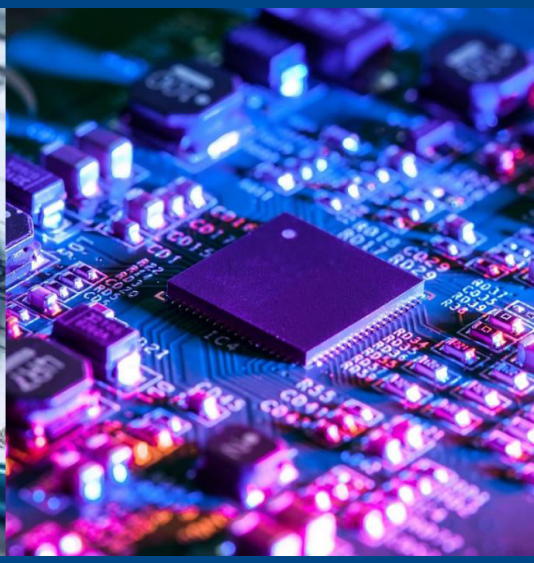
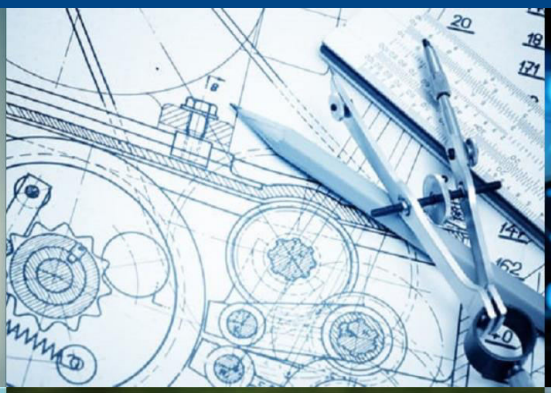
ISSN: 2582-7219

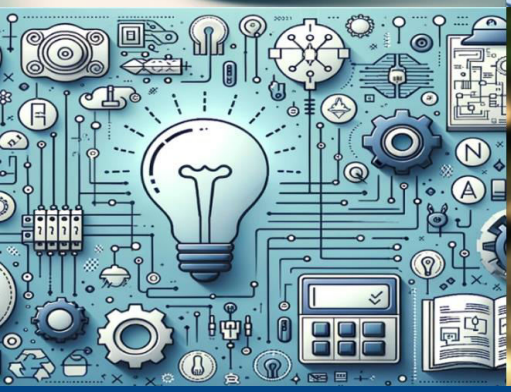




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 9, Issue 3, March 2026**

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI:10.15680/IJMRSET.2026.0903118

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Fake Job Detection Using Natural Language Processing, Logistic Regression & Naive Bayes

N.Hemala[1], Dr. N. Sumathi[2], N.Praneeta[3]

Department of Information Technology, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India [1,3]

Department of Information Technology, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: The rapid growth of online communication platforms such as email, social media, and messaging applications has created new opportunities for job seekers to find employment. However, this convenience has also led to an increase in fraudulent job messages and scams. Many individuals receive fake job offers that request personal information, registration fees, or other sensitive data, which can lead to financial loss and privacy risks. The Fake Job Message Detection System is a simulation-based web application developed to identify whether a job-related message is genuine or fraudulent. The system uses machine learning techniques and natural language processing methods to analyze the content of job messages and classify them as either real or fake.

The application allows users to manually enter or paste a job message into a web interface. The system processes the text using TF-IDF vectorization and applies a trained machine learning model to predict the authenticity of the message. The result is then displayed to the user along with a confidence score. This project demonstrates how machine learning can be applied to detect suspicious job-related messages and assist users in identifying potential scams. Although the system operates in a simulated environment and requires manual message input, it serves as a foundation for developing more advanced real-time detection systems in the future.

KEYWORDS: Fake Job Detection, Machine Learning, Natural Language Processing, TF-IDF Vectorization, Logistic Regression, Naive Bayes, Text Classification, Streamlit Web Application.

I. INTRODUCTION

1.1 AN OVERVIEW

The rapid growth of the internet and digital communication technologies has significantly transformed the way people search for jobs and how organizations recruit employees. Online job portals, email communication, social networking platforms, and professional networking sites have become the primary mediums for job advertisements and recruitment processes. These digital platforms provide convenience, speed, and accessibility for both employers and job seekers. As a result, millions of job opportunities are posted online every day. However, along with these advantages, the increasing use of online platforms has also led to the emergence of various cybercrimes. One of the most common cybercrimes related to employment is the spread of fake job postings and fraudulent job messages. Fraudsters and scammers often create fake job advertisements or send deceptive job offers to job seekers through emails, social media messages, and online job portals. These fake job messages often promise high salaries, flexible working hours, or work-from-home opportunities in order to attract victims.

Many job seekers, especially fresh graduates and unemployed individuals, may not have sufficient experience or knowledge to identify fraudulent job offers. As a result, they may unknowingly share their personal information such as bank account details, identity proof, or even pay registration fees or training charges to scammers. This leads to financial loss, identity theft, and emotional distress for victims. Fake job scams have become increasingly sophisticated in recent years. Fraudsters often design job messages that appear professional and convincing. They may use fake company names, fake websites, and fabricated job descriptions to mislead users. Sometimes, they impersonate well-known companies or recruiters to gain the trust of job seekers. Due to the realistic nature of these scams, it becomes difficult for individuals to manually verify the authenticity of job offers.

To address this issue, advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) can be used to detect fraudulent job messages automatically. Machine learning is a branch of artificial intelligence that allows

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

computers to learn patterns from data and make predictions without being explicitly programmed. In the context of fake job detection, machine learning models can be trained using datasets containing examples of real and fake job messages. Natural Language Processing (NLP), which is a subfield of artificial intelligence, plays an important role in analyzing textual data. NLP techniques enable computers to understand and process human language. By applying NLP techniques, textual job messages can be converted into numerical features that can be analyzed by machine learning algorithms. The proposed project titled "Fake Job Message Detection using Machine Learning" focuses on developing a system that can automatically analyze job-related messages and classify them as real or fake. The system uses machine learning algorithms to identify patterns commonly found in fraudulent job messages, such as suspicious keywords, unrealistic salary offers, urgent requests for payment, or lack of company details. In this project, the system first processes the job message entered by the user.

The message undergoes text preprocessing steps such as removing unnecessary characters, converting text to lowercase, and eliminating stop words. After preprocessing, the text is converted into numerical features using techniques such as Term Frequency–Inverse Document Frequency (TF-IDF). These features are then used as input for the machine learning model. The machine learning model analyzes the features and predicts whether the job message is legitimate or fraudulent. The system also provides a confidence score that indicates how confident the model is about its prediction. Additionally, an AI risk report is generated to warn users if the job message appears suspicious. The main goal of this project is to create a simple and effective tool that helps job seekers identify fake job messages before responding to them. By using machine learning techniques, the system can assist users in making informed decisions and reduce the risk of falling victim to job scams. This project also demonstrates the practical application of machine learning and natural language processing in solving real-world problems. The development of such systems can contribute to improving online security and protecting individuals from cyber fraud.

1.2 OBJECTIVES OF THE PROJECT

The main objective of this project is to develop a machine learning-based system that helps users identify fake job messages and avoid potential online scams. The system allows users to manually input job-related messages, analyzes the text using Natural Language Processing (NLP) and machine learning algorithms, and provides a prediction result along with a confidence score and risk warning.

The project aims to analyze job-related messages received through emails, social media platforms, or job portals, and classify them as real or fake. It applies NLP techniques to preprocess and clean textual data, ensuring that the machine learning model receives high-quality input. The system implements algorithms such as Logistic Regression and Naive Bayes to accurately classify messages and converts textual data into numerical features using TF-IDF vectorization for efficient analysis.

Furthermore, the system provides users with a prediction result along with a confidence score, indicating the reliability of the classification, and generates an AI-based risk warning highlighting suspicious patterns in potentially fraudulent messages. The project also focuses on developing a simple and user-friendly interface using Streamlit, enabling even non-technical users to interact with the system effortlessly. Ultimately, the system aims to raise awareness among job seekers about fake job scams, promoting safer online job search practices and helping users make informed decisions when responding to job offers.

II. LITERATURE REVIEW

Recent advancements in Artificial Intelligence (AI) and Machine Learning (ML) have significantly improved the ability of machines to analyze textual data for real-world applications. Machine learning techniques have shown remarkable performance in extracting complex patterns from text and have been widely used in spam detection, phishing detection, and fraud analysis [1]. Natural Language Processing (NLP) techniques enable machines to understand and process human language, making them suitable for analyzing messages for authenticity [2].

Supervised learning models such as Naive Bayes, Logistic Regression, and Support Vector Machines (SVM) have been widely adopted for text classification tasks due to their effectiveness and interpretability [3]. Research shows that these models can automatically learn patterns from labeled datasets of messages, distinguishing between legitimate and fraudulent content [4]. Early applications in email spam detection demonstrated that machine learning classifiers could achieve high accuracy in classifying textual messages, motivating their use in fake job message detection [5].

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Further improvements in text classification techniques led to the adoption of feature extraction methods such as Term Frequency–Inverse Document Frequency (TF-IDF) and word embeddings like Word2Vec and BERT. TF-IDF converts textual content into numerical vectors by evaluating the importance of words in a document relative to a corpus, enabling machine learning models to process textual patterns efficiently [6]. Pre-trained models such as BERT introduced deep contextual understanding of text, which allows the system to capture subtle patterns in fraudulent messages [7].

Traditional rule-based approaches for detecting fraudulent messages, such as keyword matching and blacklist verification, were widely used in earlier systems. However, these methods were limited by their inability to adapt to evolving scam patterns and sophisticated message structures [8]. Modern machine learning approaches overcome these limitations by learning from large datasets, making them capable of detecting unseen fraudulent patterns.

Recent studies have highlighted the importance of combining NLP techniques with practical implementation tools to build effective AI systems. Programming languages such as Python, along with libraries like Scikit-learn, Pandas, and Streamlit, allow developers to preprocess text, train models, and build interactive user interfaces for message verification [9]. These tools enable the creation of practical systems capable of real-time or manual message analysis, providing prediction results, confidence scores, and risk warnings.

Researchers have also explored hybrid approaches, integrating statistical models, machine learning algorithms, and NLP preprocessing techniques to improve the accuracy of fraud detection systems [10]. Such approaches are particularly useful in the detection of fake job messages, where scammers often use professional-looking layouts, company names, and persuasive language to deceive users.

The literature shows that combining machine learning algorithms with NLP preprocessing and feature extraction techniques can effectively classify textual messages and detect fraudulent patterns. This provides a solid foundation for the development of the proposed Fake Job Message Detection system, which allows users to manually input job messages, analyze them, and receive reliable prediction results with confidence scores and risk warnings.

DRAWBACKS

- The system relies primarily on manual verification of job messages, which is time-consuming and inefficient.
- Users must search company websites, emails, or social media pages, which is prone to human error.
- It cannot detect subtle patterns or sophisticated scams, making it ineffective against professional-looking fake messages.
- There is no quantitative measure of risk or confidence, leaving users uncertain about message authenticity.
- Manual verification methods lack scalability and cannot handle multiple messages automatically or in real-time.

III. PROPOSED METHODOLOGY

The proposed system introduces an Artificial Intelligence–based approach for detecting fake job messages through textual message analysis. Unlike traditional methods that rely on manual verification of job offers, this system allows users to manually input job messages and applies Machine Learning and Natural Language Processing (NLP) techniques to classify messages as Real or Fake. The system uses a trained classification model along with TF-IDF vectorization to extract meaningful features from text. Once the user submits a message, the model predicts the authenticity, calculates a confidence score, and generates a risk report highlighting suspicious patterns or phrases. This solution provides a fast, non-invasive, and user-friendly tool intended for awareness, educational purposes, and safer job application practices.

3.1 FEATURES

- **Manual Job Message Input:** Users can enter job messages from emails, WhatsApp, or job portals.
- **Machine Learning Prediction:** A trained classification model predicts whether a message is Real or Fake.
- **Confidence Score:** Displays how certain the model is about its prediction.
- **Risk Report:** Highlights suspicious words, phrases, and patterns within the message.
- **User-Friendly Interface:** Built with Streamlit for easy interaction without programming knowledge.

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI:10.15680/IJMRSET.2026.0903118

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

3.2. MODULE DESCRIPTION

- **USER INTERFACE MODULE :** This module provides a simple input box for users to enter job messages. It displays the prediction result, confidence score, and risk warning after analysis.
- **TEXT PREPROCESSING MODULE:** The system cleans the input message by converting text to lowercase, removing punctuation, special characters, and stopwords. This ensures consistent input for the machine learning model.
- **FEATURE EXTRACTION MODULE:** TF-IDF vectorization converts textual data into numerical feature vectors, representing the importance of words relative to the dataset. These features allow the model to detect patterns indicative of fraudulent messages.
- **MACHINE LEARNING CLASSIFICATION MODULE:** This core module loads the pretrained machine learning model (e.g., Logistic Regression or Naive Bayes) and analyzes the feature vectors. The model outputs the prediction (Real/Fake) and calculates a confidence score.
- **RESULTANALYSISMODULE:** The module interprets the model output, highlighting suspicious phrases and patterns in the message. It provides a risk warning to help users understand potential threats.
- **REPORT GENERATION MODULE:** Generates a clear text-based or HTML report that includes the prediction result, confidence score, and detected suspicious phrases. The report may also include recommendations to verify the message or avoid sharing personal information.
- **SYSTEM INTEGRATION MODULE:** Ensures smooth coordination between all modules, managing the workflow from message input to result display.

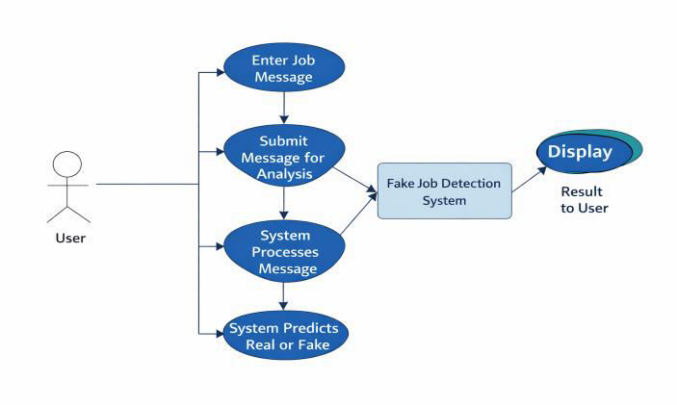


Figure 3.1 System Use case Diagram

IV. EXPERIMENTAL RESULTS

The experimental results demonstrate the effectiveness of the proposed machine learning–based system in detecting fake job messages. The system was tested using a dataset containing both genuine and fraudulent job messages. The dataset was divided into training and testing sets to evaluate the performance of the classification models. Machine learning algorithms such as **Naive Bayes and Logistic Regression** were applied to classify job-related messages based on textual patterns and keywords.

The evaluation of the models was performed using performance metrics such as **accuracy, precision, recall, and F1-score**. The results showed that the system could successfully identify suspicious job messages containing keywords like "registration fee," "earn money quickly," "urgent hiring," and "work from home." The system was also tested through the **Streamlit interface**, where users entered job messages and received prediction results with a confidence score and warning message. Overall, the results indicate that the system provides quick and reliable detection of fake job messages.

© 2026 IJMRSET | Volume 9, Issue 3, March 2026| DOI:10.15680/IJMRSET.2026.0903118

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

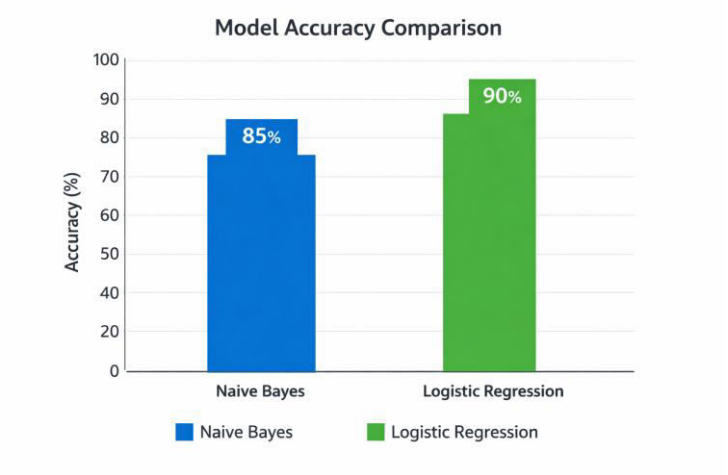


Figure 4.1: Model Accuracy

V. CONCLUSION

The Fake Job Message Detection System successfully demonstrates how machine learning and Natural Language Processing (NLP) can be applied to detect fraudulent job messages. The project provides a user-friendly interface where users can manually input job-related messages, which are then analyzed and classified as Real or Fake. The system also provides a confidence score and a risk warning, allowing users to make informed decisions and avoid potential scams.

Through the use of TF-IDF vectorization for feature extraction and machine learning algorithms such as Naive Bayes and Logistic Regression, the system is able to identify subtle patterns and suspicious keywords that are common in fake job messages. This provides a reliable and automated alternative to manual verification methods, which are often time-consuming and prone to errors.

The implementation of the project demonstrates that AI-based solutions can enhance the safety and efficiency of job-seeking activities, especially in the current digital environment where fraudulent messages are increasingly sophisticated. While the system is currently simulation-based and requires manual message input, it lays the foundation for future enhancements, such as real-time message monitoring and integration with email or social media platforms.

In conclusion, the project provides a practical, effective, and scalable approach to detecting fake job messages, raising awareness among job seekers, and promoting safer online job application practices. It proves that intelligent systems can assist users in navigating the online job market more safely and confidently.

VI. FUTURE SCOPE

The proposed Fake Job Message Detection System can be further enhanced in several ways to improve its functionality and real-world applicability. In the future, the system can be integrated directly with email services, social media platforms, and job portals so that suspicious job messages can be detected automatically without requiring manual input from the user. Advanced deep learning techniques such as Recurrent Neural Networks (RNN) or Transformer-based models can also be implemented to improve the accuracy and capability of the system in understanding complex textual patterns. Additionally, the system can be expanded to support multiple languages, enabling users from different regions to identify fraudulent job offers more effectively. Another possible enhancement is the development of a mobile application or browser extension, which can provide real-time alerts when users encounter potentially fraudulent job advertisements online. By incorporating these improvements, the system can evolve into a more powerful tool that helps protect job seekers from online recruitment scams and promotes safer digital job searching practices.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

REFERENCES

[1] Tom M. Mitchell, Machine Learning, McGraw-Hill Education, New York, 1997.
[2] Christopher M. Bishop, Pattern Recognition and Machine Learning, Springer, New York, 2006.
[3] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, Deep Learning, MIT Press, 2016.
[4] Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach, 4th Edition, Pearson Education, 2020.
[5] C. D. Manning, P. Raghavan, and H. Schütze, Introduction to Information Retrieval, Cambridge University Press, 2008.
[6] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," Proceedings of NAACL-HLT, 2019.
[7] Pedregosa F., Varoquaux G., Gramfort A., et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, Vol. 12, pp. 2825–2830, 2011.
[8] Steven Bird, Ewan Klein, and Edward Loper, Natural Language Processing with Python, O'Reilly Media, 2009.
[9] Aurélien Géron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, O'Reilly Media, 2019.
[10] OpenAI, "Language Models are Few-Shot Learners," Advances in Neural Information Processing Systems, 2020.
[11] Scikit-learn Documentation. Available: https://scikit-learn.org

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com