University of Toronto
ECE496 Project Proposal

Credit Card Fraud Detection

Team Number: 2022524

Supervisor: Zeb Tate

Shadman Kaif, Abdurrafay Khan, Krutarth Patel, Shanthosh Sivayogaligam

Executive Summary

Recently, e-commerce has seen tremendous growth similar to transaction trends using borrowed funds from credit cards. With more transactions being processed by the bank, an increased number of legitimate transactions are classified as fraudulent. It has been reported that banks have a false positive rate of above 90% in some cases. With over $118 billion being lost in revenue due to false positives in 2014, the impact on banks and businesses is only going to get worse in the near future if fraud detection methods are not improved. Ensemble learning, a machine learning (ML) method, has been proven to be effective in other areas of detection such as malware and detecting spam posts on platforms such as Twitter. Using this proven method as a basis, the design team will focus on implementing an ensemble ML algorithm that will minimize the number of false positives down to 20-30% benefitting both banks and merchants alike.

The final product will allow financial institutions to implement this fraud detection model in the backend of their system where they would only need to input transaction details and receive flags for potential fraudulent ones. Artificial Intelligence (AI) models such as bagging, high confidence and majority voting will be built by the team but open-source code and datasets will be used to accelerate the development of an ensemble model. A successful model will meet the objectives of a 95% accuracy in identifying fraud as well as processing 65,000 transactions per second. Constraints include being limited to simulated transaction data for privacy and security reasons as well as not being able to process real-time data without a history of transactions for the model to learn from. The team's timeline from here is to complete the model by mid-November and begin training with the goal to have a working prototype by the end of November. These internal deadlines provide adequate time to complete those tasks. Due to the ease of software accessibility this project will not require financial

Motivation

With consumers shifting towards e-commerce, it is important that transaction processing standards are improved. From 2019 to 2020, the US Census Bureau Annual Retail Trade Survey reported that there was roughly a 43% increase in e-commerce sales [1]. During the same time, the credit card payment market has seen an increasing trend and is expected to grow roughly 7.4% annually over the course of the next 5 years [2]. With clear indications of a growing trend in consumer habits and credit card usage, it is imperative that banks are able to authenticate and approve genuine transactions and accurately reject those that could be fraudulent. Today, credit card companies use a mix of machine learning (ML) models and algorithms to evaluate and classify purchases that are likely to be fraudulent [3]. Even with such protocols in place, in 2014, $118 billion was lost in legitimate sales due to false positives [3]. The overwhelming money lost due to false positives makes it clear that a new way to minimize them would

lead to better profit margins for credit card companies and merchants. Considering that ML is currently employed in the industry, expanding on that work and using ensemble learning can be a solution. AdaBoost the current state of the art has shown only an 83% accuracy when distinguishing between fraudulent and legitimate transactions [4]. Ensemble learning showed promising results in other markets such as malware detection and detecting spam twitter posts [5][6]. The lack of testing with ensemble learning in the credit card industry leaves the question of how well can they work to solve the issue of false positives.

Problem Statement

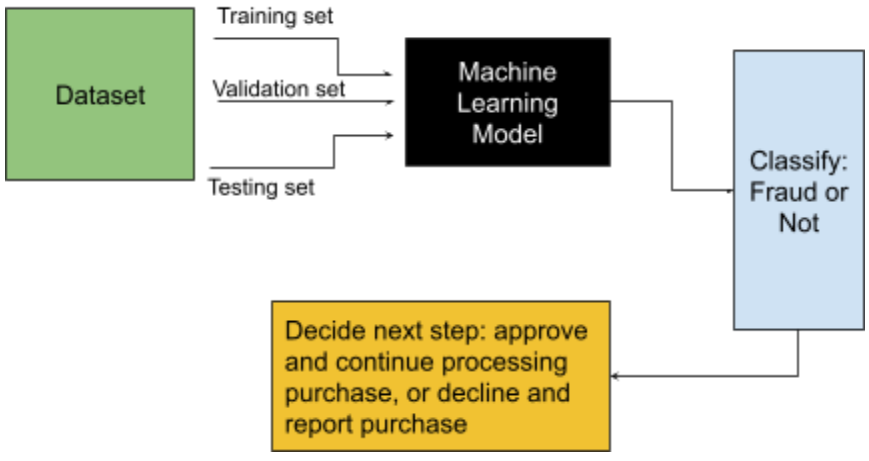
False positives among credit card transactions are a major issue amongst financial institutions; research shows that many banks have a false positive rate above 90% [7]. As a result, legitimate transactions are declined for being suspicious or fraudulent, reducing the revenue of banks and merchants alike.

Project Goal

The goal of this project is to create a linearly classifiable ensemble ML algorithm that minimizes the number of false positives to at least 20-30% [3] in a credit card dataset.

Scope of Work

The problem here lies with the banks and credit card companies dealing with their current systems flagging legitimate transactions as fraudulent. For this project, the team will develop individual AI models that will be used together for ensemble learning which will be the final product. Online open-source code will be used from existing ensemble models, from different applications, to accelerate the learning process. Further, due to privacy concerns, the team will not collect unique data on credit card transactions but instead use an online dataset with the required information [8]. The idea is that the final model will be operated on the backend of banking systems where the inputs will be real transactions and the output would be the flagging of suspicious sales. Suspicious sales will then be processed by the banks and are not within the scope of this project.



Requirements Specification

Functions

The project's major task is to detect fraudulent credit card transactions using ensemble learning. Primary functions correspond to this functional basis while secondary functions were generated as a result.

Primary	Detect fraudulent credit card transactions using ensemble learning
Secondary	Use bagging, high confidence, and majority voting ML models

Objectives

Table below outlines aspects the team must consider when measuring the success of possible solutions.

No.	Objectives: Should	Metric	Goal
1	Minimize the amount of false positives	False Positives (%)	20-30% [3]
2	Be accurate	Model Accuracy (%)	95% [9]
3	Processing speed	Speed (transactions/s)	65,000 [10]

Constraints

Table below shows project limitations based on the gap and certain codes/regulations within financial institutions.

Constraint:	Type	Reasoning
Model cannot make a prediction for a real-time transaction when the transaction does not have historical data	Functional	There must be a sequence length for our model to base previous transactions made by a card in order to predict the next transaction.
No access to real data from credit card companies	Ethical	Financial institutions must adhere to "Protection of Personal Information" [11]. As a result, the design team will resort to a simulated dataset [8].

Conclusion

Financial systems using credit cards require a way to reduce their losses due to fraudulent transactions. It is evident that a large contributor to these losses in profit is from current detection systems having high numbers of false positives. Due to the established success and credibility of ensemble learning in other markets, we plan to implement it as our solution for credit card fraud detection. The success of this design

will be measured through its ability to minimize the false positives to 20-30% and provide banks with a more efficient way to solve this issue.

References

[1] M. Brewster, "Annual Retail Trade Survey Shows Impact of Online Shopping on Retail Sales During COVID-19 Pandemic," *Census.gov*, 26-Apr-2022. [Online]. Available: https://www.census.gov/library/stories/2022/04/ecommerce-sales-surged-during-pandemic.html.

[2] Vantage Market Research, "Global $72+ Bn Credit Card Payment Market is Expected to Grow at a CAGR of over 7.4% During 2022-2028," *GlobeNewswire News Room*, 11-Apr-2022. [Online]. Available:https://www.globenewswire.com/en/news-release/2022/04/11/2419928/0/en/Global-72-Bn-Credit-Card-Payment-Market-is-Expected-to-Grow-at-a-CAGR-of-over-7-4-During-2022-2028-Vantage-Market-Research.html.

[3] F. Wallny, "False Positives in Credit Card Fraud Detection: Measurement and Mitigation," 2022. [Online]. Available: https://scholarspace.manoa.hawaii.edu/.

[4] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," *IEEE Access*, vol. 10, pp. 16400–16407, 2022.

[5] K. N. Khasawneh, M. Ozsoy, C. Donovick, N. Abu-Ghazaleh, and D. Ponomarev, "Ensemble learning for low-level hardware-supported malware detection," *Research in Attacks, Intrusions, and Defenses*, pp. 3–25, 2015.

[6] S. Liu, Y. Wang, J. Zhang, C. Chen, and Y. Xiang, "Addressing the class imbalance problem in Twitter spam detection using Ensemble Learning," *ScienceDirect*, 13-Dec-2016. [Online]. Available: https://reader.elsevier.com/reader/sd/pii/S0167404816301754?token=39F0203C8C0EBCE1DCDE4495D153A4678D27E055F52E742164DF963E5A26E2FE66C0291FB67B1909BA70F32E70EABD4D&originRegion=us-east-1&originCreation=20220923030108.

[7] D. Holmes, "The Real Costs of False Positives for Banks," *Feedzai*, 16-May-2022. [Online]. Available: https://feedzai.com/blog/the-real-costs-of-false-positives-for-banks.

[8] K. Shenoy, "Credit Card Transactions Fraud Detection Dataset," *Kaggle*, 05-Aug-2020. [Online]. Available: https://www.kaggle.com/datasets/kartik2112/fraud-detection?select=fraudTrain.csv.

[9] R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of Machine Learning Approach on credit card fraud detection," *Human-Centric Intelligent Systems*, vol. 2, no. 1-2, pp. 55–68, 2022.

[10] "Visanet: Global Electronic Payment Network," *Visa*. [Online]. Available: https://www.visa.ca/en_CA/about-visa/visanet.html.

[11] "Protection of Personal Information," *Bank of Canada*. [Online]. Available: https://www.bankofcanada.ca/privacy/protection-of-personal-information/.