URL Phishing detection

REMLA - Team 5

28th of June, 2024

Saga Sunnevudóttir, Tim den Blanken,
Jurriaan Buitenweg, Rado Todorov

TU Delft

Introduction

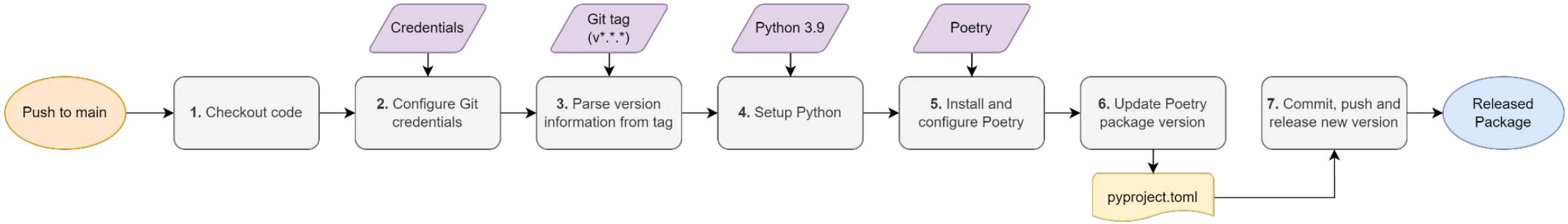
- Machine learning model for phishing detection
- Focus on infrastructure

Contents

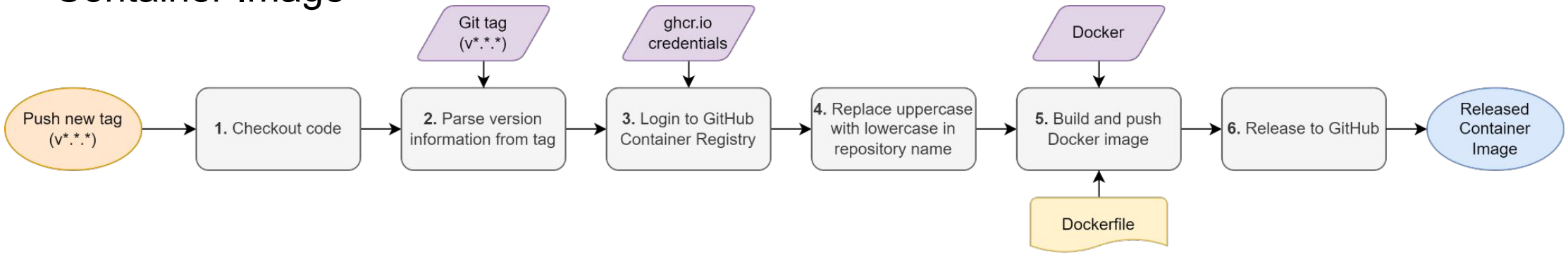
- Release Pipelines
- Deployment
- Auto-scaling Extension
- Shadow Launch and Canary Release
- ML Pipeline
- ML Testing

Release Pipeline

- Software Package



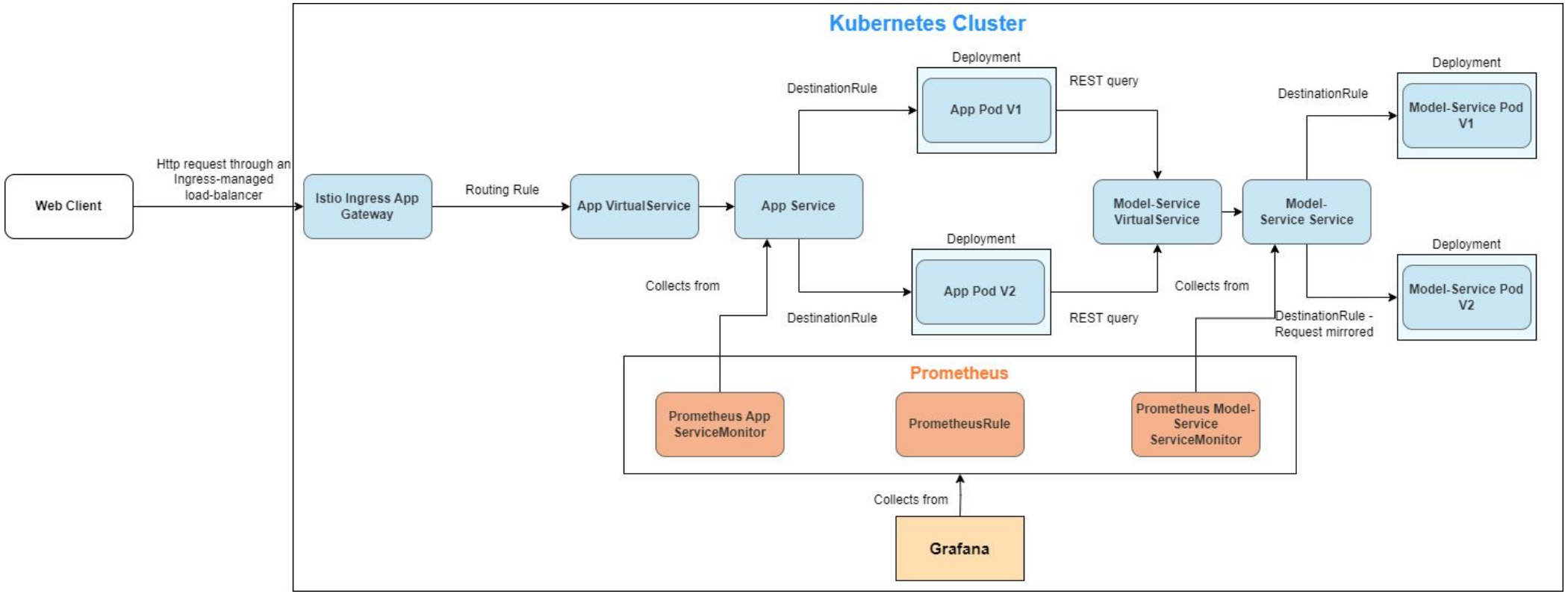
- Container Image



TU Delft

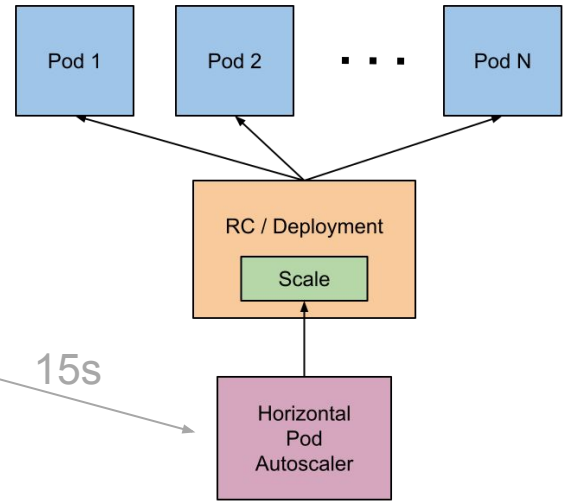
Deployment

- Provisioning and configuration with Vagrant and Ansible
- Kubernetes cluster deployed with K3s using Deployments, Services and ConfigMaps etc.
- Istio for traffic management and experimentation using VirtualServices, Gateways and DestinationRules
- Monitoring with Prometheus and Grafana using custom metrics and dashboards

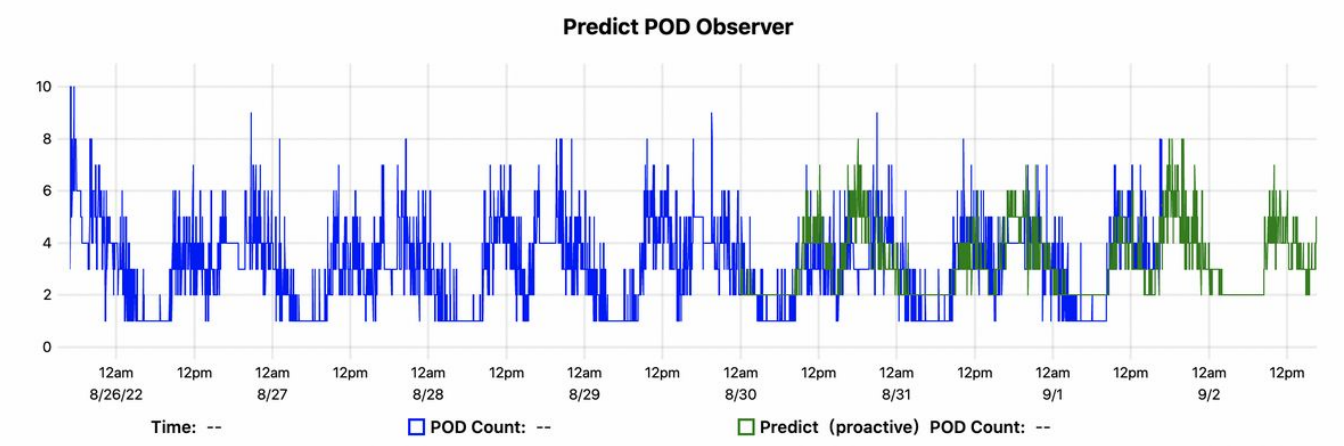


Auto-scaling extension

$$\text{desiredReplicas} = \left\lceil \text{currentReplicas} \times \left(\frac{\text{currentMetricValue}}{\text{desiredMetricValue}} \right) \right\rceil$$



Horizontal Pod Autoscaler [1]



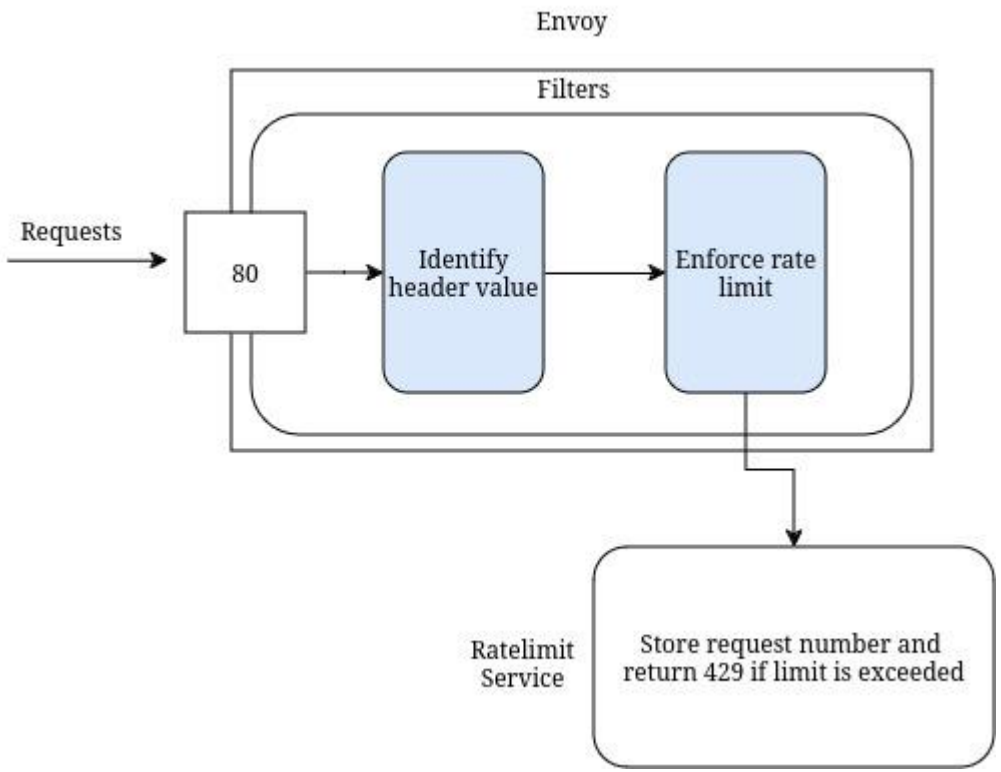
AHPA [2] predictive pod solution

Cron [3] scheduled scaling

TU Delft

Additional Use Case - Rate Limiting

- Using Istio Envoy filters to restrict user requests
- The gateway has a global limit and user-based limit

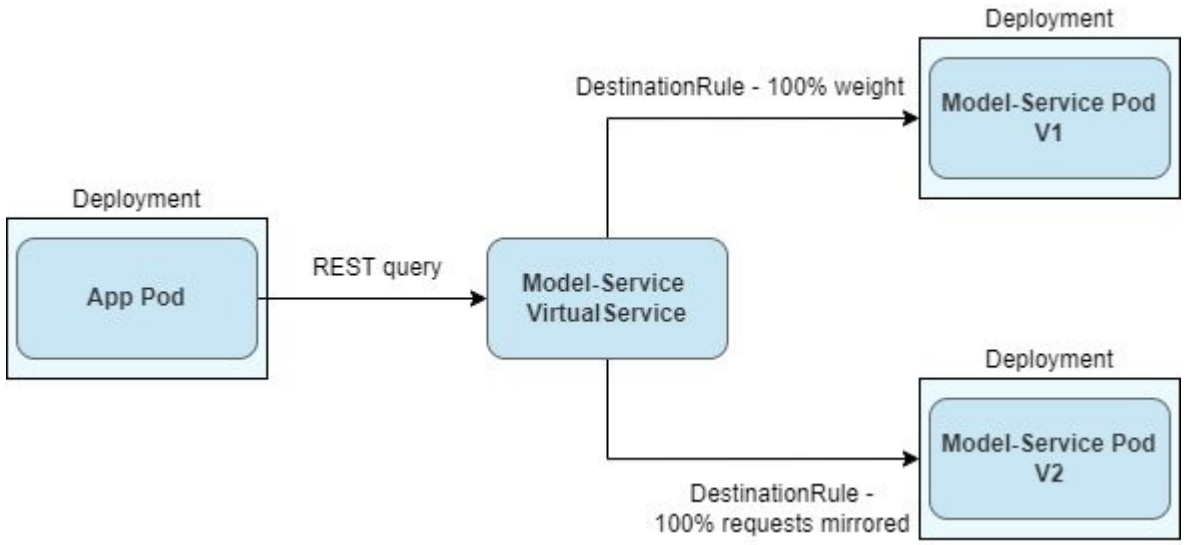



```
vagrant@controller:~$ for i in $(seq 1 12); do curl -H "Authorization: Bob"
-s -o /dev/null -w "%{http_code}\n" http://192.168.56.10:80/; done
200
200
200
200
200
200
200
200
200
200
429
429
vagrant@controller:~$ for i in $(seq 1 12); do curl -H "Authorization: Nick"
 -s -o /dev/null -w "%{http_code}\n" http://192.168.56.10:80/; done
200
200
200
200
200
200
200
200
200
200
200
429
429
```

TU Delft

Additional Use Case - Shadow Launching

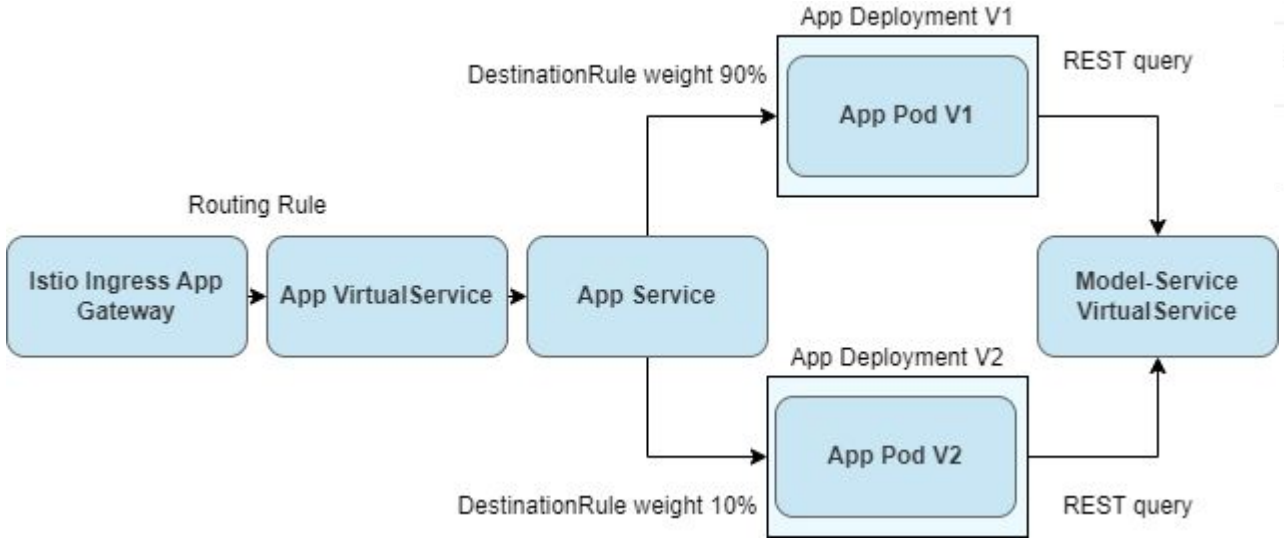
- Using Istio traffic mirroring capabilities
- Test a new version of the model (model-service) by shadow-launching it
- All requests mirrored to new model without user being affected
- Prometheus and Grafana to evaluate new version

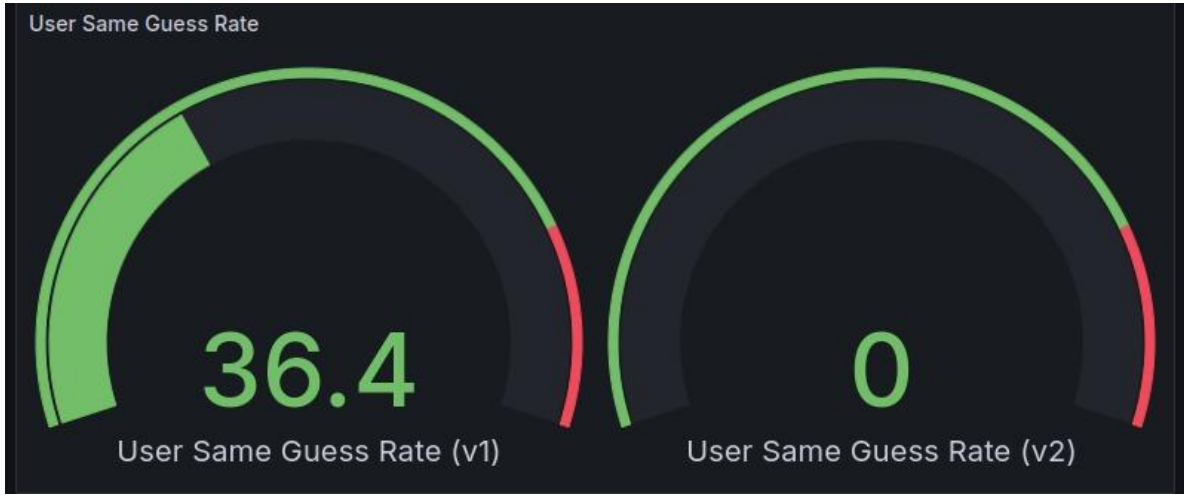


TU Delft

Experimental Setup - Canary Release

- Using Istio advanced traffic management capabilities
- Test new app deployment to a fraction of the users
- 10% of requests are directed to new app version
- New version fixes a usability problem improving clarity - red button for phishing and green for innocent
  - May result in closer user alignment with the assessment of the model
- Prometheus and Grafana to evaluate new version

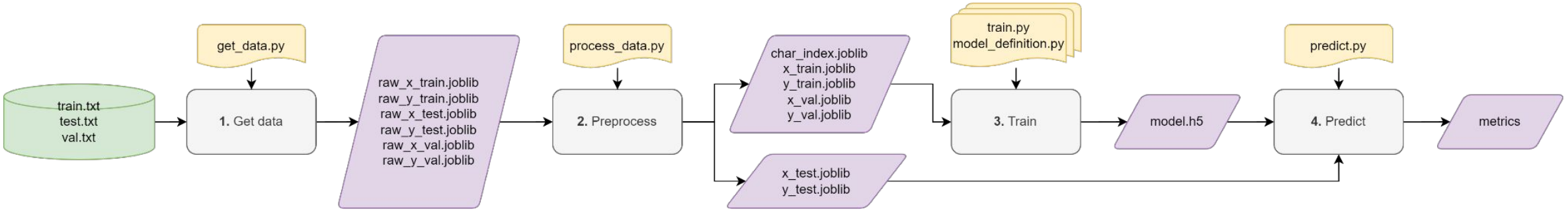




TU Delft

ML Pipeline

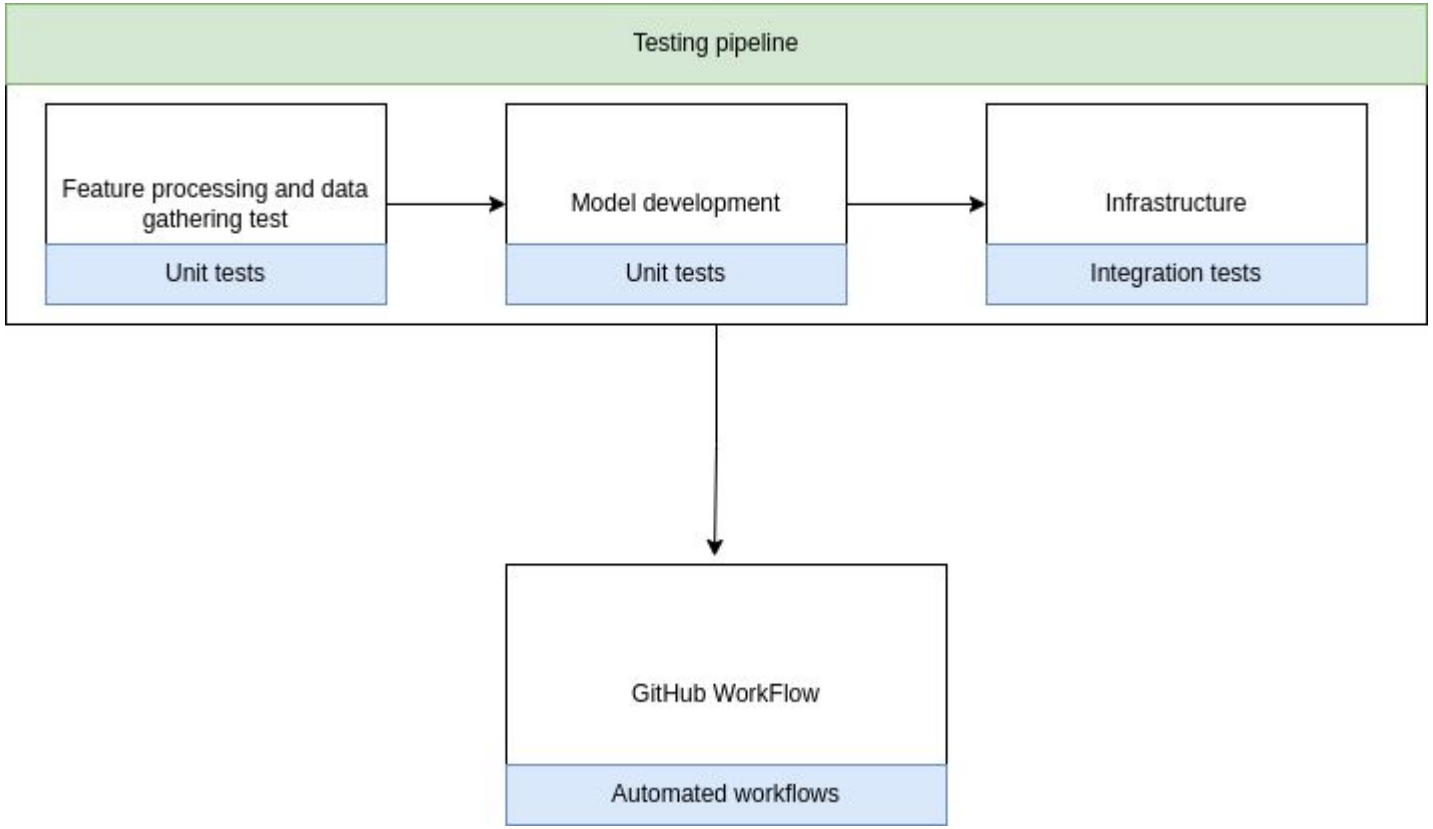
- Project structure
- Package/dependency management with Poetry
- Data Version Control (DVC)



TU Delft

ML Testing

- Feature processing & Data gathering
  - File existence checks
  - Data slicing
- Model development
  - Non determinism
  - Robustness
  - Accuracy checks
  - Mutamorphic testing
- Infrastructure
- Monitoring
  - Size checks
  - Staleness (Model outdated checks)
- Workflow
- Fixtures for pytest
  - Setup
  - Tear down
- Difficulties



TU Delft

Thank you for Listening!

Questions?

References

[1] - Kubernetes Horizontal Pod Autoscaling

[2] - Alibaba Cloud Documentation

[3] - Cron

TU Delft