

PEOPLE'S DEMOCRATIC REPUBLIC OF  
ALGERIA

MINISTRY OF HIGHER EDUCATION AND  
SCIENTIFIC RESEARCH



FERHAT ABBAS UNIVERSITY OF SETIF

1

FACULTY OF SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

**MASTER'S THESIS**

Presented for the degree of  
**Master 2 in Computer Science**

Option: Cybersecurity

# Secure Banking System with AI Fraud Detection

*Implementation of Fraud Prevention Using Machine  
Learning and Behavioral Analytics*

**Presented by:**

El-Aid TEBABKHA

**Supervisor:**

Dr. Lyazid TOUMI

Academic Year 2024-2025

# Contents

<b>Abstract</b>	<b>vii</b>
<b>Résumé</b>	<b>viii</b>
<b>List of Abbreviations</b>	<b>ix</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Background and Motivation . . . . .	1
1.2 Research Objectives . . . . .	1
1.3 Thesis Structure . . . . .	2
<b>2 Literature Review</b>	<b>3</b>
2.1 Evolution of Banking Security . . . . .	3
2.1.1 Traditional Banking Security . . . . .	3
2.1.2 Digital Banking Security Challenges . . . . .	3
2.2 Artificial Intelligence in Fraud Detection . . . . .	4
2.2.1 Machine Learning Approaches . . . . .	4
2.2.2 Behavioral Biometrics . . . . .	4
2.3 Microservices Architecture in Banking . . . . .	4
2.3.1 Benefits of Microservices for Banking Systems . . . . .	4
2.3.2 Security Challenges in Microservices . . . . .	5
2.4 Blockchain in Financial Security . . . . .	5
2.4.1 Immutable Logging and Audit Trails . . . . .	5
2.4.2 Smart Contracts for Security Rules . . . . .	6
2.5 Containerization in Financial Services . . . . .	6
2.5.1 Benefits of Containerization . . . . .	6

---

2.5.2	Security Best Practices for Containers . . . . .	6
<b>3</b>	<b>System Architecture</b>	<b>7</b>
3.1	System Overview and Requirements . . . . .	7
3.1.1	Functional Requirements . . . . .	7
3.1.2	Non-Functional Requirements . . . . .	8
3.2	High-Level System Architecture . . . . .	9
3.2.1	Microservices Architecture Overview . . . . .	9
3.2.2	Component Diagram . . . . .	9
3.2.3	Deployment Architecture . . . . .	11
3.3	Authentication Flow and Security Model . . . . .	11
3.3.1	Multi-Factor Authentication Sequence . . . . .	11
3.4	Architectural Patterns and Design Considerations . . . . .	13
3.4.1	Circuit Breaker Pattern . . . . .	13
3.4.2	API Gateway Pattern . . . . .	13
3.4.3	CQRS Pattern . . . . .	14
3.5	Security Architecture and Defense-in-Depth . . . . .	14
3.5.1	Security Layers . . . . .	14
3.6	AI Service Architecture . . . . .	15
3.6.1	Class Structure . . . . .	15
3.6.2	Zero Trust Architecture . . . . .	16
3.7	Data Flow Architecture . . . . .	16
3.7.1	Authentication and Fraud Detection Data Flow . . . . .	16
<b>4</b>	<b>AI Fraud Detection Service</b>	<b>18</b>
4.1	Overview of the AI Fraud Detection Service . . . . .	18
4.2	Data Models and Structures . . . . .	18
4.2.1	Core Data Models . . . . .	18
4.2.2	Class Diagram . . . . .	19
4.3	Enhanced Threshold Classification . . . . .	19
4.3.1	Enhanced Classifier Architecture . . . . .	19
4.4	Fraud Detection Performance Analysis . . . . .	21
4.4.1	Test Results . . . . .	21
4.5	Model Selection and Implementation . . . . .	22

---

4.5.1	CatBoost Implementation . . . . .	22
4.5.2	Feature Engineering . . . . .	24
4.6	Real-Time Prediction Architecture . . . . .	25
4.6.1	Enhanced Threshold Classification . . . . .	25
4.6.2	Optimized Model Serving . . . . .	26
4.6.3	Model Versioning and Deployment . . . . .	27
4.7	Comparative Analysis with Other Approaches . . . . .	29
4.7.1	Comparison with Traditional Approaches . . . . .	29
4.7.2	Performance Across Different Fraud Types . . . . .	30
4.8	Model Interpretability for Financial Systems . . . . .	31
4.8.1	Explainable AI Implementation . . . . .	31
4.8.2	Regulatory Compliance . . . . .	32
4.9	Summary . . . . .	33
<b>5</b>	<b>Model Training and Optimization</b>	<b>35</b>
5.1	Introduction to Model Training Strategy . . . . .	35
5.2	CatBoost Model Implementation . . . . .	36
5.2.1	Model Architecture . . . . .	36
5.2.2	Training Process . . . . .	36
5.3	Feature Importance Analysis . . . . .	38
5.4	Threshold Optimization . . . . .	38
5.4.1	Standard Threshold Distribution . . . . .	38
5.4.2	ThresholdClassifier Implementation . . . . .	39
5.4.3	Threshold Impact Analysis . . . . .	39
5.4.4	EnhancedThresholdClassifier for Multi-level Risk Assessment . .	41
5.4.5	ROC Curve Analysis . . . . .	41
5.4.6	Performance Metrics . . . . .	42
5.5	Formal Definitions of Evaluation Metrics . . . . .	42
5.5.1	Confusion Matrix . . . . .	43
5.5.2	Accuracy . . . . .	43
5.5.3	Precision . . . . .	43
5.5.4	Recall . . . . .	44
5.5.5	F1 Score . . . . .	44
5.5.6	$F_\beta$ Score . . . . .	44

---

5.5.7	ROC Curve and AUC . . . . .	45
5.5.8	Precision-Recall Curve . . . . .	45
5.6	Threshold Optimization for Imbalanced Data . . . . .	45
5.6.1	Challenges with Imbalanced Data . . . . .	46
5.6.2	Re-sampling Techniques . . . . .	46
5.6.3	Cost-sensitive Training . . . . .	47
5.6.4	Evaluation Metric Optimization . . . . .	47
5.6.5	Ensemble Methods . . . . .	47
5.6.6	Threshold Adjustment Post-Training . . . . .	48
5.6.7	Continuous Monitoring and Adaptation . . . . .	48
<b>6</b>	<b>Risk Assessment Engine</b>	<b>50</b>
6.1	Overview of the Risk Assessment Engine . . . . .	50
6.2	Risk Distribution Analysis . . . . .	51
6.3	Risk Assessment Algorithm . . . . .	51
<b>7</b>	<b>Docker Implementation</b>	<b>53</b>
7.1	Introduction to Containerization . . . . .	53
7.2	Project Docker Architecture . . . . .	54
7.2.1	Service Containerization . . . . .	54
7.3	Container Orchestration and Management . . . . .	54
7.3.1	Security Considerations in Containerization . . . . .	55
<b>8</b>	<b>Conclusion</b>	<b>56</b>
8.1	Summary of Contributions . . . . .	56
8.2	Lessons Learned . . . . .	57
8.3	Limitations and Future Work . . . . .	57
8.4	Concluding Remarks . . . . .	58
8.5	Final Words and Research Impact . . . . .	58
	<b>Bibliography</b>	<b>60</b>
	<b>Source Code Listings</b>	<b>62</b>
.1	Enhanced Threshold Classification Algorithm . . . . .	62
.2	Adaptive Risk Scoring Algorithm . . . . .	65
.3	Blockchain-Based Immutable Logging . . . . .	68

# Abstract

This thesis presents the design, implementation, and evaluation of a secure banking system with integrated artificial intelligence for fraud detection. The research addresses the critical challenge of financial fraud in digital banking platforms through a comprehensive approach combining advanced machine learning techniques with robust security architecture.

The proposed system employs a microservices architecture to ensure scalability, fault tolerance, and security isolation. At its core, an AI-powered fraud detection service analyzes user behavior patterns and transaction characteristics in real-time to identify potentially fraudulent activities. The system implements enhanced threshold classification techniques that improve upon traditional binary classification methods, resulting in higher precision and recall metrics even with imbalanced datasets.

Additionally, the research explores the integration of a risk assessment engine that complements the machine learning model with rule-based analysis. This hybrid approach provides both the adaptability of AI and the explainability of rule-based systems. The implementation leverages Docker containerization to ensure consistent deployment across environments while maintaining security isolation between components.

Experimental results demonstrate significant improvements over traditional fraud detection approaches, with the proposed system achieving 93.7% accuracy and 91.2% precision in identifying fraudulent transactions while maintaining a low false positive rate of 3.8%. The thesis contributes to the field of financial cybersecurity by presenting a comprehensive architecture that can be adapted by banking institutions to enhance their fraud prevention capabilities while maintaining high performance and user experience standards.

# Résumé

Cette thèse présente la conception et l'implémentation d'un système bancaire sécurisé intégrant l'intelligence artificielle pour la détection des fraudes. Face à l'augmentation des menaces dans les plateformes bancaires numériques, notre recherche développe une approche combinant techniques avancées d'apprentissage automatique et architecture de sécurité robuste.

Le système s'articule autour d'une architecture de microservices offrant évolutivité et isolation sécuritaire. Son composant central est un service de détection alimenté par l'IA qui analyse en temps réel les comportements utilisateurs et les caractéristiques des transactions. Notre implémentation emploie une technique de classification par seuil optimisée surpassant les méthodes binaires traditionnelles, particulièrement efficace avec les ensembles de données déséquilibrés typiques des cas de fraude.

L'architecture intègre également un moteur d'évaluation des risques basé sur des règles qui complète l'apprentissage automatique. Cette approche hybride combine l'adaptabilité de l'IA avec l'explicabilité nécessaire dans le secteur financier. L'ensemble du système est déployé via conteneurisation Docker, garantissant cohérence environnementale et isolation sécuritaire entre composants.

Les résultats démontrent des performances supérieures aux approches traditionnelles : 93,7% de précision et 91,2% d'exactitude dans l'identification des fraudes, avec seulement 3,8% de faux positifs. Notre contribution principale réside dans la conception d'une architecture complète que les institutions financières peuvent adopter pour renforcer leur sécurité tout en maintenant une expérience utilisateur fluide.