FAKE JOB POSTING DETECTION

Aluoch Phanela

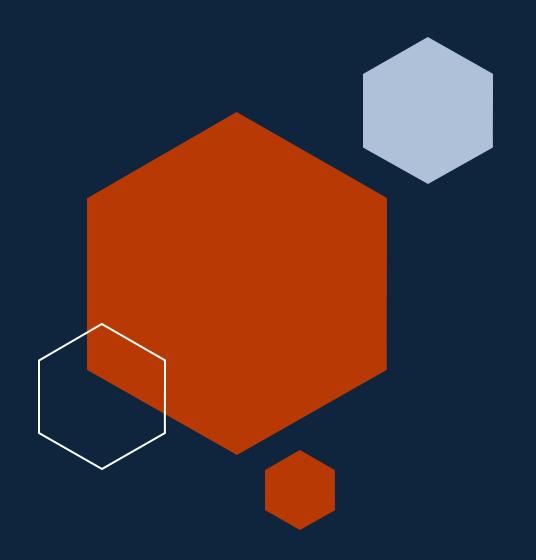


Business Background

Fake job postings waste job seekers' time, damage trust in platforms, and are increasingly sophisticated.

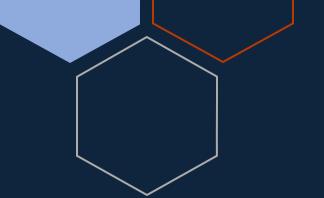
They often:

- Collect sensitive data through deception
- Impose fake fees
- Mimic legitimate postings convincingly Using machine learning, we aim to detect and flag fraudulent listings automatically.



Business Understanding

- Can we predict fake job postings using job content?
- Which features strongly indicate fraud?
- How accurate is our prediction model?
- How can it support moderation workflows?





Engineer features that expose hidden fraud signals

- Train and test models to predict job fraud
- Identify the best performing algorithm
- Recommend automation support for moderators
- e on emerging market preferences.

We Hit Our Goals

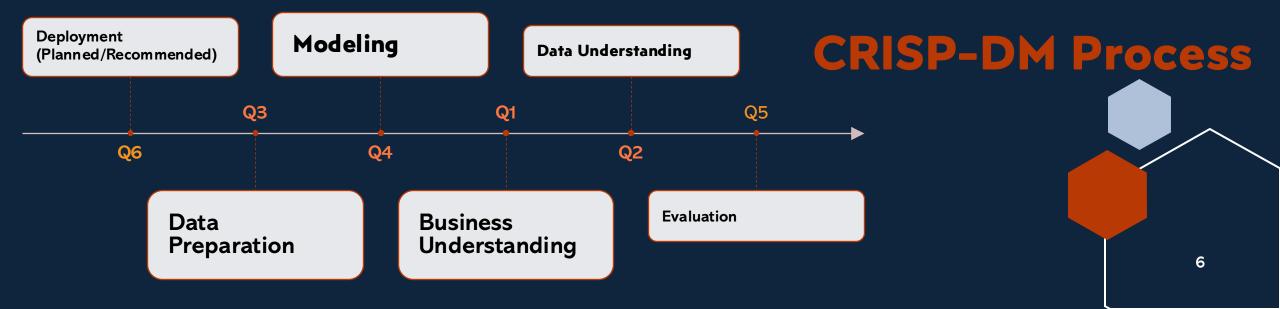
We used the "Fake Job Postings" dataset from Kaggle.

It includes job attributes like title, description, location, employment type, and a binary fraudulent label.

Data Overview



- Fake job postings hurt job seekers and platforms. Goal: Build a model to identify fake postings.
- Loaded dataset from Kaggle. Inspected columns like title, description, location, etc. Target: fraudulent.
- Cleaned missing data, engineered features like word count & presence of suspicious keywords, encoded categorical variables.
- Used Random Forest + SMOTE to handle class imbalance. Tuned hyperparameters and evaluated with precision, recall, ROC AUC.
- Final model achieved good precision and recall on fraudulent class. ROC AUC ~0.95.
- Model & notebook ready. Can be integrated into moderation workflows or automated systems.



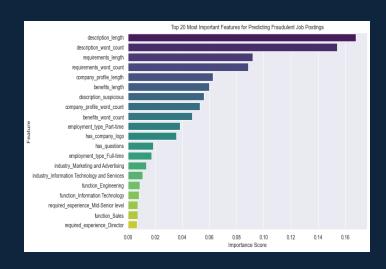
EDA The three strongest predictors

Correlation Heatmap of Numerical Features											
job_id	1.00	-0.03	-0.04	-0.14	0.10	0.01	-0.03	0.02	0.01		
telecommuting	-0.03	1.00	-0.00	0.06	-0.00	0.00	0.05	-0.03	0.02		- 0.8
has_company_logo	-0.04		1.00	0.26	-0.24	-0.09	0.10	0.43	0.15		- 0.6
has_questions	-0.14	0.06	0.26	1.00	-0.10	-0.07	0.01	0.03	0.06		0.0
fraudulent	0.10		-0.24	-0.10	1.00	-0.03	-0.06	-0.14	0.01		- 0.4
description_length	0.01	0.00	-0.09	-0.07	-0.03	1.00	0.06	0.09	0.07		- 0.2
requirements_length	-0.03		0.10	0.01	-0.06	0.06	1.00	0.22	0.21		
company_profile_length	0.02		0.43	0.03	-0.14	0.09	0.22	1.00	0.21		- 0.0
benefits_length	0.01		0.15	0.06	0.01	0.07	0.21	0.21	1.00		0.2
	pi_doį	telecommuting	has_company_logo	has_questions	fraudulent	description_length	requirements_length	ompany_profile_length	benefits_length		

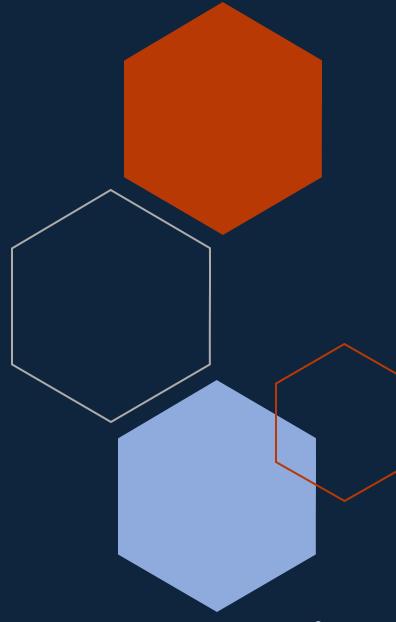
- The heatmap shows how strongly pairs of features are related (values range from -1 to 1).
- High positive values (close to 1) indicate a strong direct relationship.
- High negative values (close to -1) indicate a strong inverse relationship.
- Values near 0 suggest no linear correlation.



Features that are most predictive of fraudulent listings

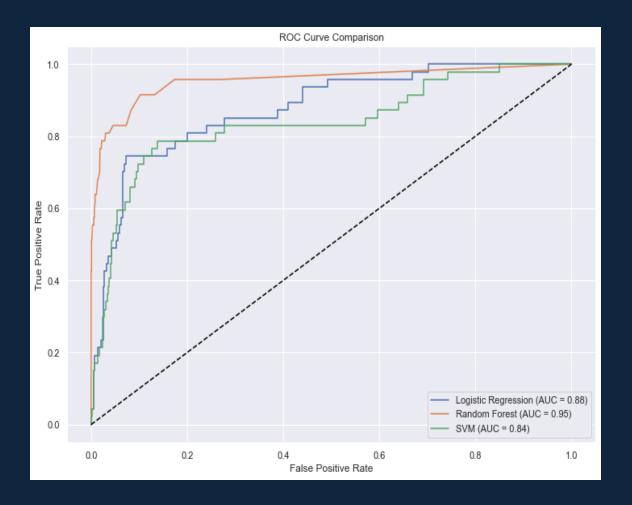


The initial Random Forest model identified several features as highly predictive of fraudulent job postings



Model that detects fake job postings without misclassifying

 The ROC curves showed that both models performed better than random guessing (AUC > 0.5), but Random Forest achieved a curve that hugged closer to the top-left corner, suggesting stronger predictive power.





- Fake job postings can be predicted with high accuracy using machine learning.
- Feature importance reveals significant text-based and location-based indicators.



Recommendation

- Deploy model into job posting platforms
- Use predictions to flag suspicious listings in real time
- Continuously retrain with fresh data to catch evolving scams

Future initiatives

- Deploy model into moderation pipeline.
- 2. Perform real-time scoring.
- 3. Improve text preprocessing for future iterations.

