AT&T DESP Internship
June 4th, 2025

Fake News Project

By Aaron Luu and Jacob Truong

Project roadmap

Microservices

Web scraper for articles, obtain credibility from website, ML model

ML Model

Binary classification with NLP, deployment on Databricks

API Security

JWTs, logging, error handling, rate limiting, and proxy routes

Demo

Interactive UI, API calls, ML prediction, and analysis

Retrospective

Challenges, hurdles, lessons learned

Project Overview

Problem: The spread of misinformation.

- **Fake News breaks down public trust, democracy, and social cohesion.**

- **Important to develop scalable and intelligent tools to distinguish credible sources from deceptive articles.**

Project Overview

Solution: The Fake News Detection App.

- ML Model trained on hundreds of thousands of datasets, extracting features like title and text.
- Uses NLP and classification pipelines to accurately predict the credibility of an article.
- Simple UI for users to input URLs of articles to determine its legitimacy.

Meet the team

Jacob Truong

CI/CD, Frontend, Machine Learning, and API Development

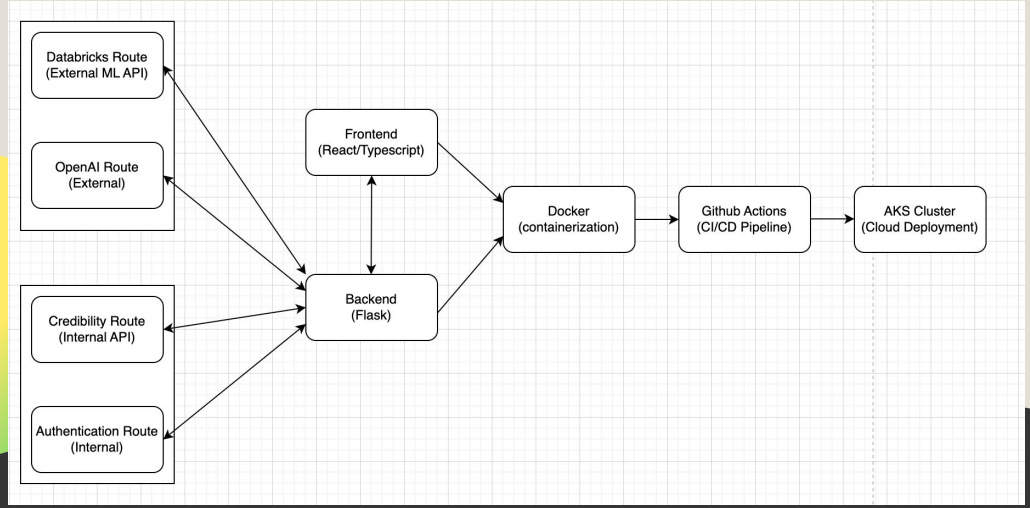
Configured CI/CD to allow automatic deployment on AKS, created home page and analysis page elements, developed binary classification model, implemented endpoints to call web scraper and ml model

Aaron Luu

Deployment, Data Pipeline, API Security, Data Visualization, GenAI

Configured Docker Images to deploy on AKS, Inserted and visualized data on Databricks, implemented JWT, rate limiting, logs of errors, and GenAI use to summarize and assist in analysis of articles.

Microservices And Architecture



Technologies:

- **Frontend**: TypeScript + React
- **Backend**: Flask (Python)
- **Authentication**: JWT Auth (Flask-JWT-Extended)
- **ML Model**: Databricks (Spark ML / PySpark)
- **Article Analysis**: OpenAI GPT via Flask route
- **Containerization**: Docker
- **CI/CD**: GitHub Actions
- **Deployment**: Azure Kubernetes Service (AKS)

Endpoints:

- Docker images built from frontend and backend
- Github actions trigger CI/CD workflow
- Images deployed to AKS
- AKS serves frontend/backend
- Frontend calls backend APIs

ML Model and Results

What was Used?

TFIDF:

- Lightweight
- Extracts key term frequencies

FastText:

- Captures semantic meaning and word relationships

Logistic Regression:

- Provides linear decision boundaries

Random Forest:

- Handles non linear patterns and reduces overfitting

Deployment and API Interaction

Model is deployed on a serving endpoint with rate limiting on databricks. Returns a prediction and confidence score given text.

Limitations

- No GPU
- Memory limitations

```
Test Set Metrics:
F1 Score (weighted): 0.8008
Precision (weighted): 0.8039
Accuracy: 0.8013
Recall (weighted): 0.8013
AUC (OvR): 0.9068

Classification Report:
              precision    recall  f1-score   support

           0       0.78      0.85      0.81      9943
           1       0.83      0.75      0.79      9864

    accuracy                           0.80     19807
   macro avg       0.80      0.80      0.80     19807
weighted avg       0.80      0.80      0.80     19807
```

Security and Monitoring

Protecting endpoints:

Rate limiting / Retries

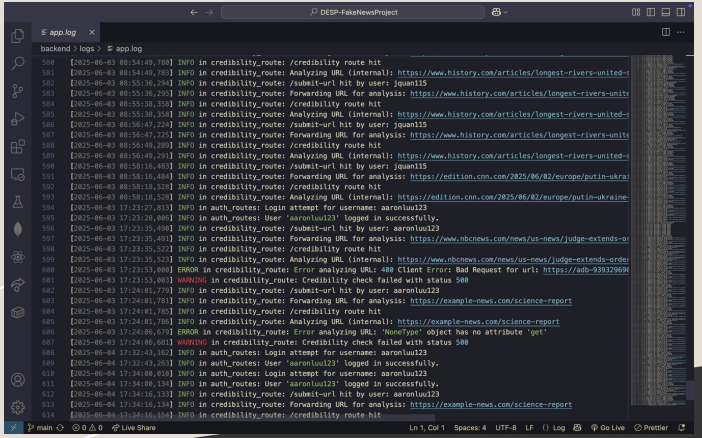
Introduced Flask Limiter to allow up to 100 API calls per min, Also included Tenacity and retries in case of unforeseen errors (network crashes, rate limiting, timeout)

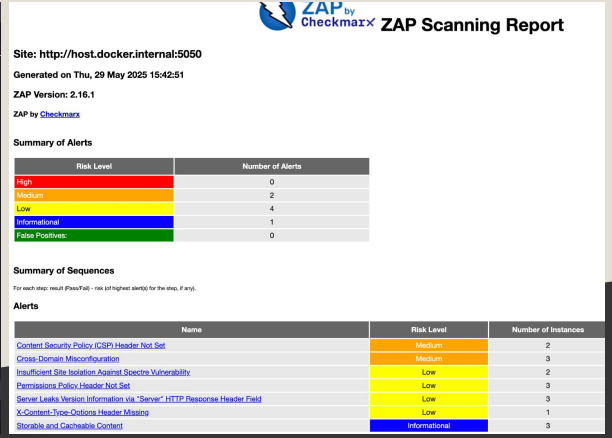
Error Logging

Included helpful error messages to debug code and troubleshoot problems during API calls. Includes a file App.log to keep track of all logs.

JWTs

Users create an account with an associated token, every API call is verified with that token.





ZAP by Checkmarx ZAP Scanning Report

Site: http://host.docker.internal:5050

Generated on Thu, 29 May 2025 15:42:51

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

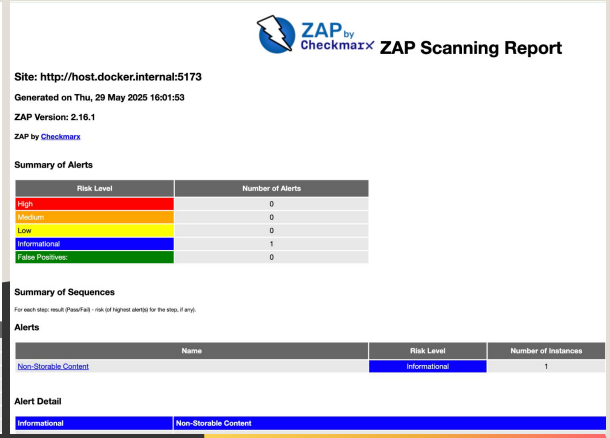
Risk Level	Number of Alerts
High	0
Medium	2
Low	4
Informational	1
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	2
Cross-Domain Misconfiguration	Medium	3
Insufficient Site Isolation Against Spectre Vulnerability	Low	2
Permissions Policy Header Not Set	Low	3
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	3
X-Content-Type-Options Header Missing	Low	1
Storable and Cacheable Content	Informational	3



ZAP by Checkmarx ZAP Scanning Report

Site: http://host.docker.internal:5173

Generated on Thu, 29 May 2025 16:01:53

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	0
Informational	1
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

Name	Risk Level	Number of Instances
Non-Storable Content	Informational	1

Alert Detail

Informational	Non-Storable Content

GenAI Usage

What was Used?

ChatGPT-4o / Github Copilot:

- Article summarization
- Credibility analysis assistance
- Code Generation:
  - Data cleanup
- Machine Learning Research/Guidance

Canva AI

- UI design and starting point

Usefulness

- Accelerated UI development with reusable templates
- Helped debug backend and deployment issues

Limitations

- Struggled with large codebases or context-heavy debugging
- Sometimes produced overly generic or incorrect suggestions
- Required manual validation of outputs (Postman)

Demo!!

Retrospective

Challenge 1

Limited funding restricted our ability to train large models like BERT or Roberta, which required more compute resources than we could afford.

Challenge 2

CPU-only training was slow and inefficient. We lacked access to GPUs and had issues with insufficient and messy data.

Lessons Learned

Lesson 1

Always test code thoroughly before pushing to avoid unnecessary AKS costs.

Lesson 2

Ask questions early—waiting until the last minute adds stress and risk.

Lesson 3

Use logging and error tracking consistently to debug issues faster, especially in production (Postman to test API calls!)

Thank you everyone, and Thank you to AT&T for making this program possible!

Any questions?
Ask away!

AT&T