

**Department of Electrical and Computer Engineering**

EECE 490 – Introduction to Machine Learning

Project Report

Credit Card Fraud Detection Using ML

Abdellatif Itani

Abdullah Itani

Mohammed Omar Mkhallati

# **Abstract**

Financial fraud is a growing issue, projected to cost up to $10.5 trillion annually by 2025. Our project addresses this problem by developing a robust fraud detection system using machine learning (ML) techniques. We utilized a feed-forward neural network model trained on an anonymized credit card transaction dataset. The methodology included advanced preprocessing steps such as scaling transaction amounts, addressing severe class imbalance using the Synthetic Minority Over-sampling Technique (SMOTE), and splitting the dataset into training and testing subsets. Our neural network architecture, optimized through grid search, featured multiple hidden layers with ReLU activation and a sigmoid output for binary classification. Results demonstrate the efficacy of our approach, achieving high accuracy and precision. This paper outlines the problem's motivation, methodology, results, ethical considerations, and future improvements.

# **Motivation and Background**

Financial fraud and cybercrime are currently some of the most prevalent crimes in our digital day and age. There are always new and innovative ways used by criminals to manipulate their way into a person’s bank account, whether it be through hacking, or through social engineering. This is a growing issue with cybercrime expecting to cost up to $10.5 trillion annually by 2025.

Banks and financial institutions face the issue of fraud and cybercrime multiple times, and it is essential to build a strong fraud detection and prevention system in order to counteract any possible malpractice.

Fraud does not only impact the customer, where they lose money that could add up to their entire life savings; it also affects banks heavily since the more people get defrauded for their money, the less they will trust the banks. This causes people to turn to other forms of financial institutions such as crypto, or as were seeing a lot in Lebanon, independent platforms that allow users to deposit and withdraw money with a certain fee (Whish, MyMonty, etc.).

Regardless of which financial institution one might use, there is always a chance of them getting defrauded for their money. There are multiple examples of crypto fraud as well as multiple Ponzi schemes.

Our goal through this project is to develop a system that will use AI and machine learning in order to properly label a transaction as fraud or not. We will use the classic available methods and improve upon them. We will also utilize the customers history of transactions in order to determine whether a transaction is fit with what is usually taking place or if it is an intruder.

# **Methodology**

We started by studying our problem more deeply by looking at datasets on Kaggle and projects that are similar to ours in nature. A common trait in all these projects was the hidden and encoded features they used; this involves AI ethics which we will talk about later on.

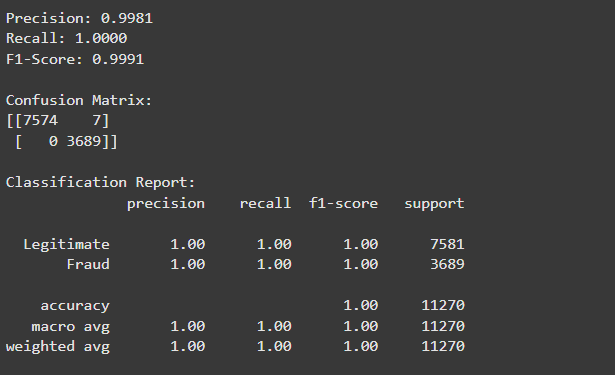
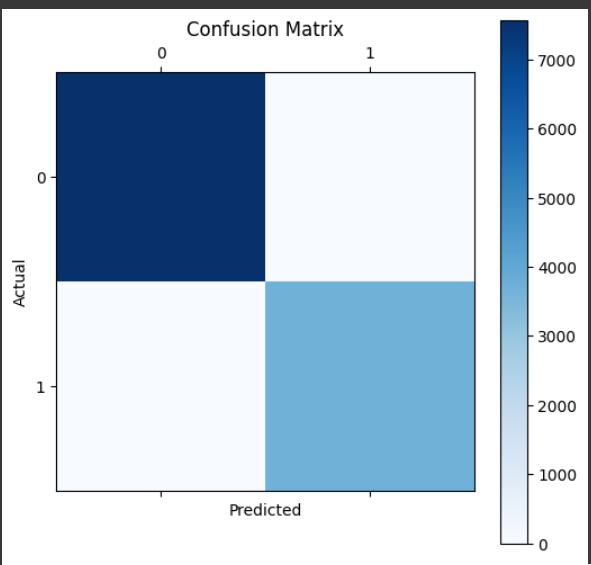
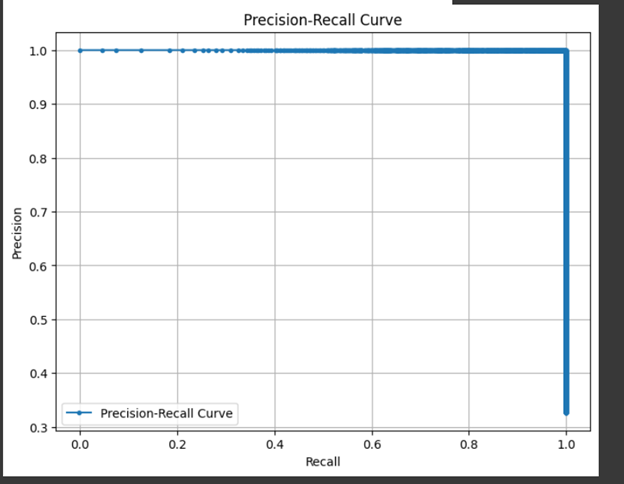
We then started discussing what model we would choose for our project, we immediately ruled out linear regression as it definitely doesn’t meet the requirements of our project. We tested out logistic regression but error was too high, we then moved on to what we all believed would be our best choice which was neural networks, the results were pretty satisfactory, we also tried K-means and random forest after that but implementing a neural network seemed like the best choice (Note that the dataset we used during testing was split into Training, Test and Val).

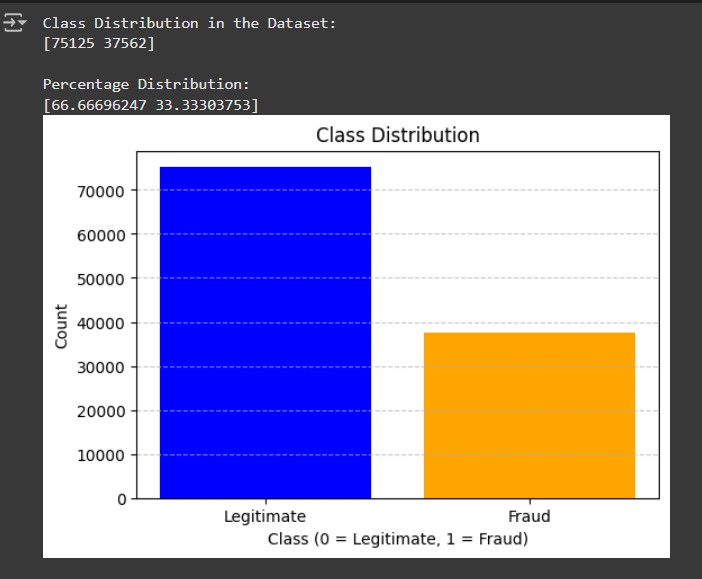
After deciding on our model, we started trying to optimize it, the model uses pattern recognition to classify fraudulent or non-fraudulent meaning our output will be 0 or 1. We balanced the first dataset we found using smote to see how our model would deal with a balanced dataset, we also found a second dataset that has 0.15% fraudulent credit card activity which we also planned on testing. Both datasets were fairly recent, our first being in 2023 but the second in 2013. The reason the discrepancy between the two datasets is high is likely due to the 2013 dataset being a real-world dataset whilst the 2023 one isn’t.

We then added a code to show results for both datasets represented by F1-score, precision, recall, precision-recall curve, all of which will be shown below.

# **Results**

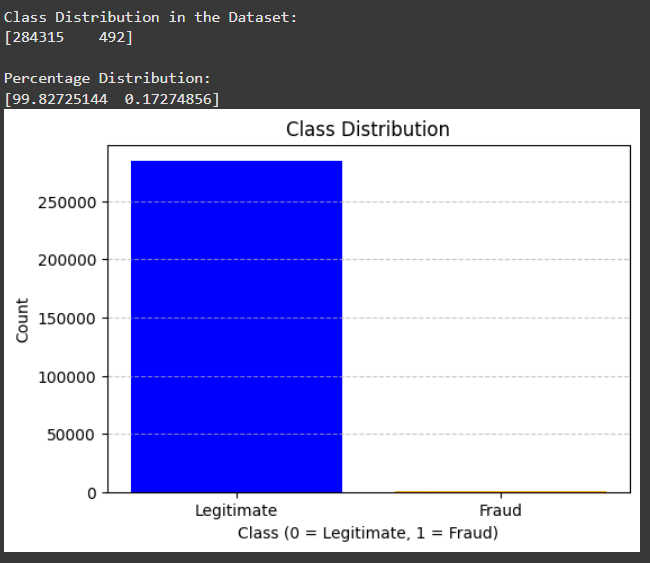
After a series of tests and hours of waiting for datasets to finish training we obtained a series of positive results. The balanced dataset ended up with a high accuracy with training loss decreasing every epoch (note that on Collab we trained using 10 epochs but in reality, we chose to implement 100 epochs).

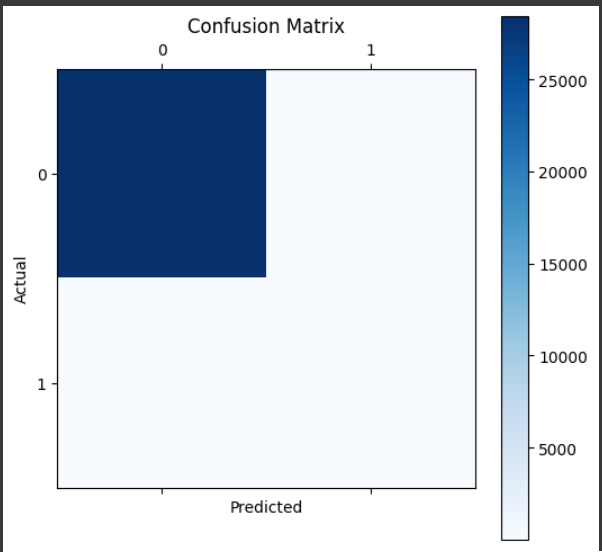
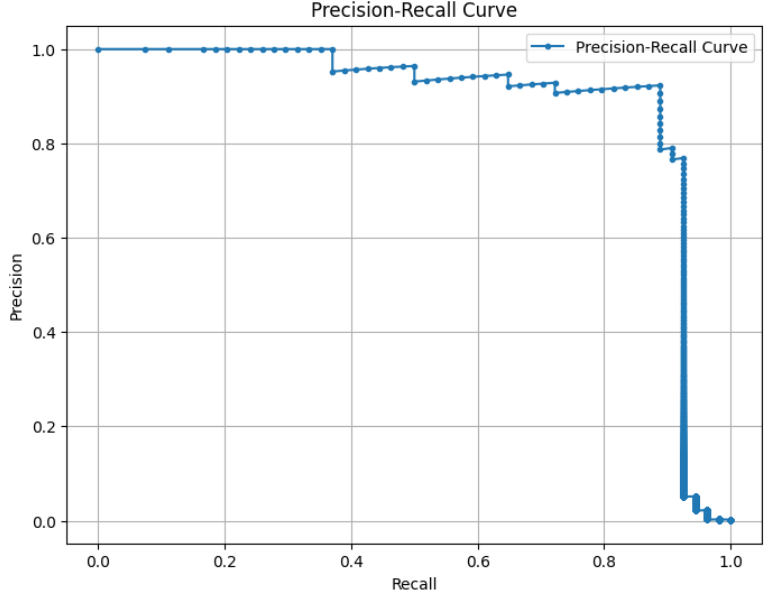
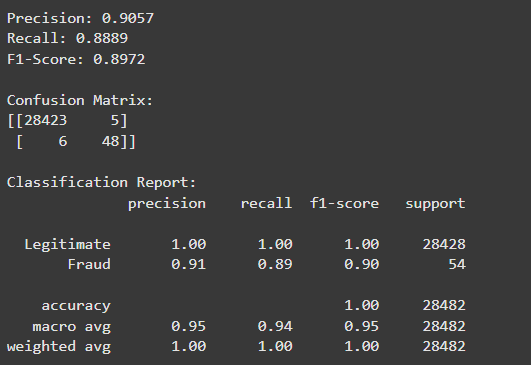


The above results were really good as they accurately predict the test set, they have a high F1-Score along with various positive indicators however the problem is the following:

This dataset is balanced compared to what you would expect from fraud in credit crads, as much as credit cards are the leading case in global fraudulent activity, the number of credit card transactions per year is enormous. This is why we tried out the following dataset even though it is mildly outdated (2013).



We then pivoted to this dataset. You can barely see the yellow line depicting fraud (0.15%)



While the results are fairly good, they are not good enough, our F1-Score must be at least 0.99 for our model to be viable in the real world, however it’s really difficult. We tried adding fraudulent patterns manually but couldn’t due to the hidden nature of the data being used.

# **Ethical Implications**

The use of artificial intelligence (AI) in credit card fraud detection has significant ethical implications that must be addressed to ensure fairness, transparency, and societal trust. One primary concern is the issue of bias in AI models. Fraud detection systems often rely on datasets that are heavily imbalanced, with far fewer fraudulent transactions than legitimate ones. This imbalance can lead to biases in the model’s predictions, where legitimate transactions from certain user groups are disproportionately flagged as fraudulent. Such biases could result in financial inconvenience or reputational damage for individuals unfairly targeted by these systems.

Another critical ethical concern involves data privacy. Fraud detection systems typically require access to sensitive and personal information, including transaction histories and behavioral patterns. While this data is vital for training accurate models, its collection, storage, and use raise questions about consent and security. Customers might not be fully aware of how their data is being utilized or who has access to it, potentially leading to a breach of trust. Furthermore, the risk of data breaches or misuse of this sensitive information by malicious actors adds another layer of ethical complexity. To address this, it is crucial to anonymize data, use encryption techniques, and ensure compliance with stringent data protection regulations like the GDPR.

Transparency and accountability are also significant ethical considerations. Advanced AI models, particularly deep neural networks, often operate as "black boxes," making it difficult to explain why a certain transaction was flagged as fraudulent. This lack of interpretability can frustrate users who are wrongly targeted and make it challenging for institutions to justify the AI's decisions. Furthermore, when errors occur, such as failing to detect fraud or incorrectly flagging legitimate transactions, it becomes difficult to determine accountability. Is the fault with the developers of the AI system, the financial institution using it, or the AI itself? Establishing clear accountability frameworks and incorporating explainability techniques can help alleviate these concerns.

Finally, there is the potential for misuse of AI fraud detection systems. These tools, while designed to combat financial fraud, could be repurposed for invasive surveillance or profiling of individuals, raising ethical questions about the boundaries of their use. Additionally, if the system is compromised by bad actors, it could be used to exploit or manipulate users. These risks necessitate robust security measures and strict regulations to govern how and where such systems can be deployed.

Addressing these ethical implications requires a multifaceted approach, combining technical solutions, legal frameworks, and ongoing ethical oversight. By proactively engaging with these concerns, developers and institutions can create AI systems that not only enhance fraud detection but also uphold the values of fairness, transparency, and trust in society.

# **Conclusion and Future Work**

<https://github.com/Alphaman1321/490_Final_Project.git>

Contributions: All members contributed to the project

CCFD is a project that filters out fraudulent transactions in credit cards using a feed-forward neural network. The project achieved very good accuracy when testing on a balanced dataset and an okay accuracy when testing on an imbalanced dataset. Unfortunately, due to various ethical issues we were unable to implement any patterns we wanted to add to our project as all data we found was always encrypted. However, this project really highlights the importance of ethics in AI and how privacy, fairness and transparency are respected.

Future Work:

While the project achieved promising results, there are several areas where improvements and expansions could significantly enhance the system’s effectiveness and applicability. Most important is improving the model's performance on highly imbalanced real-world datasets. This could involve experimenting with advanced machine learning techniques, such as hybrid approaches that combine supervised and unsupervised learning.

Additionally, getting our hands on a dataset that is not encrypted and is diverse whilst being up-to-date can really help us figure out what models we should use and can help us mimic the complexities of actual fraudulent scenarios. Data augmentation techniques could also be employed to artificially generate realistic fraudulent transactions, further enhancing the model's training.

Ethical and transparency concerns remain a critical focus for future work. Incorporating explainability frameworks, such as SHAP or LIME, can make the model’s decisions more interpretable for both users and auditors. This transparency is particularly important in scenarios where incorrect classifications could lead to financial inconvenience or customer dissatisfaction. Additionally, ensuring that the system complies with legal standards for data privacy and security, such as GDPR, will further reinforce its ethical standing.

Finally, deploying the model in a real-time environment and testing its performance under high transaction volumes would be a pivotal step forward. Simulating large-scale usage will help uncover practical limitations and guide optimizations for real-world deployment. Collecting feedback from end-users and financial institutions during this phase can provide valuable insights for iterative development. By addressing these aspects, the system can evolve into a highly effective, scalable, and ethically responsible tool for combating financial fraud globally.

# **References**

1. [Chawla et al. 2002] Chawla, N. V.; Bowyer, K. W.; Hall, L. O.; and Kegelmeyer, W. P. 2002. SMOTE: Synthetic Minority Over-sampling Technique. *Journal of Artificial Intelligence Research* 16:321–357.
2. [Kingma and Ba 2014] Kingma, D. P., and Ba, J. 2014. Adam: A Method for Stochastic Optimization. *arXiv preprint* arXiv:1412.6980.
3. [Pedregosa et al. 2011] Pedregosa, F.; Varoquaux, G.; Gramfort, A.; Michel, V.; Thirion, B.; Grisel, O.; Blondel, M.; Prettenhofer, P.; Weiss, R.; Dubourg, V.; Vanderplas, J.; Passos, A.; Cournapeau, D.; Brucher, M.; Perrot, M.; and Duchesnay, E. 2011. Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research* 12:2825–2830.
4. [Lundberg and Lee 2017] Lundberg, S. M., and Lee, S. I. 2017. A Unified Approach to Interpreting Model Predictions. In *Advances in Neural Information Processing Systems*, 4768–4777.
5. [He and Garcia 2009] He, H., and Garcia, E. A. 2009. Learning from Imbalanced Data. *IEEE Transactions on Knowledge and Data Engineering* 21(9):1263–1284.
6. [LeCun et al. 2015] LeCun, Y.; Bengio, Y.; and Hinton, G. 2015. Deep learning. *Nature* 521(7553):436–444.
7. [Ribeiro et al. 2016] Ribeiro, M. T.; Singh, S.; and Guestrin, C. 2016. Why should I trust you? Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 1135–1144.
8. [Kaggle 2023] Kaggle. 2023. Credit Card Fraud Detection Dataset. Available at: <https://www.kaggle.com/datasets>.