Journal of Information Technology and Digital World (ISSN: 2582-418X)
www.irojournals.com/itdw/

Recallio AI: An Intelligent Multimodal Forensic Platform for Recruitment Fraud Detection and Prevention

Shanthi S.[1], Palani Surya S.[2], Petchiammal S.[3], Prasheetha R.[4], Santhiya M.[5]

[1]Assistant Professor, [2,3,4,5]UG Student, Department of Computer Science and Engineering, V V College of Engineering, Tisaiyanvilai, India.

E-mail: [1]shanthi@vvcoe.org, [2]palanisurya908@gmail.com, [3]petchiammalsenthil7@gmail.com, [4]prasheethaprasheetha50@gmail.com, [5]sanmrssk@gmail.com

Abstract

Recruitment fraud has become one of the major problems for cybersecurity owing to the exponential rise of online recruiting tools, social networking sites, and messaging services. Fraudsters use fake identities of recruiters, scams in job postings, phishing websites and links, and other techniques, leading to monetary loss and identity theft. In this paper, the Recallio AI tool, a multimodal forensic intelligent system for detecting recruitment fraud, is discussed. In this system, the use of Google Gemini AI, Optical Character Recognition (OCR), and web full-stack technologies in analyzing resumes, job description, recruiter chat, screenshots, physical posters, and information about the company is suggested. A combined approach based on scam detection, conversation forensic investigation, OCR-based street-side scanning, company verification, victim assistance, and analytical tools was implemented. The test data included 155 samples that were genuine and fake relating to recruitment processes. It was discovered that the framework under consideration delivered a 91.0% accurate detection rate. It becomes apparent that the framework can be effective when it comes to detecting cases of recruitment fraud both offline and online, promoting cybersecurity and forensic awareness.

Keywords: Recruitment Fraud, AI Forensics, Multimodal Analysis, Scam Detection, Gemini AI, OCR, Cybersecurity, Job Scam Prevention.

DOI: https://doi.org/10.36548/jitdw.2026.3.002
Extended version of article received from **International Conference on Next Generation Engineering Innovations, AI and Sustainable Automation – 2026**
Received: 31.03.2026, received in revised form: 03.05.2026, accepted: 25.05.2026, published: 05.06.2026
© 2026 Inventive Research Organization. This is an open access article under the Creative Commons Attribution-NonCommercial International (CC BY-NC 4.0) License

1. Introduction

The fast development of online recruiting platforms and digital communication technologies has considerably reshaped the recruitment process in today's world. Unfortunately, it has also opened new avenues for cybercriminals who commit fraud against job seekers via online recruiting. The typical methods include posing as a legitimate company, sending false recruiting ads, and tricking the targets by means of phishing messages, instant messengers, and websites that appear to belong to a reputable firm. The FTC has recently reported that the number of online recruiting scams has increased sharply causing financial damage and emotional stress for their victims [1].

Contemporary recruitment scams are characterized by the use of social engineering techniques that include fake recruiter personas, advance-fee fraud, identity fraud, and malintent data harvesting. Fresh graduates and unemployed people are frequently the targets of fraudsters due to promising high salaries, remote jobs, and urgent employment process. Currently available systems based on keyword-based and blacklist-based approaches fail to detect scam activity [2], [5].

Advances in the field of AI, specifically LLMs and multimodal AI, have enhanced the functionality of automatic scam detectors. LLMs can detect manipulative and phishing activities in messaging platforms [3]. Likewise, multimodal AI models like Google's Gemini can process texts, images, and structured data at once, which makes them good candidates for recruiting scam analyses [7]. OCR technologies can also aid in extracting text from images like screenshot images, posters, or scanned images [9]. Unfortunately, current techniques primarily concentrate on individual processes like phishing email detection, fake profile detection, or using OCR technology. Comprehensive systems that can incorporate all these processes into a single platform are not common yet.

In order to overcome the limitations highlighted above, this research proposes Recallio AI, an intelligent multimodal forensic platform for detecting and preventing recruitment fraud. The platform combines Google Gemini AI, OCR, and full stack web technology in analyzing job posts, recruiters' conversation, screenshots, physical postings, and companies' details. Some of the components integrated within Recallio AI include: scam detector, chat forensic module, OCR street scanner, company verification, awareness provision, and forensic report generation.

2. Related Works

Studies related to fraud detection in recruitment have shifted their attention towards analyzing phishing scams, detecting fake profiles, digital forensics, and scams detection using artificial intelligence. Nevertheless, multimodal systems that aim at combating fraud in recruitment are scarce.

Online recruitment scams have emerged as one of the major security threats, with an increase in number of recruitment frauds that target potential employees online [1]. Methods of identifying fraudulent recruiter profiles in social networking sites by means of machine learning and behavior analysis have been suggested [2]. The ability of Large Language Models to detect scams in conversations and psychological manipulation of victims in messages has attracted a lot of interest [3]. Such methods are efficient to detect signs of urgency, impersonation, phishing attacks, and emotion manipulation that are common in recruitment scams.

The role of digital forensics in cybercrime investigation has proved its efficiency in collecting evidence, generating forensic reports, and tracking scammers online [4], [6]. The efficiency of machine learning for fraud detection using deceptive linguistic techniques in traditional phishing attacks has also been shown [5]. Nevertheless, current systems pay little attention to multimodal recruitment scams.

Multimodal AI modeling research has significantly contributed to multimodal analysis of text, images, and structured data analysis [7], [8]. Optical character recognition technologies like the Tesseract OCR engine are also applied for analysis of images of text and physical papers [9]. In addition, recent approaches to job advertisement screening with AI have applied text analysis and behavioral intelligence methods to identify fraud [10].

Despite these valuable contributions, current approaches only tackle certain aspects of recruitment fraud problem without providing an integrative approach that would incorporate all these factors and techniques mentioned above into one system. Recallio AI fills this gap through development of an integrated multimodal forensic technology aimed specifically at recruitment fraud detection and prevention.

3. System Architecture and Methodology

Recallio AI is intended to be an intelligent multimodal forensic platform that helps detect and prevent recruitment fraud in both online and offline communication channels. The platform uses a combination of multimodal AI technology, OCR technology in processing documents, and forensic evidence management in a single full-stack solution. The platform was developed using a React 18 and TypeScript frontend, Python Flask backend, MongoDB database, Redis session management, and the Google Gemini AI as the main multimodal reasoning platform.

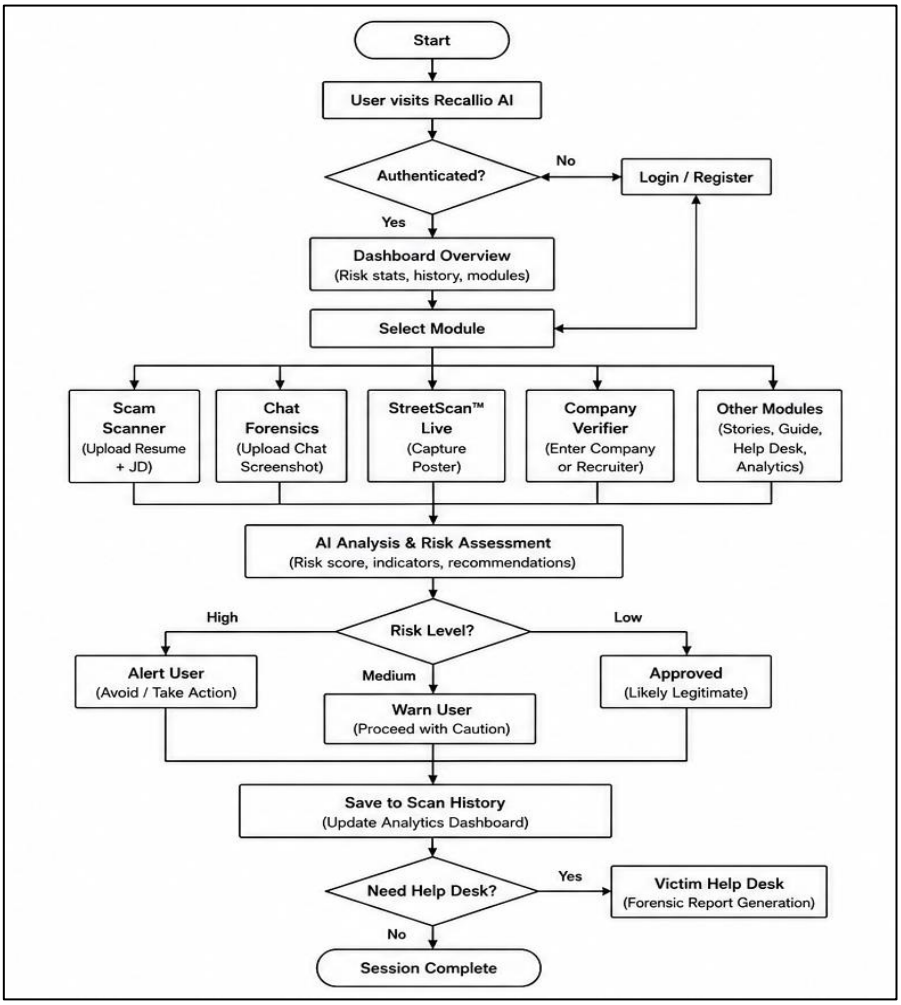

Figure 1. Recallio AI - Operational Workflow

Overall process of operation within Recallio AI is depicted in Figure 1, which shows how users log in to the system, select the required module for conducting a particular analysis related to fraud, submit evidence, and obtain scam risk assessment results as well as forensics advice. Different types of input data can be accommodated by the system architecture,

including CVs, job ads, screenshots, scanned copies, chats, and images of physical job ads. The processing of such data is done by analyzing inputs through the use of artificial intelligence systems, and results in structured output data, such as risk ratings, scam factors, manipulation detection, and forensics reports.

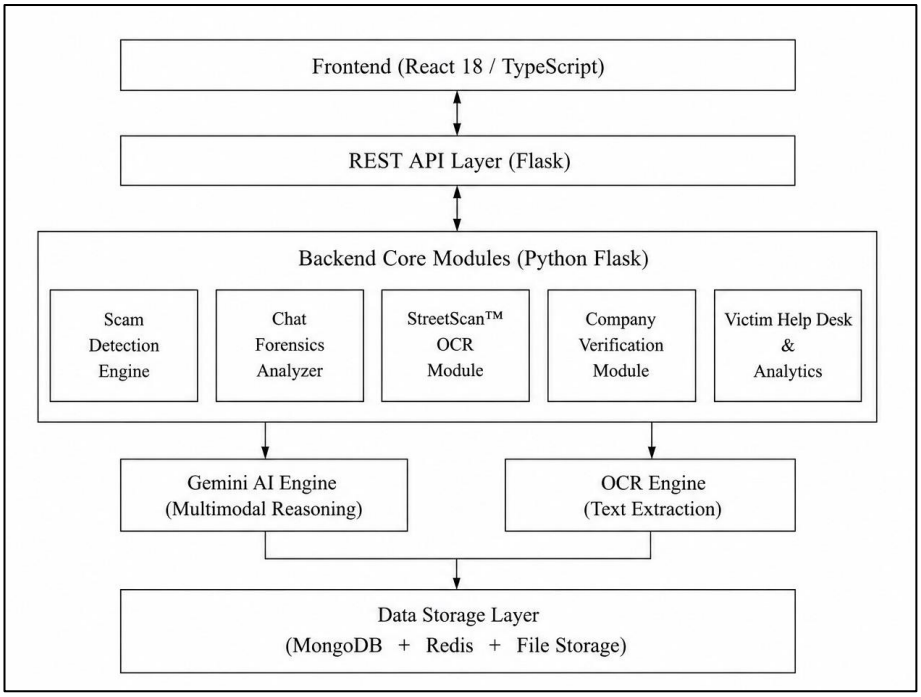

Figure 2. Recallio AI - System Architecture

Overall architecture of the system is represented in Figure 2. The scam detection engine is built around the context analysis of the resume uploads and the job descriptions for detecting scams. The module considers factors like exaggerated salaries, confusing job description criteria, urgency messages, financial transaction requests, and the lack of a fit between the candidates' credentials and job descriptions to provide an automatic risk evaluation based on the result of contextual analysis in form of a numerical value with descriptive indicators.

The chat forensic analyzer works with screenshot images of the conversations made through communication channels like WhatsApp, Telegram, LinkedIn, and emails. OCR processing and multi-modal AI algorithms are applied to detect manipulative psychological techniques such as urgency appeals, authority claims, phishing links, confidentiality appeals, and financial demands.

For offline recruitment scams, the Recallio AI offers the StreetScan™ Live module, which is used to analyze job postings that are made in the physical world. The poster can be

photographed using the mobile device and uploaded into the system. The text on the poster is extracted using OCR technology, while the AI technology evaluates factors such as no contact number registration, lack of company branding, exaggerated salaries, and suspicious posting patterns. This feature extends scam recognition capabilities to include non-traditional online methods.

Other AI features that are incorporated in the system to prevent scams include verification of recruiter and organizational identity using corporate data and behavior indicators. Other components include scam awareness materials, tips for newcomers, forensic evidence management, and automated victim assistance reporting services. Exposure analysis of scams is presented using dashboards that show risk trends, types of scams, and personal exposure records. Table 1 below shows the main modules with their corresponding AI features in Recallio AI.

Table 1. Module Summary and AI Capability

Module	Input	AI Function
Scam Scanner	Resume + JD	Gap analysis, risk scoring
Chat Forensics	Screenshots	Manipulation detection
Street Scanner	Poster images	OCR + signal extraction
Company Verifier	Name / Image	Corporate verification
Stories Feed	None	Pattern awareness
Security Guide	None	Archetype education
Help Desk	Multi-file	Forensic report gen.
Analytics	Scan history	Risk trend analysis

The backend employs Flask REST APIs with JWT token authentication and Bcrypt encryption for security purposes. The flexibility in data storage is achieved with the MongoDB database while Redis acts intelligently to cache the responses and avoid the need to repeatedly request the same data. Multimodal analysis requests will be processed by Gemini AI through specific service layers responsible for handling OCR, response parsing, contextual reasoning, and forensic report generation.

4. Experimental Results

Functional testing of Recallio AI was carried out through a carefully selected dataset comprising both valid and fraudulent contents related to recruitment services. This testing was geared toward evaluating the viability of the suggested forensic approach in detecting recruitment scams through various communication modes such as job ads, recruiter interactions, company information, and actual job postings. Evaluation experiments were carried out in four main areas: contextual scam detection, conversational forensic assessment, OCR, and company verification.

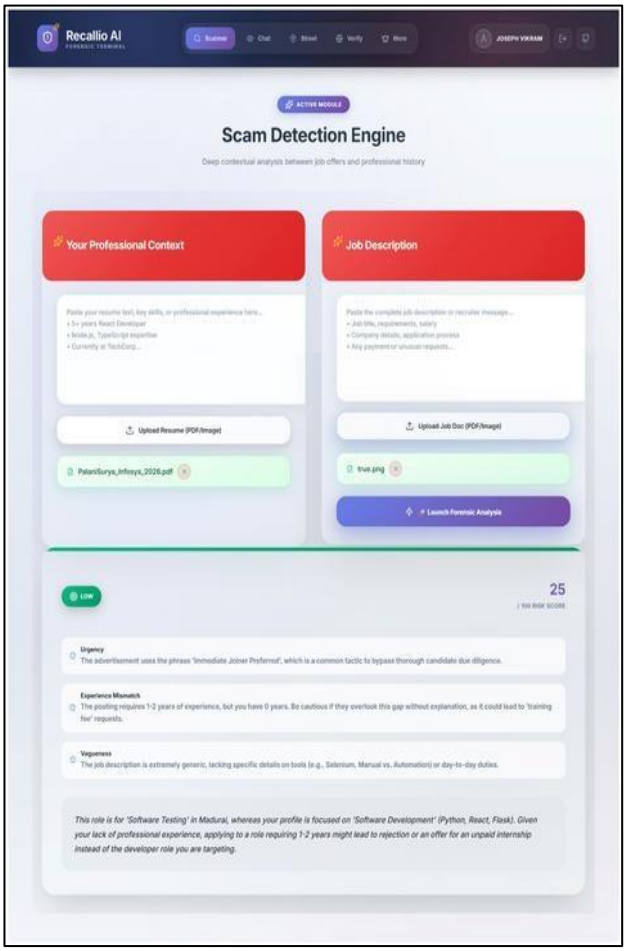

Figure 3. Context-Aware Recruitment Fraud Analysis Using the Scam Detection Engine

Figure 3 illustrates the process performed by the Scam Detection Engine in cross-analyzing the candidate's resume and the job description. A LOWrisk score was assigned to the analysis, namely, 25 out of 100, alongside the detection of contextual red flags such as the usage of urgent language in the recruitment process, vague demands, and experience mismatch.

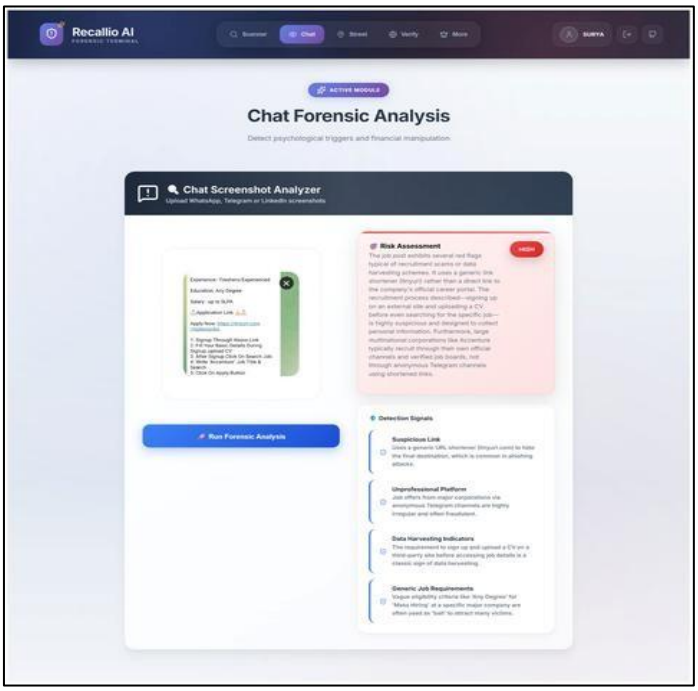

Figure 4. Conversational Scam Detection Using the Chat Forensics Analyzer

Figure 4 shows how the Chat Forensic Analyzer analyzed the recruitment chat on Telegram. The tool classified the chat as being of HIGH risk and successfully detected manipulation techniques such as suspicious URLs, inappropriate channels for recruitment, and attempts at harvesting data.

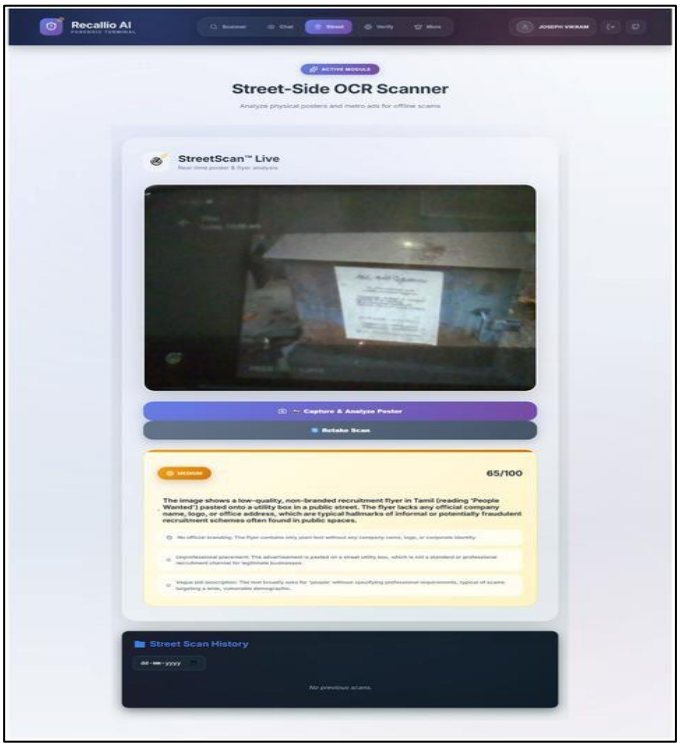

Figure 5. OCR-based Analysis of Physical Job Advertisements using StreetScan™

Figure 5 depicts the analysis carried out by the StreetScan™ OCR module for detecting recruitment fraud on a physical job posting written in Tamil. Although multiple languages and varying image qualities were present, the OCR system managed to successfully extract the textual information and detect suspicious signs like lack of corporate brand identity and unclear details about employment. A medium risk score of 65/100 was assigned, thus showing the possibility of recruiting scams detection without an internet connection.

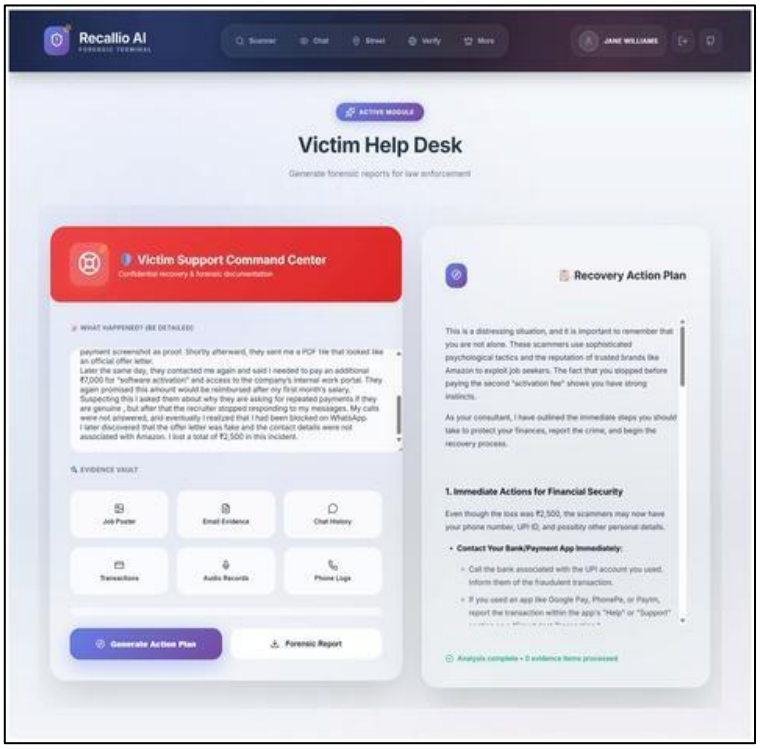

Figure 6. AI-assisted Victim Support and Forensic Report Generation

Figure 6 demonstrates how the Victim Help Desk module creates a well-structured plan of actions needed for fraud recovery based on a recruited scam narrative. In particular, the module offers tips on money protection, reporting, and evidence preservation along with automatically creating an electronic case file based on submitted evidences.

In order to conduct a quantitative assessment, a test dataset was designed based on publicly available recruitment information, scam incidents, company career postings, and synthetic scam conversation transcripts created by utilizing reported recruitment scamming patterns (refer to Table 2). All items in this dataset were manually classified according to predefined recruitment scamming indicators as Legitimate or Fraudulent.

Table 2. Dataset Composition

Category	Legitimate	Fraudulent	Total
Job Descriptions	25	25	50
Recruiter Chats	20	20	40
Physical Posters	15	20	35
Company Profiles	15	15	30
Total	75	80	155

Table 3. Performance Evaluation of Recallio AI

Module	Test Samples	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Scam Scanner	50	92	91.3	93.1	92.2
Chat Forensics	40	90	89.2	91.4	90.3
Street Scanner (OCR)	35	88.6	87.5	89.7	88.6
Company Verifier	30	93.3	92.8	94	93.4
Overall System	155	91	90.2	92.1	91.1

The findings (see Table 3) show that Recallio AI is capable of delivering high-level efficiency when implemented in all fraud detection modules. Specifically, Company Verifier managed to deliver the highest level of accuracy reaching 93.3%. As for Scam Scanner, it delivered 92.2% F1-score through contextual analysis of resumes and job description. The Chat Forensics module was successful in identifying manipulation recruitment frauds with the F1-score of 90.3%. It should be pointed out that despite the difficulties caused by image quality and linguistic differences in OCR-based analysis, Street Scanner was still capable of maintaining its accuracy level at 88.6%.

Overall, the proposed approach reached an accuracy level of 91.0% and F1-score of 91.1%, which proves that multimodal AI reasoning, OCR analysis, conversational forensics, and company verification prove to be efficient in detecting recruitment frauds both in online and offline space. Thus, Recallio AI can be considered a universal cybersecurity tool.

5. Conclusion

The current study introduced Recallio AI, which is a forensically intelligent multimodal platform designed specifically for detecting and preventing recruitment fraud. Multimodal AI, text extraction through OCR technology, conversational forensic techniques, and company verification are incorporated into this framework to form a safe and full-stack architecture. This solution was able to conduct comprehensive investigations on various recruitment materials such as CVs, job postings, screenshots from chats, printed advertisements, and recruiter details. Validation showed successful identification of various scam patterns related to such features as creating a sense of urgency, fake recruiter characteristics, suspicious links, job advertisements, and company practices. Furthermore, integration of reporting and victim assistance modules increased the practicality of the suggested approach to support cybersecurity and forensics. In contrast to other solutions aimed at identifying phishings through textual data only, Recallio AI offers an integrated environment for conducting a multimodal forensic investigation. Further research may include testing the system on larger datasets, threat intelligence integration, multilingual capabilities, and performance benchmarking.

References

[1] New FTC Data Show Skyrocketing Consumer Reports About Game-Like Online Job Scams. (2025, July 31). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2024/12/new-ftc-data-show-skyrocketing-consumer-reports-about-game-online-job-scams.

[2] Roy, Pradeep Kumar, and Shivam Chahar. "Fake Profile Detection on Social Networking Websites: A Comprehensive Review." IEEE Transactions on Artificial Intelligence 1, no. 3 (2021): 271-285.

[3] Chang, Yuan-Chen, and Esma Aïmeur. "Chat or Trap? Detecting Scams in Messaging Applications with Large Language Models." In 2024 8th Cyber Security in Networking Conference (CSNet), IEEE, 2024, 92-99.

[4] Edwards, Graeme. Cybercrime Investigators Handbook. John Wiley & Sons, 2019.

[5] Fette, Ian, Norman Sadeh, and Anthony Tomasic. "Learning to Detect Phishing Emails." In Proceedings of the 16th international conference on World Wide Web, 2007, 649-656.

[6] Ihekweazu, Chukwuemeka, Elizabeth Adepeju Adelowo, and Naomi Aghado. "Digital Forensics in Action: A Case Study of Tracing Cybercriminals Behind Job Offer Spear Phishing Scams in Academic Institutions." In Proceedings of the ISCAP Conference ISSN, vol. 2473, 2024, 4901.

[7] Team, Gemini, Rohan Anil, Sebastian Borgeaud, Jean-Baptiste Alayrac, Jiahui Yu, Radu Soricut, Johan Schalkwyk et al. "Gemini: A Family of Highly Capable Multimodal Models." arXiv preprint arXiv:2312.11805 (2023).

[8] Anthropic, A. I. "Model Card and Evaluations for Claude Models." Anthropic Blog (2023).

[9] Smith, Ray. "An Overview of the Tesseract OCR Engine." In Ninth international conference on document analysis and recognition (ICDAR 2007), vol. 2, IEEE, 2007, 629-633.

[10] Sudharsan, S., and R. Sudha. "AI-Powered Fake Job Detection Using Multimodal Hybrid Intelligence." In 2026 4th International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), IEEE, 2026, 964-970.