



Project Proposal

Real-Time Credit Card Fraud Detection Using Adaptive Machine Learning
and Behavioral Analytics

Prepared By

Name: Ahmad Mostafa Abutalib

ID No.: 243002097

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

At

Collage of Informatics

Midocean University

UAE

Supervisor Name: Dr.Amjad Qatish

Collage of Informatics, Midocean University, Comoros

Email: 243002097@st.midocean.edu.km

Table of Contents

1Real-Time Credit Card Fraud Detection Using Adaptive Machine Learning and Behavioral Analytics	1
1. Project Overview	3
2. Project Goal	3
3. Related Work	3
4. Approach	4
Data Collection.....	4
Data Processing.....	4
Model/Method Selection	5
Testing and Evaluation.....	5
5. Project Steps and Timeline	5
6. Expected Results.....	5
7. Resources Needed	5
8. References.....	6

1. Project Overview

Credit card fraud constitutes a significant issue for financial transactions, incurring billions of dollars in losses annually. Conventional detection methods struggle to adapt to evolving fraud trends, leading to false positives or overlooked instances. This research involves developing a real-time adaptive fraud detection model that integrates machine learning with behavioral analytics to enhance accuracy and speed of detection.

The technology seeks to surpass static models and address emerging fraud strategies by analyzing transaction patterns and user behavior. This will provide banks and payment processors with a robust solution.

2. Project Goal

- Develop a real-time machine learning model that adapts to detect fraudulent credit card transactions while minimizing false positives.
- Integrate behavioral data with transactional data.
- Employ incremental learning to adapt detection techniques progressively over time.
- Ensure the system operates effectively in high-traffic real-world environments.

3. Related Work

Papers	Year	Methods	Datasets	Results
https://ieeexplore.ieee.org/abstract/document/10595068	2024	MLP	https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud	98%
https://onlinelibrary.wiley.com/doi/full/10.1155/2023/8134627	2023	hybrid CNN-SVM	https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud	91.05%
https://ieeexplore.ieee.org/abstract/document/9480639	2021	MLP-OSCNN results	https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud	98%
https://ccis2k.org/iajit/images/year2023/No.2/20341.pdf	2023	the CNN without Pooling layer	https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud	83.72%
https://www.researchgate.net/profile/Ibraheem-Ibraheem-2/publication/377830394_Credi	2024	LSTM	https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud	96.3%

t_Card_Fraud_Detection_Using_Improved_Deep_Learning_Models/links/65d47c8e5fbf6f295177e8a6/Credit-Card-Fraud-Detection-Using-Improved-Deep-Learning-Models.pdf				
https://www.researchgate.net/publication/340968896_Credit_Card_Fraud_Detection_Based_on_Machine_and_Deep_Learning	2020	BiLSTM-MaxPooling-BiGRU-MaxPooling	https://www.kaggle.com/datasets/muhakabartay/yourallmodelsdata	91.37%
https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-01048-8?utm_source=chatgpt.com#Abstract	2024	combining CNN, GRU, and MLP architectures	https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud	100%
https://www.researchgate.net/publication/378583709_Enhancing_Credit_Card_Fraud_Detection_A_Neural_Network_and_SMOTE_Integrated_Approach	2024	(NN) and (SMOTE	https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud	99%
https://www.sciencedirect.com/science/article/abs/pii/S1568494620308218				

4. Approach

Data Collection

- Kaggle's dataset comprising anonymized credit card transactions, encompassing time, quantity, and various other anonymized characteristics.
- The dataset exhibits significant imbalance, with only 0.172% of cases classified as fraud.

Data Processing

- Eliminate entries that are erroneous or incomplete.
- Normalize continuous variables.

- Employ SMOTE and cost-sensitive learning to address the issue of class imbalance.
- Segment the data into three portions: 70% for training, 15% for validation, and 15% for testing.

Model/Method Selection

- Evaluate various algorithms, including Logistic Regression, Random Forest, XGBoost, LSTM, and DNN.
- For minor changes, implement adaptive learning and ensemble techniques.
- Monitor concept drifts to adjust the model in response to evolving fraud tendencies.

Testing and Evaluation

- Metrics: Area Under the Curve (AUC), F1-score, Precision, Recall, and Latency.

5. Project Steps and Timeline

Weeks	Phase	Tasks
1–2	Data Preparation	Acquire dataset, clean, normalize, and balance data
3–4	Model Selection & Baseline	Train initial models and compare results
5–6	Adaptive Learning Integration	Implement incremental updates and drift detection
7–8	Testing & Optimization	Optimize model parameters, evaluate performance
9–10	Deployment & Reporting	Prepare real-time pipeline and final project report

6. Expected Results

- Enhanced accuracy in detection with reduced false positives compared to conventional models.
- A fraud detection system that evolves in response to emerging fraud patterns.
- A practical framework applicable immediately in banks, internet retailers, or digital payment platforms.

7. Resources Needed

- Software: Python with requisite libraries including Scikit-learn and either TensorFlow or PyTorch (choose one), in addition to Pandas and NumPy for data manipulation.
- Hardware: A conventional laptop is adequate for preliminary tasks, with optional GPU access to enhance training efficiency.
- Dataset: The publicly accessible credit card fraud detection dataset from Kaggle.
- Expertise: Fundamental understanding of machine learning and data analysis, which can be enhanced through online courses throughout the project.

8. References

- [1] Mienye, Ibomoie Domor, and Nobert Jere. "Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions." *IEEE Access* (2024).
- [2] Berhane, Tesfahun, et al. "A Hybrid Convolutional Neural Network and Support Vector Machine-Based Credit Card Fraud Detection Model." *Mathematical Problems in Engineering* 2023.1 (2023): 8134627.
- [3] Abd El Naby, Aya, Ezz El-Din Hemdan, and Ayman El-Sayed. "Deep learning approach for credit card fraud detection." *2021 International conference on electronic engineering (ICEEM)*. IEEE, 2021.
- [4] Al Balawi, Salwa, and Njood Aljohani. "Credit-card Fraud Detection System using Neural Networks." *International Arab Journal of Information Technology (IAJIT)* 20.2 (2023).
- [5] Sulaiman, Sumaya S., Ibraheem Nadher, and Sarab M. Hameed. "Credit Card Fraud Detection Using Improved Deep Learning Models." *Computers, Materials & Continua* 78.1 (2024).
- [6]https://www.researchgate.net/publication/340968896_Credit_Card_Fraud_Detection_Based_on_Machine_and_Deep_Learning
- [7] https://dl.futuretechsci.org/id/eprint/100/1/12021-Article%20Text-43381-2-10-20250212.pdf?utm_source=chatgpt.com
- [8]https://www.researchgate.net/publication/378583709_Enhancing_Credit_Card_Fraud_Detection_A_Neural_Network_and_SMOTE_Integrated_Approach
- [9] Javad Forough, Saeedeh Momtazi, Ensemble of deep sequential models for credit card fraud detection, *Applied Soft Computing*, Volume 99, 2021, 106883, ISSN 1568-4946, <https://doi.org/10.1016/j.asoc.2020.106883>. (<https://www.sciencedirect.com/science/article/pii/S1568494620308218>)