Project Proposal
Detecting Job Scam Emails Using Machine Learning

Sreenidhi Hayagreevan
Masters in Data Analytics, San Jose State University
DATA245 - Machine Learning
Vishnu S. Pendyala
March 7, 2025

Project Proposal: Detecting Job Scam Emails Using Machine Learning

Abstract

In the present digital age, since the end of the 20th century, people have increasingly applied for jobs via the internet rather than using the traditional job application methods like walk-in interviews and newspaper advertisements. This has provided fraudsters with a wonderful platform for identifying vulnerable job seekers and scamming them. This is a recurring problem, raising social, economic, and technological sustainability issues, as in most cases scams cause loss of money, identity theft, and emotional distress. Traditional filters in email are not able to identify these kinds of scams as they are designed to look real. The main aim of this project is developing an ML model for accurately identifying and categorizing job scam emails. With the help of Natural Language Processing (NLP) and advanced ML algorithms, the project will create a tool to help users prevent themselves from becoming victims of these scams.

Motivation for the Project

The motivation for doing this project comes from my own experience as a victim of a high-tech job scam. I received an invitation to a Social Media Manager remote position at PLOS, a known institution, by email from a recruiter. After researching the company online, I proceeded and conducted a text-based interview with Microsoft Teams. When I questioned the lack of a video interview, I was told it was more convenient for the hiring team.

I was offered the position one day later and handed an official offer letter with the seals and signatures of the company. The salary package was attractive, and I was thrilled. Red flags materialized, though, when I was instructed to purchase my own gadgets using a cashier's check they will provide. Suspicious as ever, I did some digging and discovered the job post was fake. The address on the offer letter was an actual Taco Bell store in San Francisco, and the fraudsters had created a fake website and forged documents.

But, by the time I realized it was a scam, I had already provided my ID and paperwork showing eligibility to work in the United States. While I managed to avoid monetary loss by not cashing in the cashier's check, my identity was stolen. Further online research educated me that my ID could be used to open lines of credit, get mortgages, or loans in my name. There was a significant emotional toll, and I had to incur preventive costs such as freezing my credit card and purchasing an Identity Theft Protection plan.

This experience encouraged me to create a machine learning system to detect job scam emails. By using technology to combat fraud, this project aims to protect millions of other job seekers from these scams, establish trust in online labor markets, and contribute to social, economic, and technological sustainability.

Literature Survey

1. **Naive Bayes for Spam Detection**
    - Rahman et al. (2023) achieved **97.666% accuracy** in spam detection using **Naive Bayes** with preprocessing (tokenization, stop word removal) and **Correlation-Based Feature Selection (CFS)**.
    - **Relevance**: Supports using Naive Bayes as a baseline model for job scam email detection.
2. **Hybrid Space Analysis for Employment Scams**
    - Gong et al. (2025) used **NLP and ML** to analyze job scams, finding that **inconsistent geographic information** and **spatial heterogeneity** are key indicators of fake job postings.
    - **Relevance**: Highlights the importance of combining text-based features with metadata for accurate scam detection.
3. **Machine Learning for Fake Job Identification**
    - Swapna (2023) achieved **99% accuracy** in fake job detection using **Random Forest**, emphasizing the importance of **feature extraction** and **stratified cross-validation**.
    - **Relevance**: Validates the use of ensemble methods like Random Forest for job scam detection.

Gap: Existing research lacks focus on **job scam emails** as a distinct category, which this project addresses.

Methodology

Experiment Design:

1. **Data Collection:**
    - Public datasets of job scam emails (e.g., Enron dataset, BBB scam tracker, Reddit scam reports, Kaggle)
    - Scraping online job scam complaints from peers (using google forms)
    - Synthetic data generation for balancing the dataset (using AI)
2. **Feature Engineering:**
    - **Text Features:** Job descriptions, urgency words, grammatical errors, salary expectations, etc.
    - **Metadata Features:** Sender domain reputation, email headers, time of sending.
    - **Link Analysis:** Presence of suspicious URLs, domain age, URL shortening services.
3. **Machine Learning Models:**
    - Naïve Bayes, Random Forest, and Support Vector Machines (SVM)
    - Neural networks (if feasible, lightweight MLP models)
    - Explainable AI (SHAP/LIME) for interpretability
    - TinyML for batch processing of email archives

4. **Evaluation Metrics:**
    - Accuracy, Precision, Recall, and F1-score
    - ROC-AUC for binary classification performance
    - False Positive Rate to avoid flagging genuine job offers

Deliverables and Milestones

- **Week 1:** Data collection and preprocessing
- **Week 2:** Feature engineering and exploratory data analysis (EDA)
- **Week 3:** Model training and initial evaluation
- **Week 4:** Model optimization and explainability integration
- **Week 5:** Final model deployment and documentation
- **Final Submission:** Report including findings, analysis, and future scope

Relevance to Course and Technical Difficulty

This project applies machine learning classification techniques and finds veracity of the job related email, aligns with NLP methodologies, and integrates social sustainability concerns. It involves handling real-world datasets, ensuring data preprocessing, feature engineering, and evaluating model performance on unseen scam patterns.

Team Roles and Responsibilities

1. **Data Collection & Preprocessing** (Done by Laxmi Thrishitha Kalvakota - 017605640**)**
    - Collect job postings from online sources and clean the data. Perform text preprocessing (tokenization, stopword removal) and feature engineering (TF-IDF, Word Embeddings).
2. **EDA & Feature Selection** (Done by Janani Kripa Manoharan - 016721159)
    - Conduct EDA to identify scam patterns and select key features. Use PCA or feature selection methods to reduce dimensionality.
3. **Model Training & Optimization** (Done by Shivani Atul Beri - 018205018)
    - Train and optimize ML models (Logistic Regression, SVM, Random Forest). Evaluate performance and convert the best model to TinyML format (TFLite, ONNX).
4. **Model Deployment & Evaluation** (Done by Sreenidhi Hayagreevan - 018195489)
    - Deploy the model in a web/cloud-based API for large-scale scam detection. Optimize the model using tools like Flask/FastAPI, Scikit-learn, TensorFlow/Keras, and Edge Impulse.

Novelty and Impact

Existing email filtering techniques often fail to detect **job-specific scams** due to their professional structure. This project will help enhance traditional spam detection by integrating domain-specific features and metadata-based classification. Additionally this project has the potential to contribute to:

- **Ethical AI development** in fraud detection.
- **Real-world applications**, such as a browser extension or API for job seekers.
- **Academic contribution**, with potential for research publication.

Heilmeier Catechism Questions

1. **What are we trying to do?**
    - Develop a ML model to detect job scam emails.
2. **How is it done today, and what are the limitations?**
    - Traditional spam filters lack domain-specific job scam detection capabilities.
3. **What's new in our approach?**
    - Combining **text analysis, metadata evaluation, and explainable AI** to improve scam detection.
4. **Who cares?**
    - Job seekers, HR professionals, students, cybersecurity experts, and job platforms.
5. **What are the risks?**
    - False positives affecting legitimate job offers.
6. **How will we measure success?**
    - Model performance metrics (F1-score, precision-recall balance) and usability evaluations.

Conclusion

This project presents a **novel and practical** approach to tackling online job scams using machine learning. It balances **technical feasibility, social impact, and sustainability**, contributing to online job safety and fraud prevention.

Mandatory Question:

I have used Generative AI (ChatGPT) only to help with my response for sentence reorganization, grammar correction, and synonym recommendations to increase readability and to generate alternative phrasing while preserving the essential concept.

References:

K, S. (2023, July 1). *A machine learning approaches for fake job identification*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4703728

A Comparative Study on Fake Job Post Prediction Using Different Data mining Techniques. (2021, January 5). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9331230

Gong, W., Lee, C. S., Li, S., Adkison, D., Li, N., Wu, L., & Ye, X. (2025). Cyber victimization in hybrid space: an analysis of employment scams using natural language processing and machine learning models. *Journal of Crime and Justice*, 1–22. https://doi.org/10.1080/0735648x.2024.2448804

Rahman, M. F., 19101514, Enam, M., 19101179, Shahreyar, S., 19101510, & Mithylin, V., 19101242. (2023). Enhancing email management and filtering through naive Bayes based spam detection : a proposed email application solution. In Brac University, *Department of Computer Science and Engineering* [Thesis]. https://dspace.bracu.ac.bd/xmlui/handle/10361/21921