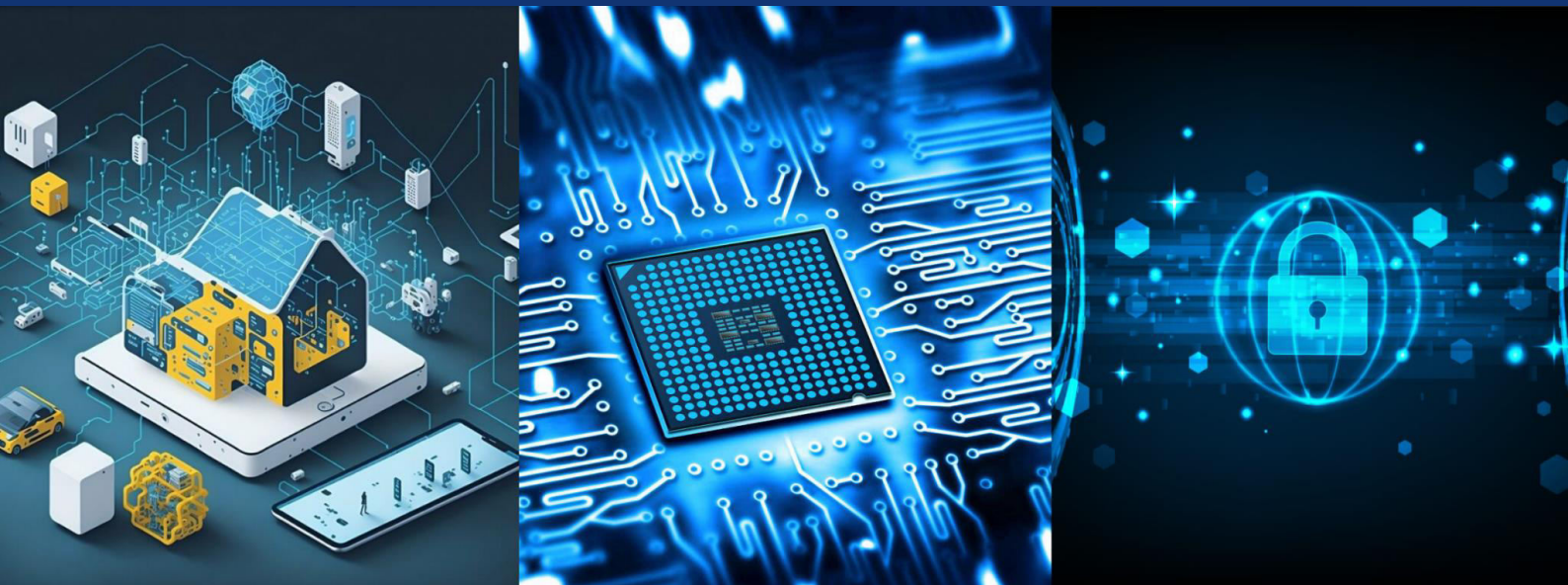




# International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

# Employee Recruitment Scam Detection System

S.Mohamed Ibrahim<sup>1</sup>, Mrs.S.Vinitha Mary<sup>2</sup>

PG Scholar, Dept. of Master of Computer Applications, R.V.S. College of Engineering, Dindigul,  
Tamil Nadu, India<sup>1</sup>

Assistant Professor, Dept. of Master of Computer Applications, R.V.S. College of Engineering, Dindigul,  
Tamil Nadu, India<sup>2</sup>

**ABSTRACT:** Employee Recruitment Scam Detection System is an AI-powered web application developed using Python Flask, MySQL, Bootstrap 5, HTML, CSS, and JavaScript to detect fraudulent job postings and protect job seekers from recruitment scams. The system uses a Random Forest machine learning model trained on the EMSCAD dataset with TF-IDF vectorization over 20,000 features, achieving 97.5% accuracy and 98.3% AUC-ROC score. In addition to ML prediction, the platform applies 30+ heuristic red-flag rules for improved scam detection. Key features include company reporting, fraud registry management, admin dashboard, scan history, company verification, rolebased access control, automated notifications, and audit logging. The application is structured into seven functional blueprints: Auth, Main, Predict, History, Admin, Company, and Reports, ensuring scalability, security, and user-friendly recruitment fraud detection.

## I. INTRODUCTION

The rapid growth of online job portals has increased both employment opportunities and recruitment scams, where fake job postings deceive applicants into sharing personal information or paying fraudulent fees. Traditional detection methods are inadequate against modern scams, creating the need for intelligent automated solutions. EMPLOYEE RECRUITMENT SCAM DETECTION SYSTEM is an AI-powered platform that detects fraudulent job postings using a Random Forest machine learning model with TF-IDF feature extraction and 30+ heuristic red-flag rules. The system also includes community-based company reporting, an auto-updating fraud registry, and an admin dashboard for moderation, analytics, and audit tracking. Developed using Python Flask with SQLite3/MySQL support, the platform provides a scalable, secure, and effective solution for preventing online recruitment fraud.

## II. EXISTING SYSTEM

Existing methods for detecting fake job postings mainly rely on manual moderation, basic keyword filtering, or research-based prototypes. Major job portals such as LinkedIn, Indeed, and Naukri depend heavily on human moderators and user reports, which are difficult to scale and often lead to delayed action. Keyword-based filters are also ineffective because fraudsters can easily bypass them by slightly modifying suspicious phrases. Although academic NLP-based detection models achieve high accuracy on benchmark datasets, most lack practical deployment features such as user reporting, fraud registries, and administrative monitoring tools.

### Disadvantages of Existing Systems

- Manual moderation makes scam detection slow and difficult to scale.
- Keyword-based filters can be easily bypassed through minor text changes.
- Existing systems lack community reporting and an auto-updating fraud registry.
- Users are not clearly informed why job postings are flagged as suspicious.
- Most platforms do not provide proper admin controls, audit logging, or moderation tracking.
- Research-based ML models are rarely implemented as practical real-time web applications.
- No automatic escalation exists for companies receiving repeated fraud reports.





## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

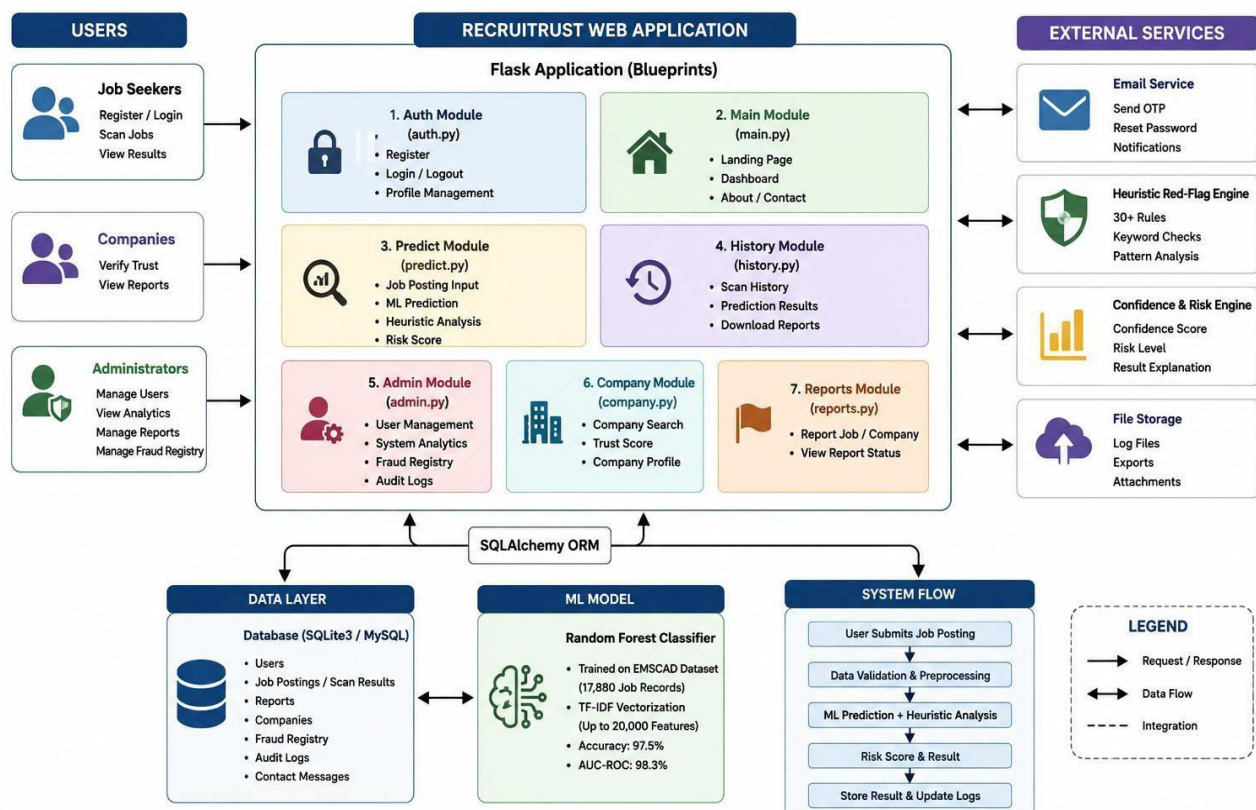
### III. PROPOSED SYSTEM

EMPLOYEE RECRUITMENT SCAM DETECTION SYSTEM is an AI-powered, community-integrated web platform designed to detect fraudulent job postings through multi-layered analysis. The system combines machine learning prediction, heuristic red-flag detection, community reporting, and centralized administrative monitoring to overcome the limitations of manual and keyword-based approaches. Its core ML engine uses a Random Forest classifier trained on the EMSCAD dataset containing 17,880 job records, with TF-IDF vectorization extracting up to 20,000 textual features. The model achieves 97.5% accuracy and 98.3% AUC-ROC score and is stored as a serialized pickle file for fast prediction. If the ML model becomes unavailable, the platform automatically switches to a heuristic scoring engine that detects suspicious keywords, abnormal salary patterns, and incomplete job information to maintain scam detection functionality.

#### Advantages of the Proposed System

- High-accuracy ML classification (97.5%) using a real-world recruitment fraud dataset.
- Dual-layer detection combining ML prediction with 30+ heuristic red-flag rules.
- Community reporting system for identifying suspicious companies and job postings.
- Auto-updating fraud registry for repeatedly reported organizations.
- Role-based access control for users, admins, and company portals.
- Transparent confidence scoring with LOW, MEDIUM, and HIGH risk levels.
- Audit logging for admin actions, logins, and system activities.
- REST API support and scalable Flask blueprint architecture for future expansion.

### IV. SYSTEM ARCHITECTURE





## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

### V. MODULE DESCRIPTION

- Authentication Module
- Main Module
- Job Scan / Prediction Module
- Scan History Module
- Admin Module
- Company Module
- Reports / Fraud Registry Module

#### 1. Authentication Module

The Authentication Module manages user registration, login, logout, and profile handling. It validates inputs, prevents duplicate accounts, and securely hashes passwords using Werkzeug's PBKDF2-SHA256 algorithm. Admin users are restricted to a separate login portal, while FlaskLogin handles session management with "remember me" support. All authentication activities are recorded in the audit log for security monitoring.

#### 2. Main Module

The Main Module provides the public-facing pages of the application including the landing page, user dashboard, About page, and Contact page. The dashboard aggregates the authenticated user's scan statistics, recent predictions, and notifications. The contact form writes enquiries to the contact\_messages database table, which are visible to administrators via the admin panel.

#### 3. Job Scan / Prediction Module

The Prediction Module is the core component of EMPLOYEE RECRUITMENT SCAM DETECTION SYSTEM, responsible for analyzing job postings and detecting recruitment scams. It processes job details such as title, company, salary, description, requirements, and benefits using a FakeJobPredictor that combines TF-IDF feature extraction with a trained Random Forest model to generate FAKE/REAL predictions, confidence scores, and risk levels. A heuristic engine simultaneously checks for 30+ suspicious keywords and patterns, while the system also verifies companies against the Fraud Registry and community reports. Companies receiving three or more reports are automatically flagged as FAKE. All prediction results are stored in the database, and a REST API endpoint enables external integration.

#### 4. Scan History Module

The History Module provides registered users with a filterable, paginated record of all job scans they have performed. Each history entry links to a detailed result view displaying the original job fields, ML prediction outcome, confidence score, risk level, detected red flags, and any admin verification status applied by an administrator.

#### 5. Admin Module

The Admin Module provides a secure dark-themed portal accessible through /admin/, protected by role-based authentication using a custom admin\_required decorator. The dashboard displays real-time statistics such as total users, scans, fake/real predictions, pending reports, unread messages, and fraud registry data, along with analytical charts. Administrators can manage users, verify predictions, handle community reports, update the fraud registry, review contact messages, and export reports. All administrative activities are recorded in the SystemLog audit table for accountability and tracking.

#### 6. Company Module

The Company Module provides company verification and reporting features. The Company Check function allows users to search for a company and view its fraud registry status, community report count, and previous scam prediction records. The Company Report function enables registered users to report suspicious employers by selecting a reason category, adding a description, and optionally providing evidence links.

#### 7. Reports / Fraud Registry Module

The Reports Module renders the public fraud registry — a searchable listing of all companies currently active in the FraudCompanyRegistry table. Each entry displays the company name, the reason for flagging, whether the entry was



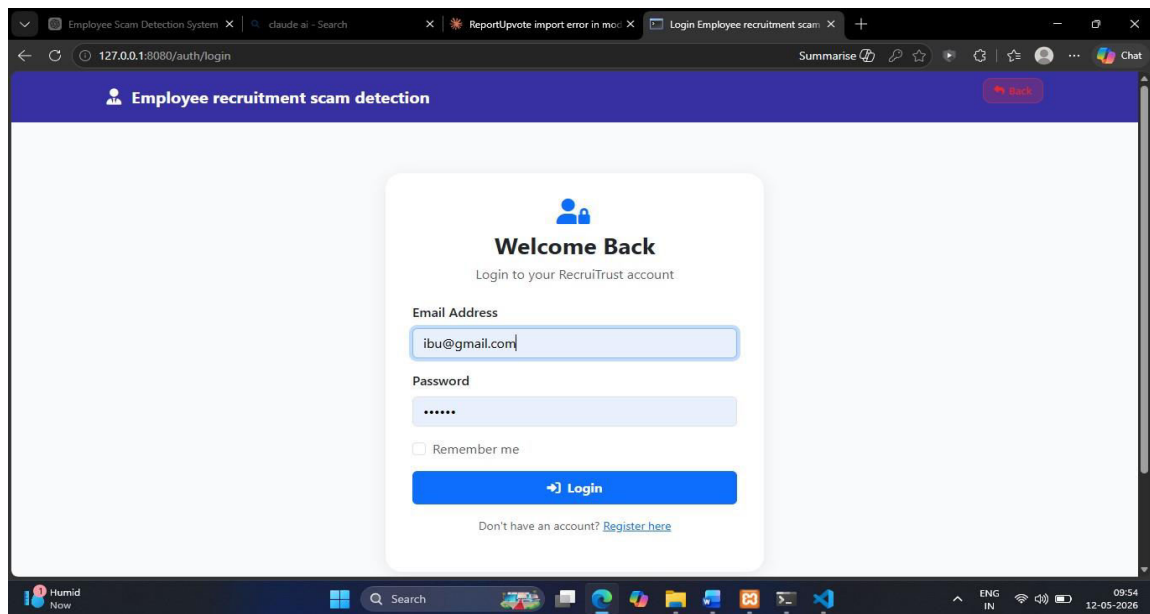
## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

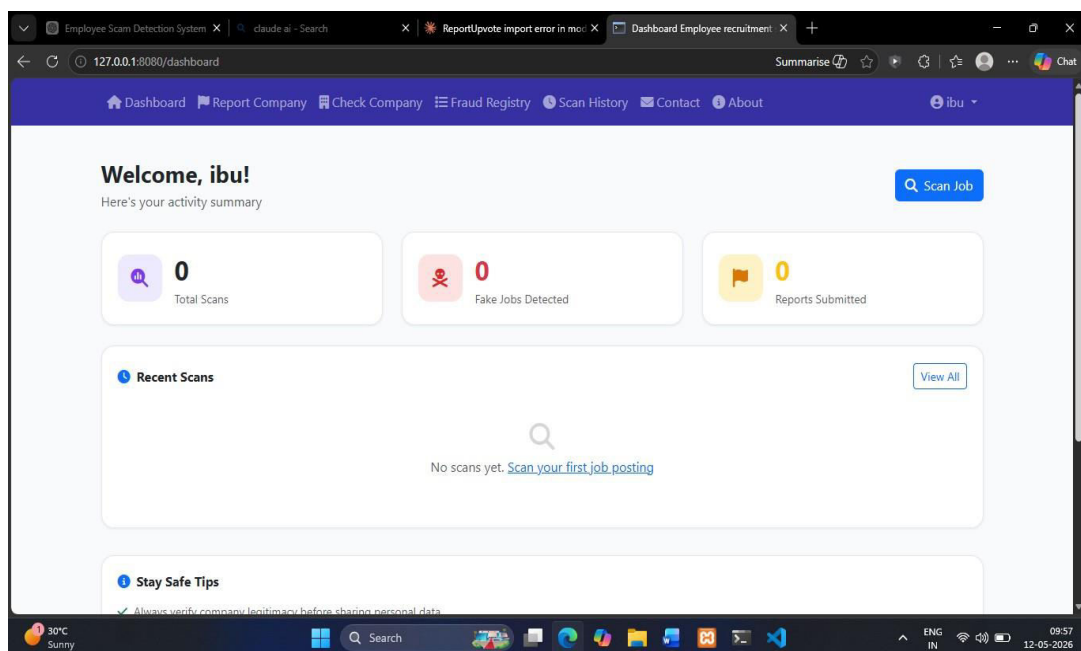
auto-generated by the threshold mechanism or added manually by an admin, and the date of addition. This module promotes community transparency and allows job seekers to proactively check employers before applying.

### VI. SCREENSHOTS

#### Login Page



#### User Dashboard





## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

### Job Scan / Prediction Form

**Scan a Job Posting**

Paste the job details below — our AI will detect if it's fake in seconds

**BASIC INFORMATION**

Job Title \*  Company Name

Location  Department

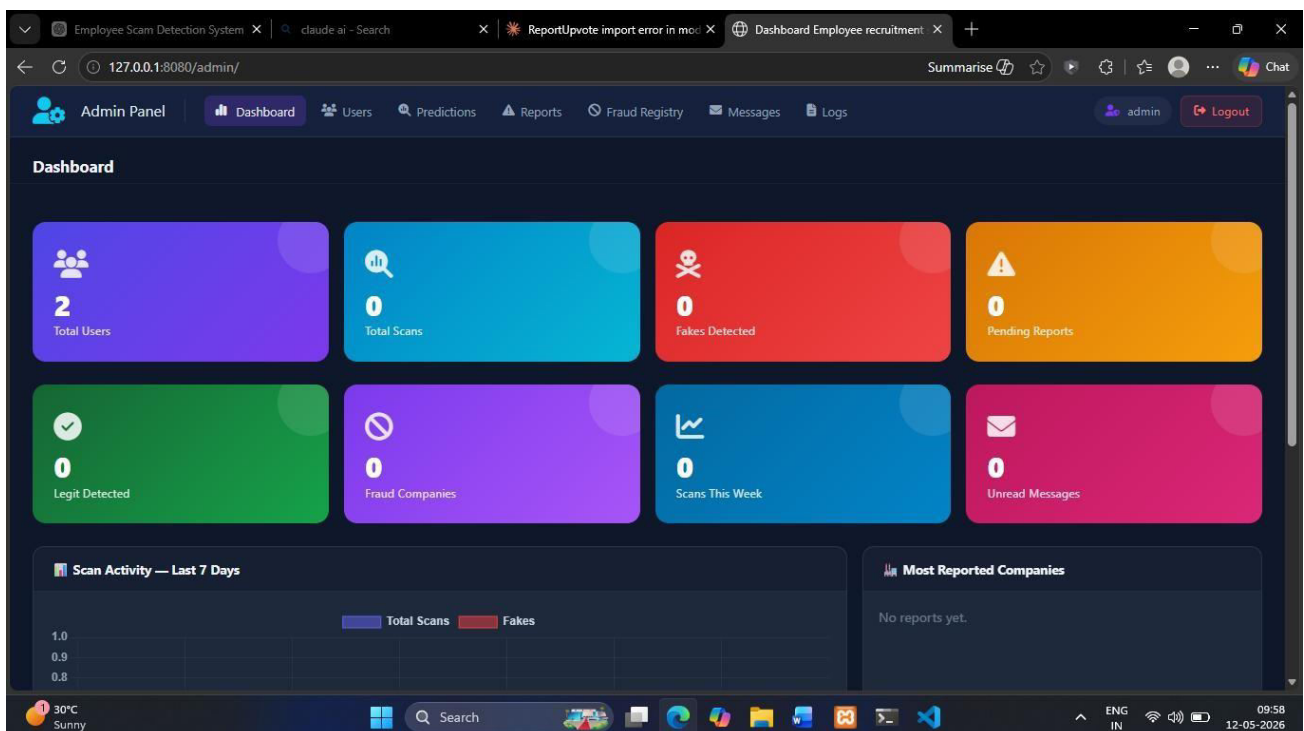
Employment Type  Required Experience  Required Education

Industry  Salary Range

**JOB DETAILS**

Job Description (paste full description for best accuracy)

### Admin Dashboard

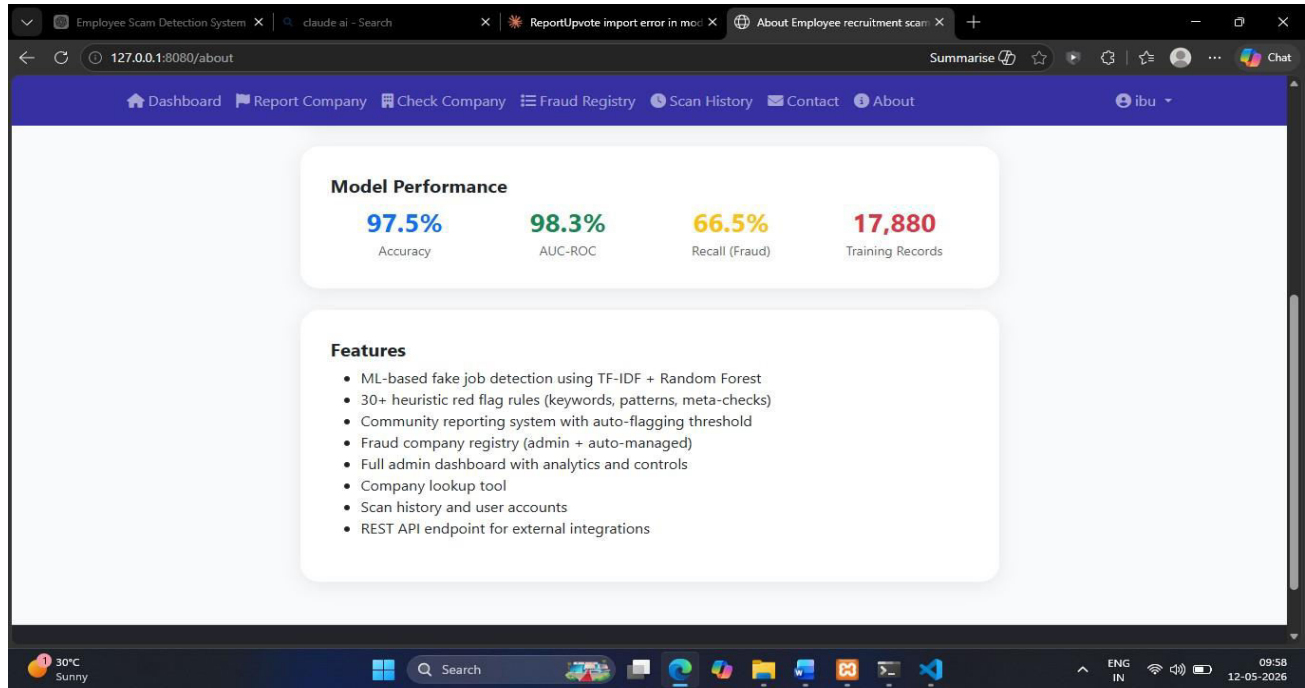




## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

### OUTPUT



### VII. CONCLUSION

EMPLOYEE RECRUITMENT SCAM DETECTION SYSTEM provides a complete AI-powered platform for detecting online recruitment scams by combining machine learning, heuristic analysis, community reporting, and administrative monitoring. The system uses a Random Forest classifier trained on the EMSCAD dataset along with 30+ heuristic red-flag rules to achieve 97.5% accuracy and 98.3% AUC-ROC performance. Its Flask blueprint-based architecture ensures modularity, scalability, and maintainability, while security features such as role-based access control, password hashing, CSRF protection, and audit logging enhance system reliability. The community reporting and auto-flagging mechanisms further strengthen detection by continuously identifying suspicious companies beyond the trained dataset. Overall, the platform demonstrates that integrating AI with community intelligence and administrative oversight creates a more effective and trustworthy recruitment fraud detection system.

### VIII. FUTURE ENHANCEMENT

Several future enhancements are planned to improve the functionality and scalability of EMPLOYEE RECRUITMENT SCAM DETECTION SYSTEM. Future versions may integrate advanced deep learning models such as BERT for better detection of sophisticated scam postings, provide multilingual support for regional languages, and include explainable AI techniques like SHAP or LIME to improve transparency in prediction results. The platform can also be extended through cloud deployment, browser extensions, mobile applications, and social media monitoring to increase accessibility and real-time scam detection capabilities.

- Deep learning integration using BERT-based models for improved scam detection.
- Browser extension for real-time job analysis on platforms like LinkedIn, Indeed, and Naukri.
- Mobile application support for Android and iOS devices.
- Multilingual NLP support for Hindi, Tamil, and other regional languages.
- Email scanning and social media job-post monitoring features.
- Cloud deployment using Docker and Kubernetes for scalability.
- Advanced admin analytics and fraud trend detection tools.





## International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

### REFERENCES

1. P. VIDROS, C. KOLIAS, G. KAMBOURAKIS, AND L. AKOGLU, "AUTOMATIC DETECTION OF ONLINE RECRUITMENT FRAUDS: CHARACTERISTICS, METHODS, AND A PUBLIC DATASET," *FUTURE INTERNET*, VOL. 9, NO. 1, P. 6, 2017.
2. S. AMAAR, A. ALJEDAANI, M. MKAOUER, M. LUDI, AND A. RUSTAM, "DETECTION OF FAKE JOB POSTINGS BY COMBINING UNSUPERVISED AND SUPERVISED MACHINE LEARNING," *INFORMATION (MDPI)*, VOL. 13, NO. 9, P. 439, 2022.
3. T. MAHBUB AND T. HOSSAIN, "FAKE JOB RECRUITMENT DETECTION USING MACHINE LEARNING APPROACH," *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS (IJACSA)*, VOL. 12, NO. 3, PP. 714–720, 2021.
4. F. PEDREGOSA ET AL., "SCIKIT-LEARN: MACHINE LEARNING IN PYTHON," *JOURNAL OF MACHINE LEARNING RESEARCH (JMLR)*, VOL. 12, PP. 2825–2830, 2011.
5. FLASK OFFICIAL DOCUMENTATION, PALLETS PROJECTS, 2023. AVAILABLE: [FLASK DOCUMENTATION](#)
6. SQLALCHEMY DOCUMENTATION, SQLALCHEMY AUTHORS, 2023. AVAILABLE: [SQLALCHEMY DOCUMENTATION](#)
7. M. GRINBERG, *FLASK WEB DEVELOPMENT: DEVELOPING WEB APPLICATIONS WITH PYTHON*, 2ND ED., O'REILLY MEDIA, 2018.
8. BOOTSTRAP 5 DOCUMENTATION, BOOTSTRAP AUTHORS, 2023. AVAILABLE: [BOOTSTRAP DOCUMENTATION](#)
9. A. GÉRON, *HANDS-ON MACHINE LEARNING WITH SCIKIT-LEARN, KERAS, AND TENSORFLOW*, 2ND ED., O'REILLY MEDIA, 2019.
10. R. S. PRESSMAN AND B. R. MAXIM, *SOFTWARE ENGINEERING: A PRACTITIONER'S APPROACH*, 8TH ED., MCGRAW-HILL EDUCATION, 2015.





INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  [ijircce@gmail.com](mailto:ijircce@gmail.com)



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details