AI-Enhanced Retail Cybersecurity Threat Detection System

Team Members
Arjit Jain - AI22BTECH11002
Saketh C - AI22BTECH11005
Umanshiva - AI22BTECH11016
Mayank- AI22BTECH11018

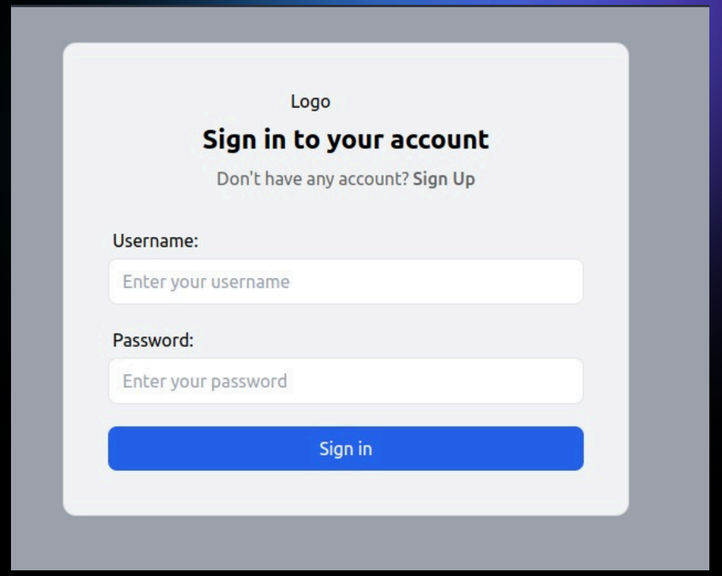
The AI-Enhanced Retail Cybersecurity Threat Detection System is an innovative solution designed to address the growing cybersecurity challenges faced by retail environments, particularly Point-of-Sale (POS) systems and their associated network infrastructures.

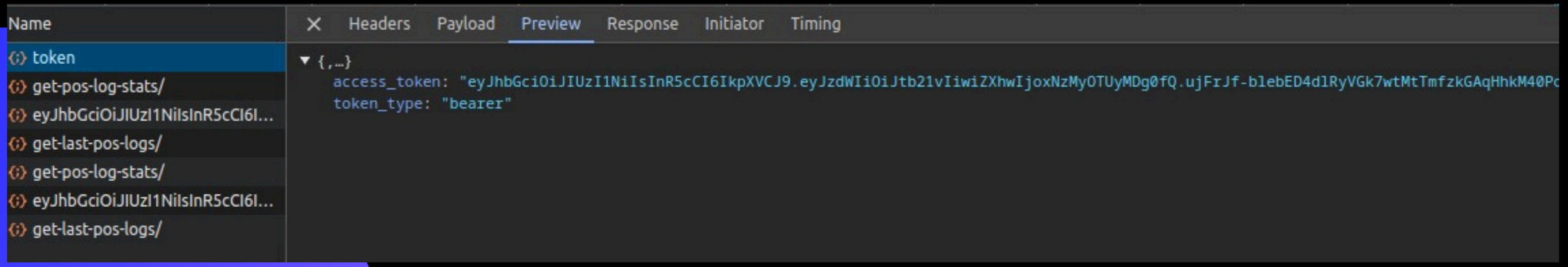
API Docs


FastAPI
0.1.0
OAS 3.1
Authorize
default
POST /register Register User
POST /token Login For Access Token
GET /verify-token/{token} Verify User Token
POST /upload-pos-logs/ Upload Pos Logs
GET /get-last-pos-logs/ Get Last Pos Logs
GET /get-pos-log-stats/ Get Pos Log Stats

Authentication

- We are using JWT Authentication for login.
- Protects sensitive data with encryption and secure token handling.
- JWT Token is created using username and password and its returned with token endpoint.
- Tokens provide a lightweight, scalable, and stateless authentication mechanism.
- The token is then stored in local Storage, for every other authenticated requests,
- this token is sent in headers.



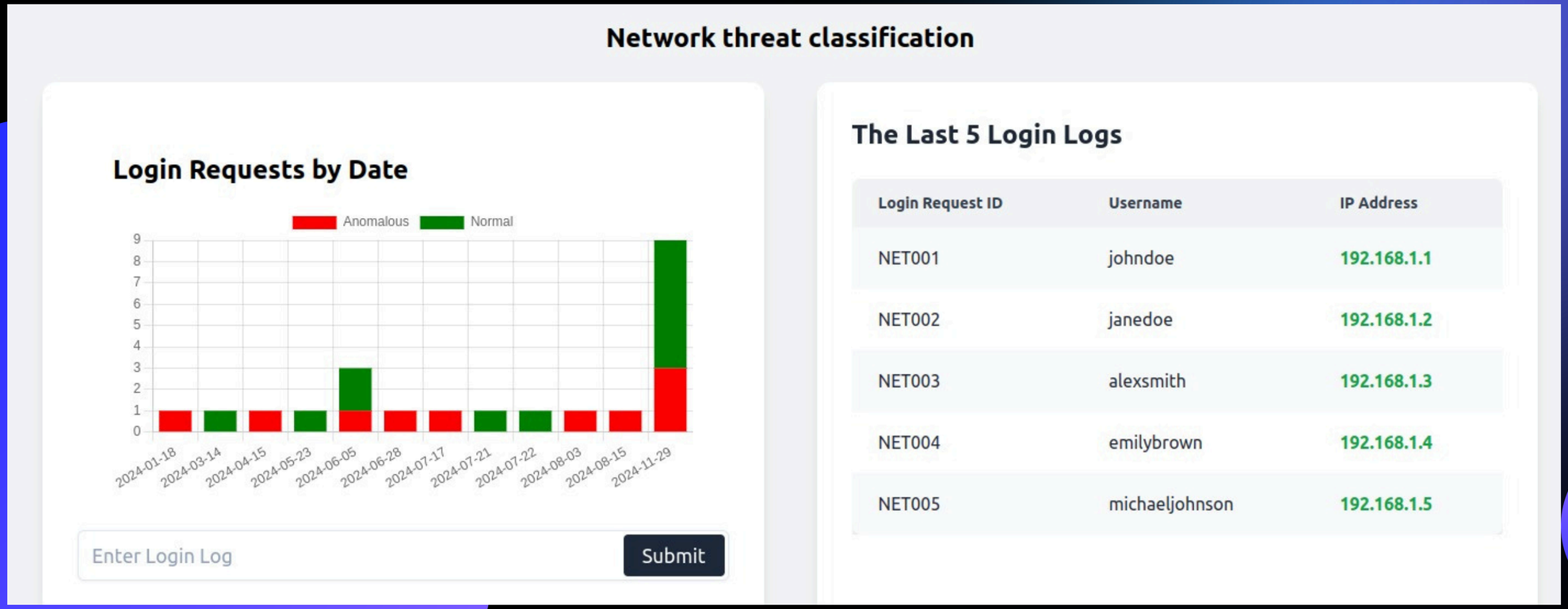


Threat Classification

- Classifies detected anomalies into predefined 10 categories (DOS, Exploit, Fuzzers, Backdoor, Analysis, Generic, Shellcode, Worms, Reconnaissance and Normal).
- Uses a feed forward neural network with labeled data from UNSW-NB15.
- Classifies the network information into normal or one of the threats

Threat Classification Model using Neural networks

To address network threats like DoS attacks, backdoors, phishing, and worms, we implemented a Sequential Neural Network model trained on the UNSW-NB15 dataset. The architecture includes two hidden layers with 64 and 32 neurons, ReLU activations, and 30% dropout. The softmax output layer classifies threats using features like protocols and timestamps. The dataset's rich features enabled us to build a robust classifier capable of detecting threats like phishing and worms with high accuracy.



POS Logs Generation

- Simulates retail-specific attack scenarios for better model training.
- Generated synthetic logs mimic real-world POS malware behaviors.
- Includes features like transaction anomalies and unauthorized access logs.
- POS Log is of this type :

timestamp	transaction_id	duration_time	item_code	amount	user_id	payment_method
2024-01-05 12:12:39	3a706b67-948c-4771-ba75-dca7d7d16ab9	7.52	C789	39.61	07f7721b-37eb-4787-9b2e-8076eeafcea7	credit_card

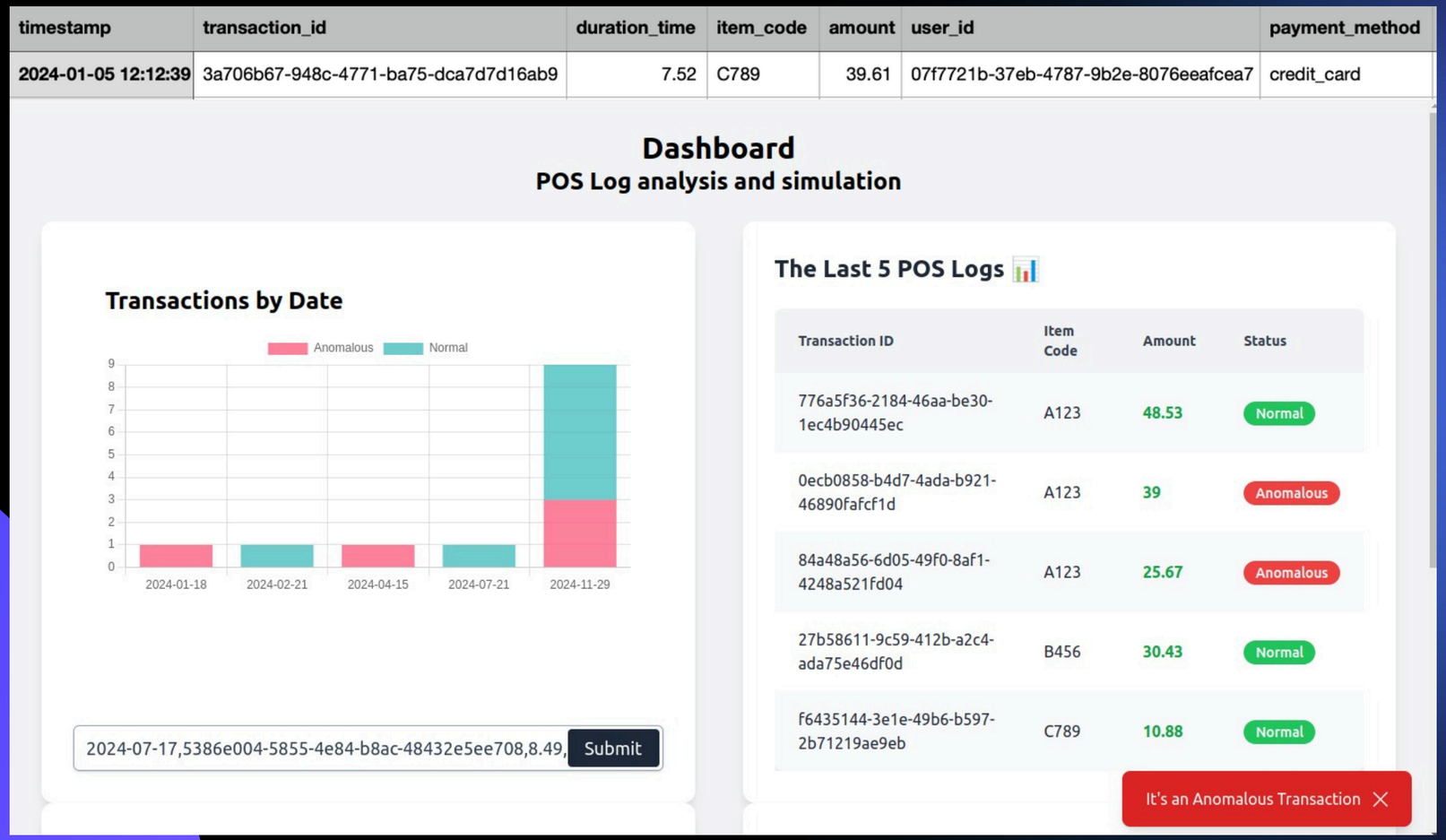
Data ingestion → Machine Learning → Threat Classification → Dashboard Visualization.

Anomaly Detection on POS Logs

Synthetic POS logs are generated with 1% labeled as fraudulent, using features like transaction amounts, timestamps, and payment methods. The Isolation Forest model detects fraud by predicting anomaly scores and isolating unusual transactions. The model is configured with 100 trees, expects 5% fraud, uses 256 samples per tree. This configuration allows efficient identification of fraudulent transactions in imbalanced datasets.

Data ingestion → Machine Learning → Threat Classification → Dashboard Visualization.

timestamp	transaction_id	duration_time	item_code	amount	user_id	payment_method
2024-01-05 12:12:39	3a706b67-948c-4771-ba75-dca7d7d16ab9	7.52	C789	39.61	07f7721b-37eb-4787-9b2e-8076eeafcea7	credit_card



SQL Injection

- We are using SQLAlchemy for database connection
- SQLAlchemy by default uses parameterised SQL Query, hence SQL Injection will not be a threat here.

Thank You