



Project Proposal

Fraud Detection in Financial Industries Using Machine Learning as a Tool

Prepared By

Name: XXXXXXXXXXXXXXXXXXXX

ID No.: XXXXXXXXX

Name: XXXXXXXXXXXXXXXXXXXX

ID No.: XXXXXXXXX

Submitted in fulfillment of the requirements for the degree Master of Science in
Artificial Intelligence

At

Collage of Informatics - Midocean University

Supervisor Name: Dr. Khaled Eskaf

Collage of Informatics, Midocean University, Comoros

1. Project Overview

Loan fraud represents a significant and growing challenge in the Saudi Arabian financial sector. According to the Saudi Central Bank (SAMA), financial institutions experienced **4,377 financial fraud cases in 2020**, resulting in total losses of approximately **SAR 765 million** (USD 204 million). The number of fraud cases increased by **34.1% compared to 2019**, while total losses increased by **17.5%**.

SAMA has documented "**a notable increase in the number of fraudulent websites and social media accounts, and a persistent recurrence of financial fraud incidents**," particularly social engineering scams where consumers are deceived into revealing personal financial data. Traditional manual review processes and rule-based detection systems are inadequate for identifying these sophisticated fraud schemes.

The proposed system is envisioned with potential for future extensions such as continuous learning and adaptation to new fraud pattern.

Future extensions of the system could potentially incorporate **continuous learning and adaptation capabilities** to learn from new fraud patterns that emerge during operation.

The project will have **compliance with SAMA's Counter-Fraud Framework (2022) and Cybersecurity Framework**, which will lead financial institutions to achieve a higher maturity level 3 in counter-fraud controls and includes implementing fraud detection system capabilities.

By combining AI techniques with regulatory compliance, this system will help financial institutions in the GCC make faster and more accurate loan decisions while reducing fraud losses and enhancing financing security.

2. Project Goal

The main goal of the project is to create an intelligent fraud detection system that helps Financial industry automatically identify suspicious loan applications and refer them to human experts for final validation before fund disbursement.

Specific objectives:

- 1) Using force learning in an AI model using real historical loan data to detect fraud patterns and behaviors specific to the digital landing applications.
- 2) Achieve fraud detection accuracy of $\geq 85\%$ in regulation valuation fraud cases with false positive rate $\leq 5\%$ to ensure effective fraud identification.
- 3) Process loan applications and flag suspicious cases for expert review.
- 4) Implement model explainability features using SHAP and LIME techniques to meet regulatory transparency requirements.
- 5) Demonstrate measurable improvement in fraud detection effectiveness through comparative analysis with existing manual review methods and established literature benchmarks.
- 6) Ensure compliance with the Saudi Central Bank (SAMA) Counter-Fraud Framework requirements, achieving at least Level 3 maturity in counter-fraud controls.

- 7) Implement the SAMA Cybersecurity Framework protocols to protect data integrity and ensure system security throughout the development and deployment phases.
- 8) Quantify potential operational improvements through automated processing efficiency and enhanced detection accuracy compared to current manual processes.

3. Approach

This project will follow a **machine learning approach** to develop an effective fraud detection system for the financial industry “Digital Loan Origination”. The approach is designed to be flexible, and aligned with industry compliant best practices, and regulations.

3.1 Data Collection

The research will use real-world financial data from a mobile lending financial company. The dataset contains 2,200 legitimate loan applications and 2,000 fraudulent cases, providing a naturally balanced dataset of 4,200 records in a period of Q4 2024 until Q2 2025.

Data includes standard financial variables (loan amounts, income, credit scores) and non-financial. This balanced distribution simplifies the modeling process by eliminating class imbalance issues common in fraud detection.

This project will comply with institutional ethical approval requirements to ensure responsible data usage. Formal data sharing agreements will govern access and ensure compliance with confidentiality requirements.

3.2 Data Processing

Basic preprocessing will include handling missing values, outlier detection, and feature normalization. Simple feature engineering may create financial ratios and behavioral indicators relevant to mobile lending fraud.

The dataset will be split into training (80%), and testing (20%) sets. The balanced nature of the data eliminates the need for complex sampling techniques.

3.3 Model/Method Selection

The project will primarily employ **Logistic Regression** and **Random Forest**, with the potential inclusion of XGBoost and **Decision Trees**. Logistic Regression is chosen as the baseline model due to its native interpretability and ability to capture linear relationships. Decision Trees are also inherently explainable, making them valuable for comparison. In contrast, Random Forest and XGBoost are more complex ensemble methods that typically require external frameworks (e.g., SHAP) to achieve model explainability. Random Forest is particularly selected for its robustness and strong performance on tabular financial datasets, while XGBoost is considered for its efficiency and superior handling of non-linear feature interactions.

Given the sample size under consideration, computational resources will not be a limitation. Both Random Forest and XGBoost can be executed effectively, even with cross-validation and extensive hyperparameter tuning.

Model selection will ultimately be guided by a comprehensive evaluation across multiple performance metrics, ensuring balanced fraud detection capabilities and practical feasibility for deployment in real-world financial environments.

3.4 Testing and Evaluation

Performance metrics will include Precision, Recall, F1-Score, to provide comprehensive evaluation. Cross-validation will assess model reliability and generalization.

Comparative analysis will benchmark results against existing fraud detection research. The evaluation aims to achieve competitive performance while demonstrating practical value for mobile lending applications.

Success criteria focus on developing a working system that performs well on the available data and shows potential for real-world deployment.

4. Project Steps and Timeline

The following timeline outlines the structured phases of the project, strategically distributed over an 10-week period. Each phase has been carefully designed to align with the project's objectives while ensuring feasibility within the available timeframe. The timeline maintains a balance between technical development, analytical rigor, and regulatory integration to deliver a practical and research-driven fraud detection solution.

Week	Phase	Description
1	Data Collection & Initial Setup	Collect real loan data (2,200 legitimate + 2,000 fraudulent cases), establish data security protocols, set up development environment (Python, Jupyter, required libraries), and perform initial data quality assessment.
2	Data Cleaning & Preprocessing	Handle missing values, outlier detection and treatment, data normalization and standardization, address data inconsistencies, and create clean master dataset with documentation of all preprocessing steps. Concurrent literature review and theoretical chapter writing
3	Exploratory Data Analysis & Feature Engineering	Analyze data distributions, explore fraud patterns and correlations, identify key fraud indicators, create new features (financial ratios, behavioral indicators, risk scores), and generate comprehensive EDA report with visualizations. Concurrent literature review and theoretical chapter writing
4	Model Building - Implementation	Implement Logistic Regression (baseline) and Random Forest models, perform initial training using 80/20 split, establish baseline performance metrics, and document initial model architectures and parameters. Concurrent literature review and theoretical chapter writing
5	Model Optimization & Hyperparameter Tuning	Conduct systematic hyperparameter tuning for both models using grid search or random search, implement cross-validation strategies, optimize model performance, and document optimal configurations. Concurrent literature review and theoretical chapter writing
6	Model Explainability	Provide explainability along with the score to ensure transparency for both the business and regulators by using SHAP and LIME
7	Comprehensive Testing & Evaluation	Test models on the test dataset. Evaluate using Precision, Recall, F1-Score,. Use cross-validation for reliability.
8	Comparative Analysis & Model Selection	Compare results with literature benchmarks, noting contextual differences (Al Marri 99.79% on simulated data), analyze business impact of each model, evaluate deployment feasibility, select optimal model, and begin methodology documentation.
9	SAMA Compliance Integration & Final Refinements	Map system against SAMA Counter-Fraud Framework requirements, ensure maturity compliance, integrate cybersecurity framework requirements, perform final model refinements, and continue comprehensive documentation.
10	Final Documentation & Presentation	Prepare a full report with methodology, results, regulatory alignment, and lessons learned. Develop slides or materials for final presentation or viva.

5. Expected Results

This project is expected to yield several key outcomes that contribute both academically and practically to the field of financial fraud detection. The anticipated results include:

- **Enhanced Accuracy in Loan Fraud Detection:** Development of a machine learning model that significantly improves the accuracy of detecting fraudulent loan applications when compared to traditional manual or rule-based systems targeting to achieve $\geq 85\%$, based on benchmarks reported in Al Marri & AlAli (2020) and Awoyemi et al. (2017).
- **Contextual Insights into Fraud Patterns in the GCC:** Identification of unique behavioral and transactional patterns specific to the Gulf region, including fraud schemes related to social engineering, trust-based networks, and data accessibility—factors often overlooked in Western studies.
- **A Functional AI-based Detection Tool:** A working prototype of a fraud detection system that can be integrated into financial institutions' loan processing workflows to assist in early detection and risk mitigation.
- **Evaluation of Algorithms for Mobile Lending Fraud:** Comparative performance analysis of several machine learning models (e.g., Random Forest,) on mobile lending datasets, offering a reference point for future studies.
- **Regulatory Compliance Demonstration:** A system architecture and process design aligned with the Saudi Central Bank's (SAMA) Anti-Fraud Rules and Cybersecurity Framework, demonstrating how AI tools can operate within the required legal and security standards.

6. Resources Needed

To successfully complete this project, the following resources will be essential across different stages of development, training, and evaluation:

Tools and Software

- **Python Programming Language** – for model development, data preprocessing, and evaluation.
- **Jupyter Notebook** – for interactive code execution and experimentation.
- **Scikit-learn, XGBoost, Pandas, NumPy, Matplotlib, Seaborn** – key Python libraries for machine learning, data manipulation, and visualization.
- **Google Colab / Local IDE** – for model development and prototyping.

Dataset

- **Real Loan Application Data** – A balanced dataset consisting of 2,200 genuine and 2,000 fraudulent mobile loan applications, including financial and non-financial data.
- **Additional synthetic datasets** (e.g., PaySim or Kaggle fraud datasets) may be used for benchmarking or validation.

Computing Resources

- **MacBook M1** – for initial training and testing.
- **Optional Access to Cloud Services** (e.g., Google Colab Pro, Oracle) – for faster training of advanced models or handling larger datasets.

Limitations and Risks

- **Data Accessibility:** Access to real loan datasets may be limited due to privacy and confidentiality restrictions.
- **Regional Specificity:** Available datasets may not fully represent fraud patterns unique to the Saudi or GCC context.
- **Bias and Fairness:** Model predictions may be affected by bias in features (e.g., income or demographic attributes).
- **Time Constraints:** The 10-week project timeline poses challenges for extensive experimentation and validation.
- **Regulatory and Compliance Requirements:** Adhering to SAMA regulations may impose additional constraints on model transparency, explainability, and access to sensitive features.

Risk Mitigation Strategies

- Use of synthetic or publicly available datasets to supplement real-world data if access is restricted.
- Regular bias checks and fairness assessments to ensure balanced performance across data segments.
- Prioritization of key features and models to meet deadlines without compromising on scientific rigor.
- Close consultation with industry experts to validate findings against real fraud scenarios.

Expert Guidance

- **Eng. Sultan Abdullah Alqahtani** – CIO at Emkan Finance Company – for consultation on the required AI infrastructure and integration mechanism of the tool with financial Core System.
- **Mr. Thamer Fahad Alhathal** – COO at Emkan Finance Company – for consultation on real Fraud scenarios and data.
- **Eng. Salam Hassan** – AI expert at Emkan Finance Company – for regular feedback on methodology, ethical considerations, and regulatory alignment.
- **Abdulrahman Alanazi – CISO** – Emkan Finance Company - Cybersecurity and Compliance Expert – for consultation regarding integration of SAMA's Anti-Fraud Rules and Cybersecurity Framework.

The results will be translated into practical recommendations for Emkan Finance, including integration with the Core Banking System and alignment with real fraud scenario

Documentation Tools

- **Microsoft Word** – for report writing and structuring project documentation.
- **PowerPoint** – for preparing the final presentation or defense.

7. Literature Review

The following studies and articles represent the foundational literature and prior research that inform the development of this project. These references provide theoretical background, methodological guidance, and benchmarking insights for fraud detection in financial transactions using AI techniques:

#	Reference	Title	Name of Researchers	Summary	Methodologies	Accuracy	
1	Al Marri, M. & AlAli, A. (2020)	Financial Fraud Detection using Machine Learning Techniques	Matar Al Marri, Ahmad AlAli	Applied machine learning techniques for fraud detection in financial transactions using simulated PaySim data. Focus on addressing class imbalance and comparing different algorithms for fraud detection performance.	Logistic Regression, Random Forest, Data Undersampling, Cross-validation	Logistic Regression: 51.7% (Recall), Random Forest: 99.79%	Relied on simulated dataset (PaySim), not real financial transactions → limits real-world applicability
2	Awoyemi et al. (2017)	Credit Card Fraud Detection using Machine Learning	Awoyemi et al.	Comparative analysis of different machine learning techniques on European credit card data using hybrid sampling techniques to address dataset imbalance issues.	Naive Bayes, K-Nearest Neighbors, Logistic Regression, Hybrid Sampling	Logistic Regression: 54.86% , Naive Bayes: 97.92%, KNN: 97.69%	Dataset limited to European credit cards; not generalizable to loan fraud or other regions
3	Benchaji et al. (2021)	Enhanced Credit Card Fraud Detection using GA and K-means	Benchaji et al.	Used genetic algorithm with K-means clustering to address data imbalance and improve fraud detection in credit card transactions through feature optimization.	Genetic Algorithm, K-means Clustering, Random Forest, ANN, Decision Tree	GA-RF: 77.95% , GA-ANN: 81.82%, GA-DT: 81.97%	Focused on optimization; applied only to credit card fraud, not loans
4	Kumar et al. (2022)	Loan Fraud Detection using Machine Learning Algorithm	Kumar et al.	Developed loan fraud detection system using machine learning techniques with focus on addressing class imbalance through novel undersampling methods.	Gaussian Mixture Undersampling, SVM, Random Forest, Neural Networks	GMUS-SVM: 68.5% , GMUS-RF: 78.2%	Limited to undersampling; achieved modest accuracy; not region-specific

5	Smith & Valverde (2021)	Financial Transaction Fraud Detection	Smith, Valverde	Case study on South African retail transaction data (2014–2016)	Support Vector Machine, Logistic Regression, Neural Networks	SVM: 72.4% , Logistic Regression: 69.8%, NN: 74.1%	Older dataset (2014–2016), narrow scope; not tailored for loan fraud
6	Dharwa et al. (2011)	Hybrid Approach Based Transaction Risk Score Model	Dharwa et al.	Developed transaction risk scoring model using hybrid data mining techniques for online financial transaction fraud detection with cost-sensitive approach.	Density-based Clustering, Decision Trees, Association Rules	Hybrid Model: 76.3%	Focused on scoring, not full fraud detection system; outdated approach
7	Sahin et al. (2013)	Cost-Sensitive Decision Tree for Fraud Detection	Sahin et al.	Applied cost-sensitive decision trees for credit card fraud detection to address the different costs of false positives and false negatives in fraud detection.	Cost-sensitive Decision Trees, Random Sampling	Cost-sensitive DT: 73.8%	Limited to cost-sensitive trees; focused on credit card data only
8	Phua et al. (2004)	Minority Report in Fraud Detection	Phua et al.	Addressed the class imbalance problem in fraud detection data using various techniques to improve detection of minority fraud cases in large datasets.	Neural Networks, Naive Bayes, Decision Trees	Neural Networks: 65.2% , Naive Bayes: 71.4%, Decision Trees: 69.8%	Very old study; datasets and techniques outdated; Western-focused
9	Sorournejad et al. (2016)	Survey of Credit Card Fraud Detection Techniques	Sorournejad et al.	Comprehensive review of credit card fraud detection techniques comparing performance of supervised and unsupervised learning approaches for fraud identification.	ANN, SVM, HMM, Clustering, Logistic Regression	HMM: 67.5% , SVM: 72.1%, ANN: 74.3%	Broad review, not empirical; focused on credit cards, not GCC loan fraud

7.1 Overview of Existing Research

The literature reveals extensive research in fraud detection using machine learning techniques, with studies achieving varying performance levels depending heavily on dataset characteristics and contextual factors. While some studies report high accuracy rates - such as 99.79% for Random Forest (Al Marri & AlAli, 2020) on **simulated PaySim data** and 97.92% for Naive Bayes (Awoyemi et al., 2017) on **European credit card** transactions - these results reflect specific contexts that **may not generalize to real loan fraud detection in different regional settings**. Performance on real-world loan data shows more modest results, with Kumar et al. (2022) achieving 78.2% accuracy for loan fraud detection, highlighting the complexity of this specific domain.

7.2 Key Research Findings

Credit Card Fraud Focus: Most studies concentrate on credit card fraud detection (Awoyemi et al., 2017; Benchaji et al., 2021; Sahin et al., 2013) using European and North American datasets. These achieved high accuracy rates, with Naive Bayes reaching 97.92% and KNN achieving 97.69% on European credit card data.

Limited Loan Fraud Research: Only Kumar et al. (2022) specifically addressed loan fraud detection, achieving modest performance (GMUS-RF: 78.2%, GMUS-SVM: 68.5%) compared to credit card fraud studies, suggesting this domain requires further investigation.

Class Imbalance Challenge: Multiple studies (Phua et al., 2004; Awoyemi et al., 2017; Benchaji et al., 2021) addressed the fundamental challenge where fraudulent cases represent less than 1% of typical datasets, employing various sampling techniques with mixed success.

Algorithm Performance Variation: Results show significant variation across algorithms and contexts, with ensemble methods and optimized approaches (GA-ANN: 81.82%, GA-DT: 81.97%) generally outperforming traditional single algorithms.

7.3 Critical Research Gap: Regional and Cultural Context

Geographic Limitation: All reviewed studies focus on European, North American, or simulated datasets. No research specifically addresses fraud detection in the Gulf Cooperation Council (GCC) region, where unique cultural and regulatory factors fundamentally influence fraud patterns.

Cultural Factors Affecting Fraud Patterns: The GCC region presents distinct characteristics that may significantly impact fraud detection effectiveness:

- **Social Engineering Patterns:** Trust-based community networks create different vulnerability patterns compared to Western individualistic societies
- **Cultural Community Trust:** High levels of interpersonal trust may lead to different fraud scheme structures and victim behaviors
- **Data Accessibility:** Different privacy norms and data sharing practices may influence both fraud perpetration methods and detection approaches
- **Regulatory Environment:** None of the reviewed studies address compliance with region-specific regulatory frameworks such as SAMA's Counter-Fraud Framework, which requires specific implementation standards and transparency measures.

7.4 Research Justification and Expected Contribution

This research addresses the identified geographic and contextual gap by focusing specifically on loan fraud detection within the Saudi Arabian financial sector. The combination of:

- **Real loan data** (versus simulated datasets used in high-performing studies like Al Marri & AlAli, 2020)
- **Naturally balanced dataset** (eliminating the class imbalance problems that affected studies like Phua et al., 2004)
- **Regional cultural context** (addressing social engineering and trust patterns unique to the GCC)
- **Regulatory compliance integration** (incorporating SAMA framework requirements)

This creates a unique research opportunity that cannot be directly compared with existing studies, due to differences in context, data, and regulatory requirements.

While previous studies achieved high accuracy in their specific contexts, the applicability of these results to the GCC regional environment with its distinct cultural patterns and regulatory frameworks remains unexplored. This research aims to establish performance benchmarks for fraud detection in this unique context while contributing to the broader understanding of how regional factors influence fraud detection effectiveness.

Therefore, this proposal outlines a research plan that will not only address the regional gap in loan fraud detection but also provide actionable insights for Saudi financial institutions to strengthen compliance and reduce fraud losses.

7. References

- 1) Phua, C., Lee, V., Smith, K. and Gayler, R. (2004) 'A comprehensive survey of data mining-based fraud detection research', *arXiv preprint*, arXiv:1009.6119. Available at: <https://arxiv.org/abs/1009.6119>
- 2) Dharwa, J. and Jain, D. (2011) 'A data mining with hybrid approach based transaction risk score generation model (TRSGM) for online financial transaction fraud detection', *International Journal of Computer Applications*, 12(3), pp. 1–6. Available at: https://www.researchgate.net/publication/50230684_A_Data_Mining_with_Hybrid_Approach_based_Transaction_Risk_Score_Generation_Model_TRSGM_for_Online_Financial_Transaction_Fraud_Detection
- 3) Sahin, Y. and Duman, E. (2013) 'Detecting credit card fraud by using cost-sensitive decision trees', *Expert Systems with Applications*, 40(15), pp. 5916–5923. doi:10.1016/j.eswa.2013.05.021
- 4) Sorournejad, D., GhasemiGol, M. and Rezaei, A. (2016) 'A survey of credit card fraud detection techniques: Data and technique oriented perspective', *Applied Artificial Intelligence*, 30(8), pp. 673–698. doi:10.1080/08839514.2016.1193701
- 5) Awoyemi, J.O., Adetunmbi, A.O. and Oluwadare, S.A. (2017) 'Credit card fraud detection using machine learning techniques: A comparative analysis', *2017 International Conference on Computing Networking and Informatics (ICCNI)*, pp. 1–9. IEEE. doi:10.1109/ICCNI.2017.8123782
- 6) Al Marri, M. and AlAli, A. (2020) *Financial fraud detection using machine learning techniques*. Master's Thesis. Rochester Institute of Technology. Available at: <https://repository.rit.edu/theses/10695>
- 7) Benchaji, H., Elkoutbi, M. and Belhaj, O. (2021) 'Enhanced credit card fraud detection using genetic algorithm and K-means clustering', *International Journal of Advanced Computer Science and Applications*, 12(2), pp. 134–140. doi:10.14569/IJACSA.2021.0120216
- 8) Smith, Q.J. and Valverde, R. (2021) 'Financial transaction fraud detection using pattern recognition techniques', *WSEAS Transactions on Systems and Control*, 16, pp. 56–67. Available at: <https://www.wseas.org/multimedia/journals/control/2021/b165107-074.php>
- 9) Kumar, S., Verma, A. and Rani, R. (2022) 'Loan fraud detection using machine learning algorithm', *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 2(1), p. 589. doi:10.48175/IJARSCT-4637. Available at: <https://ijarsct.co.in/Paper4637.pdf>
- 10) Saudi Central Bank (SAMA) (2022) *Counter-fraud framework*. Saudi Central Bank Rulebook. Available at: <https://rulebook.sama.gov.sa/en/counter-fraud-framework-0>
- 11) Saudi Central Bank (SAMA) (2022) 'Saudi Central Bank to take urgent measures to protect banking consumers from financial fraud', *Official Press Release*. Available at: <https://www.sama.gov.sa/en-us/news/pages/news-752.aspx>
- 12) Bureau ID (2024) *Decoding KSA's SAMA mandate: Analysis of SAMA counter-fraud framework requirements and statistics*. Available at: <https://bureau.id/blog/decoding-ksas-sama-mandate>