Credit Card Fraud Detection

A report on Mini Project I (SRS and Design) submitted in partial fulfilment of the requirements for the award of the degree of

Master of Computer Applications

By

SAURABH MISHRA

MCA IV Semester

Roll No.: 14

Enrolment No.:U1875042

Under the Supervisions of

Dr. Mahendra Tiwari

Department of Electronics and Communication

(J K Institute of Applied Physics & Technology)

University of Allahabad

Prayagraj – 211002, India

March, 2019

CANDIDATE'S DECLARATION

I **,Saurabh Mishra** ,hereby certify that the work, which is being presented in the report, entitled **Credit Card Fraud Detection ,** in partial fulfillment of the requirement for the award of the Degree of **Master of Computer Applications** and submitted to the institution is an authentic record of my own work carried out during the period *March-2020* to *October-2020* under the supervision of Dr. Mahendra Tiwari. I also cited the reference about the text(s) /figure(s) /table(s) /equation(s) from where they have been taken.

I declare that I have cited the reference about the text(s) /figure(s) /table(s) /equation(s) from where they have been taken. I further declare that I have not willfully lifted up some other's work, para, text, data, results, etc. reported in the journals, books, magazines, reports, dissertations, thesis, etc., or available at websites and included them in this report/thesis and cited as my own work.

Date:15-April-2021 Signature:

Saurabh Mishra Saurabh Mishra

CERTIFICATE FROM THE SUPERVISOR

This is to certify that Mr. Saurabh Mishra has carried out this project/dissertation entitled **Credit Card Fraud Detection** under my supervision. And the above statement made by the candidate is correct to the best of my knowledge.

Date:

Signature of the Supervisor
Dr. Mahendra Tiwari
(Supervisor)
Seal/Designation

The Viva-Voce examination of *Saurabh Mishra*, M.C.A. V Semester has been held on _____.

Signature of		Signature and seal of
Examiner(s)		Head of the Department

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organisations. I would like to extend my sincere thanks to all of them.

I am highly indebted to Dr. Mahendra Tiwari , for his guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

I would like to express my gratitude towards my parents & member of J.K. Institute of Applied Physics and Technology for their kind co-operation and encouragement which help me in completion of this project.

I would like to express my special gratitude and thanks to industry persons for giving me such attention and time.

My thanks and appreciations also go to my friends in developing the project and people who have willingly helped me out with their abilities.

-Saurabh Mishra

ABSTRACT

Credit card fraud detection is presently the most frequently occurring problem in the present world. This is due to the rise in both online transactions and e-commerce platforms. Credit card fraud generally happens when the card was stolen for any of the unauthorized purposes or even when the fraudster uses the credit card information for his use. In the present world, we are facing a lot of credit card problems. To detect the fraudulent activities the credit card fraud detection system was introduced. This project aims to focus mainly on machine learning algorithms. The algorithms used are random forest algorithm and the Adaboost algorithm. The results of the two algorithms are based on accuracy, precision, recall, and F1-score. The ROC curve is plotted based on the confusion matrix. The Random Forest and the Adaboost algorithms are compared and the algorithm that has the greatest accuracy, precision, recall, and F1-score is considered as the best algorithm that is used to detect the fraud.

It is vital that credit card companies are able to identify fraudulent credit card transactions so that customers are not charged for items that they did not purchase. Such problems can be tackled with Data Science and its importance, along with Machine Learning, cannot be overstated. This project intends to illustrate the modelling of a data set using machine learning with Credit Card Fraud Detection. The Credit Card Fraud Detection Problem includes modelling past credit card transactions with the data of the ones that turned out to be fraud. This model is then used to recognize whether a new transaction is fraudulent or not. Our objective here is to detect 100% of the fraudulent transactions while minimizing the incorrect fraud classifications. Credit Card Fraud Detection is a typical sample of classification. In this process, we have focused on analysing and pre-processing data sets as well as the deployment of multiple anomaly detection algorithms such as Local Outlier Factor and Isolation Forest algorithm on the PCA transformed Credit Card Transaction data.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1 INTRODUCTION

1.1 GENERAL

WHAT IS A CREDIT CARD ?

- A credit card is issued by a credit card provider, like Capital One, and they are designed to pay for things in shops or online.

- You can also use credit cards for balance transfers and taking out cash from an ATM.

- You can use your credit card worldwide as they are accepted in millions of places, There are often fees or charges for using your credit card overseas.

- When you get a credit card you will be given a credit limit. This is the total amount you have available to spend using the credit card.

- You should always leave some available credit on your credit card for any interest to be applied.

Details of all transactions you make will be shown on your statement, along with:

- the minimum amount you must pay
- the date by which your credit card provider must receive at least your minimum payment

If you do not pay off your balance in full each month, you will be charged interest on the amount remaining on your account.

Check your credit card agreement to make sure you know how much you will be charged.

WHAT ARE FRAUDULENT TRANSACTIONS ?

The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

Fraudulent transactions are orders and purchases made using a credit card or bank account that does not belong to the buyer.

One of the largest factors in identity fraud, these types of transactions can endup doing damage to both merchants and the identity fraud victim.

Avoiding fraudulent transactions is in the interest of both merchants and buyers, so it is important to take proper precautions when managing money accounts.

WHAT IS FRAUD DETECTION ?

Fraud detection involves monitoring the behaviour of users in order to estimate, detect, or avoid undesirable behaviour. To counter the credit card fraud effectively, it is necessary to understand the technologies involved in detecting credit card frauds and to identifyvarious types of credit card frauds.

The credit card is a small plastic card issued to users as a system of payment. it allows its cardholder to buy goods and services based on the cardholder's promise to pay for these goods and services. credit card security relies on the physical security of the plastic card as well as the privacy of the credit card number. globalization and increased use of the internet for online shopping has resulted in a considerable proliferation of credit card transactions throughout the world. thus a rapid growth in the number of credit card transactions has led to a

substantial rise in fraudulent activities.

Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card as a fraudulent source of funds in a given transaction. credit card fraudsters employ a large number of techniques to commit fraud. to combat the credit card fraud effectively, it is important to first understand the mechanisms of identifying a credit card fraud. over the years credit card fraud has stabilized much due to various credit card fraud detection and prevention mechanisms

.

1.2 OBJECTIVES

The purpose of this document is to define the requirements of credit card fraud detection. In detail, this document will provide a general description of our project, including user requirements, product perspective, and overview of requirements, general constraints. In addition, it will also provide the specific requirements and functionality needed for this project

- such as interface, functional requirements and performance requirements

Objective of this project is to propose a credit card fraud detection system using genetic algorithm.

Genetic algorithms are evolutionary algorithms which aim at obtaining better solutions as time progresses. When a card is copied or stolen or lost and captured by fraudsters it is usually used until its available limit is depleted.

Thus, rather than the number of correctly classified transactions, a solution which minimizes the total available limit on cards subject to fraud is more prominent. It aims in minimizing the false alerts using genetic algorithm where a set of interval valued parameters are optimized.

1.3 MOTIVATION

Due to the rise and rapid growth of E-Commerce, use of credit cards for online purchases has dramatically increased and it caused an explosion in the credit card fraud. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. Implementation of efficient fraud detection systems has thus become imperative for all credit card issuing banks to minimize their losses.

1.4 PROJECT CATEGORY

MACHINE LEARNING

1.5 TOOLS AND TECHNOLOGIES /PLATFORM REQUIREMENT

following tools are used:

- Jupyter Notebook

following technologies are used:

- Python

Platform Requirement :

Window name	**Architecture**
Windows Xp	32bit,64 bit
Windows 7	32bit,64 bit
Windows 8	32bit,64 bit
Windows 8.1	32bit,64 bit
Windows 10	32bit,64 bit

HARDWARE REQUIREMENTS

- Processor type :Pentium III-compatible processor or faster.
- Processor speed : Minimum: 1.0 GHz, Recommended: 2.0 GHz or faster
- RAM : 4 GB or more
- HARD DISK : 20GB or more
- Monitor : VGA or higher resolution 800x600 or higher resolution
- Pointing device : Microsoft Mouse or compatible pointing device
- CD-ROM : Actual requirements will vary based on system configuration and the applications and features chosen to install.

SOFTWARE REQUIREMENTS

- Front End: Python
- Back End : SQL Server

- Operating System : Windows XP Professional or more
- Browser: Chrome/IE

CHAPTER 2 LITERATURE REVIEW

Fraud detection has been usually seen as a data mining problem where the objective is to correctly classify the transactions as legitimate or fraudulent. For classification problems many performance measures are defined most of which are related with correct number of cases classified correctly.

A more appropriate measure is needed due to the inherent structure of credit card transactions. When a card is copied or stolen or lost and captured by fraudsters it is usually used until its available limit is depleted. Thus, rather than the number of correctly classified transactions, a solution which minimizes the total available limit on cards subject to fraud is more prominent.

Since the fraud detection problem has mostly been defined as a classification problem, in addition to some statistical approaches many data mining algorithms have been proposed to solve it. Among these, decision trees and artificial neural networks are the most popular ones. The study of Bolton and Hand provides a good summary of literature on fraud detection problems.

However, when the problem is approached as a classification problem with variable misclassification costs as discussed above, the classical data mining algorithms are not directly applicable; either some modifications should be made on them or new algorithms developed specifically for this purpose are needed. An alternative approach could be trying to make use of general purpose meta heuristic approaches like genetic algorithms.
Numerous literatures pertaining to anomaly or fraud detection in this domain have been published already and are available for public usage. A comprehensive survey conducted by Clifton Phua and his associates have revealed that techniques employed in this domain include data mining applications, automated fraud detection, adversarial detection. In another paper, Suman, Research Scholar, GJUS&T at Hisar HCE presented techniques like Supervised and Unsupervised Learning for credit card fraud detection. Even though these methods and algorithms fetched an unexpected success in some areas, they failed to provide a permanent and consistent solution to fraud detection.
A similar research domain was presented by Wen-Fang YU and Na Wang where they used Outlier mining, Outlier detection mining and Distance sum algorithms to accurately predict fraudulent transaction in an emulation experiment of credit card transaction data set of one certain commercial bank. Outlier mining is a field of data mining which is basically used in monetary and internet fields. It deals with detecting objects that are detached from the main system i.e. the transactions that aren't genuine. They have taken attributes of customer's behaviour and based on the value of those attributes they've calculated that distance between the observed value of that attribute and its predetermined value.

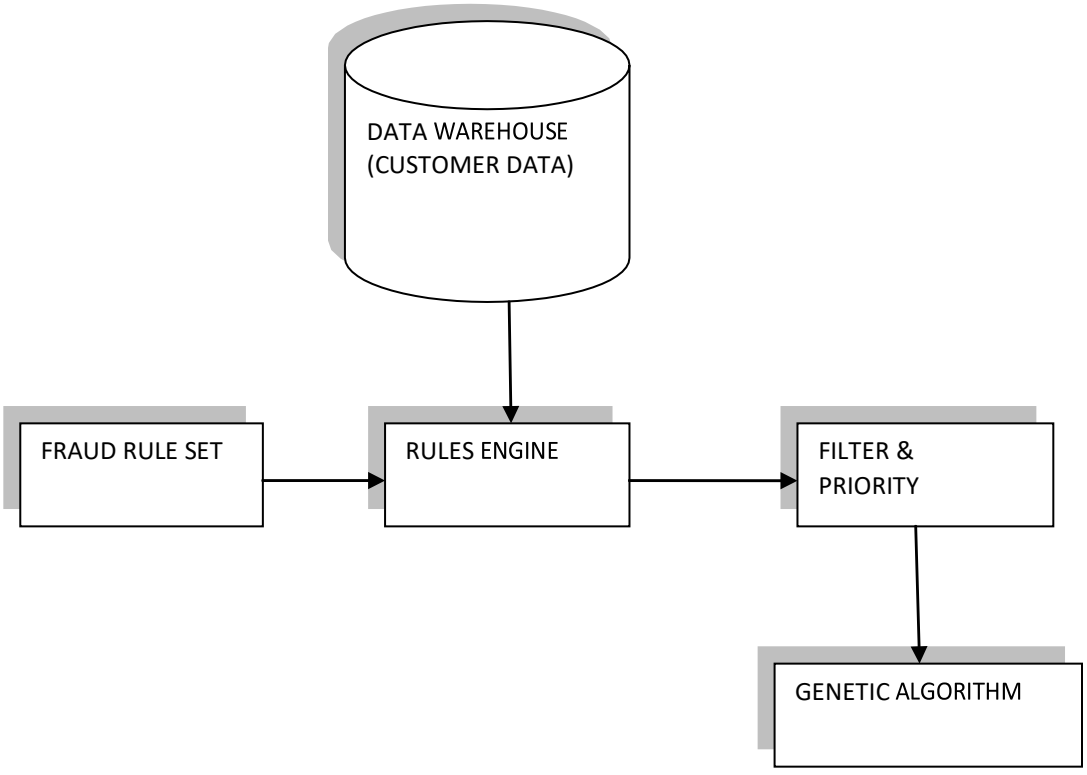
CHAPTER 3 DESIGN DETAILS

3.1 INTRODUCTION

The process of design involves –conceiving and planning out in mind and making a drawing, pattern or a sketch‖. The system design transforms a logical representation of what a given system is required to do into the physical reality during development. Important design factors such as reliability, response time, throughput of the system, maintainability, expandability etc., should be taken into account. Design constraints like cost, hardware limitations, standard compliance etc should also be dealt with. The task of system design is to take the description and associate with it a specific set of facilities-men, machines (computing and other), accommodation, etc., to provide complete specifications of a workable system.

Describing the overall features of the software is concerned with defining the requirements and establishing the high level of the system. During architectural design, the various web pages and their interconnections are identified and designed. The major software components are identified and decomposed into processing modules and conceptual data structures and the interconnections among the modules are identified. The following modules are identified in the proposed system.

SYSTEM ARCHITECTURE



The above architecture describes the work structure of the system.

- The customer data in the data warehouse is subjected to the rules engine which consists of the fraud rule set.
- The filter and priority module sets the priority for the data and then sends it to the genetic algorithm which performs its functions and generates the output.

3.2 REQUIREMENT SPECIFICATIONS

HARDWARE REQUIREMENTS

- Processor type : Pentium III-compatible processor or faster.
- Processor speed : Minimum: 1.0 GHz, Recommended: 2.0 GHz or faster
- RAM : 4 GB or more
- HARD DISK : 20GB or more
- Monitor : VGA or higher resolution 800x600 or higher resolution
- Pointing device : Microsoft Mouse

SOFTWARE REQUIREMENTS

- Front End : Python
- Back End : SQL Server
- Operating System : Windows XP Professional or more
- Browser : Chrome/IE

NON FUNCTIONAL ATTRIBUTES

SECURITY

The project provides a security to different kind of customers by means of authentication level. The authorization mechanism of the system will block the unwanted attempts to the server.

RELIABILITY

The project is guaranteed to provide reliable results for the entire user. The system shall operate 95% of the time. The number of defect should not exceed 10 per function. In addition, before the submission of the final release the calendar must be tested in case of the defects over 10 per function.

USABILITY

- Since GUI interface is used, it can be used by a user.
- Since the system is placed on for online users any type user can use the system.
- The system detects the fraud and reports to the user.

SCALABILITY

The need for scalability has been a driver for much of the technology innovations of the past few years. The industry has developed new software languages, new design strategies, and new communication and data transfer protocols, in part to allow web sites to grow as needed.

MAINTAINABILITY

Maintainability is our ability to make changes to the product over time. We need strong maintainability in order to retain our early customers. We will address this by anticipating several types of change, and by carefully documenting our design and implementation.

3.3 SYSTEM DESIGN

Detailed design deals with the various modules in detail explaining them with appropriate Diagrams and notations. The Use case diagram is designed to see the working logic of the proposed system. The sequence

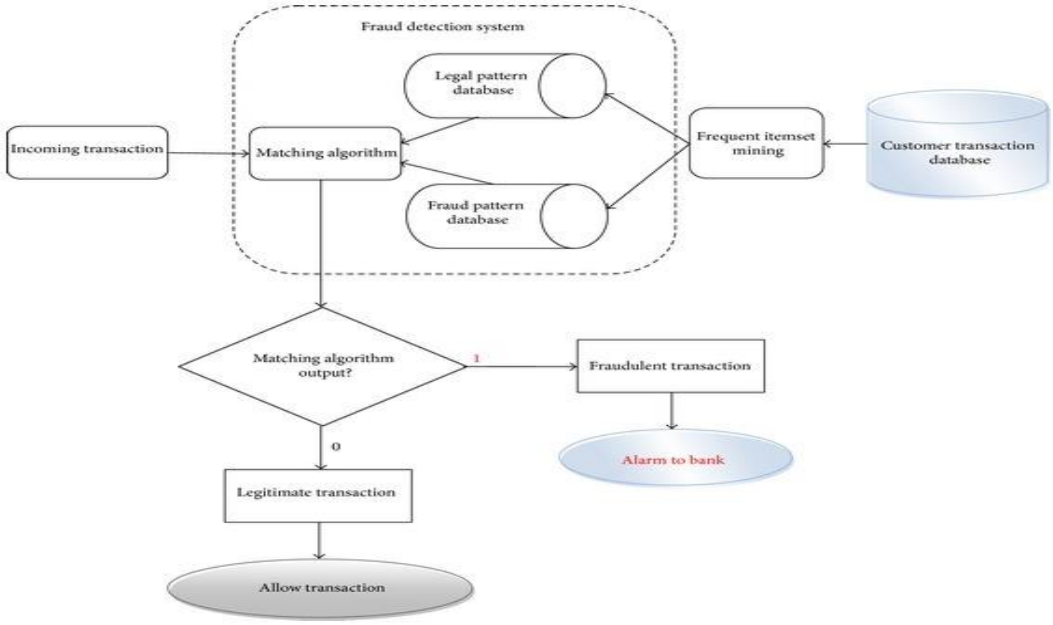
diagram is designed to describe, how the client and the server interacts with each other when processing a content. The flow of the proposed system is described with the activity diagram. We know where the application starts and when it ends after processing the keywords and the current URL link. This will help the programmers to implement the internal logic for the module in the given specification.

In this part of design phase, the design is carried out using the top-down strategy. First the major modules are identified. Then they are divided into sub modules so that each module at the lowest level would address a single function of the whole system. Each module design is explained detail.

This chapter tells us how the input module is design in getting the users requirements. The detailed input design provides as information regarding what are tools used in getting inputs and send to the server.

Output design is gives the user with good interacting option on the screen. The information delivered to the users through the information system. Useful output is essential to ensure the use and acceptance of the information system. Users often judge the merit of a system based upon its output. Productive output can only be achieved via close interaction with users. The output is designed in attractive and effective way that user can access them with a problem .

Figure: Credit Card Fraud Detection Model:

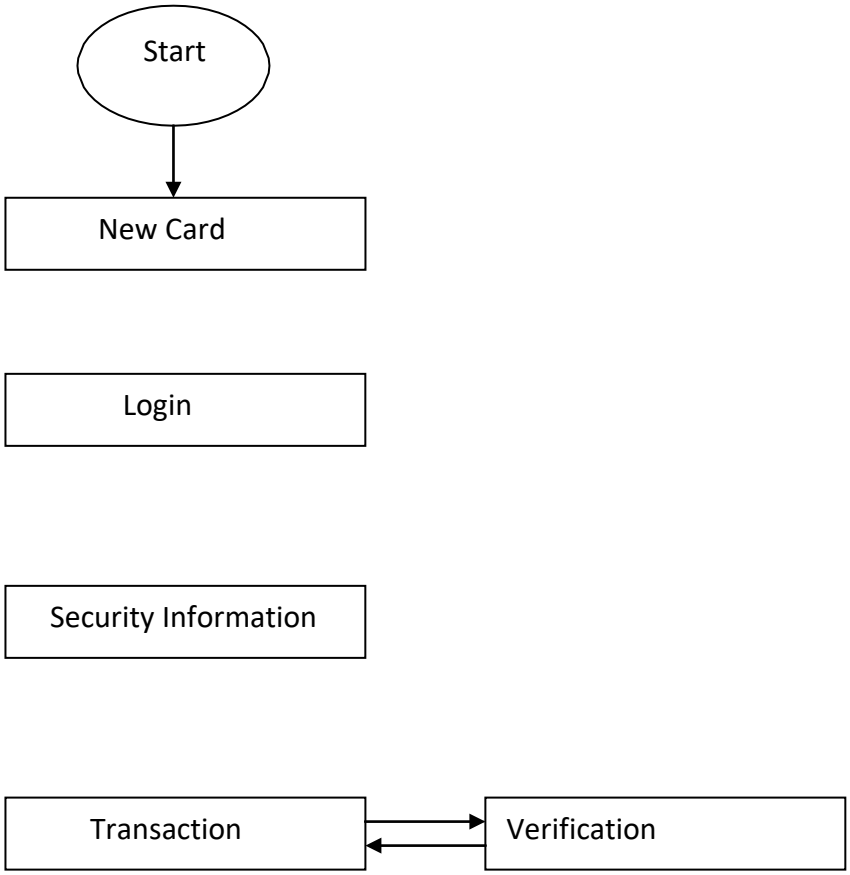


3.3 METHODOLOGY USED

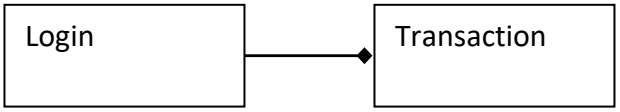
Using genetic algorithm the fraud is detected and the false alert is minimized and it produces an

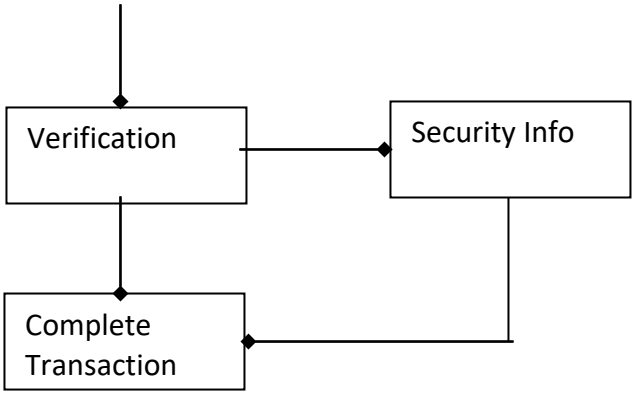
optimized result. The fraud is detected based on the customers behavior. A new classification problem which has a variable misclassification cost is introduced. Here the genetic algorithms is made where a set of interval valued parameters are optimized.

Module diagram

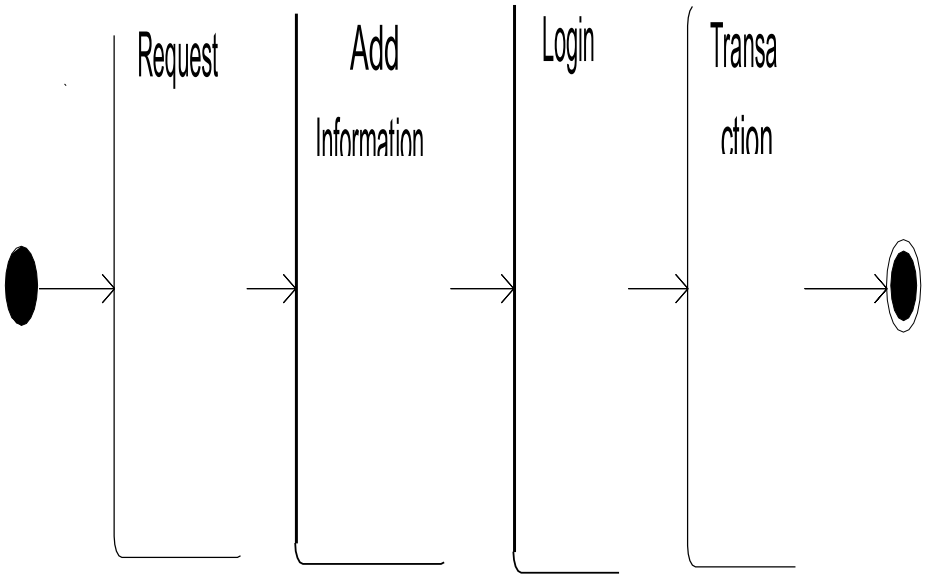


Object diagram

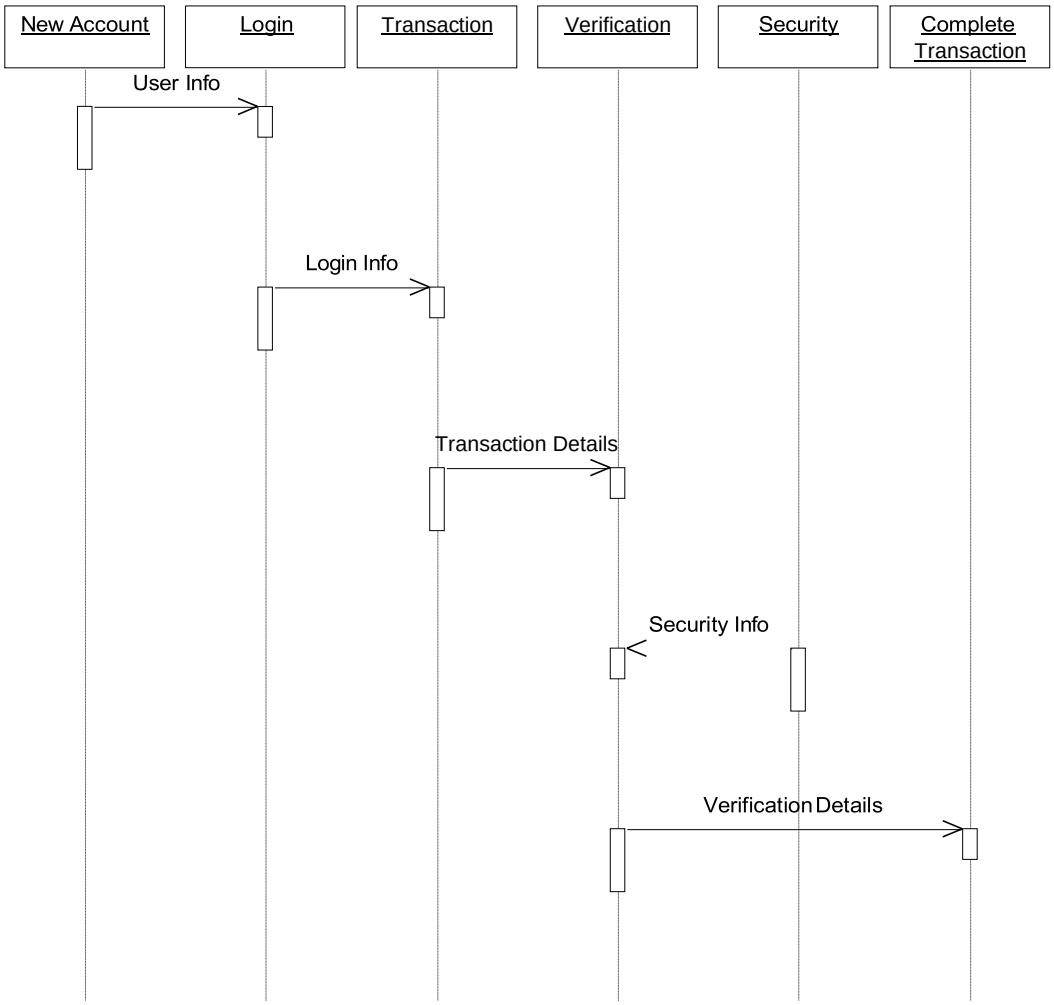




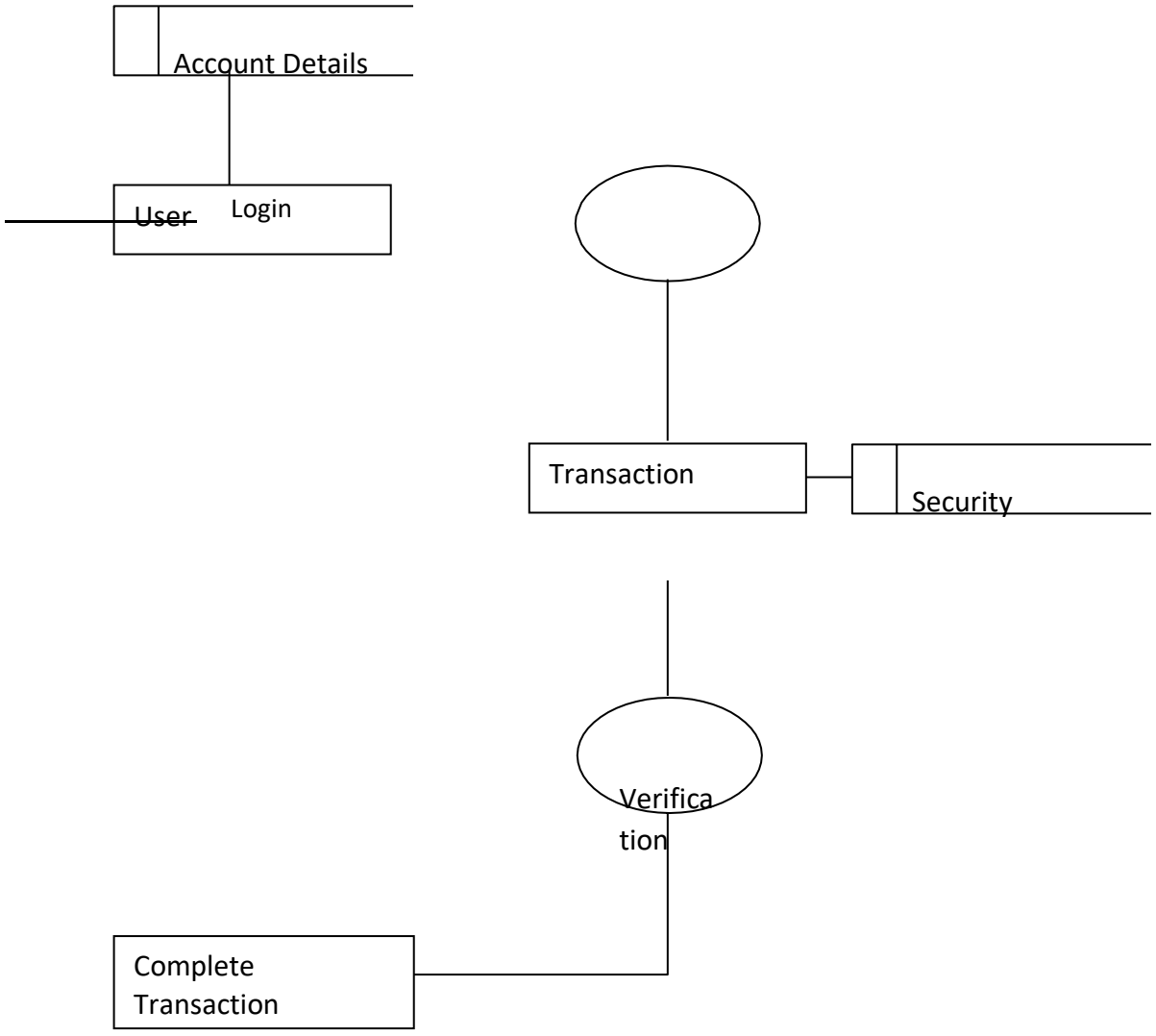
State diagram



Sequence diagram



Dataflow diagram



3.5 ALGORITHM

Genetic algorithm

Genetic algorithms are evolutionary algorithms which aim at obtaining better solutions as time progresses. Since their first introduction by Holland, they have been successfully applied to many problem domains from astronomy to sports, from optimization to computer science, etc. They have also been used in data mining mainly for variable selection and are mostly coupled with other data mining algorithms. In this study, we try to solve our classification problem by using only a genetic algorithm solution.

Pseudo code of genetic algorithm

Initialize the population

Evaluate

initial

population

Repeat

Perform competitive selection

Apply genetic operators to generate new solutions Evaluate solutions in the population

Until some convergence criteria is satisfied.

Selection process

Selection is used for choosing the best individuals, that is, for selecting those chromosomes with higher fitness values. The selection operation takes the current population and produces a ‗mating pool' which contains the individuals which are going to reproduce. There are several selection methods, like biased selection, random selection, roulette wheel selection, tournament selection. In this work the following selection mechanisms are used.

Tournament Selection

Tournament selection has been used in this as it selects optimal individuals from diverse groups. It selects t individuals from the current population uniformly at random, forms a tournament and the best individual of a group wins the tournament and is put into the mating pool for recombination. This process is repeated the number of times necessary to achieve the desired size of intermediate population. The tournament size controls the selection strength. The larger the tournament size, the stronger is the selection process.

Elitist Selection

In order to make sure that the best individuals of the solution are passed to further generations, and should not be lost in random selection, this selection operator is used. So we used a few best chromosomes from each generation, based on the higher fitness value and are passed to the next generation of population.

Reproduction

To generate a second generation population of solutions from those selected through genetic operators: crossover (also called recombination), and/or mutation.

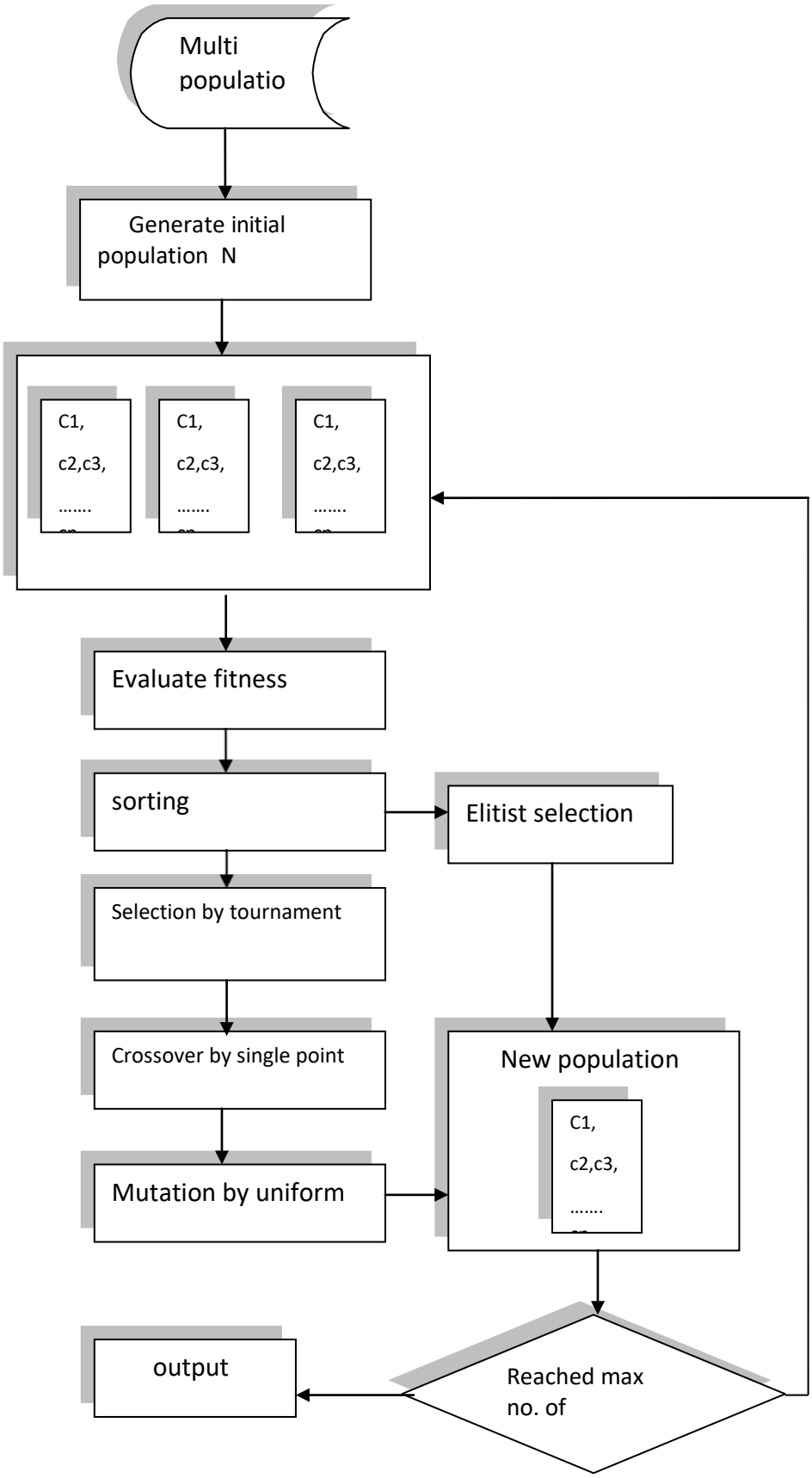
For each new solution to be produced, a pair of "parent" solutions is selected for breeding from the pool selected previously. By producing a "child" solution using the above methods of crossover and mutation, a new solution is created which typically shares many of the characteristics of its "parents". New parents are selected for each new child, and the process continues until a new population of solutions of appropriate size is generated. Although reproduction methods that are based on the use of two parents are more "biology inspired", some research suggests more than two "parents" are better to be used to reproduce a good quality chromosome.Although Crossover and Mutation are known as the main genetic operators, it is possible to use other operators such as regrouping, colonization-extinction, or migration in genetic algorithms.

Termination

This generational process is repeated until a termination condition has been reached.
Common terminating conditions are:

- A solution is found that satisfies minimum criteria
- Fixed number of generations reached
- Allocated budget (computation time/money) reached the highest ranking solution's fitness is reaching or has reached a plateau such that successive.
- Iterations no longer produce better results.
- Manual inspection.
- Combinations of the above

Flow of Genetic algorithm



CHAPTER 4 IMPLEMENTATION, CODE, RESULTS AND OUTPUT

FraudDetection.ipynb

Download GitHub Binder Code

[2]:
```
import sys
import numpy
import pandas
import matplotlib
import seaborn
import scipy
```

[3]:
```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns
```

[4]:
```
data = pd.read_csv('creditcard.csv')
```

[5]:
```
print(data.columns)
```

```
Index(['Time', 'V1', 'V2', 'V3', 'V4', 'V5', 'V6', 'V7', 'V8', 'V9', 'V10',
       'V11', 'V12', 'V13', 'V14', 'V15', 'V16', 'V17', 'V18', 'V19', 'V20',
       'V21', 'V22', 'V23', 'V24', 'V25', 'V26', 'V27', 'V28', 'Amount',
       'Class'],
      dtype='object')
```

[6]:
```
print(data.columns)
```

```
Index(['Time', 'V1', 'V2', 'V3', 'V4', 'V5', 'V6', 'V7', 'V8', 'V9', 'V10',
       'V11', 'V12', 'V13', 'V14', 'V15', 'V16', 'V17', 'V18', 'V19', 'V20',
       'V21', 'V22', 'V23', 'V24', 'V25', 'V26', 'V27', 'V28', 'Amount',
       'Class'],
      dtype='object')
```

[7]:
```
print(data.shape)
```

```
(7973, 31)
```

[8]:
```
data["Class"].value_counts()
```

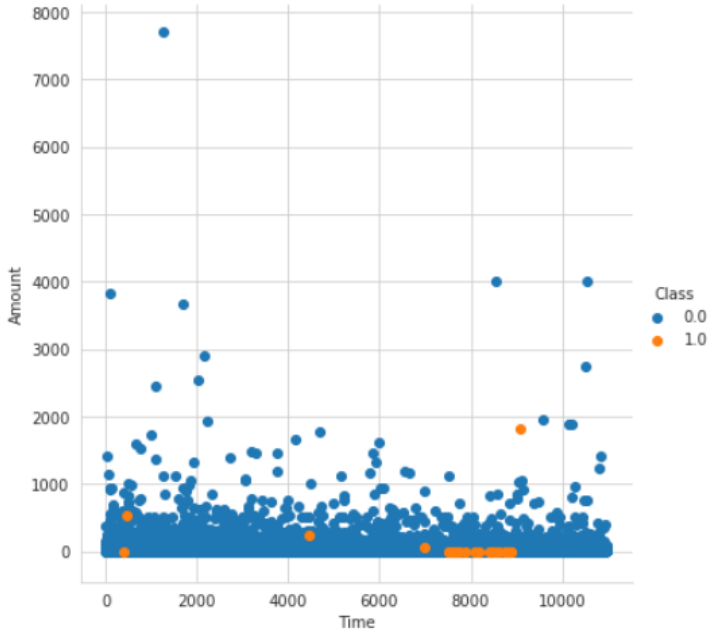
[8]:
```
0.0    7947
1.0      25
Name: Class, dtype: int64
```

FraudDetection.ipynb

Download GitHub Binder Code

2D:- Scatter Plot

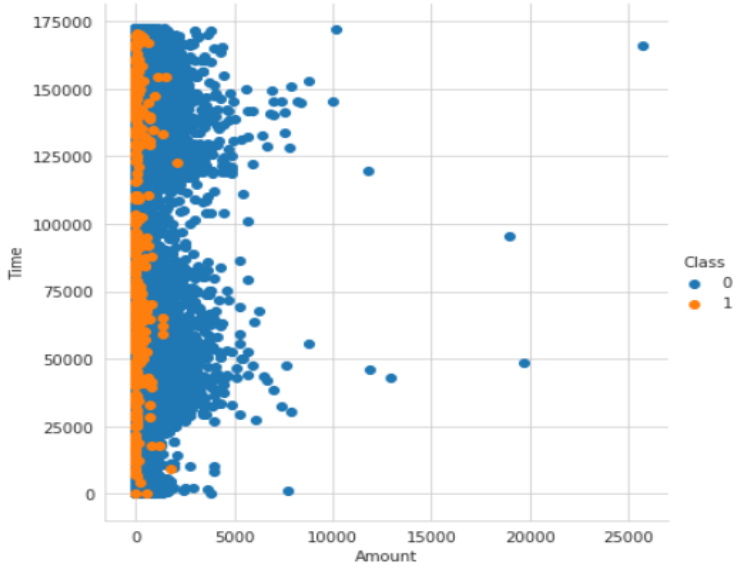
[9]:
```
sns.set_style("whitegrid")
sns.FacetGrid(data, hue="Class", height = 6).map(plt.scatter, "Time", "Amount").add_legend()
plt.show()
```



FraudDetection.ipynb

Download GitHub Binder Code

[9]:
```
sns.set_style("whitegrid")
sns.FacetGrid(data, hue="Class", height = 6).map(plt.scatter, "Amount", "Time").add_legend()
plt.show()
```



FraudDetection.ipynb

Download GitHub Bind

3D:- Scatter Plot

[10]:
```
FilteredData = data[['Time','Amount', 'Class']]
```

[11]:
```
FilteredData
```

[11]:

	Time	Amount	Class
0	0.0	149.62	0
1	0.0	2.69	0
2	1.0	378.66	0
3	1.0	123.50	0
4	2.0	69.99	0
...	...	...	...
284802	172786.0	0.77	0
284803	172787.0	24.79	0
284804	172788.0	67.88	0
284805	172788.0	10.00	0
284806	172792.0	217.00	0

284807 rows × 3 columns

[12]:
```
print(FilteredData.shape)
```

```
(284807, 3)
```

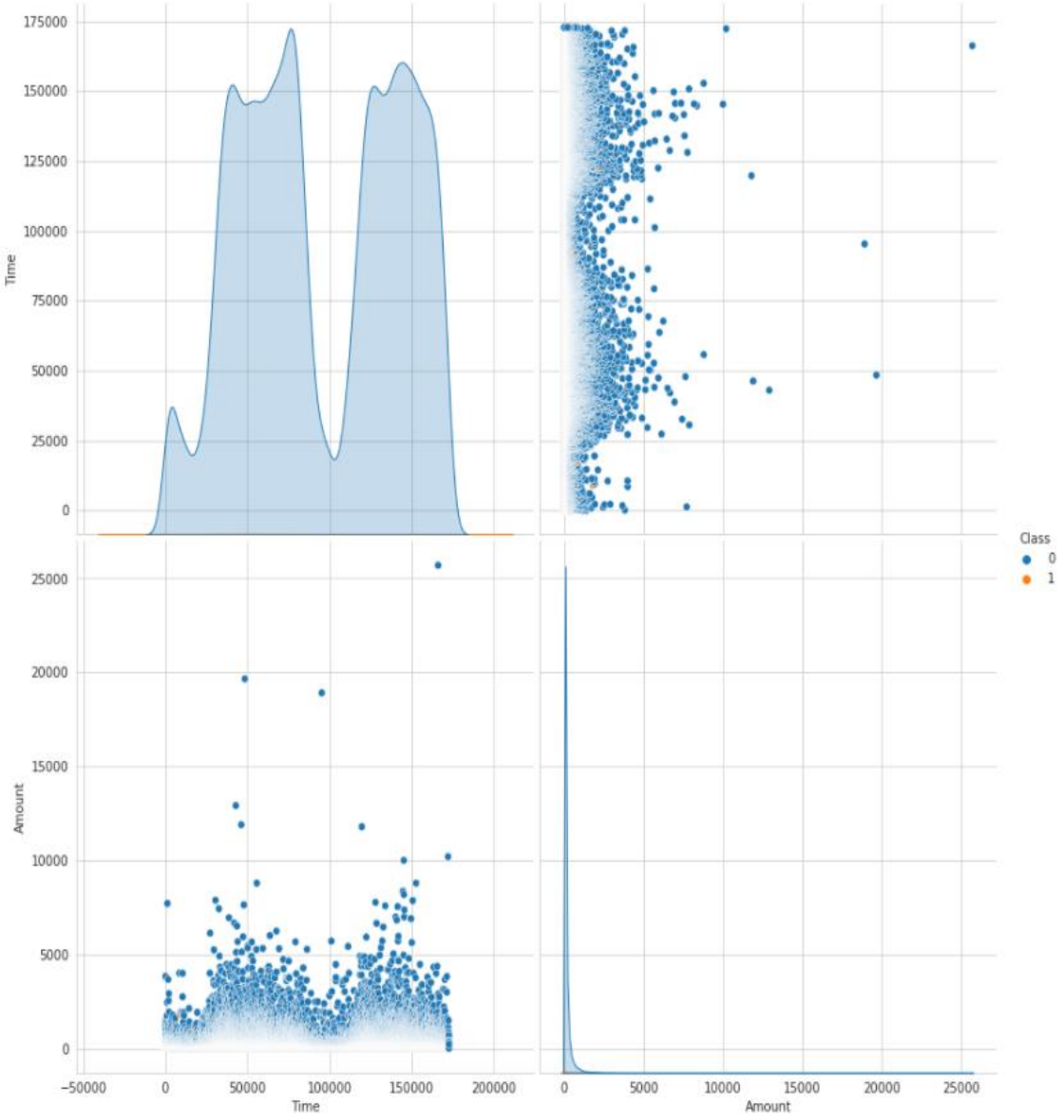
[13]:
```
FilteredData["Class"].value_counts()
```

[13]:
```
0    284315
1       492
Name: Class, dtype: int64
```

FraudDetection.ipynb

Download GitHub Binder Code

[17]:
```
plt.close();
sns.set_style("whitegrid");
sns.pairplot(FilteredData, hue="Class", height=6);
plt.show()
```



FraudDetection.ipynb

Download GitHub Binder

[18]:
```
countLess = 0
countMore= 0
for i in range(284806):
    if(FilteredData.iloc[i]["Amount"] < 2500):
        countLess = countLess + 1
    else:
        countMore = countMore + 1
print(countLess)
print(countMore)
```

```
284357
449
```

[19]:
```
percentage = (countLess/284807)*100
percentage
```

[19]:
```
99.84199826549207
```

[20]:
```
class0 = 0
class1 = 0
for i in range(284806):
    if(FilteredData.iloc[i]["Amount"] < 2500):
        if(FilteredData.iloc[i]["Class"] == 0):
            class0 = class0 + 1
        else:
            class1 = class1 + 1

print(class0)
print(class1)
```

```
283865
492
```

[21]:
```
FilteredData["Class"].value_counts()
```

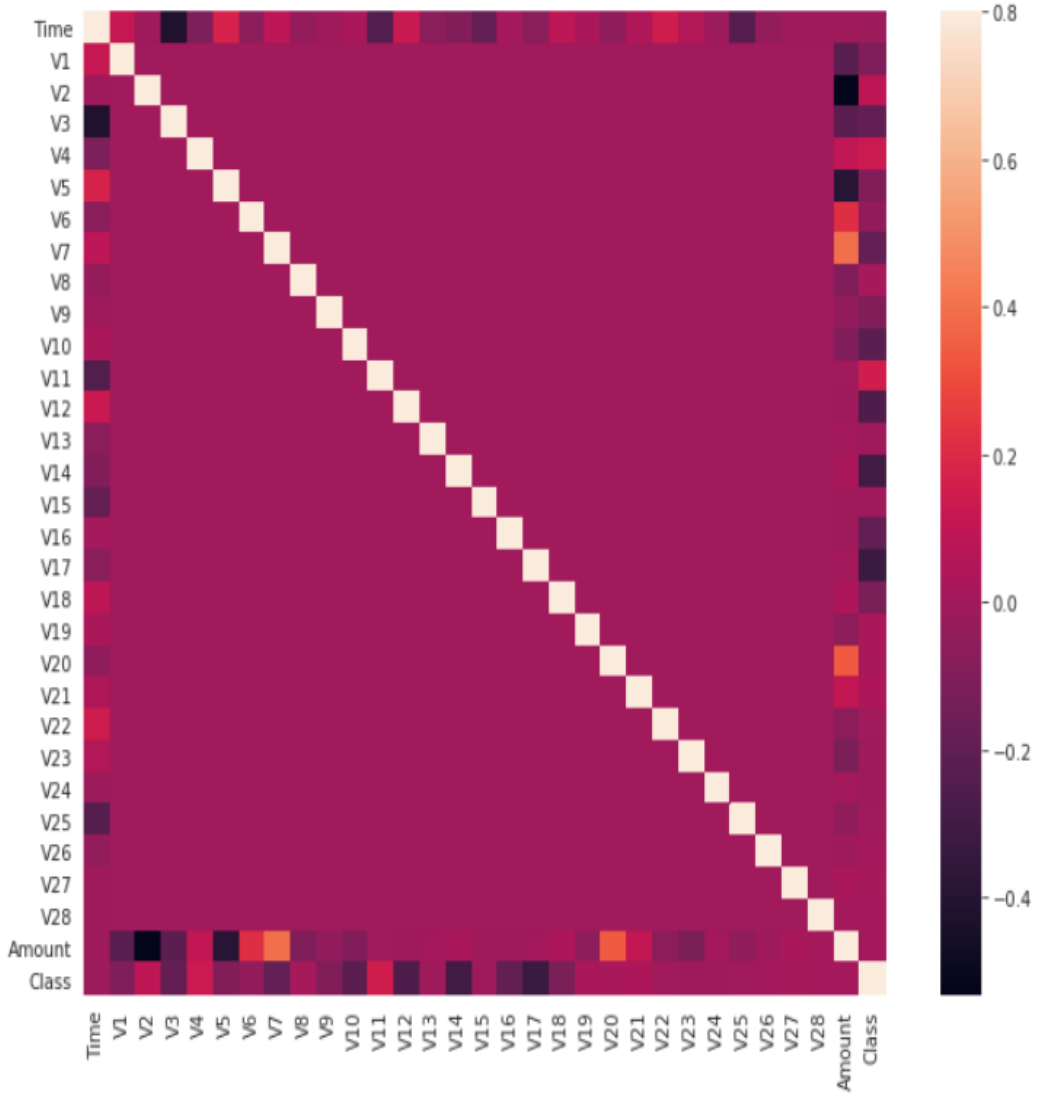
[21]:
```
0    284315
1       492
Name: Class, dtype: int64
```

FraudDetection.ipynb

Download GitHub Binder Code

[22]:
```
corrmat = data.corr()
fig = plt.figure(figsize = (12, 9))

sns.heatmap(corrmat, vmax = .8, square = True)
plt.show()
```



[ ]:

CHAPTER 5 CONCLUSION

6.1 SUMMARY

Concluding my Data Science project, I have learned how to develop a credit card fraud detection model using machine learning. Here I have used a variety of Machine Learning algorithms to implement this model and also plotted the respective performance curves for the models. I have learned how data can be analyzed and visualized to discern fraudulent transactions from other types of data. So now,using this project we can easily detect the fraud.

6.2 CONCLUSION

This method proves accurate in deducting fraudulent transaction and minimizing the number of false alert. Genetic algorithm is a novel one in this literature in terms of application domain. If this algorithm is applied into bank credit card fraud detection system, the probability of fraud transactions can be predicted soon after credit card transactions. And a series of anti- fraud strategies can be adopted to prevent banks from great losses and reduce risks.

The objective of the study was taken differently than the typical classification problems in that we had a variable misclassification cost. As the standard data mining algorithms does not fit well with this situation we decided to use multi population genetic algorithm to obtain an optimized parameter.

6.3 FUTURE WORK

While we couldn't reach out goal of 100% accuracy in fraud detection, we did end up creating a system that can, with enough time and data, get very close to that goal. As with any such project, there is some room for improvement here. The very nature of this project allows for multiple algorithms to be integrated together as modules and their results can be combined to increase the accuracy of the final result. This model can further be improved with the addition of more algorithms into it. However, the output of these algorithms needs to be in the same format as the others. Once that condition is satisfied, the modules are easy to add as done in the code. This provides a great degree

of modularity and versatility to the project. More room for improvement can be found in the dataset. As demonstrated before, the precision of the algorithms increases when the size of dataset is increased. Hence, more data will surely make the model more accurate in detecting frauds and reduce the number of false positives. However, this requires official support from the banks themselves.

REFERENCES

[1] M. Hamdi Ozcelik, Ekrem Duman, Mine Isik, Tugba Cevik, Improving a credit card fraud detection system using genetic algorithm, International conference on Networking and information technology 2010.

[2] Wen-Fang YU, Na Wang, Research on Credit Card Fraud Detection Model Based on Distance Sum, IEEE International Joint Conference on Artificial Intelligence 2009.

[3] clifton phua, vincent lee1, kate smith & ross gayler, A Comprehensive Survey of Data Mining-based Fraud Detection Research,2005.

[4] Elio Lozano, Edgar Acu˜na, Parallel algorithms for distance-based and density-based outliers,2006.

[5] Credit card fraud detection using hidden markov model – Abinav Srivastava,Amlan Kundu,Shamik Sural,Arun K.majumdar

[6] "Survey Paper on Credit Card Fraud Detection by Suman" , Research Scholar, GJUS&T Hisar HCE, Sonepat published by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 3, March 2016

[7] "Research on Credit Card Fraud Detection Model Based on Distance Sum – by Wen-Fang YU and Na Wang" published by 2009 International Joint Conference on Artificial Intelligence.

[8] "Credit Card Fraud Detection through Parenclitic Network Analysis-By Massimiliano Zanin, Miguel Romance, Regino Criado, and SantiagoMoral" published by Hindawi Complexity Volume 2018, Article ID 5764370, 9 pages

[9] "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy" published by IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, VOL. 29, NO. 8, AUGUST 2018

[10] "Credit Card Fraud Detection-by Ishu Trivedi, Monika, Mrigya, Mridushi" published by International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016.

Websites:

[1] http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/tcw2/report.html

[2] http://www.kxcad.net/cae_MATLAB/toolbox/gads/f6691.html

[3] http://java.sun.com/developer/onlineTraining/Programming/BasicJava1/front.html [4]http://www.easywayserver.com/blog/user-login-in-jsp/

[5]http://www.faqs.org/patents/app/20100094765

Textbooks:

[1]Pressman, Roger S. Software engineering: a practitioner's approach / Roger S. Pressman.—5th ed.p. cm (McGraw-Hill series in computer science).

[2]E.Balagurasamy, Programming with java, Tata McGraw-Hill Publication.

[3]Ali Bahrami,Oject Oriented system Development, Tata McGraw-Hill Publication . [4]Jiwei Han et,al., –Data Mining :Concepts and Techniques, MorganKaufmaan Series2020