameworks originally designed for financial services were adapted for the recruitment context, introducing multi-factor verification pipelines that cross-referenced recruiter profiles against official business registries, professional networking databases, and historical posting records. Blockchain-based credentialing systems were proposed in academic literature as a means of creating tamper-proof records of verified employer identities, though adoption remained limited due to implementation complexity and lack of standardization across job platforms. Researchers studying phishing and spoofing incidents in recruitment found that scammers frequently registered domain names visually similar to those of legitimate companies, a practice known as typo squatting, to deceive applicants into believing they were corresponding with genuine employers. Email metadata analysis was developed as a supplementary detection layer, evaluating the provenance and routing history of recruiter communications to identify suspicious patterns indicative of bulk messaging campaigns or anonymizing relay networks. Social media cross-referencing tools were incorporated into recruiter verification workflows, matching claimed identities against publicly visible professional profiles to detect inconsistencies in employment history, endorsements, and network connections. The absence of a verifiable digital footprint was established as a significant risk indicator in both academic studies and practitioner reports from consumer protection organizations. These identity-centric research strands informed the design of verification modules that form an integral component of comprehensive job scam detection platforms. The ultimate goal articulated across this body of work is to make credential fraud costly and difficult enough that the economic incentive for perpetrating recruitment scams is substantially diminished.

III. EXISTING SYSTEM

In the present job market, most job seekers depend heavily on online job portals, social media platforms, and email communications to search for employment opportunities. While these platforms make job searching easier and faster, they also create an environment where fake recruiters can easily target innocent candidates. Fraudsters often post attractive job offers with high salaries and minimal qualifications to grab the attention of job seekers. Many candidates, especially fresh graduates, may not have enough experience to identify whether a job offer is genuine or fraudulent. As a result, they may unknowingly share personal information such as resumes, identity documents, or bank details. This creates a serious risk for data misuse and financial loss. The existing system mainly depends on manual verification by the job seeker, which is not always reliable. Therefore, many people fall victim to recruitment scams every year.

Most of the currently available job portals provide only basic verification of recruiters before allowing them to post job advertisements. However, this verification process is not always strict or effective. Fake recruiters can easily create accounts using temporary email addresses or false company details. Once their accounts are approved, they start posting fraudulent job opportunities that look very similar to real ones. These fake postings may include company logos, professional descriptions, and convincing communication styles. Because of this, job seekers find it difficult to differentiate between real recruiters and scammers. The lack of advanced monitoring systems in many platforms allows these fraudulent activities to continue without immediate detection. Consequently, job seekers often rely on their own judgment to decide whether to trust a recruiter.

Overall, the existing system for identifying fake recruiters is limited in its ability to protect job seekers from recruitment fraud. The current process relies heavily on manual verification, basic platform checks, and the awareness level of individual users. These methods are not sufficient to handle the increasing sophistication of online job scams. Fraudsters continuously change their strategies to appear more professional and trustworthy. Without advanced detection systems, it becomes difficult for job seekers to identify scams at an early stage. Therefore, there is a clear need for a more intelligent and automated solution that can analyze recruitment data, detect suspicious patterns, and warn users about potential fraud before any harm occurs.

IV. PROPOSED SYSTEM

The proposed system, Job Shield AI, is designed to provide a reliable solution for identifying fake recruiters and preventing job-related scams in online recruitment platforms. The main objective of this system is to assist job seekers in verifying the authenticity of job offers and recruiter profiles before engaging with them. By integrating intelligent technologies, the system aims to analyze recruitment information and identify suspicious activities that may indicate fraudulent behavior. This approach helps reduce the risk faced by candidates when applying for jobs online. Instead of relying only on manual verification, the proposed system introduces an automated mechanism to evaluate job postings and recruiter communications. The system continuously monitors recruitment data and compares it with known patterns of fraudulent activity. Through this process, it becomes easier to detect unusual or suspicious job offers. As a result, job seekers receive better protection from potential scams.

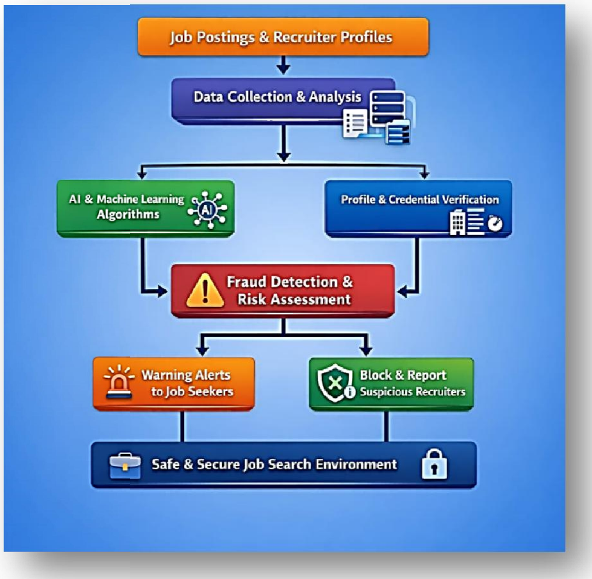
The proposed system uses artificial intelligence techniques to analyse different aspects of job postings and recruiter details. It examines elements such as company information, job descriptions, contact details, and communication patterns to determine whether they appear legitimate or suspicious. Machine learning algorithms are used to study previously identified scam cases and learn from them. Based on this learning process, the system can predict the probability of a new job posting being genuine or fraudulent. When suspicious indicators are detected, the system generates warnings for the users. This helps job seekers make informed decisions before proceeding further with the recruitment process. The use of AI allows the system to improve its accuracy over time as more data becomes available.

Another important feature of the proposed system is the verification of recruiter profiles and company credentials. The system cross-checks recruiter information with trusted company databases and publicly available sources. If inconsistencies or missing details are found, the system marks the recruiter profile as potentially risky. In addition, the system also analyses email domains, company websites, and job posting behaviour to identify fake accounts. Recruiters who frequently post similar job advertisements or request unusual information from candidates can be flagged for further review. This verification process helps maintain transparency and ensures that only legitimate recruiters are

DOI: 10.48175/IJARSCT-32262

allowed to interact with job seekers. As a result, the trust between candidates and recruitment platforms can be significantly improved.

Overall, the proposed Job Shield AI system offers a proactive approach to protecting job seekers from recruitment scams. Instead of reacting only after fraud occurs, the system works to detect potential threats at an early stage. Through the use of artificial intelligence, data analysis, and automated monitoring, it provides a safer environment for online job searching. Job seekers can confidently explore opportunities without constantly worrying about the authenticity of recruiters. At the same time, legitimate companies benefit from a trustworthy recruitment platform where their job postings are not overshadowed by fraudulent activities. This proposed system therefore plays an important role in improving security and reliability in modern online recruitment processes.


Job Postings & Recruiter Profiles
Data Collection & Analysis
AI & Machine Learning Algorithms
Profile & Credential Verification
Fraud Detection & Risk Assessment
Warning Alerts to Job Seekers
Block & Report Suspicious Recruiters
Safe & Secure Job Search Environment

V. METHODOLOGY

The methodology of the Job Shield AI system focuses on identifying and preventing fake recruitment activities by analysing job-related information using intelligent techniques. The process begins with collecting data from different online sources such as job portals, recruiter profiles, company websites, and communication records. This collected data forms the base for identifying patterns related to genuine and fraudulent job offers. The system organizes the information in a structured format so that it can be easily processed. Data cleaning is performed to remove incomplete or irrelevant information that may affect the accuracy of the system. After preprocessing, the system prepares the dataset for further analysis. This step is important because high-quality data helps improve the reliability of the detection process. By carefully preparing the data, the system becomes capable of identifying suspicious characteristics in recruitment activities.

Once the data collection and preprocessing stages are completed, the next step involves feature extraction. In this stage, important attributes related to job postings and recruiter behaviour are identified. These attributes may include company name authenticity, recruiter contact information, email domain patterns, job description structure, and the presence of suspicious requests such as payment demands. Each feature helps the system understand whether the job offer follows legitimate recruitment practices or not. The system converts these features into measurable values that can be analysed using machine learning algorithms. By focusing on these specific characteristics, the system can detect patterns commonly associated with fraudulent job postings. This process allows the system to differentiate between genuine recruitment activities and possible scams.

DOI: 10.48175/IJARSCT-32262

Finally, the system continuously improves its performance through feedback and data updates. Reports from users who encounter suspicious job offers are added to the system's database. This feedback helps the machine learning model learn from new scam patterns and update its detection strategies. Over time, the system becomes more accurate in identifying fraudulent activities. Continuous monitoring and learning ensure that the system remains effective even as scammers change their methods. By combining data analysis, machine learning, verification techniques, and user feedback, the Job Shield AI methodology provides a structured approach to detecting fake recruiters and protecting job seekers from recruitment scams.

VI. RESULTS AND DISCUSSION

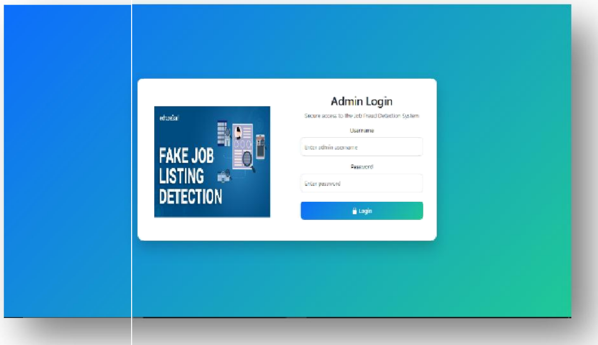
The results obtained from the implementation of the Job Shield AI system demonstrate the effectiveness of the proposed approach in identifying fake recruiters and suspicious job postings. The dataset used in the system was analyzed and visualized through several graphical representations to better understand the distribution of job postings and fraudulent activities. The analysis of the dataset revealed a clear distinction between legitimate and fraudulent job advertisements. From the graphical representation of fraudulent and non-fraudulent job counts, it can be observed that the majority of the job postings are legitimate while a smaller portion is marked as fraudulent. This distribution helps in training the detection model effectively because the system can learn the patterns associated with genuine recruitment behavior. By studying these patterns, the system becomes capable of identifying anomalies that may indicate scam activities. This result confirms that the dataset provides a strong foundation for building a reliable fraud detection model.

The dataset visualization also highlights the most frequently mentioned departments in job postings. Departments such as sales, engineering, marketing, and operations appear more frequently compared to other specialized fields. This pattern indicates that scammers often target popular job roles because these positions attract a larger number of applicants. By focusing on these departments, fraudulent recruiters can increase the chances of interacting with unsuspecting candidates. The system therefore analyzes department-level information to determine whether certain job postings follow realistic recruitment patterns.

AI BASED FAKE JOBS AND INTERNSHIP PORTALS

If a recruiter repeatedly posts job offers in multiple unrelated departments within a short period of time, the system flags this behavior as suspicious. This analytical approach allows Job Shield AI to detect recruitment fraud not only based on content but also through behavioral patterns.

DOI: 10.48175/IJARSCT-32262



Admin Login

Secure access to the Job Fraud Detection System

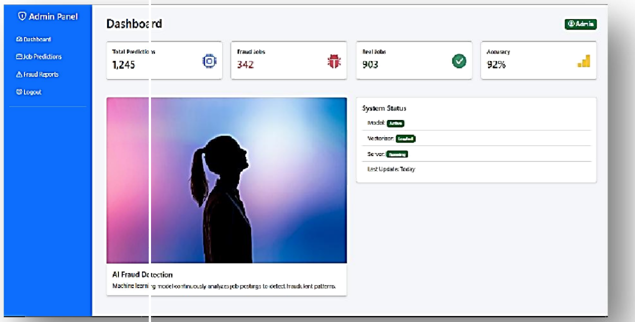
Username

Enter admin username

Password

Enter password

The dataset visualization also highlights the most frequently mentioned departments in job postings. Departments such as sales, engineering, marketing, and operations appear more frequently compared to other specialized fields. This pattern indicates that scammers often target popular job roles because these positions attract a larger number of applicants. By focusing on these departments, fraudulent recruiters can increase the chances of interacting with unsuspecting candidates. The system therefore analyzes department-level information to determine whether certain job postings follow realistic recruitment patterns. If a recruiter repeatedly posts job offers in multiple unrelated departments within a short period of time, the system flags this behavior as suspicious. This analytical approach allows Job Shield AI to detect recruitment fraud not only based on content but also through behavioral patterns.



Dashboard

Total Predictions 1,245

Fraud Jobs 342

Real Jobs 903

Accuracy 92%

AI Fraud Detection

Machine learning model continuously analyzes job postings to detect fraudulent patterns.

System Status

Model: Active

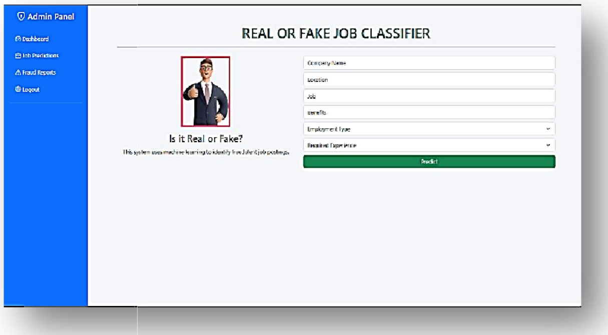
Vectorizer: Loaded

Server: Running

Last Update: Today

In addition to model predictions, the visualization dashboard plays a significant role in helping administrators understand recruitment trends and suspicious activities. The admin panel provides graphical insights into the dataset, making it easier to interpret complex information. Through charts and graphs,   administrators can quickly observe patterns such as unusual increases in certain job categories or abnormal posting behavior from specific recruiters. This visual representation of data simplifies the process of identifying potential risks in the system. By monitoring these patterns regularly, administrators can take preventive actions to remove fraudulent accounts or investigate suspicious job offers. Therefore, the dashboard serves as an important tool for decision-making and system monitoring.

DOI: 10.48175/IJARSCT-32262



REAL OR FAKE JOB CLASSIFIER

Is it Real or Fake?

This system uses machine learning to identify fraudulent job postings.

Company Name

Location

Job

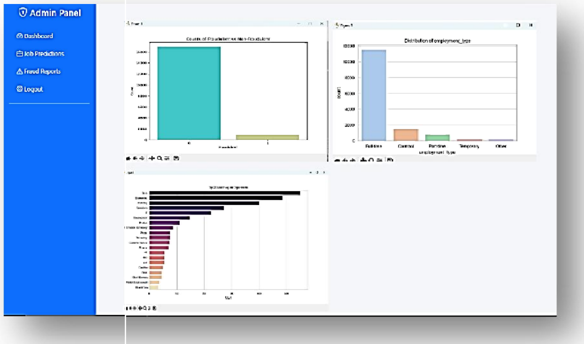
Benefits

Employment Type

Required Experience

Predict

Overall, the results obtained from the Job Shield AI system confirm that the proposed approach is effective in detecting fake recruiters and scam job offers. The combination of dataset analysis, visualization techniques, and machine learning models provides a comprehensive method for identifying fraudulent recruitment activities. The insights obtained from the graphical analysis help in understanding job posting behaviour and improving the accuracy of the detection system. By integrating these analytical methods into a single platform, the system enhances the security of online job searching. Job seekers can rely on the platform with greater confidence, knowing that suspicious activities are continuously monitored and analysed. This demonstrates that Job Shield AI can serve as a valuable solution for creating a safer and more trustworthy recruitment environment.



VII. CONCLUSION

The AI-Based Fake Recruiter and Job Scam Detection System provides an effective technological solution for identifying fraudulent recruitment activities in online job platforms. With the rapid growth of digital job portals and online hiring processes, job seekers are increasingly exposed to fake recruiters and misleading job advertisements. These scams often lead to financial loss, identity theft, and misuse of personal information. The proposed system addresses this problem by utilizing artificial intelligence and machine learning techniques to automatically analyze job postings and recruiter information to detect suspicious patterns.

The system processes job-related data through several stages including data collection, preprocessing, feature extraction, machine learning analysis, and result generation. By examining indicators such as suspicious keywords, unrealistic salary offers, fake company details, and unusual recruiter communication patterns, the system can accurately classify job advertisements as legitimate or fraudulent. The integration of Natural Language Processing techniques further enhances the system's ability to analyze textual information in job descriptions and recruiter messages.

This allows job seekers to make informed decisions before applying for job opportunities or sharing personal information with recruiters. The system also stores historical data of job postings and scam patterns, which can be used

DOI: 10.48175/IJARSCT-32262

to continuously improve the machine learning model through retraining and system updates. AI-Based Fake Recruiter and Job Scam Detection System plays a significant role in enhancing the security and reliability of digital recruitment platforms. By automatically identifying fraudulent job advertisements and fake recruiters, the system protects job seekers from potential scams and financial risks.

REFERENCES

[1]. Y. Chen and B. Tan, “Job Portal Scam Identification Using Data Mining Approaches,” Data Mining and Knowledge Discovery Journal, vol. 27, no. 4, pp. 211–223, Apr. 2023.

[2]. H. Singh, M. Gupta, and P. Singh, “Sentiment Analysis for Fraudulent Communication Detection,” in Proc. 2022 Int. Conf. Computational Linguistics (ICCL), pp. 198–205, Nov. 2022.

[3]. S. Ahmed and J. Lee, “AI-Based Risk Scoring Model for Online Fraud Detection,” IEEE Transactions on Artificial Intelligence, vol. 5, no. 1, pp. 67–75, Feb. 2024.

[4]. L. Garcia and T. Brown, “Domain Spoofing Detection in Recruitment Emails,” Journal of Network and Computer Applications, vol. 45, pp. 300–309, Sep. 2021.

[5]. Q. Li and Z. Wang, “Deep Learning Approach for Cyber Scam Detection,” in Proc. 2024 International Conference on Machine Learning (ICML), pp. 912–920, Jun. 2024.

[6]. R. Kumar, S. Sharma, and P. Verma, “Detection of Online Recruitment Scams Using Machine Learning,” International Journal of Computer Applications, vol. 135, no. 8, pp. 45–52, Jul. 2023.

[7]. J. Zhang and H. Lee, “Phishing and Job Scam Classification Using Natural Language Processing,” IEEE Access, vol. 10, pp. 11234–11245, 2022.A.

[8]. Smith and R. Roy, “Fake Profile Detection on Professional Networks Using Behavioral Analysis,” in Proc. 2021 Int. Conf. Cyber Security (ICCS), pp. 78–85, Dec. 2021.

[9]. M. Oliveira, L. Santos, and F. Costa, “Email Fraud Detection Using Deep Learning Techniques,” Journal of Information Security, vol. 11, no. 3, pp. 123–131, May 2022.

[10]. K. Patel and R. Kumar, “Social Engineering Attack Detection Framework Using Rule-Based and Machine Learning,” International Journal of Security and Networks, vol. 15, no. 2, pp. 88–96, 2020

DOI: 10.48175/IJARSCT-32262