REMLA–Team 7

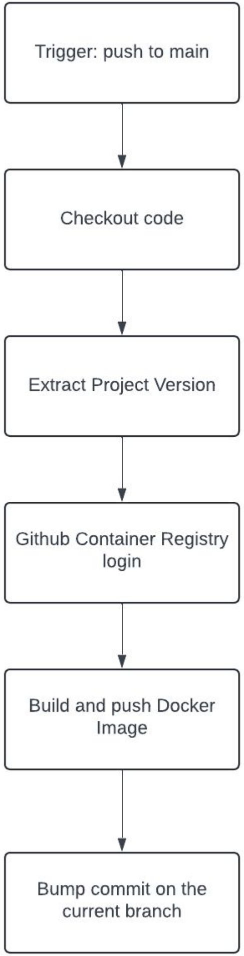
Melle Koper, Alex Ivanov, Arjun Vilakathara, Kevin Tran

Content

- Release pipeline
- Deployment
- Extension proposal
- Additional use case
- Experimental setup
- ML Pipeline and testing

Release Pipeline

- Poetry for *dependency* and *version* management
- Versioned GitHub releases
- Versioned images (GHCR-hosted)



Trigger: push to main

Checkout code

Extract Project Version

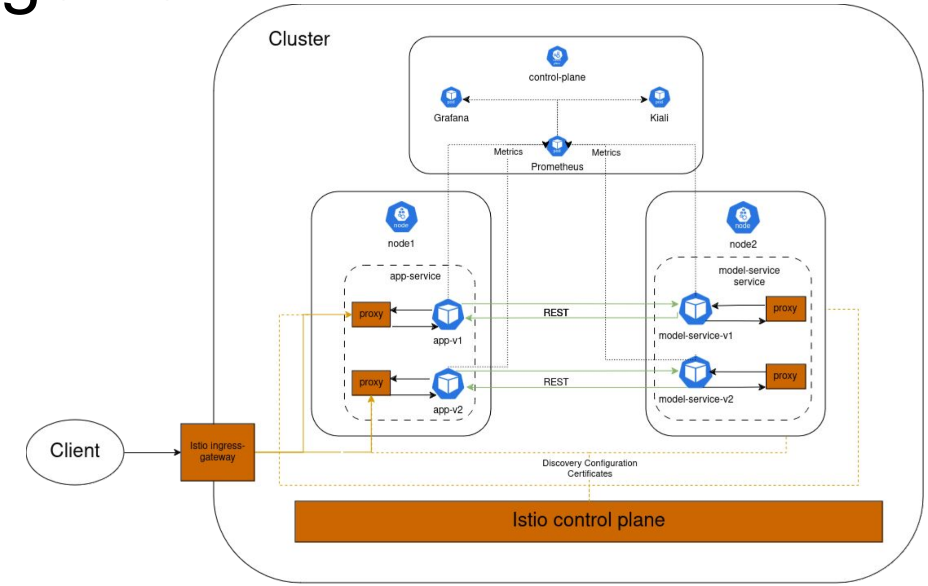
Github Container Registry login

Build and push Docker Image

Bump commit on the current branch

Deployment

- Multi-node cluster
- Traffic Management

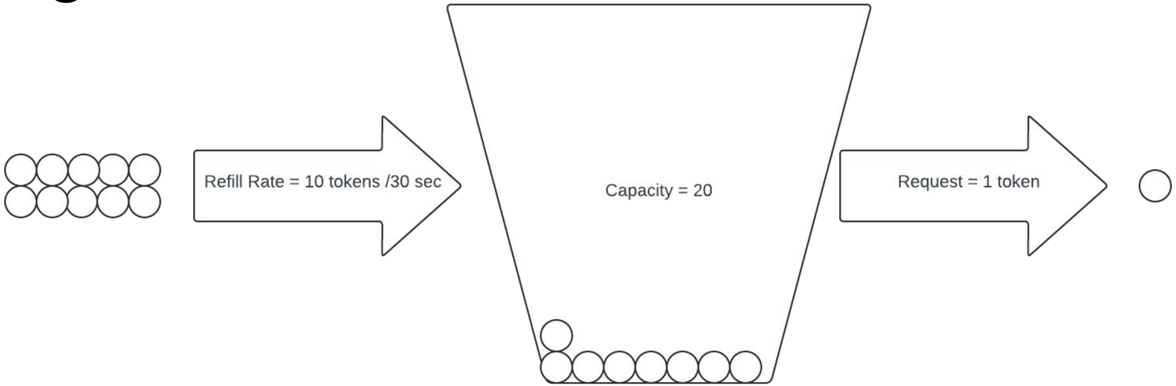


Extension Proposal

- Kubernetes Deployment with Helm
- Remove manual steps
- Installed multiple times into the same cluster.
- Condense multiple yaml files into one cluster.
- Secret management

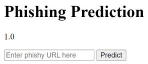
Additional Use Case

- Local Rate Limiting
- Implemented through an EnvoyFilter
- Only allow 20 requests per 30 sec from single client.



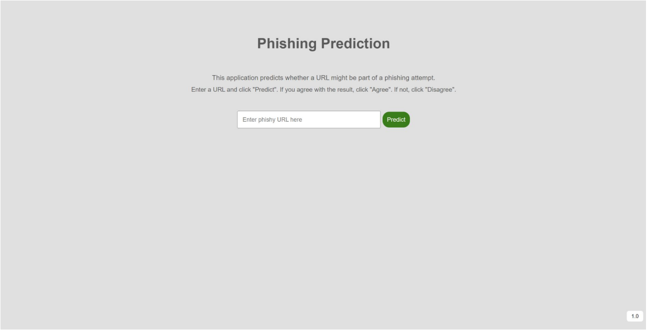
Experimental Setup

- Control: Core functionality, no styling
- Test: User instructions + styling
- Metrics:
  - View Counter
  - Requests counter
  - Agree/Disagree Counters



Phishing Prediction

1.0



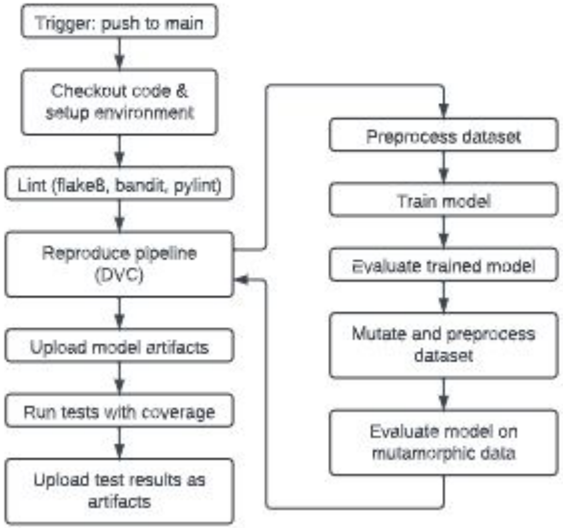
Phishing Prediction

This application predicts whether a URL might be part of a phishing attempt.

Enter a URL and click "Predict". If you agree with the result, click "Agree". If not, click "Disagree".

ML Pipeline and Testing

- Automated testing based on ML Test score guidelines
- Code Quality:
  - Flake8
  - Bandit
  - pylint



Trigger: push to main

Checkout code & setup environment

Lint (flake8, bandit, pylint)

Reproduce pipeline (DVC)

Upload model artifacts

Run tests with coverage

Upload test results as artifacts

Preprocess dataset

Train model

Evaluate trained model

Mutate and preprocess dataset

Evaluate model on mutamorphic data

Q&A