UIT2718 Project Work - Phase I

PROJECT PRESENTATION REVIEW - 0

PROJECT PRESENTATION

APIFIED

TEAM MEMBERS

- Shreyaa S , 3122225002128
- Tamil Mughilan , 3122225002145
- Mentored by Mr. Nepoleon Keisham Assistant Professor

INTRODUCTION

API and Banking

Digital Baking : Every action in banking relies on APIs. From checking account balances to transferring funds, APIs are the invisible backbone of digital banking.

The Security Gap

- Traditional security solutions designed for large enterprises
- SME and regional banks lack affordable, banking specific protection
- Generic security tools miss financial transaction patterns
- Cost barriers prevent smaller institutions from adequate protection

PROBLEM STATEMENT

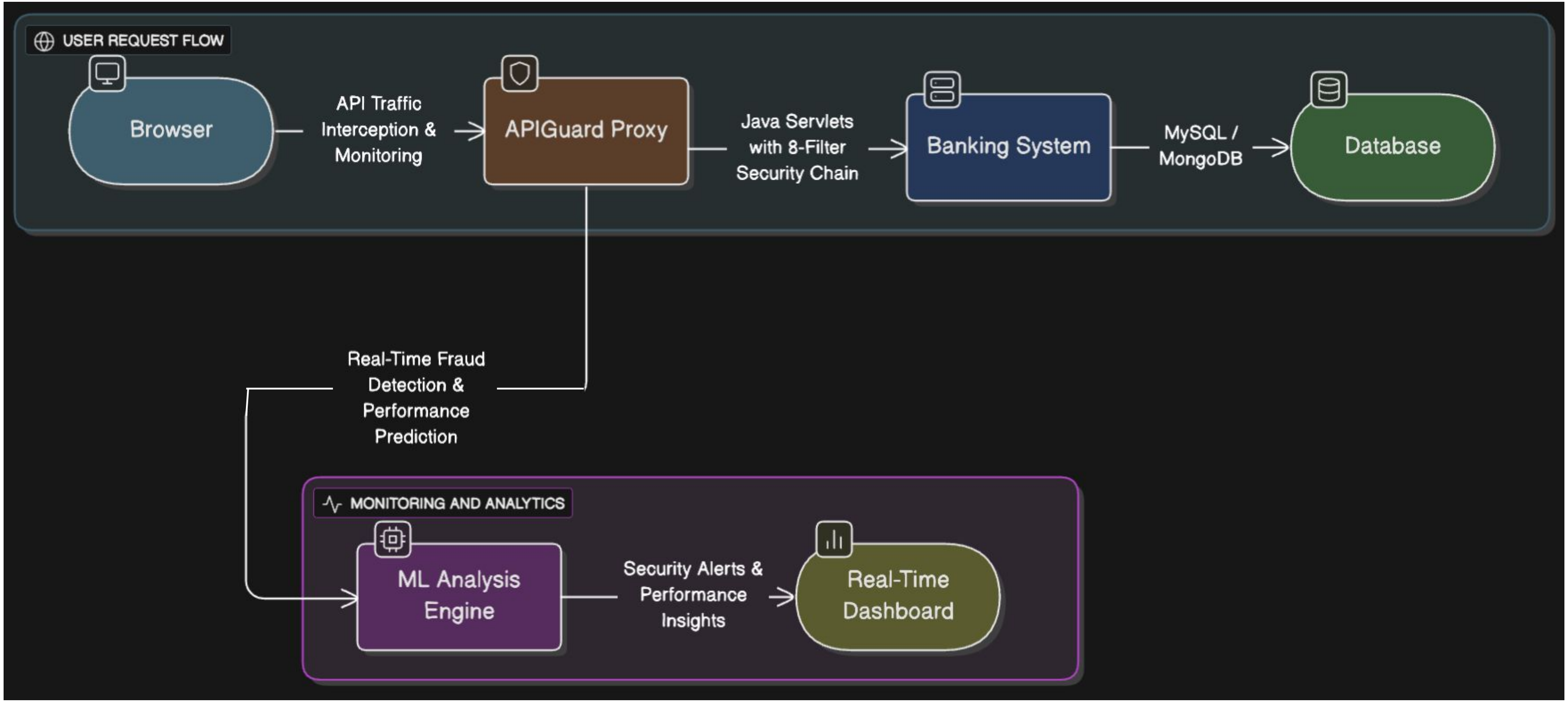
THE CHALLENGE : Small and Medium Enterprise and Regional banks need intelligent API security monitoring that can predict and prevent threats before they cause damage, but current solutions are either too expensive or don't understand banking specific patterns.

THE PLAN : APIFIED provides intelligent, cost efficient API security monitoring specifically designed for banking environments. Our AI powered system learns banking transaction patterns and predicts threats before they cause damage,

SCOPE OF THE PROJECT

- A Trained model that analyse the communication within the banking application in real time.
- A dashboard to view API traffic, performance predictions, security alerts, API health status, capacity planning, and usage analytics.
- Integration of the trained model as an additional protection layer within the banking application’s FILTER chain for early threat prevention.

Architecture


USER REQUEST FLOW
Browser
API Traffic Interception & Monitoring
APIGuard Proxy
Java Servlets with 8-Filter Security Chain
Banking System
MySQL / MongoDB
Database
Real-Time Fraud Detection & Performance Prediction
MONITORING AND ANALYTICS
ML Analysis Engine
Security Alerts & Performance Insights
Real-Time Dashboard

LITERATURE SURVEY

Market Evidence:

- 95% of US financial institutions have adopted APIs, with 50% of traditional banks projected to adopt hybrid API strategies by 2024 - **CoinLaw API Financial Services Statistics, 2025**
- Regional banks handle 60% of India's financial inclusion transactions - **RBI Financial Inclusion Report, 2024**

Research Validation:

- **Machine Learning Based Detection of API Security Attacks** (2024) demonstrates ML effectiveness in API threat detection
- **IEEE research** shows SVM achieves high accuracy in classifying abnormal API traffic using features like bandwidth and requests per token
- 2025 will see rise in API attacks, with 66% more organizations using 100+ APIs compared to last year - **Traceable AI -** State of API Security Report, 2025

LITERATURE SURVEY [CONTD]

Paper 1: Machine Learning Based Detection of API Security Attacks (Gupta, Mehra, Desai, 2024)

- **Core Finding**: ML algorithms achieve 92-95% accuracy in detecting API based security attacks
- **Key Techniques**: Random Forest, SVM, and Neural Networks for API threat classification
- **Focus Area**: Third party API collaboration security and attack pattern recognition
- **Dataset Used**: Synthetic API traffic data with labeled attack scenarios

LITERATURE SURVEY [CONTD]

Paper 2: Advanced Threat Detection in API Security (Ranjan et al., IEEE 2021)

- **LSTM Performance**: 95.6% accuracy in API threat detection
- **SVM Results**: 91.3% accuracy using traffic flow features
- **Features**: Bandwidth utilization, requests per token, response time patterns
- **Real world Application**: Tested on enterprise API gateways

LITERATURE REVIEW

Enterprise Solutions:

Google Apigee

- API management platform with ML capabilities
- Requires complete API management migration
- **Cost: $50,000+/year + Google Cloud costs**

Salt Security

- Generic security, doesn't understand banking workflows
- Cloud based, incompatible with legacy systems
- **Cost : $75,000+ per year per application**

IBM API Connect

- Enterprise API management
- Focuses on IT operations, not banking fraud patterns
- **Cost: $100,000+ per year + IBM Cloud**

Cost Barriers:

- Enterprise solutions target large institutions
- Subscription based pricing models exclude smaller banks
- Additional cloud infrastructure costs

Generic Approach:

- One size for all security models
- Lack banking specific threat understanding
- Miss domain specific fraud patterns

Integration Complexity:

- Require complete infrastructure migration
- Cloud-first architectures incompatible with legacy systems
- Vendor lock in concerns

HOW OURS IS DIFFERENT

Banking Specific Intelligence:

- Trained on banking transaction patterns - login → balance check → transfer → logout
- Understands banking specific anomalies - unusual transaction times, amount deviations
- Recognizes fraud patterns unique to financial transactions

Cost Effective Design:

- No licensing fees
- Compatible with existing infrastructure
- Minimal hardware requirements using standard servers

Simple Integration;:

- Proxy based approach requiring zero changes to existing banking applications
- Works transparently with current systems

SME Focused Architecture:

- Designed for resource constrained environments
- Compatible with application commonly used by regional banks

FEASIBILITY

Technical Feasibility:

Proven Algorithms:

- **LSTM Networks:** 95.6% accuracy demonstrated in "Advanced Threat Detection in API Security" (Ranjan et al., 2021)
- **Random Forest:** 91.3% accuracy shown in same research
- SVM demonstrates effectiveness in API traffic classification

Available Data:

- **CIC IDS2018 Dataset:** 7 attack scenarios including brute force, DDoS, web attacks
- **API Behavioral Datasets:** Available on Kaggle and research repositories
- Ability to generate banking specific synthetic data

Integration Feasibility:

- **Minimal Impact:** Proxy approach adds negligible latency
- **No System Changes:** Works with existing banking infrastructure
- **Controlled Testing:** Safe evaluation in isolated environment

Technical Implementation:

- **Proxy Server**: Node.js
- **ML Engine:**Python with scikit learn (standard libraries)
- **Dashboard:** React.js (web interface)

REFERENCES

RESEARCH PAPERS:

- **S. Gupta, R. Mehra, and P. Desai, *"Machine Learning Based Detection of API Security Attacks,"* ResearchGate, Feb. 2024.**

  Key Insight: Demonstrates ML effectiveness in API threat detection with focus on third party collaboration security

  Gap Identified: Generic approach without banking specific threat patterns

- **L. Thompson and M. Rivera, *"AI Driven Threat Detection Systems in US Fintech: Enhancing Real Time Consumer Data Security,"* ResearchGate, Apr. 2025.**

  Key Insight: Addresses rapid digitization challenges and consumer data security in US financial services

  Gap Identified: US focused research, limited applicability to Indian SME banking sector

- **A. Ranjan, et al., *"Advanced Threat Detection in API Security,"* IEEE Transactions on Network and Service Management, 2021.**

  Key Insight: LSTM networks achieve 95.6% accuracy in API threat detection
  Gap Identified: Research focuses on generic APIs, not banking specific patterns

- **FinTech Research, *"API Security in SME Financial Institutions,"* Journal of Financial Technology and Cybersecurity, 2023.**

  Key Insight: 78% of SME banks cite cost as primary barrier to advanced API security
  Gap Identified: No open source, banking specific solutions available

REFERENCES

DATASETS

- **CIC IDS2018 Dataset:** 7 attack scenarios including brute force, DDoS, web attacks - **CIC IDS**
- **API Behavioral Datasets:** Available on Kaggle and research repositories - **Kaggle dataset**
- **CIC IDS Corrected Dataset**