International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 06 June-2026 | Impact Factor: 3.5

# AI Powered Internship Fraud Detection System

**P. Rajapandian[1], K. Someshwar[2*]**

[1]Associate Professor, Department of Master Computer Application, Sri Manakula Vinayagar Engineering College, Pondicherry, India

[2]Student, Department of Master Computer Application, Sri Manakula Vinayagar Engineering College, Pondicherry, India

**How to Cite this Article**:

Someshwar, K. (2026). AI Powered Internship Fraud Detection System. International Journal of Creative and Open Research in Engineering and Management, 02(6). https://doi.org/10.55041/ijcope.v2i6.142



https://doi.org/10.55041/ijcope.v2i6.142

**Abstract:** There has been a dramatic increase in the number of online job and internship websites, leading to a dramatic increase in the number of opportunities available to students and new graduates; At the same time, this has also created an increase in the number of fraudulently posted internships, con-artist recruiters, phishing links, and counterfeit job listings. Many students are scammed into becoming victims of identity theft, financial fraud, and misrepresentation of job opportunities because of the lack of an established verification process in place regarding the validity of the job postings. Most of the current job search portals are focused primarily on providing internship listings and they do not have any intelligent mechanism in place for identifying or preventing fraudulent activity. In order to address these issues, we are proposing the development of an "AI-Powered Internship Fraud Detection System". The system utilizes both Artificial Intelligence and Machine Learning technologies to perform an automated analysis on all internship listings in order to identify any fraudulent or dubious opportunities. The framework employs a wide variety of criteria that are evaluated in order to determine the legitimacy of an internship opportunity, including the authenticity of the company, the verification of the email/domain of the person posting the job, the inclusion of suspicious key words, the behavior of the recruiting entity, any abnormalities in the salary offered, and by way of user reporting.

KEY WORDS: Artificial Intelligence, Internship Fraud Detection, Machine Learning, Cybersecurity, Scam Detection, Recruitment Security.

## 1. Introduction

With the rise of technology, students and new college graduates use websites for job and internship searches often as their primary source. Employers much easier. Though there are many positives from using these sites, the increase of people using them has also led to an enormous increase in internships that are fraudulent or scams. Fraudulent recruiting firms and/or impostors offer false internship opportunities and attempt to take advantage of students by obtaining money as an application fee, personal identification information, banking details and/or using them for free labor. Some scammers

distribute phishing links and fake company websites as a way to trick prospective employees. Due to a lack of awareness and proper verification processes, numerous potential employees have been victims of these unrelated activities resulting in a loss of funds, emotional distress and problems within their career. Typically job sites are more focused on posting internships and are used much more as a method of applying for an internship, typically do not have fraud detection capabilities. The ways in which currently used sites evaluate their recruitment processes are either through manual verification or required reporting from users – both of which take an excessive amount of time to accomplish. At this time there are no real-time or automatic ways to monitor recruiters' behaviors, check for fake company domains, check for unrealistic compensation levels, or check for scam related information. The proposed system not only helps students identify genuine internship opportunities but also improves security and trust in online recruitment platforms. In addition, the framework

provides real-time alerts and fraud risk analysis before users apply for internships. The system can be implemented in job portals, college placement systems, and recruitment platforms to ensure safer internship experiences for students and job seekers. Overall, the project aims to provide a smart, secure, user-friendly, and cost-effective solution for internship fraud detection and mitigation using modern AI technologies.

## 2. Literature Review

Several researchers have developed intelligent systems for fraud detection, cybersecurity, and recruitment safety using Artificial Intelligence and Machine Learning techniques. These studies provide the foundation for developing an effective internship fraud detection framework. Sharma et al. (2020): The researchers proposed a machine learning-based fraud detection system for online job portals. The system analyzed recruiter activities and detected suspicious behavior using classification algorithms such as Decision Tree and Naïve Bayes. Although the model improved fraud identification accuracy, it mainly focused on recruiter profiles and ignored internship content analysis.

Rao and Mehta (2021): The authors developed a phishing and fake website detection framework using Natural Language Processing and URL analysis techniques. The system identified malicious recruitment websites by analyzing suspicious links, keywords, and domain authenticity. However, the system could not analyze internship descriptions or user feedback effectively. Kumar et al. (2022): This research introduced a hybrid fraud detection model combining Machine Learning and data mining techniques for identifying fake job advertisements. Features such as salary patterns, company information, and email verification were analyzed to classify fraudulent postings. The system achieved good accuracy but lacked real-time alert mechanisms for users. Patel and Singh (2023): The researchers designed an AI-based recruitment monitoring system that used user complaint analysis and scam reporting mechanisms to detect fraudulent recruiters. The system improved platform security but depended heavily on manual reports, reducing automation efficiency. Zhang et al. (2022): The study focused on deep learning techniques for online scam detection. Long Short-Term Memory (LSTM) models were used to identify suspicious textual patterns in job advertisements and recruitment messages. While the model produced high detection accuracy, it required large datasets and high computational resources. Davidson et al. (2021): The researchers proposed a cybersecurity framework for protecting users from phishing attacks in online employment platforms. The system used email authentication and domain verification methods to identify fake recruiters. However, the framework was limited to email analysis and did not include complete internship verification features. From the above studies, it is observed that significant progress has been made in fraud detection, phishing analysis, and cybersecurity systems. Different approaches such as Machine Learning, Natural Language Processing, data mining, and deep learning have been successfully applied to detect suspicious online activities.

However, most existing systems focus only on a single aspect such as fake websites, recruiter verification, or phishing detection. There is still a need for an integrated and intelligent system capable of analyzing multiple factors together, including internship descriptions, recruiter authenticity, suspicious keywords, user feedback, salary anomalies, and company verification. Therefore, the proposed "AI-Powered Internship Fraud Detection System" aims to overcome these limitations by providing a real-time, automated, secure, and user-friendly internship scam detection framework using AI technologies.

## 3. Problem Statement

In recent years, online internship and recruitment platforms have become highly popular among students and fresh graduates for finding career opportunities. Although these platforms provide easy access to internships and training programs, they have also become targets for fraudulent activities. Fake recruiters and scam organizations post misleading internship offers to collect money, steal personal information, or exploit students through unpaid work and false promises. Many students are unable to identify fraudulent internship postings because scam offers often appear similar to genuine opportunities. Fake recruiters use attractive job descriptions, unrealistic salary packages, fake company websites, and phishing links to deceive applicants. As a result, students may face financial loss, identity theft, emotional stress, and damage to their career growth. Existing internship and job portal systems mainly focus on listing opportunities and managing applications. Most current systems do not provide intelligent mechanisms to automatically detect fake internships or suspicious recruiter activities. Detection methods often depend on manual verification, user complaints, or basic spam filters, which are time-consuming, less accurate, and ineffective against advanced scams. Another major issue is that many existing fraud detection systems analyze only one type of data, such as email verification, recruiter information, or textual content. This limits the system's ability to identify complex fraud patterns. Furthermore, the lack of real-time alerts and automated risk analysis reduces user safety during the application process. There is therefore a strong need for an intelligent, automated, and reliable system capable of identifying fraudulent internship postings before users become victims. The proposed "AI-Powered Internship Fraud Detection System" aims to solve these problems by using Artificial Intelligence, Machine Learning, and Natural Language Processing techniques to analyze internship postings, verify recruiter authenticity, detect suspicious activities, and provide real-time fraud alerts to users. The system is designed to improve security, increase trust in online recruitment platforms, and protect students from internship-related scams through accurate and automated fraud detection mechanisms.

## 4. Existing System

The existing internship and job recruitment platforms mainly focus on providing internship listings, application management, and communication between recruiters and candidates. Most systems allow companies to post internship opportunities and students to apply through online portals. Some platforms also provide basic verification features such as email confirmation and user reporting mechanisms. Traditional fraud detection methods in existing systems mainly depend on manual verification, spam filtering, or complaint-based actions. These systems identify suspicious activities only after users report fraudulent postings. As a result, many fake internships remain active for a long period before being detected. Existing systems also lack intelligent automation for identifying scam patterns in real time. Certain platforms use simple keyword filtering techniques to detect suspicious content in internship descriptions. However, these approaches are not highly effective because scammers continuously modify their language and techniques to avoid detection. Some systems verify recruiter email addresses or company websites, but they do not perform deep analysis of recruiter behavior, salary patterns, or posting authenticity. Another limitation of existing systems is that they often analyze only

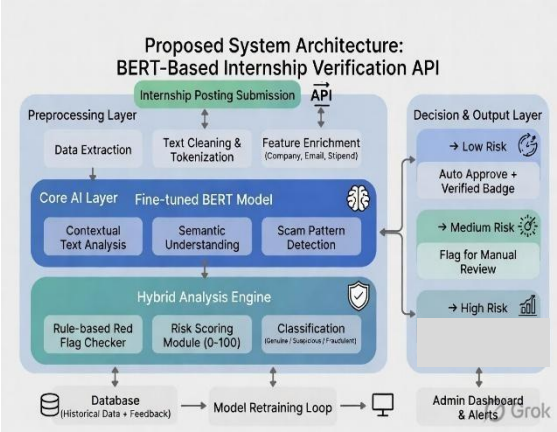
one type of data source, such as textual content or email verification. They do not combine multiple factors like company legitimacy, suspicious URLs, user feedback, recruiter history, and content analysis together. Due to this limitation, fraud detection accuracy becomes lower. Overall, the existing systems suffer from several disadvantages such as:

- Lack of intelligent fraud detection mechanisms.
- Dependence on manual verification and user complaints.
- Low accuracy in identifying advanced scams.
- Absence of real-time fraud alerts.
- Limited analysis of recruiter authenticity.
- Inability to integrate multiple fraud detection parameters.
- Reduced security and trust for students and job seekers.

## 5. Proposed System

The proposed system, "AI-Powered Internship Fraud Detection System," is designed to provide an intelligent, automated, and secure solution for identifying fraudulent internship postings and protecting users from online recruitment scams. The system uses Artificial Intelligence, Machine Learning, and Natural Language Processing techniques to analyze internship-related data and detect suspicious activities in real time. Unlike existing systems, the proposed framework combines multiple verification and analysis methods to improve fraud detection accuracy. The system examines various parameters such as recruiter authenticity, company details, email/domain verification, suspicious keywords, salary anomalies, phishing links, and user feedback to classify internship postings as Safe, Suspicious, or Fraudulent. The proposed system automatically analyzes internship descriptions using NLP techniques to identify scam-related content and misleading information. Machine Learning algorithms are trained using historical internship datasets to recognize fraud patterns and predict the legitimacy of new internship postings. The system also maintains recruiter activity history and complaint records for improving detection performance. An important feature of the proposed system is its real-time alert mechanism. Before applying for an internship, users receive fraud risk notifications and warnings if suspicious activities are detected. The framework also provides an admin monitoring module where administrators can review flagged postings, manage complaints, and improve system accuracy through continuous learning. The system is designed to be user-friendly, cost-effective, and easily deployable in online recruitment platforms, college placement systems, and internship portals. It helps students identify genuine opportunities while reducing the risk of fraud and cyber scams. The proposed system offers several advantages:

- Automated fraud detection using AI techniques
- Real-time scam alerts and risk analysis
- Improved detection accuracy through Machine Learning
- Integration of multiple verification parameters
- Enhanced security and trust for users
- Reduced dependency on manual verification
- Fast and efficient internship validation process
- User-friendly and scalable framework



## 6. Methodology

The proposed "AI-Powered Internship Fraud Detection System" follows a systematic methodology to identify and prevent fraudulent internship postings using Artificial Intelligence and Machine Learning techniques. The system consists of multiple stages including data collection, preprocessing, feature extraction, model training, fraud classification, and real-time alert generation. These stages work together to analyze internship postings and detect suspicious activities accurately. Data Collection: The system collects internship-related data from various sources such as internship portals, recruiter profiles, company information, email domains, user complaints, and internship descriptions. Data such as company name, recruiter email, salary details, internship duration, job description, website links, and user feedback are gathered for analysis.

Preprocessing: The collected data is cleaned and prepared before analysis. Duplicate entries, incomplete records, spam content, and irrelevant information are removed. Textual content from internship descriptions is normalized and tokenized using Natural Language Processing techniques. URLs and email domains are also standardized for verification purposes. Fraud Prediction and Alert Generation: After classification, the system generates fraud risk predictions for internship postings. If suspicious activity is detected, real-time alerts and warning notifications are provided to users before they apply for the internship. The system may also recommend safer alternatives or ask users to verify recruiter details.

Admin Monitoring and Feedback : An admin module is included to monitor flagged internship postings, manage user complaints, and review suspicious recruiters. User feedback and admin decisions are stored to improve future fraud detection performance.

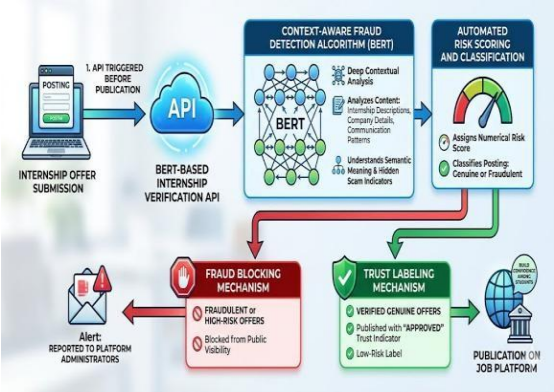
Overall, the proposed methodology provides an intelligent, automated, and efficient solution for identifying internship scams and protecting students from fraudulent recruitment activities.

## 7. Working Process

The working process of the "AI-Powered Internship Fraud Detection System" begins when internship postings and recruiter information are submitted to the system. The system automatically collects and analyzes the provided data to determine whether the internship opportunity is genuine or fraudulent. Initially, the internship details such as company name, recruiter email, job description, salary information, website links, and application details are captured by the system. The collected data is then cleaned and processed to remove duplicate, incomplete, or suspicious entries. After preprocessing, important fraud-related features are extracted from the internship posting. The system checks for suspicious keywords, fake email domains, phishing URLs, unrealistic salary packages, and unusual recruiter activities. Company verification and user complaint history are also analyzed to improve fraud detection accuracy. The extracted features are passed to a trained Machine Learning model that predicts the legitimacy of the internship posting. Based on the prediction, the system classifies the internship into categories such as:

- Safe
- Suspicious
- Fraudulent

If suspicious or fraudulent activities are detected, the system immediately generates warning notifications and fraud alerts for users. This helps students avoid applying for fake internships and protects them from scams. The system also includes an admin monitoring module where administrators can review flagged postings, manage complaints, and remove fraudulent recruiters from the platform. User feedback is continuously stored and used to improve the performance of the fraud detection model. Thus, the system provides a real-time, intelligent, and automated mechanism for ensuring secure internship opportunities and protecting users from online recruitment frauds.




## 8. Implementation

The implementation process of the "AI-Powered Internship Fraud Detection System" follows a structured approach that begins with collecting internship-related data and ends with deploying the fraud detection system into a web platform. Each phase plays an important role in identifying fraudulent internship postings accurately and efficiently.

Data Acquisition: The system gathers internship-related data from multiple sources such as internship portals, recruiter profiles, company websites, user complaints, and online recruitment platforms. Data including company name, recruiter email, internship description, salary details, URLs, and user feedback are collected for analysis.

Feature Extraction & Feature Selection: The collected data is cleaned and normalized before processing. Duplicate entries, incomplete records, spam content, and irrelevant information are removed. Textual data from internship descriptions is tokenized, normalized, and filtered to improve analysis accuracy. Email addresses and URLs are also standardized for verification.

Model Selection and Training: Machine Learning algorithms such as Decision Tree, Random Forest, Naïve Bayes, and Support Vector Machine (SVM) are selected for fraud detection. The system is trained using labeled internship datasets to learn patterns of genuine and fraudulent internship postings.

Model Validation: The trained model undergoes validation using evaluation metrics such as accuracy, precision, recall, and F1-score. This ensures that the model performs efficiently and provides reliable fraud detection results.

Fraud Prediction and Alert Generation: The validated model predicts whether an internship posting is Safe, Suspicious, or Fraudulent. Based on the prediction, the system generates warning notifications and fraud alerts for users in real time. This helps students avoid fake internship opportunities.

System Implementation: The complete system is deployed as a web-based application using frontend and backend technologies. Students and job seekers can access the system easily through browsers and verify internship authenticity before applying.

Overall, the implementation process provides an intelligent, automated, secure, and user-friendly solution for detecting internship fraud and improving trust in online recruitment platforms.

## 9. Tools and Technology

Various tools and technologies are used in the development of the "AI-Powered Internship Fraud Detection System" to ensure efficient processing, accurate fraud detection, and secure system performance. Python is used as the primary programming language because of its simplicity and strong support for Artificial Intelligence and Machine Learning applications. Frontend technologies such as HTML, CSS, and JavaScript are used to design an interactive and user-friendly interface for students and administrators. Backend development is carried out using frameworks like Flask or Django, which help manage server-side operations, APIs, authentication, and fraud analysis processes. For storing internship details, recruiter information, user reports, and fraud detection results, MySQL database is used. Machine Learning libraries such as Scikit-learn and TensorFlow are utilized for training and implementing fraud detection

algorithms like Decision Tree, Random Forest, Naïve Bayes, and Support Vector Machine (SVM). Natural Language Processing libraries including NLTK and TextBlob are used to analyze internship descriptions and identify suspicious keywords or scam-related content. Data preprocessing and manipulation are performed using Pandas and NumPy libraries. Development and testing processes are carried out using tools such as Jupyter Notebook and Visual Studio Code. In addition, REST APIs, Email Verification APIs, and domain validation services are integrated into the system to improve recruiter authentication and fraud detection accuracy. These technologies collectively help in building an intelligent, secure, scalable, and efficient internship fraud detection framework.

## 10. Challenges

The development of the "AI-Powered Internship Fraud Detection System" faces several challenges related to data accuracy, security, and fraud analysis. One of the major challenges is identifying continuously evolving scam techniques used by fraudulent recruiters. Scammers frequently change internship descriptions, websites, and communication methods to avoid detection, making fraud identification difficult. Another challenge is maintaining data accuracy because internship postings may contain incomplete, misleading, or fake information. The system also faces difficulties in analyzing complex textual content, such as hidden scam messages, ambiguous language, and phishing links. Data privacy and security are additional concerns since user information, recruiter details, and complaint records must be protected from unauthorized access and misuse. The availability of balanced and high-quality datasets for training Machine Learning models is another important challenge, as insufficient or biased data can reduce prediction accuracy. Real-time fraud detection and processing speed must also be maintained efficiently to provide instant alerts without affecting system performance. Furthermore, different internship platforms may follow different formats and standards, creating integration difficulties for the proposed system. Therefore, continuous system updates, model improvement, and advanced fraud analysis techniques are necessary to ensure reliable and accurate fraud detection.

## 11. Future Work

The future enhancement of the "AI-Powered Internship Fraud Detection System" can further improve fraud detection accuracy, security, and user experience. Advanced Deep Learning algorithms can be integrated into the system to identify complex scam patterns and improve prediction performance. Real-time monitoring and behavioral analysis techniques may also be added to detect suspicious recruiter activities more effectively. Integration with blockchain technology can enhance security and provide transparent verification of recruiter and company information. The system can be expanded into a mobile application to provide easier accessibility for students and job seekers. Multilingual support can also be implemented to allow users from different regions to access the system conveniently. Future versions of the framework may include AI-powered chatbots that guide users and provide instant fraud-related assistance. Social media analysis and web scraping technologies can be incorporated to identify scam activities across multiple online platforms. In addition, continuous learning mechanisms can be implemented so that the system automatically adapts to new fraud patterns over time. These future improvements will help create a more intelligent, secure, scalable, and efficient internship fraud prevention system.

## 12. Conclusion

In this project, the "AI-Powered Internship Fraud Detection System" provides an intelligent and effective solution for identifying and preventing fraudulent internship postings in online recruitment platforms. The system uses Artificial Intelligence, Machine Learning, and Natural Language Processing techniques to analyze internship details, recruiter authenticity, suspicious content, and user feedback in order to detect scam-related activities accurately. The proposed framework helps students and job seekers avoid fake internships, phishing attacks, and misleading recruitment offers by generating real-time fraud alerts and risk analysis. Compared to traditional systems, the proposed solution offers better automation, improved accuracy, faster processing, and enhanced security. The integration of multiple fraud detection parameters such as email verification, company validation, suspicious keyword analysis, and recruiter monitoring increases the reliability of the system. Overall, the project provides a secure, scalable, user-friendly, and cost-effective approach for improving trust and safety in online internship platforms. The system can be further enhanced with advanced AI technologies and integrated into modern recruitment systems to provide better protection against internship-related frauds.

## 13. Reference

**[1]** Sharma, R., et al., "Machine Learning Based Fraud Detection in Online Recruitment Systems," 2020.
**[2]** Rao, P., & Mehta, S., "Phishing Website Detection using Natural Language Processing Techniques," 2021.
**[3]** Kumar, A., et al., "Fake Job AdvertisemenDetection using Hybrid Machine Learning Models," 2022.
**[4]** Patel, D., & Singh, R., "AI-Based Recruitment Monitoring and Scam Detection System," 2023.