Milestone 7: API Authentication with Header Key

# Objective

To protect the prediction API from unauthorized access by adding an API key authentication layer using FastAPI's dependency injection system.

# Implementation

- Created a `.env` file to store the API key securely.

- Loaded `.env` using `python-dotenv` in `config.py`.

- Added a `verify\_api\_key` dependency in `api/v1/dependencies/auth.py`.

- Required the header `x-api-key` in `/v1/predict/predict` POST requests.

- Secured access with a `401 Unauthorized` response for missing/invalid keys.

# Security Practice

- `.env` file is excluded from version control via `.gitignore`.

- In Docker, API key is injected via `--env-file` for runtime safety.

# Test Command

curl -X POST http://localhost:8000/v1/predict/predict \  
 -H "Content-Type: application/json" \  
 -H "x-api-key: secret123" \  
 -d '{ "pm25\_lag\_1": 8.5, "pm25\_lag\_2": 8.2, "pm25\_lag\_3": 9.0,  
 "year": 2024, "month": 6, "sin\_month": 0.5, "cos\_month": 0.87 }'

# Conclusion

API key authentication was successfully implemented using FastAPI dependencies. This layer ensures that only authorized clients can access the model, which is critical for any production-level service.