apiVersion: eksctl.io/v1alpha5

kind: ClusterConfig

metadata:

  name: loan-eks-simple

  region: ap-south-1

nodeGroups:

  - name: gpu-nodes-v3

    instanceType: g4dn.xlarge

    desiredCapacity: 1

    minSize: 0

    maxSize: 1

    labels:

      workload: llm-inference

    subnets:

      - subnet-0c66df451bbe17c55

      - subnet-00823415a1ff5d785

      - subnet-0d90a0e84bb1aa792

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM> python src/train\_balanced\_models.py

Starting balanced model training...

Connected to MLflow: http://a2fd03b8d3cad4e4caa91c9d87b876ec-1422723236.ap-south-1.elb.amazonaws.com:5000

Found 1 experiments

2025/08/28 11:39:49 INFO mlflow.tracking.fluent: Experiment with name 'loan-default-balanced' does not exist. Creating a new experiment.

Dataset: 10,000 samples

Default rate: 54.5%

Training samples: 8,000

Test samples: 2,000

Training default rate: 54.5%

Training RandomForest with class balancing...

Optimizing prediction threshold...

Model Performance:

Optimal Threshold: 0.320

F1 Score: 0.771

Precision: 0.664

Recall: 0.918

Confusion Matrix:

True Negatives (correct approvals): 402

False Positives (wrong rejections): 507

False Negatives (missed defaults): 89

True Positives (caught defaults): 1002

2025/08/28 11:39:51 WARNING mlflow.models.model: `artifact\_path` is deprecated. Please use `name` instead.

2025/08/28 11:39:58 WARNING mlflow.models.model: Model logged without a signature and input example. Please set `input\_example` parameter when logging the model to auto infer the model signature.

🏃 View run balanced-training-20250828-113949 at: http://a2fd03b8d3cad4e4caa91c9d87b876ec-1422723236.ap-south-1.elb.amazonaws.com:5000/#/experiments/1/runs/69028ed6d2454dd1b92f421aa89cd250

🧪 View experiment at: http://a2fd03b8d3cad4e4caa91c9d87b876ec-1422723236.ap-south-1.elb.amazonaws.com:5000/#/experiments/1

Results logged to MLflow successfully

VALIDATION PASSED: F1 score 0.771 >= 0.3

Model can identify defaults and is ready for deployment

Training SUCCESS

Try accessing MLflow UI:

http://a2fd03b8d3cad4e4caa91c9d87b876ec-1422723236.ap-south-1.elb.amazonaws.com:5000

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM>

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM> pytest tests/test\_model\_training.py -v

=========================================== test session starts ============================================

platform win32 -- Python 3.10.0, pytest-8.4.1, pluggy-1.6.0 -- C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\Scripts\python.exe

cachedir: .pytest\_cache

rootdir: C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM

plugins: anyio-4.10.0

collected 2 items

tests/test\_model\_training.py::test\_dataset\_quality PASSED [ 50%]

tests/test\_model\_training.py::test\_model\_performance PASSED [100%]

============================================= warnings summary =============================================

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:151: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py::test\_model\_performance

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:262: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py: 10 warnings

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:618: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py::test\_model\_performance

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:813: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:1039: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(LogOutputs(run\_id=run\_id, models=[m.to\_proto() for m in models]))

tests/test\_model\_training.py: 11 warnings

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\utils\proto\_json\_utils.py:74: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

[ftype(v) for v in value]

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:771: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:233: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

-- Docs: https://docs.pytest.org/en/stable/how-to/capture-warnings.html

===================================== 2 passed, 29 warnings in 11.50s ======================================

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM>

# Test a loan prediction

@"

{

"credit\_score": 720,

"annual\_income": 75000,

"loan\_amount": 25000,

"employment\_years": 5

}

"@ | Out-File -FilePath test\_loan.json -Encoding utf8

# Make a prediction request

curl -X POST -H "Content-Type: application/json" -d "@test\_loan.json" http://abfa55c72a34c485b903ffacaa4f9164-38175384.ap-south-1.elb.amazonaws.com:8080/predict

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM> Invoke-RestMethod -Uri "http://abfa55c72a34c485b903ffacaa4f9164-38175384.ap-south-1.elb.amazonaws.com:8080/predict" -Method Post -ContentType "application/json" -Body (Get-Content test\_loan.json -Raw)

model\_info : @{f1\_score=0.31085043988269795; run\_id=cb28ae14c90c44b3b4619df5a47713d0}

prediction : approve

probability : 0.13385285011430206

risk\_score : 13.385285011430206

threshold\_used : 0.44000000000000006

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM>

**Current Architecture:**

* EKS cluster with model serving endpoints
* S3 storage for artifacts and data
* MLflow experiment tracking with external access
* Balanced RandomForest with proper class handling
* REST API providing real-time predictions
* Automated testing validating model quality

The model correctly assessed the test loan (720 credit score, stable income) as low-risk with a 13% probability of default. This demonstrates the class imbalance fix worked - the model now makes meaningful distinctions rather than blanket approvals.

Your infrastructure can now handle the full ML lifecycle from training to serving, with proper validation gates preventing deployment of poorly performing models like the original 0.0028 F1 score model.

Using open-source vulnerability database

Found and scanned 126 packages

Timestamp 2025-08-28 14:58:55

10 vulnerabilities reported

0 vulnerabilities ignored

+===========================================================================================================+

VULNERABILITIES REPORTED

+===========================================================================================================+

-> Vulnerability found in pip version 21.2.3

Vulnerability ID: 75180

Affected spec: <25.0

ADVISORY: Pip solves a security vulnerability that previously allowed maliciously crafted wheel

files to execute unauthorized code during installation.

PVE-2025-75180

For more information about this vulnerability, visit https://data.safetycli.com/v/75180/97c

To ignore this vulnerability, use PyUp vulnerability id 75180 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

-> Vulnerability found in pip version 21.2.3

Vulnerability ID: 62044

Affected spec: <23.3

ADVISORY: Affected versions of Pip are vulnerable to Command Injection. When installing a

package from a Mercurial VCS URL (ie "pip install hg+...") with pip prior to v23.3, the specified...

CVE-2023-5752

For more information about this vulnerability, visit https://data.safetycli.com/v/62044/97c

To ignore this vulnerability, use PyUp vulnerability id 62044 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

-> Vulnerability found in mlflow version 3.3.2

Vulnerability ID: 71584

Affected spec: >=1.23.0

ADVISORY: Deserialization of untrusted data can occur in versions of the MLflow platform

affected versions, enabling a maliciously uploaded LightGBM scikit-learn model to run arbitrary code...

CVE-2024-37056

For more information about this vulnerability, visit https://data.safetycli.com/v/71584/97c

To ignore this vulnerability, use PyUp vulnerability id 71584 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

-> Vulnerability found in mlflow version 3.3.2

Vulnerability ID: 71587

Affected spec: >=0.9.0

ADVISORY: Deserialization of untrusted data can occur in affected versions of the MLflow

platform, enabling a maliciously uploaded PyFunc model to run arbitrary code on an end user’s system...

CVE-2024-37054

For more information about this vulnerability, visit https://data.safetycli.com/v/71587/97c

To ignore this vulnerability, use PyUp vulnerability id 71587 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

-> Vulnerability found in mlflow version 3.3.2

Vulnerability ID: 71691

Affected spec: >=0.5.0

ADVISORY: Deserialization of untrusted data can occur in affected versions of the MLflow

platform running, enabling a maliciously uploaded PyTorch model to run arbitrary code on an end...

CVE-2024-37059

For more information about this vulnerability, visit https://data.safetycli.com/v/71691/97c

To ignore this vulnerability, use PyUp vulnerability id 71691 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

-> Vulnerability found in mlflow version 3.3.2

Vulnerability ID: 71693

Affected spec: >=1.24.0

ADVISORY: Deserialization of untrusted data can occur in affected versions of the MLflow

platform, enabling a maliciously uploaded pmdarima model to run arbitrary code on an end user’s...

CVE-2024-37055

For more information about this vulnerability, visit https://data.safetycli.com/v/71693/97c

To ignore this vulnerability, use PyUp vulnerability id 71693 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

-> Vulnerability found in mlflow version 3.3.2

Vulnerability ID: 71579

Affected spec: >=1.27.0

ADVISORY: Deserialization of untrusted data can occur in versions of the MLflow platform

running version 1.27.0 or newer, enabling a maliciously crafted Recipe to execute arbitrary code on...

CVE-2024-37060

For more information about this vulnerability, visit https://data.safetycli.com/v/71579/97c

To ignore this vulnerability, use PyUp vulnerability id 71579 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

-> Vulnerability found in mlflow version 3.3.2

Vulnerability ID: 71692

Affected spec: >=2.0.0rc0

ADVISORY: Deserialization of untrusted data can occur in affected versions of the MLflow

platform, enabling a maliciously uploaded Tensorflow model to run arbitrary code on an end user’s...

CVE-2024-37057

For more information about this vulnerability, visit https://data.safetycli.com/v/71692/97c

To ignore this vulnerability, use PyUp vulnerability id 71692 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

-> Vulnerability found in mlflow version 3.3.2

Vulnerability ID: 71577

Affected spec: >=1.1.0

ADVISORY: Deserialization of untrusted data can occur in versions of the MLflow platform

running version 1.1.0 or newer, enabling a maliciously uploaded scikit-learn model to run arbitrary...

CVE-2024-37052

For more information about this vulnerability, visit https://data.safetycli.com/v/71577/97c

To ignore this vulnerability, use PyUp vulnerability id 71577 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

-> Vulnerability found in mlflow version 3.3.2

Vulnerability ID: 71578

Affected spec: >=1.1.0

ADVISORY: Deserialization of untrusted data can occur in versions of the MLflow platform

running version 1.1.0 or newer, enabling a maliciously uploaded scikit-learn model to run arbitrary...

CVE-2024-37053

For more information about this vulnerability, visit https://data.safetycli.com/v/71578/97c

To ignore this vulnerability, use PyUp vulnerability id 71578 in safety’s ignore command-line argument

or add the ignore to your safety policy file.

+===========================================================================================================+

REMEDIATIONS

10 vulnerabilities were reported in 2 packages. For detailed remediation & fix recommendations, upgrade

to a commercial license.

+===========================================================================================================+

Scan was completed. 10 vulnerabilities were reported.

+===========================================================================================================+

+===========================================================================================================================================================================================+

DEPRECATED: this command (`check`) has been DEPRECATED, and will be unsupported beyond 01 June 2024.

We highly encourage switching to the new `scan` command which is easier to use, more powerful, and can be set up to mimic the deprecated command if required.

+===========================================================================================================================================================================================+

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM> pytest tests/ -v --cov=src --cov-report=html

=========================================== test session starts ============================================

platform win32 -- Python 3.10.0, pytest-8.4.1, pluggy-1.6.0 -- C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\Scripts\python.exe

cachedir: .pytest\_cache

rootdir: C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM

plugins: anyio-4.10.0, cov-6.2.1

collected 2 items

tests/test\_model\_training.py::test\_dataset\_quality PASSED [ 50%]

tests/test\_model\_training.py::test\_model\_performance PASSED [100%]

============================================= warnings summary =============================================

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:151: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py::test\_model\_performance

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:262: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py: 10 warnings

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:618: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py::test\_model\_performance

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:813: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:1039: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(LogOutputs(run\_id=run\_id, models=[m.to\_proto() for m in models]))

tests/test\_model\_training.py: 11 warnings

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\utils\proto\_json\_utils.py:74: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

[ftype(v) for v in value]

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:771: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

tests/test\_model\_training.py::test\_model\_performance

C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM\venv\lib\site-packages\mlflow\store\tracking\rest\_store.py:233: DeprecationWarning: label() is deprecated. Use is\_required() or is\_repeated() instead.

req\_body = message\_to\_json(

-- Docs: https://docs.pytest.org/en/stable/how-to/capture-warnings.html

============================================== tests coverage ==============================================

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ coverage: platform win32, python 3.10.0-final-0 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Coverage HTML written to dir htmlcov

===================================== 2 passed, 29 warnings in 12.55s ======================================

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM>

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM> bandit -r src/

[main] INFO profile include tests: None

[main] INFO profile exclude tests: None

[main] INFO cli include tests: None

[main] INFO cli exclude tests: None

[main] INFO running on Python 3.10.0

Run started:2025-08-28 09:42:19.464323

Test results:

No issues identified.

Code scanned:

Total lines of code: 135

Total lines skipped (#nosec): 0

Run metrics:

Total issues (by severity):

Undefined: 0

Low: 0

Medium: 0

High: 0

Total issues (by confidence):

Undefined: 0

Low: 0

Medium: 0

High: 0

Files skipped (0):

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM>

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM> safety scan

Safety 3.6.0 scanning C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM

2025-08-28 09:51:53 UTC

Account: jayesh.tulip@gmail.com

Environment: development

Scan policy: None, using Safety CLI default policies

Python detected. Found 1 Python requirement file, 1 Python environment and 1 Python pyproject.toml file

✅ requirements.txt: No issues found.

✅ venv\pyvenv.cfg: No issues found.

✅ venv\Lib\site-packages\pandas\pyproject.toml: No issues found.

Tested 173 dependencies for security issues using default Safety CLI policies

100 vulnerabilities found, 100 ignored due to policy.

0 fixes suggested, resolving 0 vulnerabilities.

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM>

venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM> pip-audit

No known vulnerabilities found

(venv) PS C:\Users\jayes\OneDrive\Desktop\jathakam\ai\LLM> pip show mlflow pip

Name: mlflow

Version: 3.3.2

Summary: MLflow is an open source platform for the complete machine learning lifecycle

Home-page: https://mlflow.org