

Project Proposal

Detecting Financial Fraud Using Artificial Intelligence: An Applied Study Based on Credit Card Transactions

mohameed mushahhin alatwi

Master's Student, Department of Artificial Intelligence

Midocean University

1. Project Overview

The quick development of online financial transactions has revolutionized the international business allowing comfort and accessibility. This growth has however enhanced the rate and complexity of fraudulent monetary practices especially on credit cards transactions. The report by Self Financial. (2024) has actually noted that over 32 billion dollars have been lost globally as a result of credit card fraud in 2022, and thus, there is a need to have effective detection systems that would help to detect and stop this vice. Although such traditional systems based on rules are frequently utilized by banks and related financial organizations, they do not always identify new trends of fraud because they are not dynamic and cannot be modified to meet the new trends of fraudsters (Avasthi & Varsha, 2024).

The proposed project will involve the creation of a machine learning (ML)-based fraud detector model using artificial intelligence (AI) algorithms to determine a transaction as a fraud or valid. It will focus on using the publicly available data, namely, the Credit Card Fraud Detection Dataset on Kaggle, to train and test the performance of different AI algorithms in identifying anomalies in a piece of transaction data.

The importance of the project is that it can make a contribution to academia and industry. Financial fraud detection has been a foundation of cyber defense in the banking system and AI application of fraud detection can be dynamic and scalable to deal with new forms of frauds (Dayyabu et al. ,

2023). Through highly sophisticated algorithms like the Logistic Regression, Random Forest and the Artificial Neural Networks (ANNs), the paper seeks to generate a comparative analysis that identifies the most successful algorithm to detect financial fraud.

In the end, the given project will help create a reliable AI system that will improve the financial cybersecurity, minimize losses, and reinforce the strategies of the institutional risk management. Besides, it will give information to financial regulators and policymakers about the ethical and practical implementation of AI in sensitive financial decision-making situations.

2. Project Goal

The primary objective of the given project is to develop, deploy, and test an artificial intelligence system that is able to identify financial fraud cases in credit card transactions, based on supervised machine learning methods.

In particular, the project will seek to:

1. Create predictive algorithms that are effective to differentiate fraudulent and genuine credit card transactions based on real-life financial information.
2. Compare the results of various machine learning models such as Logistic Regression, Random Forest and Artificial Neural Networks and decide which one offers the best detection and generalization.
3. Solve the problem of unbalanced datasets, which is typical of fraud detection, with the help of Synthetic Minority Oversampling Technique (SMOTE) or random undersampling.
4. Assess the interpretability and reliability of the models, so that the AI-based decisions may be legitimized and trusted by financial institutions.
5. Present suggestions on how AI models can be incorporated into the current Financial sector fraud management systems.

The overall expected results would be a complete model assessment framework and prototype of a fraud detection tool which can be customized by banks and financial institutions to enhance their real-time fraud detection and secure their transactions.

3. Approach

3.1 Data Collection

The main dataset that will be used in this project is the Credit Card Fraud Detection Dataset found on Kaggle. This data includes 284,807 transactions, and among them, there are 492 fraudulent transactions. Every transaction is represented with 30 features, the majority of them being numerical and anonymized due to the need in confidentiality (European cardholder data, September 2013). The criterion variable, which is Class is a binary variable with 1 being fraud and 0 a legitimate transaction.

The data is suitable to the study since it is realistic, highly skewed and publicly tested. This dataset has been used in similar studies, including those by Aayush et al. (2025), Asha & Kumar (2021), among others, which is why this dataset provides a strong empirical basis to this project.

3.2 Data Processing

Quality and consistency of the data will be maintained using data preprocessing steps before training the AI models. The major steps include:

- Data cleaning: It involves the elimination of missing or duplicate data to avoid bias.
- Scaling of features: normalisation of features to make the algorithm efficient.
- Dealing with imbalance: The use of SMOTE or undersampling to balance out the data. Data imbalance is an important issue to handle in order to enhance recall and false negatives in fraud detection, as pointed out by Avasthi & Varsha (2024).
- Selection of features and data reduction: The use of Principal Component Analysis (PCA) in order to minimize redundancy and the cost of computation.

These preprocessing steps are not exclusive to the best practices described in literature (Nandita and Mangal, 2024; Zhinin-Vera, 2020), which guarantees the robustness and generalizability of the model.

3.3 Model and Method Selection

The project will involve the application and comparison of several supervised machine learning algorithms that have been popularly known to perform well in anomaly detection:

- Logistic Regression (LR):

A baseline classification algorithm with interpretable and probabilistic results. It is a simple algorithm, although is effective at detecting patterns that are linearly separable (Aayush et al., 2025).

- Random Forest (RF):

An ensemble method that is powerful and plays with a combination of decision trees to enhance accuracy and minimize overfitting. Random Forest has recorded excellent results in fraud detection because it is capable of achieving nonlinear associations and variable interactions (Aayush et al., 2025).

- Artificial Neural Network (ANN):

An artificial intelligence model that can detect multifaceted nonlinear fraud patterns on high volumes of data. ANNs also simulate the human mind and work especially well with high-dimensional and large-scale financial data (Asha & Kumar, 2021; Habibpour et al., 2023).

All the models will be trained with 70 percent of the data and tested with 30 percent of the data. Based on Aayush et al. (2025), hyperparameter tuning will take place in the form of GridSearchCV to optimize learning rate, batch size, and estimators number.

3.4 Testing and Evaluation

The following metrics will be used in measuring model performance:

- Accuracy: summative correctness of predictions of the model.

- Precision: This is the proportion of the actual positive predictions compared to the overall positive predictions.
- Recall (Sensitivity): Testes the ability of the model to portray genuine cases of fraud.
- F1-score: Precision and recall are equalized and balancing F1-score.
- AUC-ROC Curve: Potential trade-off between the true positive rate and the false positive rate.

False negatives are minimized in fraud detection, which means that recall and AUC will be of priority. The established methodology by Pradeep Kumar and Eshwar (2020) will be used in the evaluation process because the authors consider the three success indicators of accuracy, interpretability, and scalability.

Also, the methods of uncertainty quantification (UQ) will be examined, as Habibpour et al. (2023) propose, to increase the reliability of the model by evaluating the level of prediction confidence.

4. Project Steps and Timeline

Phase	Activities	Timeline	Expected Output
Phase 1: Literature Review & Dataset Acquisition	Collect relevant studies, acquire Kaggle dataset, define variables	Weeks 1–2	Comprehensive literature framework
Phase 2: Data Preprocessing	Clean data, handle imbalance, feature scaling and selection	Weeks 3–4	Clean and balanced dataset
Phase 3: Model Development	Implement LR, RF, and ANN models	Weeks 5–7	Trained models with preliminary results
Phase 4: Model Evaluation	Evaluate models using metrics; optimize performance	Weeks 8–9	Comparative analysis and performance charts
Phase 5: Uncertainty Analysis	Apply UQ and interpret model trustworthiness	Week 10	Confidence-based fraud detection insights

Phase 6: Reporting	Final Document results, conclusions, and recommendations	Weeks 11–12	Complete project report and presentation
------------------------------	--	----------------	--

5. Expected Results

It is expected that the project will lead to the following major outcomes:

- Improved Accuracy in Fraud Detection:

The proposed system should outperform the conventional rule-based systems in terms of recall and F1-scores because it will utilize ensemble and deep learning techniques (Avasthi and Varsha, 2024).

- False Negatives will be reduced:

Even when financial institutions are willing to make a slight increase in false positives, they usually focus on reducing undetected fraudulent transactions. The AI models developed by optimizing are supposed to accomplish this trade-off (Aayush et al., 2025).

- Improved Interpretability:

The comparative approach will allow determining which models offer not only the highest degree of accuracy but also the most explainable form, which is prerequisite in relation to the regulations (Pradeep Kumar & Eshwar, 2020).

- Reliable and Ethical AI Implementation:

As proposed by Habibpour et al. (2023), the model will be designed to incorporate uncertainty quantification to make sure that the model does not make overconfident forecasts, which will be part of the trusted AI applications in the financial sector.

- Generalizable Framework:

The results will be used as a basis of future research in the field of AI-based cybersecurity both in terms of financial fraud and other types of cybercrime detection.

6. Resources Needed

This project will be impossible to complete successfully without a blend of computational tools, data resources, and the help of an expert.

6.1 Hardware and Software:

- GPU training environment or a cloud-based high-performance workstation.
- Programming language Python 3.10 with additional libraries, including TensorFlow and Scikit-learn, Pandas, NumPy, and Matplotlib.
- Jupyter notebook to experiment and visualize.

6.2 Datasets:

- Kaggle Credit Card Fraud Detection Dataset

6.3 Academic and Expert Support:

- Advice by AI and data science managers with focus on machine learning and cybersecurity.
- Literature reviews (IEEE Xplore, ScienceDirect, SpringerLink) scholarly databases.

All these resources will ensure that the project is scientifically rigorous, reproducible, and is ethical.

7. References

- Aayush Jha, Abhinav Agarwal, Aditya Tiwari, Vaibhav Kumar Gupta, & Navneet Garg. (2025). *Leveraging Machine Learning Algorithms for Robust Credit Card Fraud Detection: A Performance Comparison*. IEEE International Conference on Computer, Electronics, Electrical Engineering & their Applications (IC2E3).
- Asha, R. B., & Suresh Kumar, K. R. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings*, 2(1), 35–41. <https://doi.org/10.1016/j.gltp.2021.01.006>
- Avasthi, N., & Varsha, M. (2024). Detecting credit card fraud using machine learning. *International Journal of Creative Research Thoughts (IJCRT)*, 12(4), 1–8.
- Dayyabu, Y., Arumugam, D., & Balasingam, S. (2023). The application of artificial intelligence techniques in credit card fraud detection: A quantitative study. *E3S Web of Conferences*, 389, 07023. <https://doi.org/10.1051/e3sconf/202338907023>
- Habibpour, M., Gharoun, H., Mehdipour, M., Tajally, A. R., Asgharnezhad, H., Shamsi, A., Khosravi, A., & Nahavandi, S. (2023). Uncertainty-aware credit card fraud detection using deep learning. *Engineering Applications of Artificial Intelligence*, 123(A), 106248. <https://doi.org/10.1016/j.engappai.2023.106248>
- Pradeep Kumar, D., & Eshwar, D. (2020). Credit card fraud detection using artificial intelligence: A comprehensive approach. *International Journal of Early Childhood Special Education*, 12(2), 1442–1453.
- Self Financial. (2024, January 15). *Credit card fraud statistics: 2024 global report*. Retrieved October 24, 2025, from <https://www.self.inc/info/credit-card-fraud-statistics/>
- Zhinin-Vera, L. (2020). *Credit Card Fraud Detection using Artificial Intelligence*. ResearchGate. <https://doi.org/10.13140/RG.2.2.13642.18885>