UIT2718 Project Work - Phase I

PROJECT PRESENTATION REVIEW - 0

PROJECT PRESENTATION

APIFIED

TEAM MEMBERS

- Shreyaa S , 3122225002128
- Tamil Mughilan , 3122225002145

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 : Build a cost effective AI powered system that sits between users and banking applications to detect fraud, predict system overload, and identify suspicious behavior patterns specific to banking workflows.

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 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-first, incompatible with legacy systems
- **$75,000+/year per application**

IBM API Connect

- Enterprise API management
- Focuses on IT operations, not banking fraud patterns
- **Cost:** $100,000+/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 legacy systems 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 <100ms 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:

- **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
- **F. Hussain, B. Noye, and S. Sharieh, "Current State of API Security and Machine Learning," Royal Bank of Canada, Toronto, [2019].**
- **Key Insight:** Banking professionals confirm need for AI-driven API security
- **Gap Identified:** Paper discusses problems but doesn't provide practical, cost effective solutions
- **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

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**