Comparison of Classification Techniques for Fraud Detecting Among Credit Card Transactions

Designed, Implemented and Presented by:

Iymen Abdella 40218280

Maryam Hatami 40254179

Sepehr Seifpour 40197899

Saeed JamaliFashi, 40093292

December 23, 2022

INTRODUCTION:

Every day the impact of fraud in the lives of regular citizens and private companies increases. In the domain of fraud, credit cards are a common method for offenders to “steal credit card information or personal identification number and use it without permission” to make illegal purchases, withdraw money, or execute an online transaction. [1] Data from the Federal Trade Commission depicts a worsening trend, as more than 5.7 million incidents of fraud were reported by victims in 2021 in the United States of America. While fraud can appear in many forms, the number one reported category was identity theft which routinely involves credit card information among other forms [2]. With an estimated of $5.9 billion in losses, and continued growth in fraud incidents since 2001, financial institutions are incentivized to invest heavily in solutions that can manage the growing influx of criminal activity.

Machine Learning is a domain that is rapidly producing new solutions that can detect fraudulent activity by considering historical activity. Our report will examine four commonly used models for classifying transactions as fraudulent or benign by training on a supervised data set of transactions with 29 features. Our design is a conformable approach to better understand the foundational elements involved with solving a problem of this caliber. Our intent with this report is to experiment with different models and determine their efficacy by analyzing key metrics such as: accuracy, precision, and recall. Once we have an objective grasp of the strengths of these models, we can elaborate on more complex models that can hopefully produce more promising results.

RELATED WORKS:

GAUSSIAN MIXTURE MODELS

SVM

NAÏVE BAYES

LOGISTIC REGRESSION

RESULTS

In Figure 1 we display our accuracy results for each of the models. The top row is the ratio of data sampled from class 1 relative to class 0. We noticed our dataset was heavily imbalanced so varying the sample size had an impact on the learning ability of each of the models, and overall Performance.

Similarly, in Figure 2 and Figure 3 display the recall and precision of the models, and how sample size influenced test performance.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1:1 | 1:10 | 1:100 | 1:1000 | Total Set |
| Gaussian Mixture Model | 64 | 61 | 64 | 60 | 31 |
| SVM | 94 | 98 | 100 | 100 | 100 |
| Naïve bayes (Gaussian) | 89 | 96 | 97 | 98 | 98 |
| Logistic Regression | 95 | 98 | 100 | 100 | 100 |

Figure : Test Accuracy Score for all models in %

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1:1 | 1:10 | 1:100 | 1:1000 | Total Set |
| Gaussian Mixture Model | 20 | 68 | 93 | 82 | 90 |
| SVM | 91 | 82 | 83 | 72 | 81 |
| Naïve bayes (Gaussian) | 80 | 81 | 83 | 74 | 85 |
| Logistic Regression | 94 | 84 | 82 | 50 | 63 |

Figure : Test Precision Score for all models in %

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1:1 | 1:10 | 1:100 | 1:1000 | Total Set |
| Gaussian Mixture Model | 100 | 15 | 3 | 0 | 0 |
| SVM | 96 | 98 | 98 | 100 | 99 |
| Naïve bayes (Gaussian) | 95 | 76 | 27 | 3 | 7 |
| Logistic Regression | 95 | 94 | 97 | 78 | 88 |

Figure : Test Recall Score for all models in %

REFERENCES:

1. F. C. A. of Canada, “Government of Canada,” *Canada.ca*, 29-Aug-2022. [Online]. Available: https://www.canada.ca/en/financial-consumer-agency/services/credit-fraud.html. [Accessed: 21-Dec-2022].

2. C. S. Network , “Federal Trade Commission | protecting America's consumers,” *Consumer Sentinel Network Data Book 2021*, Feb-2022. [Online]. Available: https://www.ftc.gov/system/files/ftc\_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf. [Accessed: 22-Dec-2022].