Riphah International University

Riphah Institute of Systems Engineering (RISE)

Research/Project Thesis

A Machine Learning Based Model For Prevention of Fraud in E-commerce Transactions

Naveed Ahmad
10559

Thesis Supervisor
Dr. Muhammad Yousaf

A Machine Learning Based Model For Prevention of Fraud in E-commerce Transactions

BY
NAVEED AHMAD (CMS: 10559)

SUPERVISED BY
DR. MUHAMMAD YOUSAF

A research thesis submitted to the Riphah Institute of Systems Engineering, Faculty of Computing, Riphah International University, Islamabad in partial fulfillment of the requirement for the degree of

MASTER OF SCIENCE IN INFORMATION SECURITY

Riphah Institute of Systems Engineering
Faculty of Computing, Riphah International University

IN THE NAME OF ALMIGHTY ALLAH
THE MOST BENEFICENT
THE MOST MERCIFUL

Dedicated to Fatima & Adan.

DECLARATION

I, Naveed Ahmad
CMS No: 10559

Student of MS in Information Security at Riphah International University do hereby solemnly acknowledge that thesis titled "A Machine Learning Based Model for Prevention of Fraud in E-Commerce Transactions" submitted by me in partial fulfillment of MS in Information Security is my original work, except otherwise acknowledged in the text and has not published earlier and shall not, in future, be submitted by me for obtaining any degree from this or any other university or institution

Date: ______________________ Student's Signature: _________________

Supervisor's Signature: ____________________
(Dr. Muhammad Yousaf)

ACKNOWLEDGEMENT

Thanks to Almighty Allah for giving me knowledge and strength to accomplish this study. I learned a lot while doing my thesis. This study will help me accomplish my professional goals in my forth coming professional life. I would especially like to extend my thanks to my supervisor Dr. Muhammad Yousaf, without his support, knowledge and guidance this would have not been possible. I would also like to thank Samuel Anthon Gastro for being my mentor and providing me support and tools needed to complete this work.

Table of Contents

List Of Tables

List Of Figures

ABSTRACT

Fraud in online transactions is a continuous problem for businesses selling products online and receiving payments through Credit Card or Digital Wallets. Most of this fraud comes in the form of chargebacks and is mostly settled as a Merchant liability. This research work is an effort to address this problem with a machine learning based multilayer model. This proposed work is implemented for a business selling digital products online and is in production handling all the online transactions. The result shown are quite effective and have reduced business's loss to fraud by over 50 percent. This work can be further extended with inclusion of model that is capable of spike and communal detection and also able to analyze the economic efficiency of the model.

1

INTRODUCTION

1. INTRODUCTION

Ecommerce and payment related frauds are the illegal transactions completed by a Cyber Criminal (BigCommerce, 2016). These frauds are divided in three main categories:

1. Fraudulent or unauthorized transactions
2. Lost or stolen merchandise
3. False request for a refund, return or bounced checks and chargebacks

When it comes to payment processing mitigating fraud in ecommerce is a complex process due to the involvement of different stack holders. Verified payment processors like Braintree can help mitigate fraud at the time of processing payments. A business aware of latest fraud trends can better identify and mitigate fraud when an online payment is being processed. In this study a multi-layer model will be deployed to detect and mitigate fraud in ecommerce related transactions using ML techniques.

1.1 Problem Area

Online transactions have seen a huge increase in recent years. In order to keep things in perspective, let's look into the following facts and figures by statista.com (Statista.com, 2014):

1. **41%** of global internet users having purchased products online in 2013
2. In 2013 global e-retail sales amounted to **839 billion** US Dollars
3. projection shows the growth of up to **1.5 trillion USD** by 2018

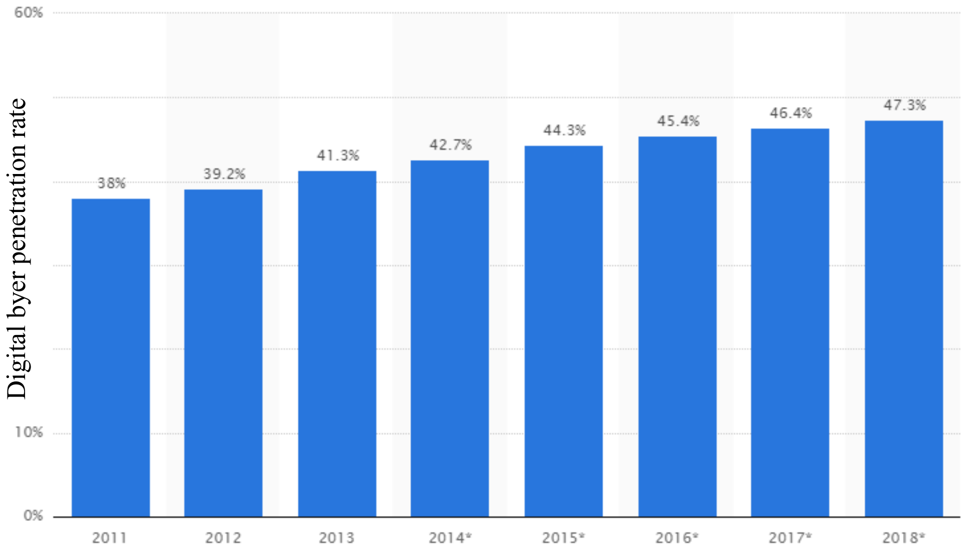


Figure 1: Ecommerce Growth In Recent Years (Statista.com, 2014)

This huge increase comes at a cost of online fraud, most of the online fraud results in merchants loses. Following statistics mentioned in the research by Payment, NCR and Alaric (Andy, et al., 2015) indicates the severity of the fraud in purchase transactions.

Table 1: Magnitude of fraud in credit & debit card transactions (Andy, et al., 2015)

All Transactions	**Fraud as % of Purchase transaction**	**Average Loss per fraudulent transaction $**
Theft of Card Details (CNP)*	53%	56
Theft of Prepaid Card Details (CNP)*	38%	37

CNP transactions possess unique challenges, and due to these challenges merchant loses are 20 times more than consumer (Ward, 2010). This study reduces these loses by deploying a model for detecting fraudulent transactions using computational intelligence and Machine Learning techniques.

1.2 Case Study

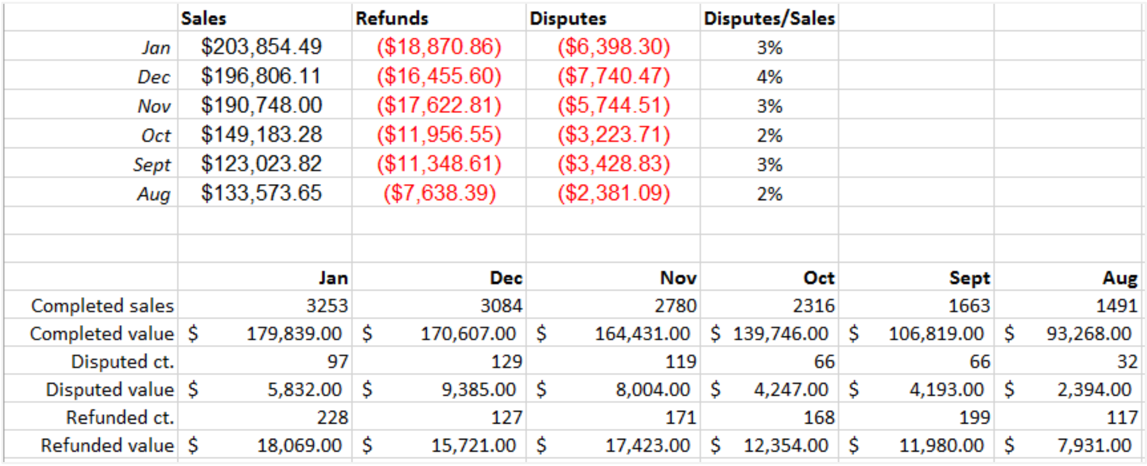
A Company in Boulder USA is selling Virtual Products online. This company sells over 70 different type of virtual products online all over the world including High-risk Countries. This company is already using several fraud management solutions to prevent the unauthorized use of consumer data in fraudulent transactions, including:

1. Risk scoring of orders
2. Manual reviews

3. Risk scoring of customers
4. Risk signals identifications
5. Manual analysis of IP related information
6. Customer history

Beside using all these techniques company is losing significant amount of money to chargebacks. Following are the statistics of the business:

Table 2: Report of Alphaboulder's loss due to chargebacks



	Sales	Refunds	Disputes	Disputes/Sales
Jan	$203,854.49	($18,870.86)	($6,398.30)	3%
Dec	$196,806.11	($16,455.60)	($7,740.47)	4%
Nov	$190,748.00	($17,622.81)	($5,744.51)	3%
Oct	$149,183.28	($11,956.55)	($3,223.71)	2%
Sept	$123,023.82	($11,348.61)	($3,428.83)	3%
Aug	$133,573.65	($7,638.39)	($2,381.09)	2%

	Jan	Dec	Nov	Oct	Sept	Aug
Completed sales	3253	3084	2780	2316	1663	1491
Completed value	$ 179,839.00	$ 170,607.00	$ 164,431.00	$ 139,746.00	$ 106,819.00	$ 93,268.00
Disputed ct.	97	129	119	66	66	32
Disputed value	$ 5,832.00	$ 9,385.00	$ 8,004.00	$ 4,247.00	$ 4,193.00	$ 2,394.00
Refunded ct.	228	127	171	168	199	117
Refunded value	$ 18,069.00	$ 15,721.00	$ 17,423.00	$ 12,354.00	$ 11,980.00	$ 7,931.00

Every fraudulent transaction is marked as disputed. These disputed transactions are not just contributing in financial losses but also effecting the reputation of the business. Which results in some indirect financial loses and deposit lock downs.

1.3 Introduction To Chargebacks

Chargebacks are one of the major cost components of merchants to accept credit card payments. Data collected from over 20% of all signature-based transaction in United States shows that about 70% to 80% of chargebacks are resolved as merchant liability, and the most common reason is fraud which is about 50 percent of the total chargebacks. Chargebacks are divided into 7 basic categories (Hayashi, et al., 2016):

1. Fraud
2. Non-receipt of goods and services
3. Product Quality
4. Cancellation
5. Non-receipt Information

6. Processing Error
7. Authorization

1.4 Lifecycle Of A Chargeback

Five different actors are involved in the chargeback process

1. Card Holders
2. Card Issuer
3. Card Network
4. Merchant Acquirer
5. Merchant

Either card issuer or Merchant holds the financial liability of a card holder’s disputed transaction this is because of consumer protection laws and zero liability rules of card networks.

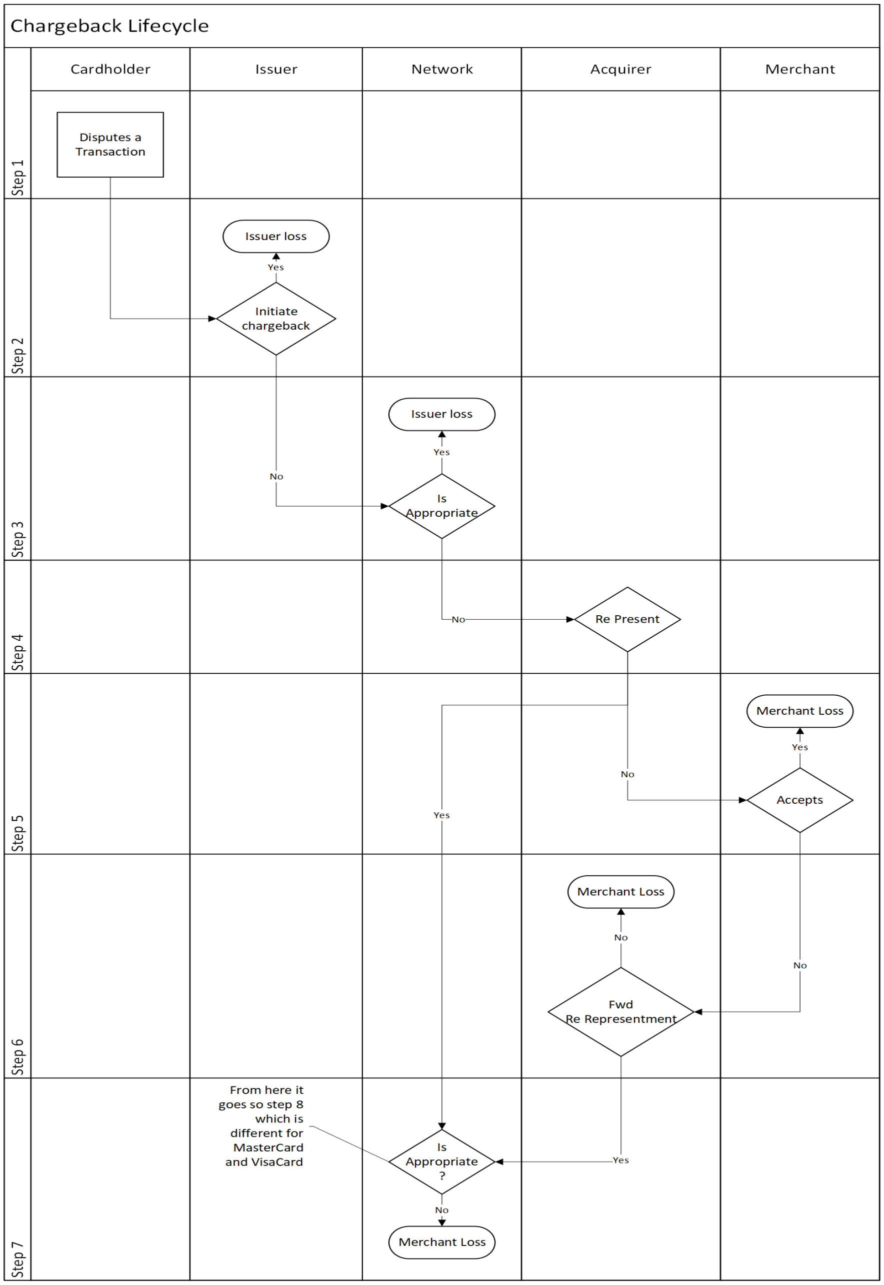


Figure 2:Lifecycle of a chargeback

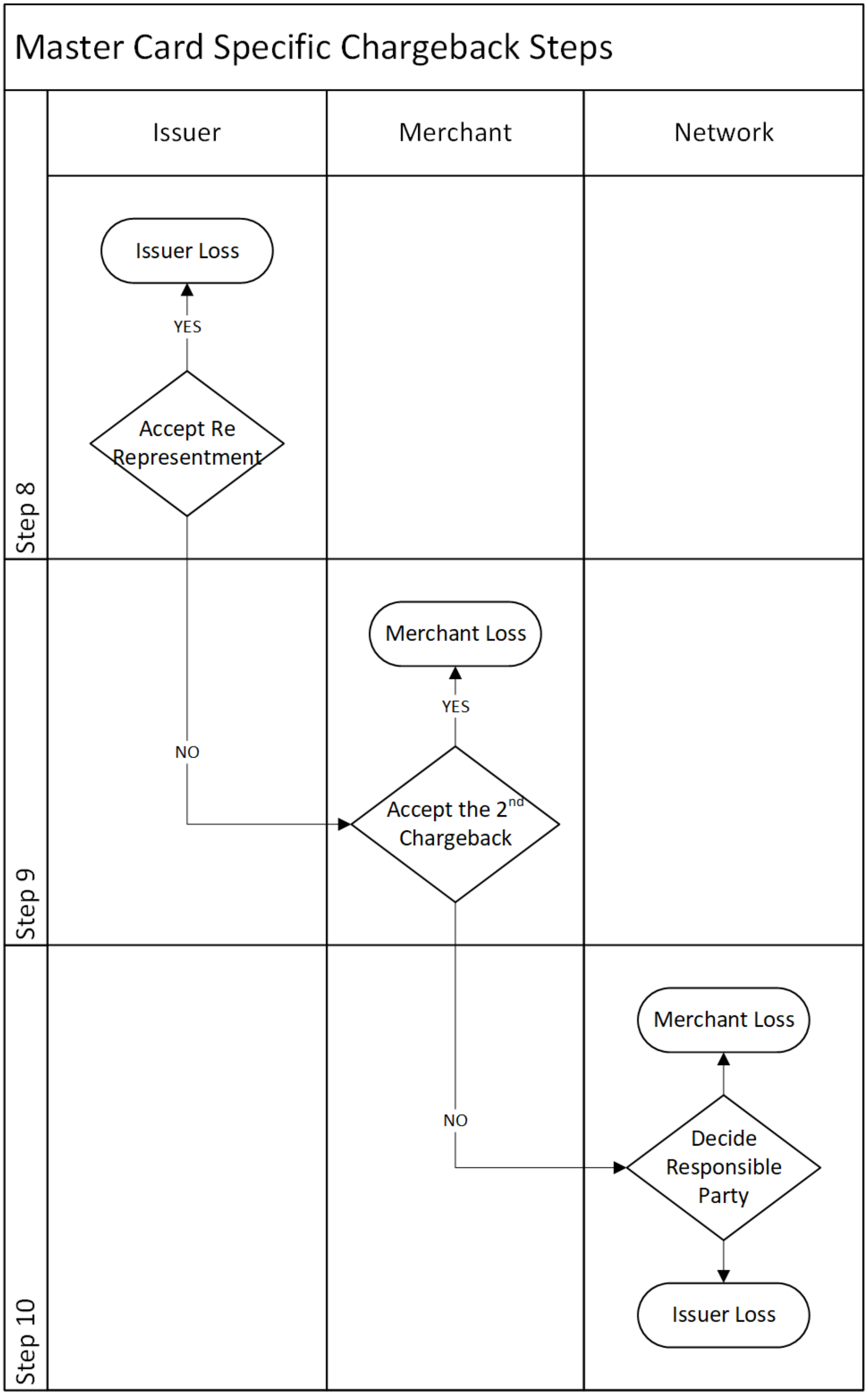


Figure 3: Master Card specific charge back steps

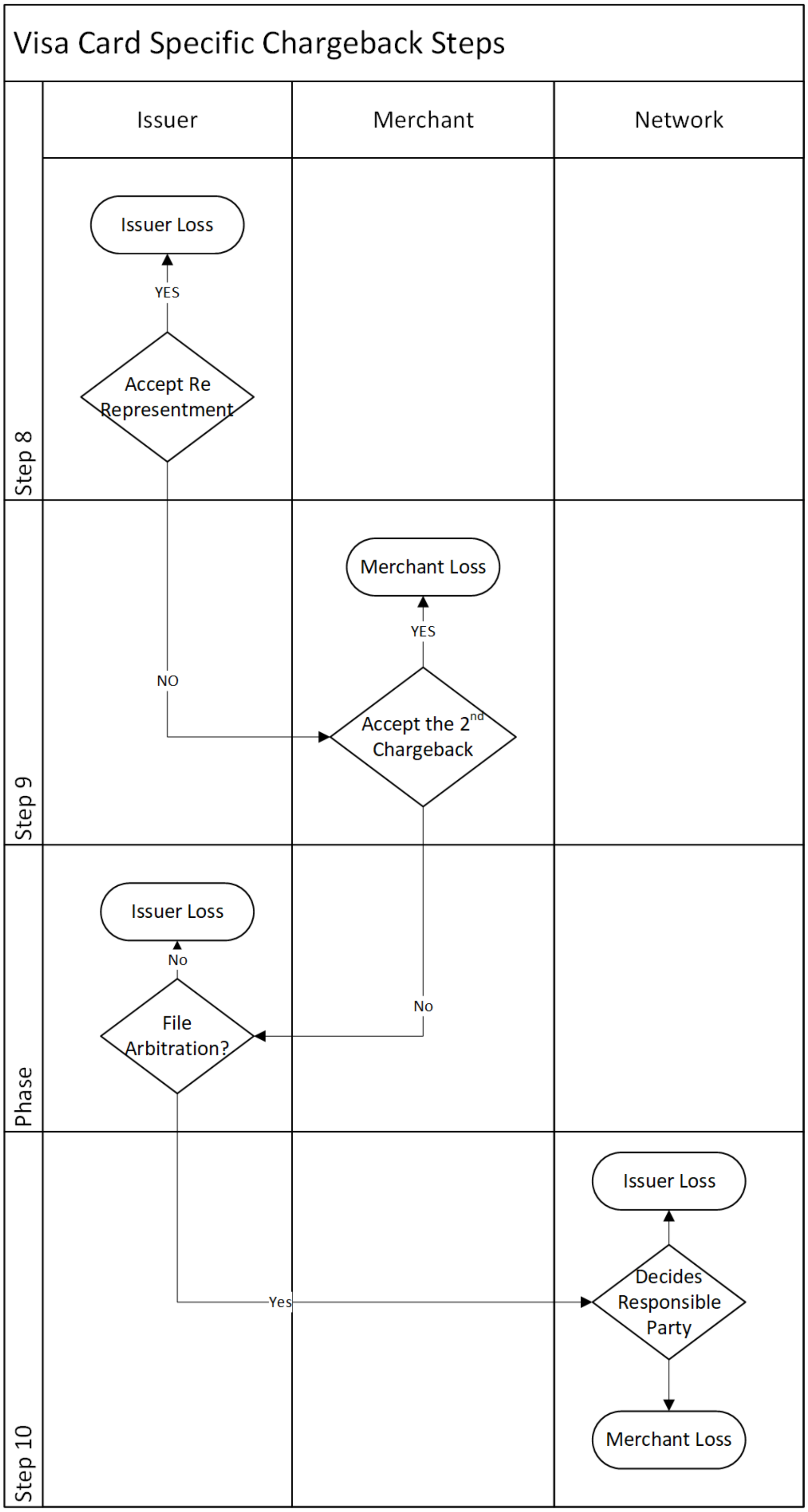


Figure 4: Visa Card specific chargeback steps (Hayashi, et al., 2016)

]

1.5 CP Vs CNP Transaction.

For CNP (Card Not Present) transactions chargeback rates are significantly higher as compared to CP (Card Present) transactions.

Starting from problem statement to type and magnitude of fraud, this study has established enough ground to move forward toward the introduction of machine learning after that this study will explore some introduction to fraud detection techniques before moving onto the significance of this work and next chapters. In general, two main types of techniques are used to detect frauds (Wikipedia, 2016):

1.6 Statistical And Data Analysis Technique

1. Data preprocessing techniques for detection, validation, error correction, and filling up of missing or incorrect data
2. Calculation of various statistical parameters such as averages, quantiles, performance metrics, probability distributions, and so on. For example, the averages may include average length of call, average number of calls per month and average delays in bill payment
3. Models and probability distributions of various business activities either in terms of various parameters or probability distributions
4. Computing user profiles
5. Time-series analysis of time-dependent data
6. Clustering and classification to find patterns and associations among groups of data.
7. Matching algorithms to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles. Techniques are also needed to eliminate false alarms, estimate risks, and predict future of current transactions or users

1.7 AI / Machine Learning Techniques

1. Data mining to classify, cluster, and segment the data and automatically find associations and rules in the data that may signify interesting patterns, including those related to fraud
2. Expert systems to encode expertise for detecting fraud in the form of rules

3. Pattern recognition to detect approximate classes, clusters, or patterns of suspicious behavior either automatically (unsupervised) or to match given inputs
4. Machine learning techniques to automatically identify characteristics of fraud
5. Neural networks that can learn suspicious patterns from samples and used later to detect them

This study focuses on the techniques related to machine learning for the detection of ecommerce related frauds which is described with details in “Chapter 4: Experimentation”

1.8 Potential Benefits

This study holds great significance for reducing merchant losses by detecting and preventing unauthorized use of consumer data for fraudulent transactions. Potential benefit of this research work is the reduction in merchant losses due to fraudulent transactions.

1.9 Chapter Summary

Online businesses are growing, and online merchants are losing money and business to the fraudulent transactions. Most of that fraud comes in the form of chargebacks and refunds. As an example, this research work noted a real business losing a significant amount of money and business value over these fraudulent transactions. Machine Learning techniques can be used to reduce these types of frauds. In next chapter a survey of different fraud prevention techniques will be explored.

2

RELATED WORK

2. RELATED WORK

Fraudulent transactions are the main reasons behind chargebacks, especially for CNP transactions where merchants have to accept remote transactions (or) online transactions. There has been a lot of work done in this field, and there are many techniques and methods which can be used to detect and mitigate fraud. Main focus of this study will be preventing fraud in CNP based transactions.

2.1 Survey Of Fraud Prevention Techniques

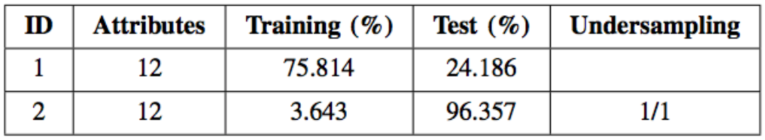
Volume of online transaction has increased and due to that, the number of fraudulent transactions also increased. Using a real dataset of one of Latin America's largest payment system it is proposed that GP (Genetic programing) is an effective algorithm with which 17 % gain is achieved (Assis, et al.) . Gains are the financial value of true positive transactions. Proposed solution is designed with the focus on online transactions. Which adopted the following methodology:

(1) Preparation of data

(2) Applying (Genetic Programing)

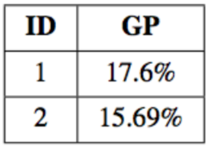
(3) Making Predictions

It is concluded that Genetic Programing provides better gains over other classification techniques.



ID	Attributes	Training (%)	Test (%)	Undersampling
1	12	75.814	24.186	
2	12	3.643	96.357	1/1

Figure 5: Division of fraud training dataset in (Assis, et al.)



ID	GP
1	17.6%
2	15.69%

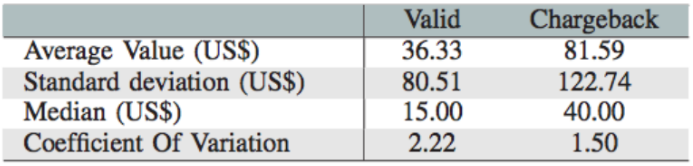
Figure 6: Result of Genetic Programing approach in (Assis, et al.)

Increase of volume of online transactions has raised scientifically due to the popularization of electronic ecommerce retailers such as Amazon and Ali Express. Increase in transaction is directly related to increase in online frauds (Caldeira, et al.).

Following techniques of computational intelligence along with data mining are used to Identify and detect fraud:

- Bayesian Networks
- Logistic Regressions
- Neural Networks
- Random Forest

In (Caldeira, et al.) the database of an online Service PagSeguro is used, in the dataset each transaction is composed of tens of attributes. Following is the overview of dataset.



	Valid	Chargeback
Average Value (US$)	36.33	81.59
Standard deviation (US$)	80.51	122.74
Median (US$)	15.00	40.00
Coefficient Of Variation	2.22	1.50

Figure 7: Overview of dataset in (Caldeira, et al.)

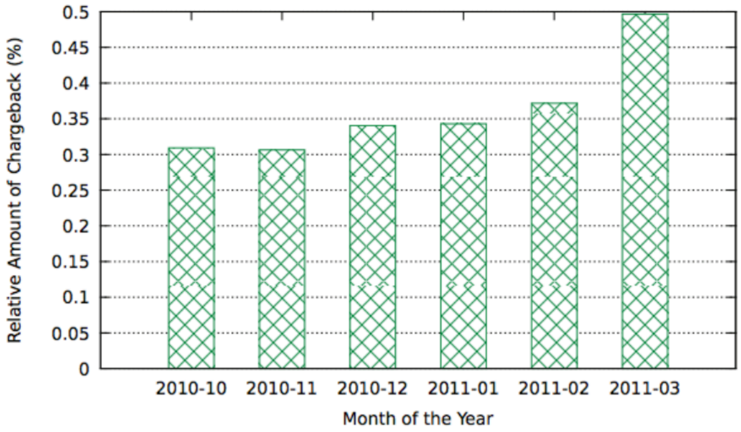
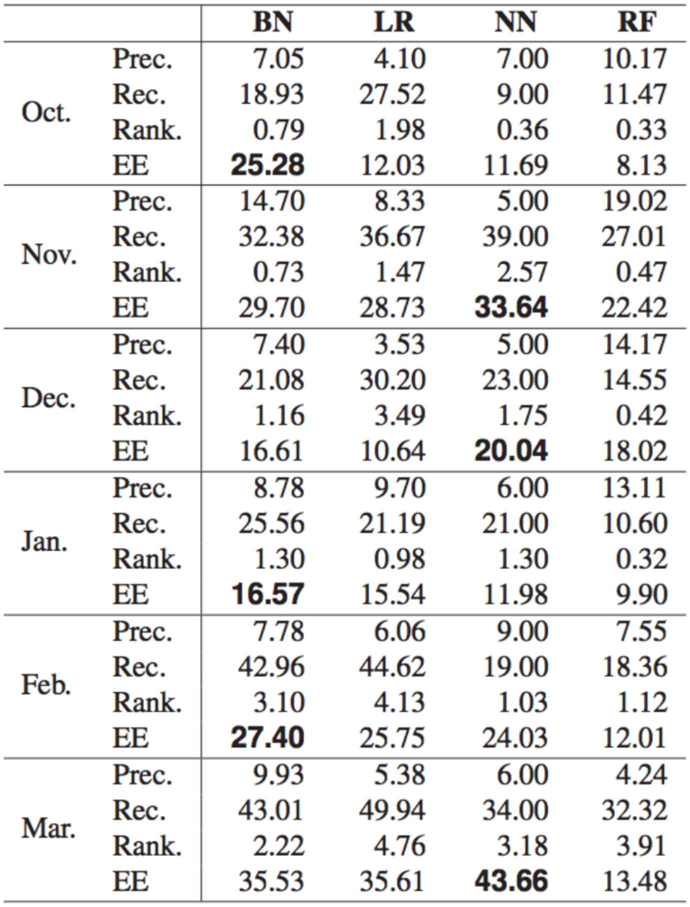


Figure 8: Relative quantity of chargebacks in (Caldeira, et al.)

It is concluded that in the best case 43.3% gain was achieved. Neural Networks and Bayesian Network performed the best results.



		BN	LR	NN	RF
Oct.	Prec.	7.05	4.10	7.00	10.17
	Rec.	18.93	27.52	9.00	11.47
	Rank.	0.79	1.98	0.36	0.33
	EE	**25.28**	12.03	11.69	8.13
Nov.	Prec.	14.70	8.33	5.00	19.02
	Rec.	32.38	36.67	39.00	27.01
	Rank.	0.73	1.47	2.57	0.47
	EE	29.70	28.73	**33.64**	22.42
Dec.	Prec.	7.40	3.53	5.00	14.17
	Rec.	21.08	30.20	23.00	14.55
	Rank.	1.16	3.49	1.75	0.42
	EE	16.61	10.64	**20.04**	18.02
Jan.	Prec.	8.78	9.70	6.00	13.11
	Rec.	25.56	21.19	21.00	10.60
	Rank.	1.30	0.98	1.30	0.32
	EE	**16.57**	15.54	11.98	9.90
Feb.	Prec.	7.78	6.06	9.00	7.55
	Rec.	42.96	44.62	19.00	18.36
	Rank.	3.10	4.13	1.03	1.12
	EE	**27.40**	25.75	24.03	12.01
Mar.	Prec.	9.93	5.38	6.00	4.24
	Rec.	43.01	49.94	34.00	32.32
	Rank.	2.22	4.76	3.18	3.91
	EE	35.53	35.61	**43.66**	13.48

Figure 9: Comparative Result of BN, LR, NN, RF

Prec = Precision, Rec = Recall, Rank = Ranking, EE = Economic Efficiency (Caldeira, et al.)

Increase in online fraud is the motivation behind this research and aim is to use some computational intelligence to Identify fraud in electronic transactions (Caldeira, et al., 2012). Concept of Economic efficiency is applied to actual data set which show significant gains in comparison to the actual gain to the current scenarios. Following techniques are used and Economic Efficiency is Applied to evaluate the gains.

- Bayesian Networks
- Logistic Regressions
- Radial Basis Function
- Neural Networks
- Random Forest
- Support Vector Mechanism

- Sequential Minimum Optimization

Another interesting characterization of data is chargebacks by age.

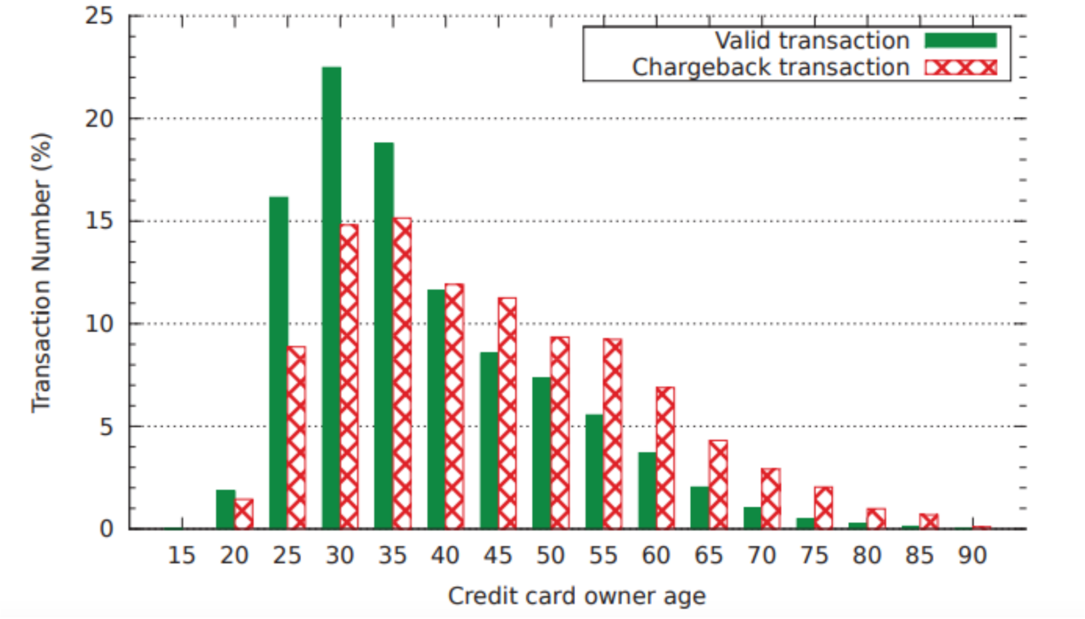
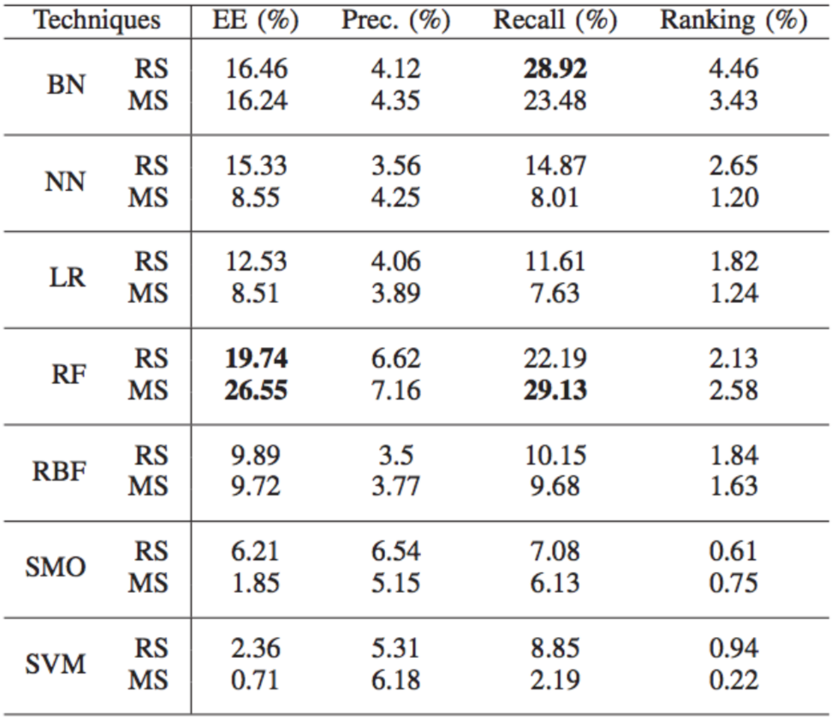


Figure 10: Number of transaction by age in (Caldeira, et al., 2012)

Random Forest achieved the best results



Techniques		EE (%)	Prec. (%)	Recall (%)	Ranking (%)
BN	RS	16.46	4.12	**28.92**	4.46
	MS	16.24	4.35	23.48	3.43
NN	RS	15.33	3.56	14.87	2.65
	MS	8.55	4.25	8.01	1.20
LR	RS	12.53	4.06	11.61	1.82
	MS	8.51	3.89	7.63	1.24
RF	RS	**19.74**	6.62	22.19	2.13
	MS	**26.55**	7.16	**29.13**	2.58
RBF	RS	9.89	3.5	10.15	1.84
	MS	9.72	3.77	9.68	1.63
SMO	RS	6.21	6.54	7.08	0.61
	MS	1.85	5.15	6.13	0.75
SVM	RS	2.36	5.31	8.85	0.94
	MS	0.71	6.18	2.19	0.22

Figure 11: Comparative analysis of BN, NN, LR, RF, RBF, SMO, SVM in (Caldeira, et al., 2012)

- *RS is a dataset composed by all transactions in weeks 1 to 3 for training and the remained weeks of the month for test*
- *MS is formed by taking all chargebacks in weeks 1 to 3, but only 10% of the valid transactions*

Online transaction processing at merchant sites determine the probability of such transactions that are fraudulent (Lee, et al., 2007). Which includes accounting of:

- Unreliable field of a transaction order
- A Scoring Server Using Statistical Models
- Weights to indicate degree to which the profile Identify

Two facts are important to online retailers (Ward, 2010):

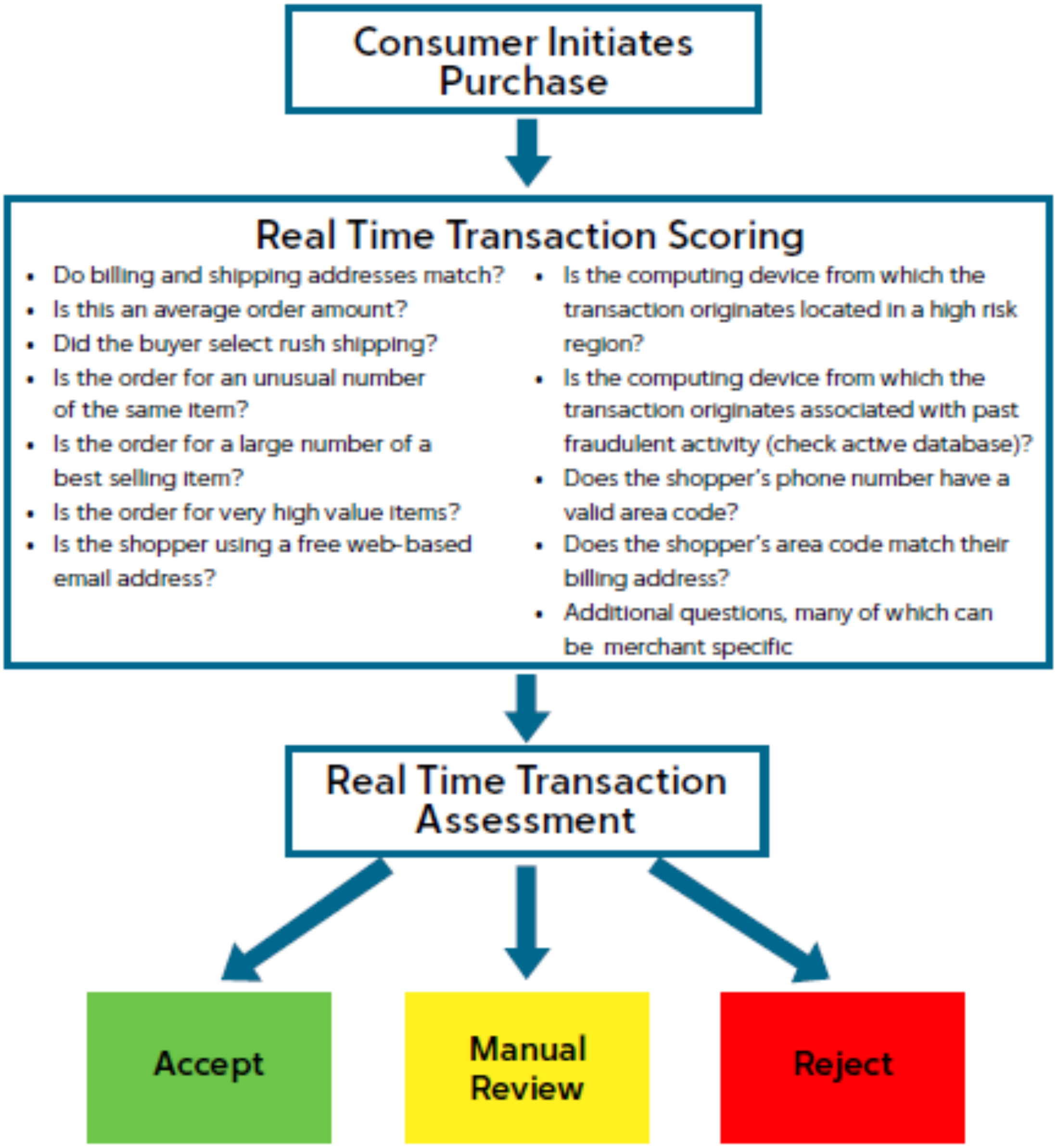
- Protecting against the theft of customer data
- Preventing unauthorized use of consumer data in fraudulent transactions.

CNP possess unique challenges. Merchant losses due to fraud are 10 times more than bank and 20 times more than consumer. To avoid these different tools for detecting and preventing fraud transactions are used which are:

- Automated Transactional risk scoring
- Real Time Categorization and Resolutions
- Post purchase transaction and management
- Adjusting fraud rules and parameters

With these aforementioned capabilities, online retailers can efficiently:

1. Determine what level of risks are acceptable for various products, order profiles and shopping behaviors.
2. Adjust rules and logic as needed
3. Easily categorize all orders
4. Stream line administrative process


Consumer Initiates Purchase
Real Time Transaction Scoring
Real Time Transaction Assessment
Accept
Manual Review
Reject

- Do billing and shipping addresses match?
- Is this an average order amount?
- Did the buyer select rush shipping?
- Is the order for an unusual number of the same item?
- Is the order for a large number of a best selling item?
- Is the order for very high value items?
- Is the shopper using a free web-based email address?
- Is the computing device from which the transaction originates located in a high risk region?
- Is the computing device from which the transaction originates associated with past fraudulent activity (check active database)?
- Does the shopper's phone number have a valid area code?
- Does the shopper's area code match their billing address?
- Additional questions, many of which can be merchant specific

Figure 12: Real Time Transaction Assessment in (Ward, 2010)

Several patents discuss risk-based scoring. Online transaction Processing at merchant location determines the probability that such transactions are fraudulent (Lee, et al., 2007).

Fraud is not just a financial problem it is one of the major ethical issue as well (Delamaire, et al., 2004) . Another approach is to identify the credit card fraud and then review the techniques used in the detection of fraud, this can save money and time. Following are the few types of fraud:

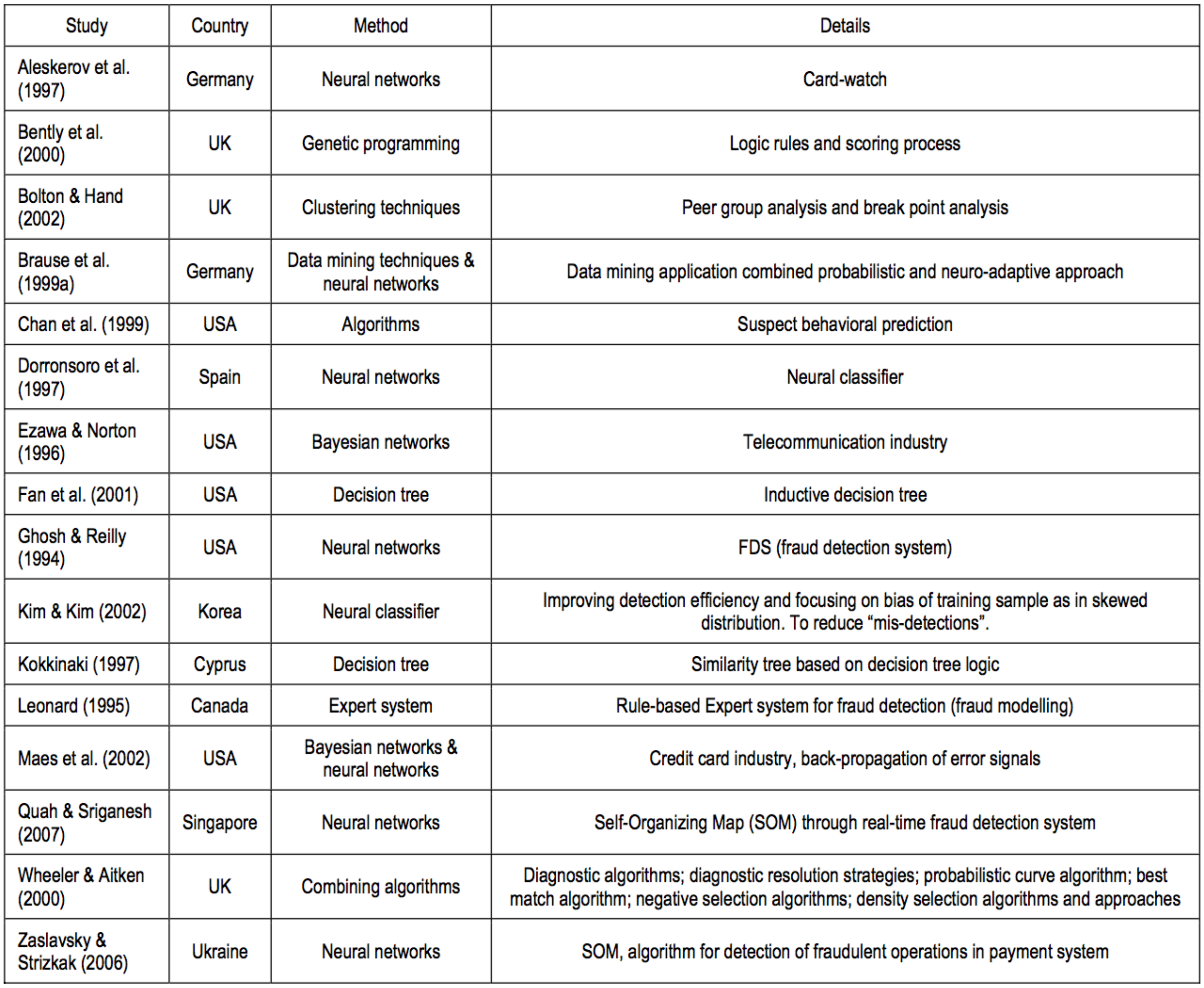
1. Theft fraud

2. Bankruptcy fraud
3. Application fraud
4. Behavioral fraud

and the following are the few fraud detection techniques:

1. Decision Tree
2. Genetic and Other Algorithms
3. Clustering Techniques
4. Neural Networks

following techniques were found effective in fraud control



Study	Country	Method	Details
Aleskerov et al. (1997)	Germany	Neural networks	Card-watch
Bently et al. (2000)	UK	Genetic programming	Logic rules and scoring process
Bolton & Hand (2002)	UK	Clustering techniques	Peer group analysis and break point analysis
Brause et al. (1999a)	Germany	Data mining techniques & neural networks	Data mining application combined probabilistic and neuro-adaptive approach
Chan et al. (1999)	USA	Algorithms	Suspect behavioral prediction
Dorronsoro et al. (1997)	Spain	Neural networks	Neural classifier
Ezawa & Norton (1996)	USA	Bayesian networks	Telecommunication industry
Fan et al. (2001)	USA	Decision tree	Inductive decision tree
Ghosh & Reilly (1994)	USA	Neural networks	FDS (fraud detection system)
Kim & Kim (2002)	Korea	Neural classifier	Improving detection efficiency and focusing on bias of training sample as in skewed distribution. To reduce “mis-detections”.
Kokkinaki (1997)	Cyprus	Decision tree	Similarity tree based on decision tree logic
Leonard (1995)	Canada	Expert system	Rule-based Expert system for fraud detection (fraud modelling)
Maes et al. (2002)	USA	Bayesian networks & neural networks	Credit card industry, back-propagation of error signals
Quah & Sriganesh (2007)	Singapore	Neural networks	Self-Organizing Map (SOM) through real-time fraud detection system
Wheeler & Aitken (2000)	UK	Combining algorithms	Diagnostic algorithms; diagnostic resolution strategies; probabilistic curve algorithm; best match algorithm; negative selection algorithms; density selection algorithms and approaches
Zaslavsky & Strizkak (2006)	Ukraine	Neural networks	SOM, algorithm for detection of fraudulent operations in payment system

Figure 13: Studies investigating different Fraud Analysis Techniques in (Delamaire, et al., 2004)

A multilayer detection system which is based on data mining, which deals with the real social relationship and find duplicates in spikes and assign suspicious score is very effective. Different type of frauds that can be dealt with multilayer model are following:

1. Bankruptcy fraud is when a purchaser uses credit card knowing that he will not be able to pay it back
2. Theft Fraud is when purchaser uses a card he does not own
3. Application Fraud is applying for a credit card with false information
4. Behavioral fraud occurs when details of legitimate cards have been obtained fraudulently and sales are made on a "cardholder present" basis

Solution which consist of five sections is proposed:

1. Credit Card Application and initial white list created
2. Communal Detection Suspicious Score
3. Spike Detection Suspicious Layer
4. Threshold Transaction Amount Calculation
5. Secure Transaction

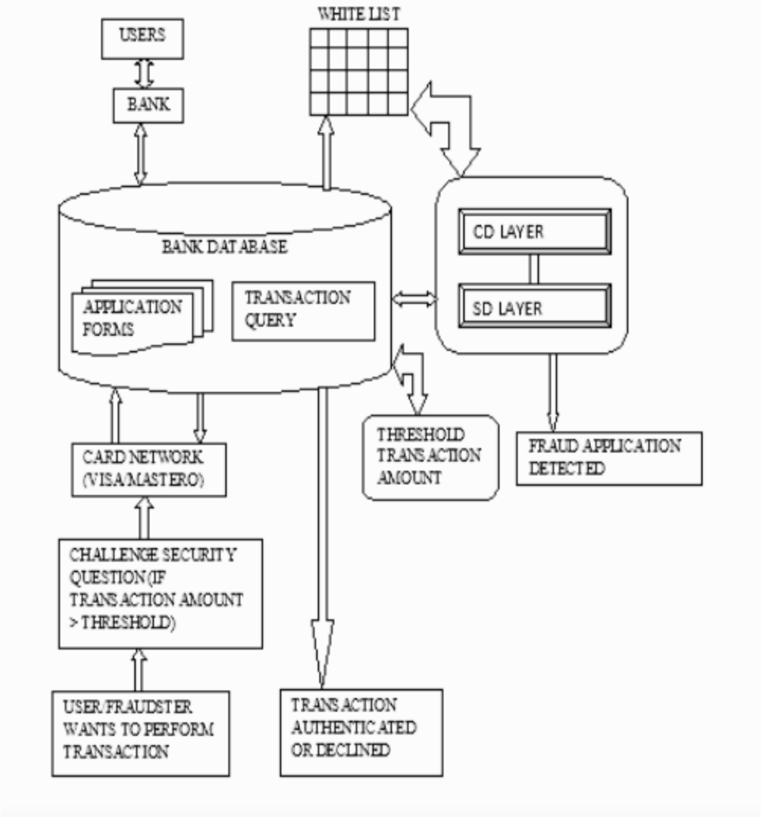

USERS
WHITE LIST
BANK
BANK DATABASE
APPLICATION FORMS
TRANSACTION QUERY
CD LAYER
SD LAYER
CARD NETWORK (VISA/MASTERO)
THRESHOLD TRANSACTION AMOUNT
FRAUD APPLICATION DETECTED
CHALLENGE SECURITY QUESTION(IF TRANSACTION AMOUNT >THRESHOLD)
USER/FRAUDSTER WANTS TO PERFORM TRANSACTION
TRANSACTION AUTHENTICATED OR DECLINED

Figure 14: Architecture diagram for Datamining approach in (Herenj, et al., 2013)

Detection of fraudsters in credit applications by implementing the new data mining layers which helps in performing a secure transaction (Herenj, et al., 2013).

Researchers have proposed rules-based auditing systems for electronic commerce transactions, which highly depend on the auditor's knowledge of ecommerce fraud. While fraud patterns may occur, the management control and application of these patterns is difficult due to the increasing number of online transactions currently handled by e-commerce systems. In (Lek, et al., 2001) Authors have proposed a prototype to an extension of auditing system which uses data mining. Research mythology included:

1. literature review
2. Investigation of AI algorithms
3. construction of early prototype
4. Testing of the prototype
5. Development of the datamining prototype
6. Testing of the datamining prototype
7. Discussions with fraud investigators
8. Review of fraud cases in order to develop e-commerce training sets
9. Field testing of the prototype using an e-commerce organization against its commercial databases
10. Development of a research model for e-commerce fraud

As it is already established that Statistics and ML are effective technologies for fraud detection and is applied successfully to detect activities such as money laundering, e-commerce fraud, telecommunications fraud and computer intrusion are a few of them (Bolton, et al., 2002). Distinction in fraud prevention and fraud detection can be established and both supervised and unsupervised learning can be used:

- **Supervised Fraud Detection** uses a method in which a database with known fraud cases from which a model can be constructed to score the new cases
- **Unsupervised Fraud Detection** used where there is no prior set of legitimate fraudulent observations

In (Bolton, et al., 2002) Authors further discussed different type of frauds and did a comprehensive review on the fraud detection techniques. Statistical methods can detect fraud even in difficult circumstances.

In (Kou, et al., 2004) the survey of techniques for fraud detection, which are following:

- Credit card fraud
- Computer intrusion
- Telecommunication fraud

Credit card fraud detection is quite confidential and is not much disclosed in public. Which is a major problem considering this some available techniques discussed as follows. Outlier Detection and observation that deviates so much from other observations as to arouse suspicion that it was generated by a different mechanism. Unsupervised Learning approaches are applied for these types of detections.

Neural Networks is a set of interconnected nodes designed to imitate the functioning of the human brain. It makes the network process the current spending patterns to detect possible anomalies. Due to privacy issues, only a few techniques for credit card fraud detection is available in public. Neural Networks approach is the most popular. Fraud Deterrence is also effective (Wikipedia, 2105) it enables the casual avoidance. Profiling is a process a in which Account level user Profiles are generated by computerized data analysis and are very effective in fraud control (Wikipedia, 2017).

Another technique which can be used with other computational intelligence methods is Data Mining in which computing process discovers patterns in large data which includes method that intersect at Machine Learning, Statistics, and Database System (Soumen Chakrabarti, 2006).

Clustering is also used in fraud prevention in this technique a finite set of categories or clusters are used to describe data e.g. Identifying target groups of customers (Sevda Soltaniziba, 2015).

In statistical modelling, regression analysis is a statistical process for estimating the relationships among variables. It includes many techniques for modelling and analysing several variables when the focus is on the relationship between a dependent variable and one or more independent variables (or 'predictors'). More specifically, regression analysis helps one understand how the typical value of the dependent variable (or 'criterion variable') changes when any one of the independent variables is varied, while the other independent variables are held fixed.

In machine learning and statistics, classification is the problem of identifying to which of a set of categories (sub-populations) a new observation belongs, on the basis of a training set of data containing observations (or instances) whose category membership is known (Wikipedia, 2017).

2.2 Survey Of Existing Products

Fraud detection and prevention is a well-researched topic therefore there are many propriety and open source products already available. In this part of the chapter a complete overview of at least 4 exiting products is explored.

2.3 Kount

Official Introduction of Kount states that Kount's award-winning anti-fraud technology empowers online merchants and payment service providers around the world. With Kount, merchants approve more orders, uncover new revenue streams, and dramatically improve their bottom line, all while minimizing fraud management cost and losses, boost sales and beat fraud with Kount.

Kount is one of the most expensive product in the market. To get started with Kount Alpha Boulder had to pay 10K USD in setup charges and the monthly service charges of 1000 USD per month. Kount assigned Alpha Boulder a dedicated product manager and it took Alpha Boulder 2 weeks to integrate with Kount. One key feature of the Kount is that it directly integrates with a payment processor.

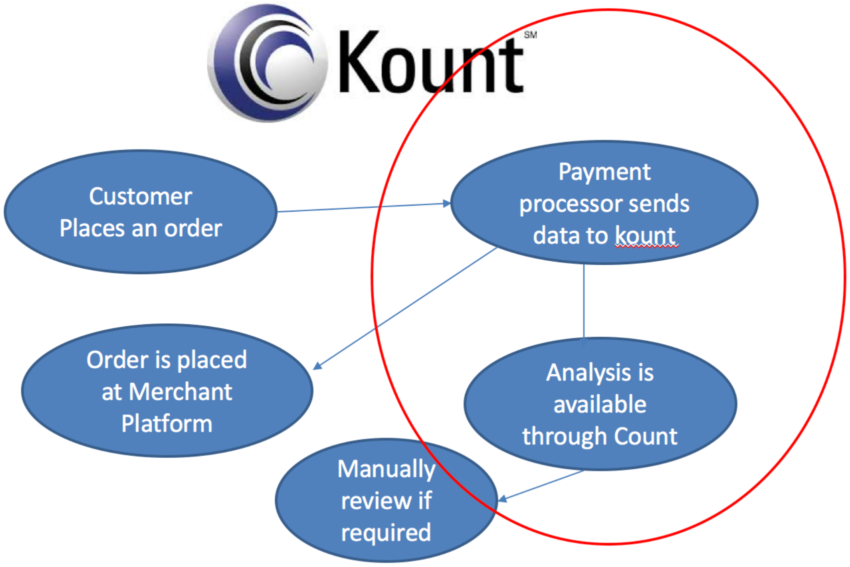

Kount SM
Customer Places an order
Payment processor sends data to kount
Order is placed at Merchant Platform
Analysis is available through Count
Manually review if required

Figure 15: Kount's Process

In figure 12 it can be seen that after customer places an order credit card info is sent to payment processor after which a payment processor sends that info to Kount for fraud analysis if analysis and once the analysis is approved the payment is processed and vendor is notified. Kount provides a comprehensive dashboard for creating rules and doing manual reviews.

2.4 FraudLabs Pro

Official introduction of FraudLabs Pro is that it helps merchants to protect their online stores from malicious fraudsters. It screens all orders transacted using credit cards, PayPal, and so on. In result, it increases e-commerce merchant profits by reducing chargeback, improving operation efficiency and increasing revenue. Merchants can investigate all complex, high-risk orders in a simple way by using merchant administrative interface.

FraudLabs Pro has an out of the box integration with many ecommerce engines and platform. Pricing model is simple and there is a trail to get started.

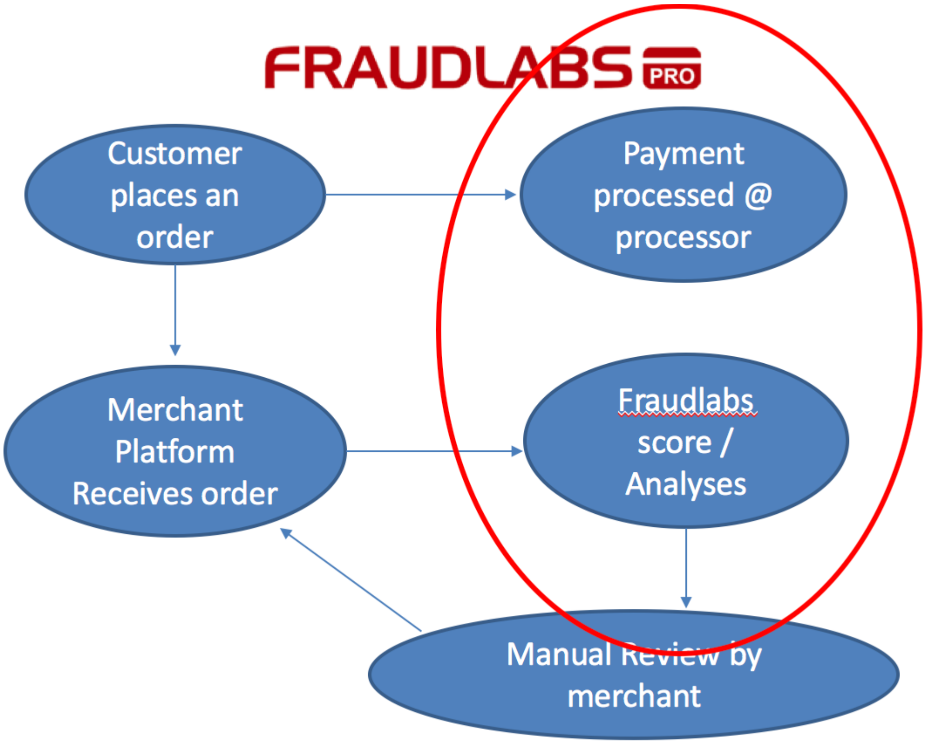

FRAUDLABS PRO
Customer places an order
Payment processed @ processor
Merchant Platform Receives order
Fraudlabs score / Analyses
Manual Review by merchant

Figure 16: FraudLabs pro's process

In figure 13 it can be seen that payment processor and FraudLabs pro does not work together vendor's platform independently connects with FraudLabs Pro. FraudLabs Pro provide a comprehensive and intuitive user interface.

2.5 Siftscience

Siftscience is a platform offers a full suite of fraud and abuse prevention, it is designed to attack every vector of online fraud for industries and business. Siftscience provides different services including:

- Account Takeover
- Payment Fraud
- Content Abuse
- Promo Abuse
- Device Fingerprinting

For payment fraud Siftscience has the following process:

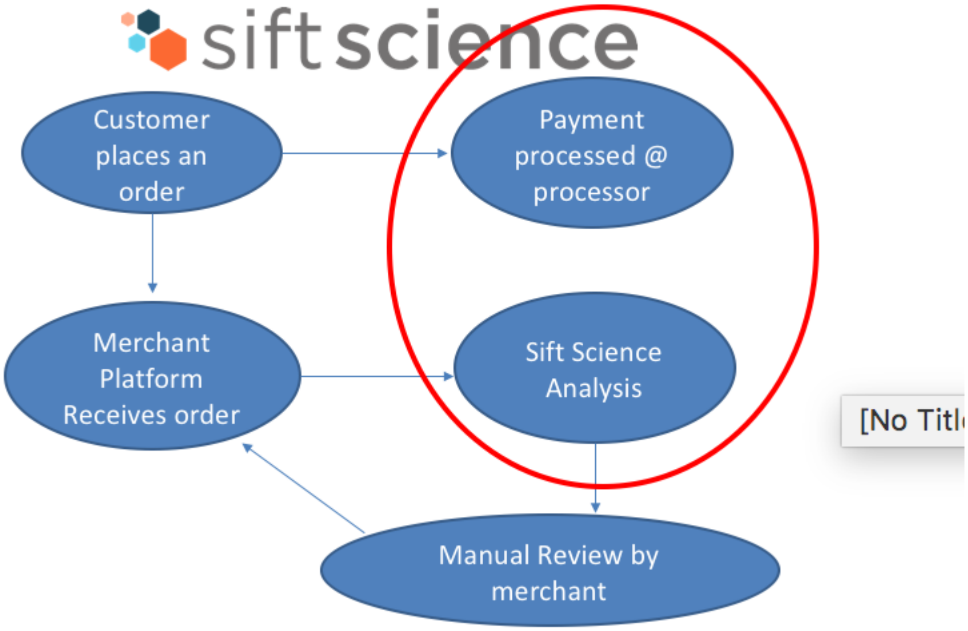

siftscience
Customer places an order
Payment processed @ processor
Merchant Platform Receives order
Sift Science Analysis
Manual Review by merchant
[No Titl

Figure 17: Siftscience's Process

Just like FraudLabs Pro it can be seen that payment processor and Siftscience does not work together vendor's platform independently connects with Siftscience.

2.6 Limitation Of Existing Techniques

Most of the techniques discussed in this chapter rely purely on machine learning and data mining. Some techniques propose a multilayer model and almost all the products discussed in this chapter use some sort of multilayer model. Relying only on machine learning cannot translate to real world scenarios.

None of the products or techniques consider the processes of human learning and observations. This limits the ability to scale the business with changing business dynamics. An opportunity is not provided to the customer when a business might think is a false positive. For example, a transaction got the score of 0.50, now there is a 50 percent chance that this transaction can be a fraudulent transaction but there is a 50 percent chance that this might be a good customer. None of these techniques discuss what can be done to establish a trust in such cases.

Why not add some deterrence? deterrence is an effective fraud control tool. Adding deterrence as an optional step can keep the fraudsters away from making any fraudulent transactions.

2.7 Chapter Summary

In this chapter Survey of different research papers and existing fraud prevention tools was done. In next chapter a solution is proposed based on machine learning techniques to prevent fraud in online transactions.

3

PROPOSED SOLUTION

3. **PROPOSED SOLUTION**

There are many different techniques which can be used to detect and prevent fraudulent transaction. Most of them are very effective and in some cases, researchers have shown the Gain of over 40 percent. That's why the theoretical foundation of this study is based on these techniques.

3.1 Theoretical Foundation

Fraud prevention and detection techniques can be divided into two main groups

Table 3: List of a few Machine Learning techniques

S.No	**ML Techniques**
1	Bayesian Networks
2	Genetic Programing
3	Genetic Programing
4	Neural Networks
5	Random Forest
6	Support Vector Machine
7	Radial Basis Function

Table 4: List of techniques Other than Machine Learning

S.No	Techniques
1	Data Mining
2	Profiling
3	White Listing
4	Communal Detection
5	Spike Detection
6	Manual Review
7	Rules
8	Labeling
9	Device Fingerprinting

While using different products available online one can see that the model these products use is pretty complex they are not based on one thing or another, for instance Siftscience has a Scoring Engine where each customer is scored using a proprietary algorithm they call it (large-scale machine learning technology). Then there are workflows, decision, actions and formulas.

When machine learning is combined with the one or more other techniques in a layered fashion it becomes a powerful model to adopt in a real-world situation for effective prevention of fraud.

For example, if a fraud is already detected from a device fingerprint then there should be instant decision and that order should be flagged as bad.

3.2 Pulses

Pluses is just a name for features and other computed values that are important, for example geological information, IP data, device fingerprint etc. An order data can have the following pulses:

Table 5: List of pulses

S.No	Pluse Name	S.No	Pluse Name
1	IP Information	12	Payment Information
2	Geo Logical Information	13	Phone Number
3	Device Fingerprints	14	Area Code
4	Frequency of Orders	15	Age of First/Last Transaction
5	Email Address	16	Billing Address
6	Order Total	17	Billing Name
7	Postal Address	18	Shipping Address
8	Customer Name	19	Number of items
9	Traffic Source	20	User Activity
10	User Browser Agent	21	User OS Agents
11	Status Of Transaction	22	Score From ML Technique

3.3 Good Pluses Vs Bad Pulses

Pulses can either be good or bad for example

Table 6: List of Good Vs Bad pulses

A Good Pulse	Bad Pulse
First Time Device Fingerprint for a new customer	A bad customer already associated with a Device Fingerprint
IP Address is not in blacklisted Database	IP Address is blacklisted
Billing Address and shipping Address matches	Billing and shipping address doesn't match
Age of email address is longer than 6 months	Age of email address is less than 24 hours
Order contains a few products	Order contains too many random products
Probability of Fraud is low	Probability of Fraud is high

Pulses can either be part of the features sent to a machine learning algorithm for the calculation of probability or to the rule engine to do initial processing on information.

3.3 Foundation Of The Proposed Model

In this section, different layers of proposed model are explained.

3.4 Architecture And Tools

1. Heroku Postgres SQL database will be use
2. For Machine Learning, Azure Machine Learning Studio will be used
3. Azure messaging queues are used to communicate between different layers of frame works
4. Heroku is used to host the management console of framework
5. Send grid is used to send emails to customers
6. Management Console is written in NodeJS
7. Machine Learning Experiments are done in R

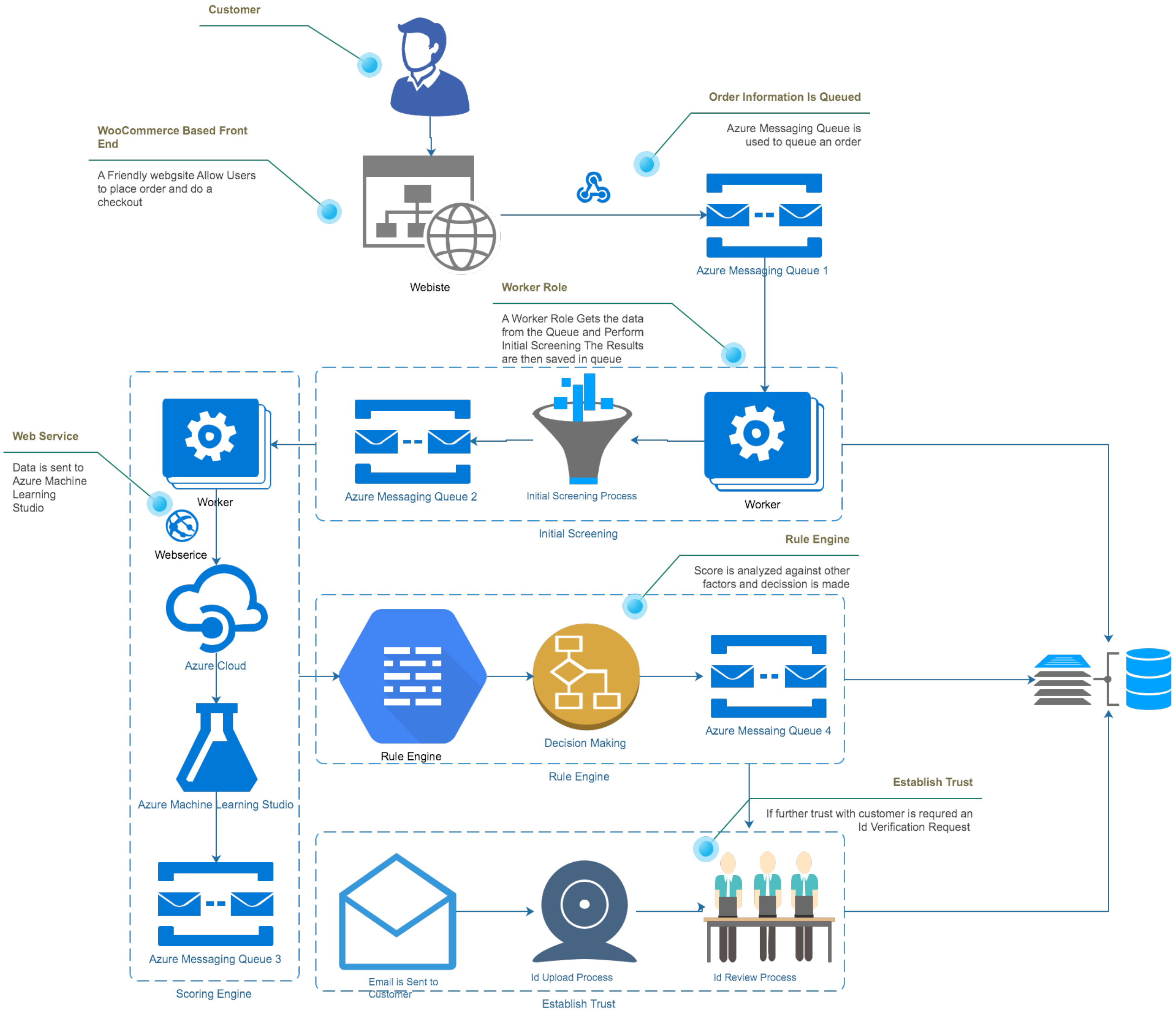

Customer
WooCommerce Based Front End
A Friendly webgsite Allow Users to place order and do a checkout
Webiste
Order Information Is Queued
Azure Messaging Queue is used to queue an order
Azure Messaging Queue 1
Worker Role
A Worker Role Gets the data from the Queue and Perform Initial Screening The Results are then saved in queue
Web Service
Data is sent to Azure Machine Learning Studio
Worker
Webserice
Azure Messaging Queue 2
Initial Screening Process
Worker
Initial Screening
Rule Engine
Score is analyzed against other factors and decission is made
Azure Cloud
Rule Engine
Decision Making
Azure Messaing Queue 4
Rule Engine
Azure Machine Learning Studio
Establish Trust
If further trust with customer is requred an Id Verification Request
Azure Messaging Queue 3
Scoring Engine
Email is Sent to Customer
Id Upload Process
Id Review Process
Establish Trust

Figure 18: Proposed System Architecture of the model

3.5 Layer 1: Initial Screening

A list of white listed and blacklisted customers customer is maintained and if an order comes in from the customer an immediate action is taken and if the customer is not matched in the database, the process proceeds to Layer 2. Example of a simple Blacklisted Pulse:

1. Customer’s Email Address is blacklisted.
2. Customer’s Device Fingerprint is blacklisted
3. Customer’s IP is blacklisted

These lists can be created manually time to time or can be created automatically by the Rule engine in Layer 3.

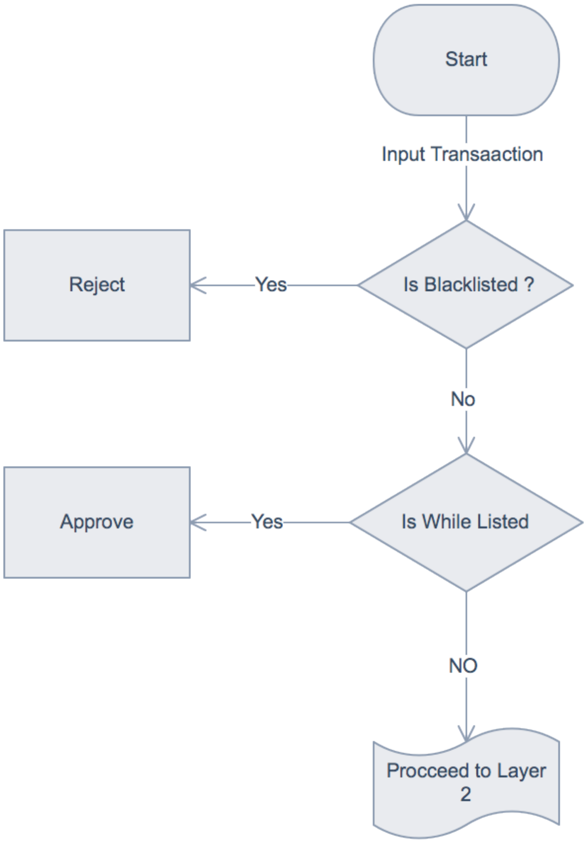


Figure 19: Layer 1 of model

3.6 Layer 2: Calculating Score

This Layer applies a ML Technique on the data and assign a probability (score) to the transaction. A web service is used to send the transaction details to the hosted machine learning trained model. Once this score is received it is attached with the transaction information and then sent to Layer 3.

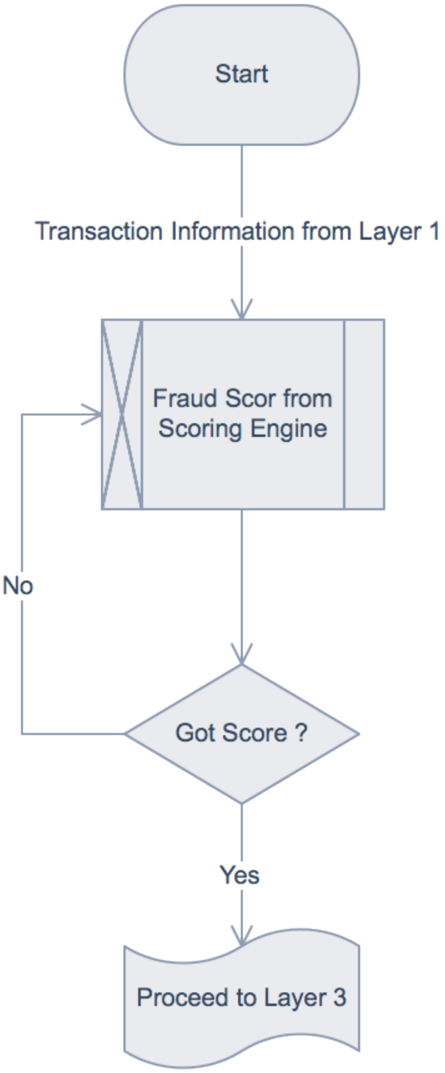

Start
Transaction Information from Layer 1
Fraud Scor from Scoring Engine
No
Got Score ?
Yes
Proceed to Layer 3

Figure 20: Layer 2 of model

3.7 Layer 3: Rule Engine

Rule engine is where the decision is made it's a filter based on pulses, it passes the transaction through these pulses and conditions. Rules can be created manually while doing manual reviews, observations and auditing. Following are the example of a few rules:

Table 7: List of Rules

Rule	Out Put
Score is less than 30 and order amount is between 0 and 100	PASS
Score is less that 40 Country is US and Order Amount is between 250 and 300	MANUAL REVIEW
Customer Email Address Matches with the Device Fingerprint of Blacklisted Customer	FAILED / UPDATE BLACKLIST
Score is 50 and Order Amount is between 150 and 200	ESTABLISH TRUST
Customer placed more than 4 orders in the same day	ESTABLISH TRUST

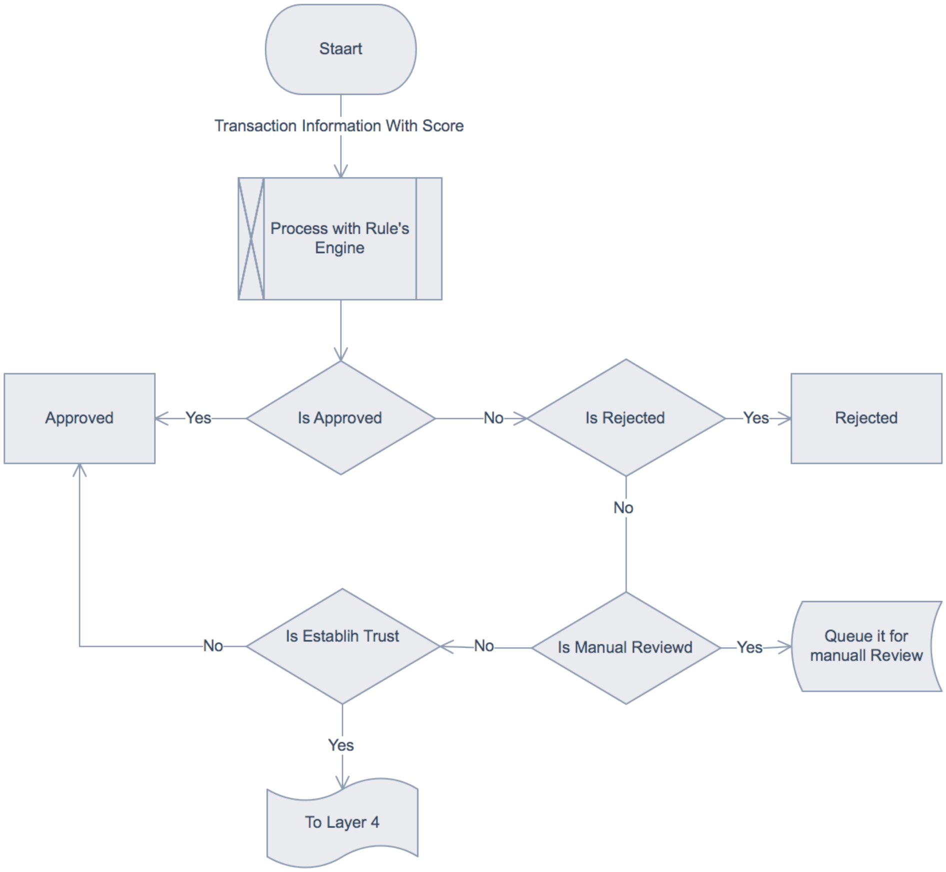


Figure 21: Layer 3 of model

3.8 Layer 4: Establishing Trust

Trust can be an important factor for doing online business, trust works both ways receiving an order means that customer who placed an order already trusted your business. But sometimes it is required to establish trust with customers. Following are the few reasons when we might want to establish a trust:

- Customer Got a score/probability of 50 that means this can either be a good a customer or bad customer in this case we might want to establish trust with the customer
- Customer Order exceeds the normal purchasing behavior
- Customers Device fingerprint changed

Trust can establish by:

- Adding verifiable information to the transaction
- Adding photo Id of a customer to the transaction

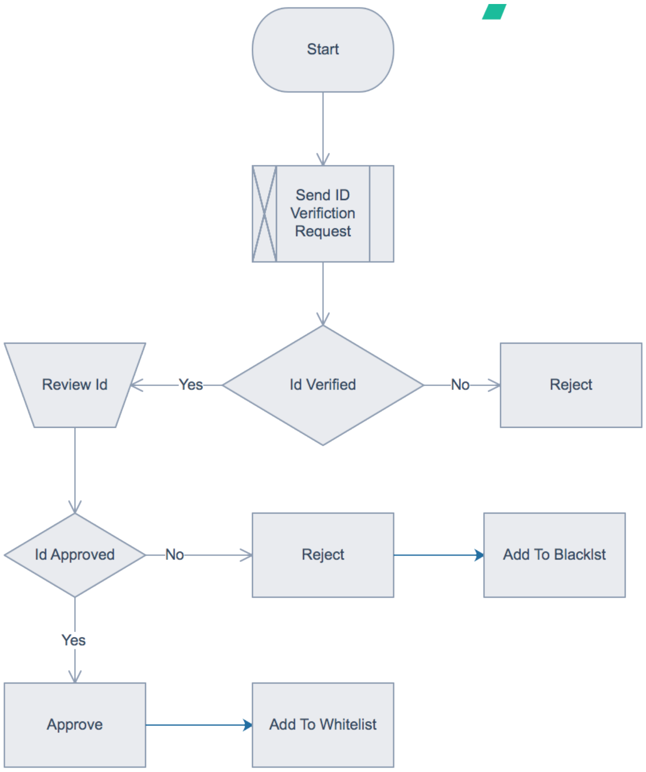


Figure 22: Layer 4 of model

3.9 Chapter Summary

In this chapter a multilayer fraud prevention model is proposed in next chapter this study will implement this model on a real business.

4

EXPERIMENTATION AND RESULTS

4. EXPERIMENTATION AND RESULTS

4.1 Dataset

Dataset is obtained from Microsoft's AI Research and Machine Learning Offerings (Research) (Research)which contains 200000 records of actual transaction data. Following are some key properties of the data.

Table 8: Dataset Properties

Total Records	Non-Fraudulent	Fraudulent
200,000	191360	8640
	95.68 %	4.32 %

There are 52 columns in the data set including the label field

1. transactionAmount
2. transactionCountryCode
3. transactionCurrencyConverstionRate
4. TransactionDate
5. transactionTime
6. localHour
7. transactionScenario
8. transactionType
9. transactionMethod
10. transactionDeviceType
11. transactionDeviceId
12. transactionIpAddress
13. ipState
14. ipPostalCode
15. ipCountry
16. isProxyIp
17. browserType
18. browserLanguage
19. paymentInstrumentType

20. cardType
21. cardNumberInputMethod
22. paymentInstrumentNumber
23. paymentBillingAddress
24. paymentBillingPostalCode
25. paymentBillingState
26. paymentBillingCountryCode
27. paymentBillingName
28. shippingAddress
29. shippingPostalCode
30. shippingCity
31. shippingState
32. shippingCountry
33. ccVerifyResult
34. responseCode
35. digitalItemCount
36. purchaseProductType
37. accountOwnerName
38. accountAddress
39. accountPostalCode
40. accountCity
41. accountCountry
42. accountOpenDate
43. accountAge
44. isUserRegisterd
45. paymentAgeInAccount
46. sumPurchaseAmount1Day
47. sumPurchaseAmount30Day
48. numPaymentRejected1Day
49. Label
50. physicalItemCount
51. accountId
52. transactionAmountUSD

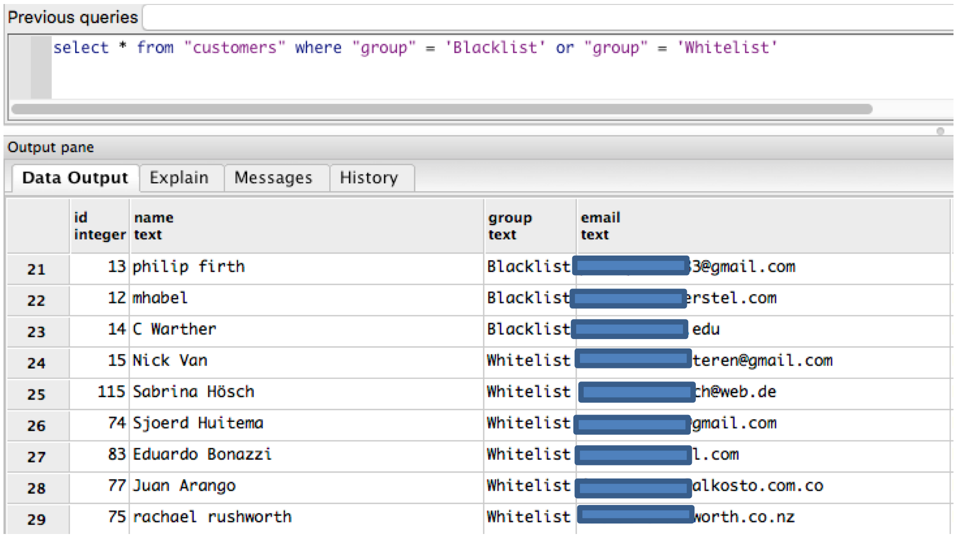
4.2 Implementing Initial Screening

Once a fraud has been confirmed from an account user can be automatically added to the database table, with a blacklisted flag. Every future order request must be denied from that customer. Following events can be noted as a signal to add a customer in a blacklisted database:

- Customer files a dispute with an "Unauthorized" reason
- Customer contacts the support and claims he didn't made any payment on your store.
- Customer lies about not getting product and incorrect quality claims

Following events can be noted as a signal to add a customer in whitelisted database:

- Customer have established a business relationship for years
- There is a trust factor established with the customer



```
select * from "customers" where "group" = 'Blacklist' or "group" = 'Whitelist'
```

	id integer	name text	group text	email text
21	13	philip firth	Blacklist	[redacted]3@gmail.com
22	12	mhabel	Blacklist	[redacted]rstel.com
23	14	C Warther	Blacklist	[redacted] edu
24	15	Nick Van	Whitelist	[redacted]teren@gmail.com
25	115	Sabrina Hösch	Whitelist	[redacted]h@web.de
26	74	Sjoerd Huitema	Whitelist	[redacted]gmail.com
27	83	Eduardo Bonazzi	Whitelist	[redacted]l.com
28	77	Juan Arango	Whitelist	[redacted]alkosto.com.co
29	75	rachael rushworth	Whitelist	[redacted]worth.co.nz

Figure 23: Whitelist & Blacklist customers saved in database

When an order comes in, it is checked in this table to see if a customer is blacklisted. If blacklisted than the order is rejected, and payment is refunded. If customer is whitelisted order is processed and if customer is neither whitelisted nor blacklisted. Order is sent to scoring engine.

4.3 Implementing Scoring Engine

Scoring engine is a module that apply machine learning to the order data and assign a score. Scoring engine is a 5-step process. Scoring engine is based on a Cortana intelligence Fraud Control Template (Microsoft). This process starts with data gathering.

4.4 Data Gathering

Data comes in two separate csv files the untagged file with all the customer transactions information and csv file with the list of fraudulent transactions. Both of these files are aggregated, and a single file is produced with the labels. Untagged transaction file fields are:

Table 9: Fields in dataset

transactionAmount	transactionCountryCode	transactionCurrencyConverstionRate	TransactionDate
transactionTime	localHour	transactionScenario	transactionType
transactionMethod	transactionDeviceType	transactionDeviceId	transactionIpAddress
ipState	ipPostalCode	ipCountry	isProxyIp
browserType	browserLanguage	paymentInstrumentType	cardType
cardNumberInputMethod	paymentInstrumentNumber	paymentBillingAddress	paymentBillingPostalCode
paymentBillingState	paymentBillingCountryCode	paymentBillingName	shippingAddress
shippingPostalCode	shippingCity	shippingState	shippingCountry
ccVerifyResult	responseCode	digitalItemCount	purchaseProductType
accountOwnerName	accountAddress	accountPostalCode	accountCity
accountCountry	accountOpenDate	accountAge	isUserRegisterd

paymentAgeInAccount	sumPurchaseAmount1Day	sumPurchaseAmount30Day	numPaymentRejected1Day
Label	physicalItemCount	accountId	transactionAmountUSD

Field in the fraudulent transaction file are:

Table 10: Fields in fraudulent transaction file

transactionID	accountID	transactionAmount
transactionCurrencyCode	transactionDate	transactionTime
localHour	transactionDeviceId	transactionIPaddress

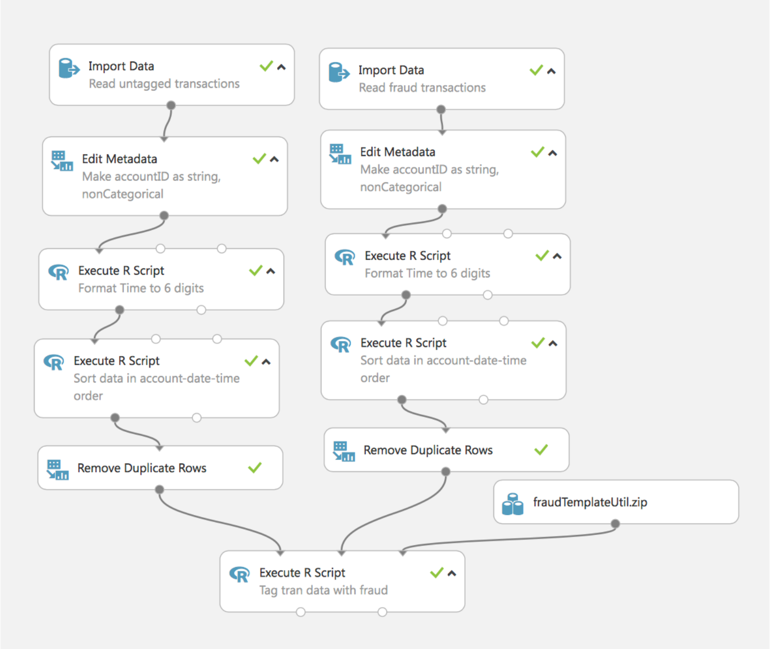


Figure 24: Data Gathering with Azure ML Studio

1. Import Data: Data is imported from data source.
2. Edit Metadata: Makes sure that “accountId” is non-numeric
3. “transactionTime” is formatted in HHMMSS format
4. Data is sorted by first “accountId”, “date” and then “time”

5. Duplicate Data is removed

When this process is complete, a CSV file with following fields is ready for the next step:

Table 11: Fields of dataset with label

transactionAmount	transactionCountryCode	transactionCurrencyConverstionRate	TransactionDate
transactionTime	localHour	transactionScenario	transactionType
transactionMethod	transactionDeviceType	transactionDeviceId	transactionIpAddress
ipState	ipPostalCode	ipCountry	isProxyIp
browserType	browserLanguage	paymentInstrumentType	cardType
cardNumberInputMethod	paymentInstrumentNumber	paymentBillingAddress	paymentBillingPostalCode
paymentBillingState	paymentBillingCountryCode	paymentBillingName	shippingAddress
shippingPostalCode	shippingCity	shippingState	shippingCountry
ccVerifyResult	responseCode	digitalItemCount	purchaseProductType
accountOwnerName	accountAddress	accountPostalCode	accountCity
accountCountry	accountOpenDate	accountAge	isUserRegisterd
paymentAgeInAccount	sumPurchaseAmount1Day	sumPurchaseAmount30Day	numPaymentRejected1Day
Label	physicalItemCount	accountId	transactionAmountUSD

4.5 Pre-processing Data

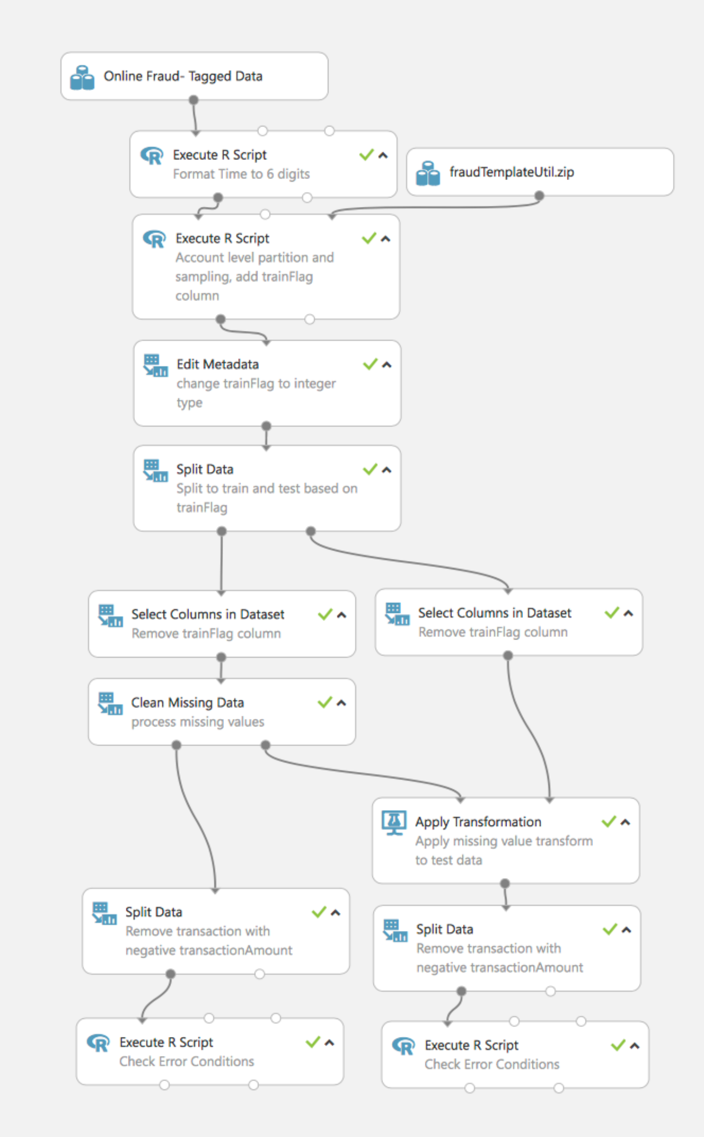

Online Fraud- Tagged Data
Execute R Script
Format Time to 6 digits
fraudTemplateUtil.zip
Execute R Script
Account level partition and sampling, add trainFlag column
Edit Metadata
change trainFlag to integer type
Split Data
Split to train and test based on trainFlag
Select Columns in Dataset
Remove trainFlag column
Select Columns in Dataset
Remove trainFlag column
Clean Missing Data
process missing values
Apply Transformation
Apply missing value transform to test data
Split Data
Remove transaction with negative transactionAmount
Split Data
Remove transaction with negative transactionAmount
Execute R Script
Check Error Conditions
Execute R Script
Check Error Conditions

Figure 25: Preprocessing Data

1. Reader reads the data generated in step 1
2. Time is formatted in 6 digits
3. “trainFlag” is added at account level, all the transactions from one account can only be in Train or Test Data Sets. Adds a column to identify “Train Data”
4. Train Data flag is converted to integer
5. Data is split into “Train Data” & “Test Data” based on the “trainFlag”
6. Missing values are replaced with “0” using a Clean missing value module provided by azure machine learning (Microsoft)

7. Removed the “trainFlag” as it is not needed after data is split
8. Using the “Apply transform module” (Microsoft) apply the “Clean Missing Values” to the data
9. Remove any transaction with negative values
10. Removed any transaction with incorrect date time or empty date time

When this step is completed data is split in two parts with 70% data for model training and 30% data as a test data. After performing this step, the data fields remain the same as step 1. Next Feature engineering is performed on this data.

4.6 Feature Engineering.

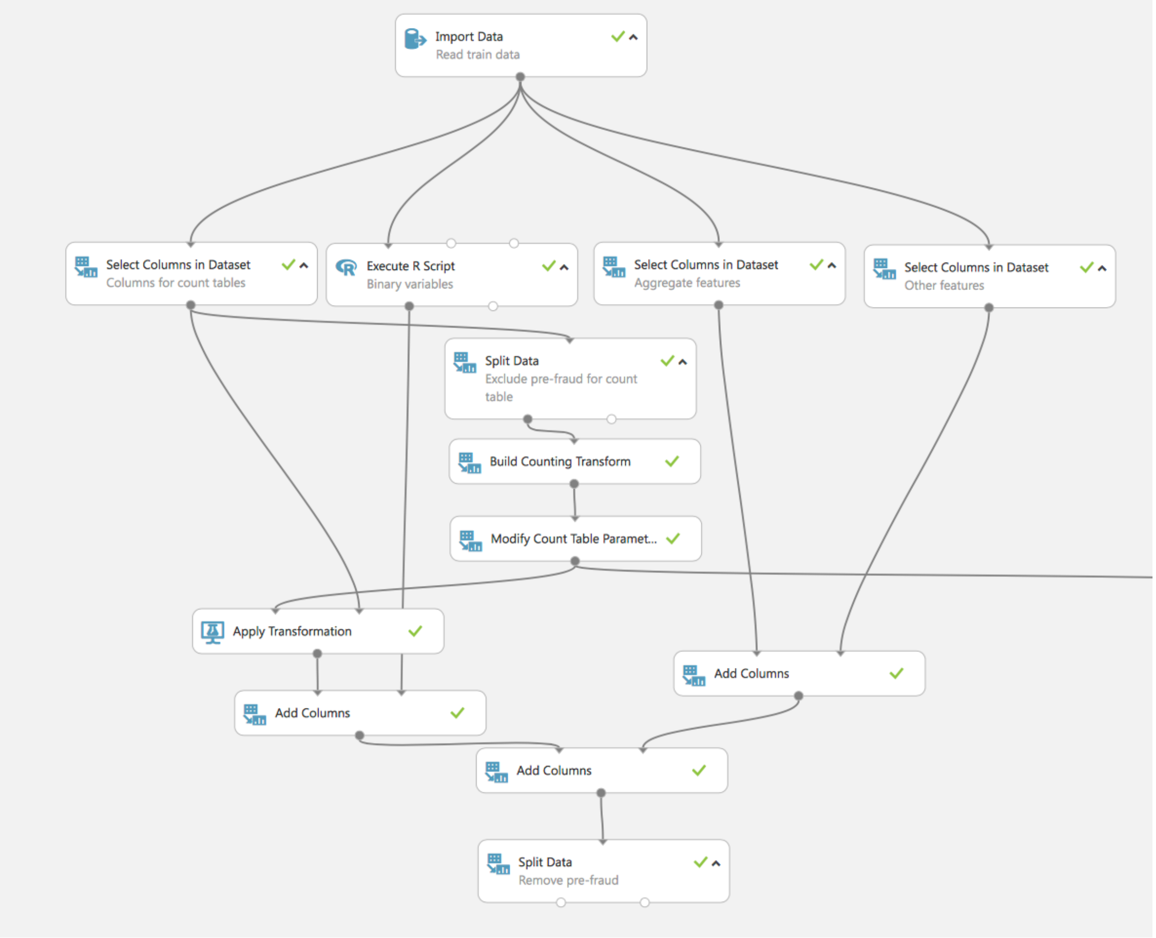


Figure 26: Feature engineering training data

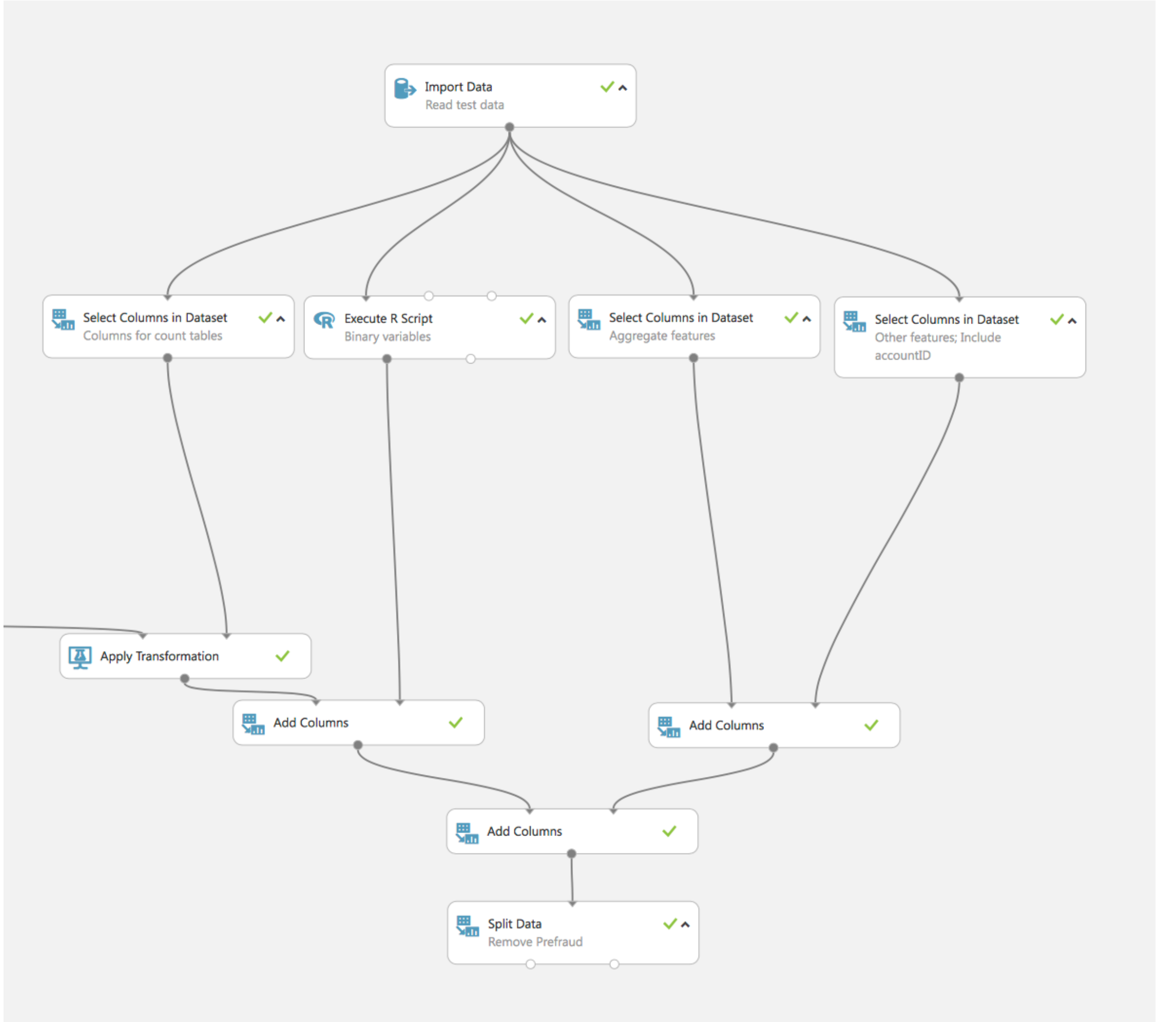


Figure 27: Feature engineering test data

Count based features: These columns have large number of unique categorical values. These are also called "count based features" .

"*The basic idea underlying* count-based featurization *is simple: by calculating counts, you can quickly and easily get a summary of what columns contain the most important information. The module counts the number of times a value appears, and then provides that information as a feature for input to a model."* (Microsoft)

Table 12: Count based features

transactionCountryCode	localHour	ipState	ipPostalCode
ipCountry	browserLanguage	paymentBillingPostalCode	paymentBillingState
paymentBillingCountryCode	shippingPostalCode	shippingState	shippingCountry
accountPostalCode	accountState	accountCountry	label

A few more binary field columns are introduced:

Table 13: Binary features

Is_highAmount	acct_billing_address_mismatchFlag	acct_billing_postalCode_mismatchFlag
acct_billing_country_mismatchFlag acct_shipping_postalCode_mismatchFlag	acct_billing_name_mismatchFlag acct_shipping_country_mismatchFlag	acct_shipping_address_mismatchFlag shipping_billing_address_mismatchFlag
shipping_billing_postalCode_mismatchFlag	shipping_billing_country_mismatchFlag	

Aggregated Account Level Features are:

Table 14: Aggregated features

sumPurchaseAmount1Day	sumPurchaseAmount30Day	sumPurchaseCount

Following are transaction related and other fields:

Table 15: Other features

transactionAmountUSD	transactionAmount	transactionType
transactionMethod	transactionDeviceType	isProxyIP
browserType	paymentInstrumentType	cardType

cardNumberInputMethod	cvvVerifyResult	responseCode
digitalItemCount	physicalItemCount	purchaseProductType
accountAge	isUserRegistered	paymentInstrumentAgeInAc

Applying Count-based Transformation To Count-based Features.

If a credit card transaction requires a validation. An important piece of information is from where the transaction was initiated. There might be 40,000 plus postal codes in the data. The important point is does the model have capacity learn 40,000 more parameters? even if that capacity is given to the data, is the training data enough to stop it from overfitting.

For large sets of data, such granularity can be very powerful, having data from a small locality all are the transaction from a specific postal code are bad or simply the data is not enough.

Solution to this problem is instead of waiting to have enough data before starting a learning process. Observe the count of the proportions of fraud in each postal code. By using these counts as features the learner can use the statistics to decide when to back-off and use other features.

A windows azure module for "Data-Transformation" module is used to transform the count-based features (jeannt). The following example demonstrate how to calculate count-based features.

Table 16: Label & input values

Label column	Input Value
0	A
0	A
1	A
0	B
1	B
1	B
1	B

For a particular set of values, you find all the other cases in that dataset that have the same value. In this case, there are three instances of A and four of B.

Next, count their class memberships as features in themselves. In this case, you get a small matrix, in which there are 2 cases where A=0, 1 case where A = 1, 1 case where B= 0, and 3 cases where B = 1.

Based on this matrix, you get a variety of count-based features, including a calculation of the log-odds ratio as well as the counts for each target class:

Table 17: Calculated count-based values

Label	class000_count	class001_count	Class000_LogOdds	IsBackoff
0	2	1	0.510826	0
0	2	1	0.510826	0
1	2	1	0.510826	0
0	1	3	-0.8473	0
1	1	3	-0.8473	0
1	1	3	-0.8473	0
1	1	3	-0.8473	0

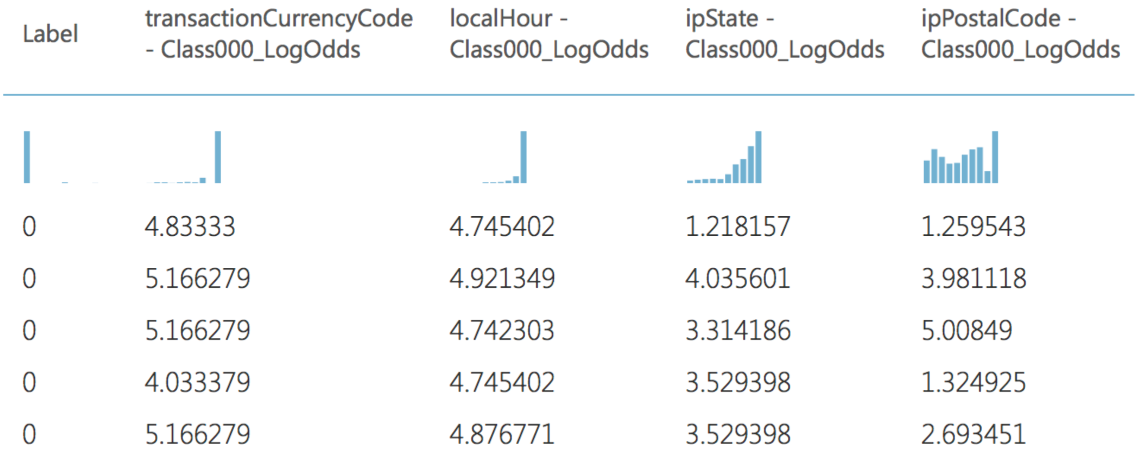
Calculation of log_odds [35]:

Log_odds[i] = Log((count[i] + prior_coefficient * prior_frequency[i]) / (sum_of_counts - count[i]) + prior_coefficient * (1 - prior_frequency[i]))

If the prior coefficient is positive, the log odds can be different from

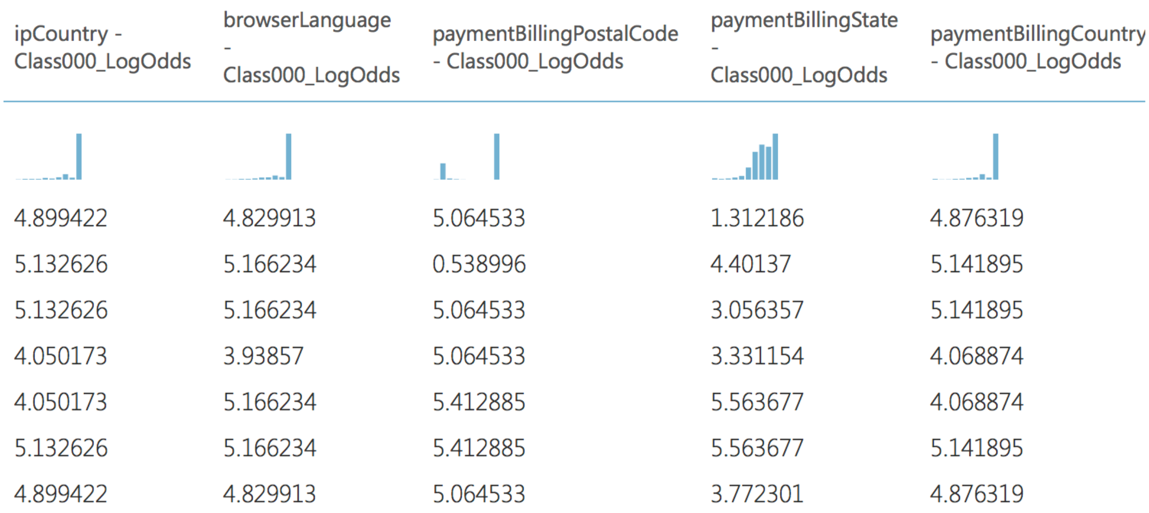
Log(count[i] / (sum_of_counts – count[i])).

After applying the “count-based” transformation the count-based features transform to



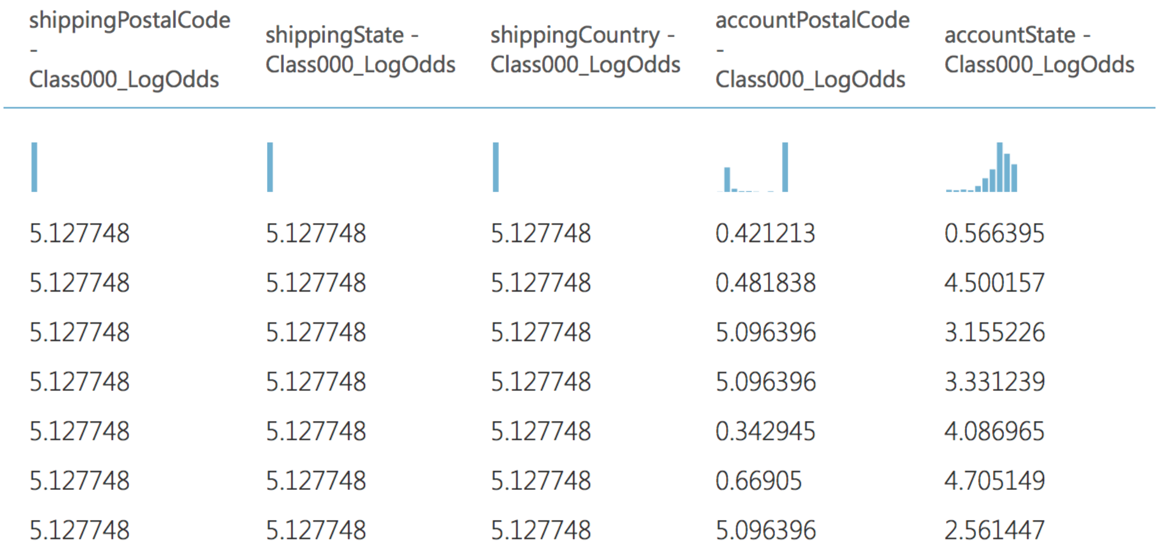
Label	transactionCurrencyCode - Class000_LogOdds	localHour - Class000_LogOdds	ipState - Class000_LogOdds	ipPostalCode - Class000_LogOdds
0	4.83333	4.745402	1.218157	1.259543
0	5.166279	4.921349	4.035601	3.981118
0	5.166279	4.742303	3.314186	5.00849
0	4.033379	4.745402	3.529398	1.324925
0	5.166279	4.876771	3.529398	2.693451

Figure 28: Values after applying count-based features (a)



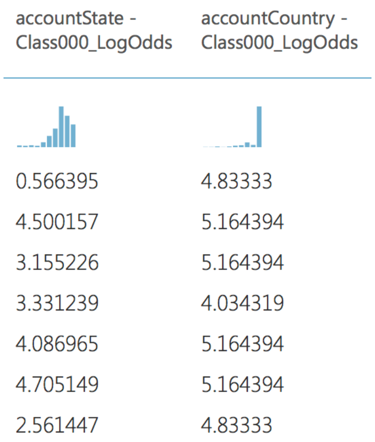
ipCountry - Class000_LogOdds	browserLanguage - Class000_LogOdds	paymentBillingPostalCode - Class000_LogOdds	paymentBillingState - Class000_LogOdds	paymentBillingCountry - Class000_LogOdds
4.899422	4.829913	5.064533	1.312186	4.876319
5.132626	5.166234	0.538996	4.40137	5.141895
5.132626	5.166234	5.064533	3.056357	5.141895
4.050173	3.93857	5.064533	3.331154	4.068874
4.050173	5.166234	5.412885	5.563677	4.068874
5.132626	5.166234	5.412885	5.563677	5.141895
4.899422	4.829913	5.064533	3.772301	4.876319

Figure 29: Values after applying count-based features (b)



shippingPostalCode - Class000_LogOdds	shippingState - Class000_LogOdds	shippingCountry - Class000_LogOdds	accountPostalCode - Class000_LogOdds	accountState - Class000_LogOdds
5.127748	5.127748	5.127748	0.421213	0.566395
5.127748	5.127748	5.127748	0.481838	4.500157
5.127748	5.127748	5.127748	5.096396	3.155226
5.127748	5.127748	5.127748	5.096396	3.331239
5.127748	5.127748	5.127748	0.342945	4.086965
5.127748	5.127748	5.127748	0.66905	4.705149
5.127748	5.127748	5.127748	5.096396	2.561447

Figure 30: Values after applying count-based features (c)



accountState - Class000_LogOdds	accountCountry - Class000_LogOdds
0.566395	4.83333
4.500157	5.164394
3.155226	5.164394
3.331239	4.034319
4.086965	5.164394
4.705149	5.164394
2.561447	4.83333

Figure 31: Values after applying count-based features (c)

The last step is to combine all features. Following fields will be sent to the model for training.

Table 18: Final features for model training

Label	shipping_billing_postalCode_mismatchFlag
transactionCurrencyCode - Class000_LogOdds	shipping_billing_country_mismatchFlag
localHour - Class000_LogOdds	sumPurchaseAmount1Day
ipState - Class000_LogOdds	sumPurchaseAmount30Day

ipPostalCode - Class000_LogOdds	sumPurchaseCount1Day
ipCountry - Class000_LogOdds	sumPurchaseCount30Day
browserLanguage - Class000_LogOdds	numPaymentRejects1Day
paymentBillingPostalCode - Class000_LogOdds	transactionAmountUSD
paymentBillingState - Class000_LogOdds	transactionAmount
paymentBillingCountryCode - Class000_LogOdds	transactionType
shippingPostalCode - Class000_LogOdds	transactionMethod
shippingState - Class000_LogOdds	transactionDeviceType
shippingCountry - Class000_LogOdds	isProxyIP
accountPostalCode - Class000_LogOdds	browserType
accountState - Class000_LogOdds	paymentInstrumentType
accountCountry - Class000_LogOdds	cardType
is_highAmount	cardNumberInputMethod
acct_billing_address_mismatchFlag	cvvVerifyResult
acct_billing_postalCode_mismatchFlag	responseCode
acct_billing_country_mismatchFlag	digitalItemCount
acct_billing_name_mismatchFlag	physicalItemCount
acct_shipping_address_mismatchFlag	purchaseProductType
acct_shipping_postalCode_mismatchFlag	accountAge
acct_shipping_country_mismatchFlag	isUserRegistered
shipping_billing_address_mismatchFlag	paymentInstrumentAgeInAccount

4.7 Model Training And Evaluation

Choosing algorithms is the first step, in “Related Study” Section of this study its noted that most of the techniques are very effective in fraud control. In fact, fraud control was one of the earliest implementations of machine learning.

In a research paper “Detecting Corporate Fraud: An Application of Machine Learning” authors found SVM got the best results, but the surprising fact was that even a single model like “logistic regression” was not far behind. (Ophir Gottlieb, 2006)
Based on “Related Study” following 3 types of models will be trained and compared and one of the best will be selected to proceed with:

1. SVM (Support Victor Machine) or Two Class Vector Machine
2. Boosted Decision Tree or Two Class Boosted Decision Tree
3. Neural Network. Or FF Neural Network or Two Class Neural Network

Name for SVM in Azure Machine Learning Studio is Two Class Support Vector Machine (jeannt). Name for Boosted Decision Tree in Azure Machine Learning Studio is Two Class Boosted Decision Tree (jeannt). Name for Neural Network in Azure Machine Learning Studio is Two Class Neural Network (jeannt).

4.8 Support Vector Machine.

ROC (Receiver Operating Characteristic Curve)

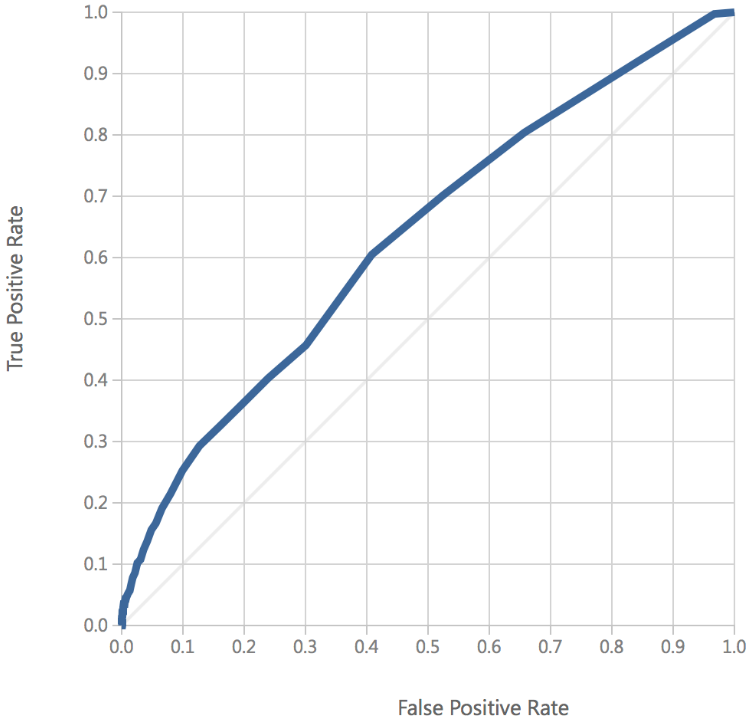


Figure 32: ROC for SVM

Table 19: Result of Experiment with SVM

True Positive	0
False Positive	0
False Negative	372
True Negative	58555
Accuracy	0.994
Recall	0.000
Precision	1.000
F1 Score	0.000

Recall = TP / (TP + FN)

Precision = TP / (TP + FP)

Where TP = True Positive, TN = True Negative, FP = False Positive, FN = False Negative

4.9 Two Class Boasted Decision Tree

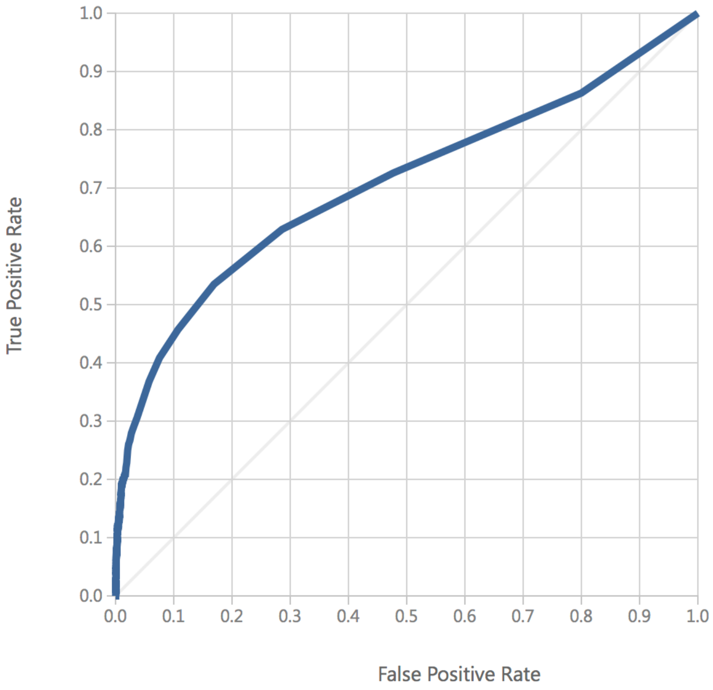


Figure 33: ROC for Boosted Decision Tree

True Positive	26
False Positive	81
False Negative	346
True Negative	58474
Accuracy	0.993
Recall	0.070
Precision	0.243
F1 Score	0.109

Figure 34: Experiment Results for Boosted Decission Tree

4.10 Feed Forward Neural Networks

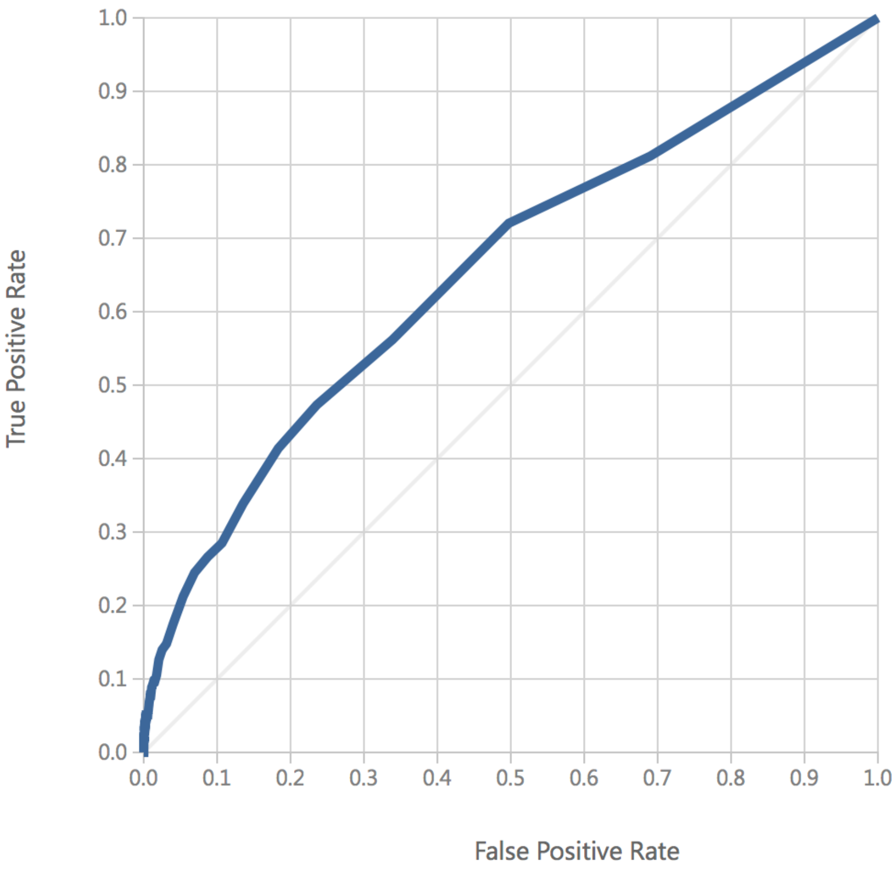


Figure 35: ROC for FF Neural Network

Table 20: Experiment results for FF NN

True Positive	0
False Positive	0
False Negative	372
True Negative	58555
Accuracy	0.994
Recall	0.000
Precision	1.000
F1 Score	0.000

4.11 SVM Vs BTD Vs FFNN

Table 21: Comparison of SVM, Boosted Decision Tree & FF Neural Networks

	SVM	**Boosted Decision Tree**	**Neural Network**
True Positive	0	26	0
False Positive	0	81	0
False Negative	372	346	372
True Negative	58555	58474	58555
Positive Label	1	1	1
Negative Label	0	0	0
Accuracy	0.994	0.993	0.994
Recall	0.000	0.070	0.000
Precision	1.000	0.243	1.000
F1 Score	0.000	0.109	0.000

Simple Accuracy: If I write an algorithm which does nothing and mark every transaction as not fraud it will still be 95.68% accurate as the total number of fraudulent transaction in the data is 4.32% that’s why only accuracy cannot be consider as the only measure of performance and efficiency

For both SVM and NN precision is very high and recall is 0, it means that both these algorithms are extremely picky and identifying a lot of false negatives.

Value of F1 score is harmonic mean of precision and recall, higher value of F1 demonstrate the better combination of precision and recall.

According to this comparative analysis Boosted Decision Tree performs better than other two.

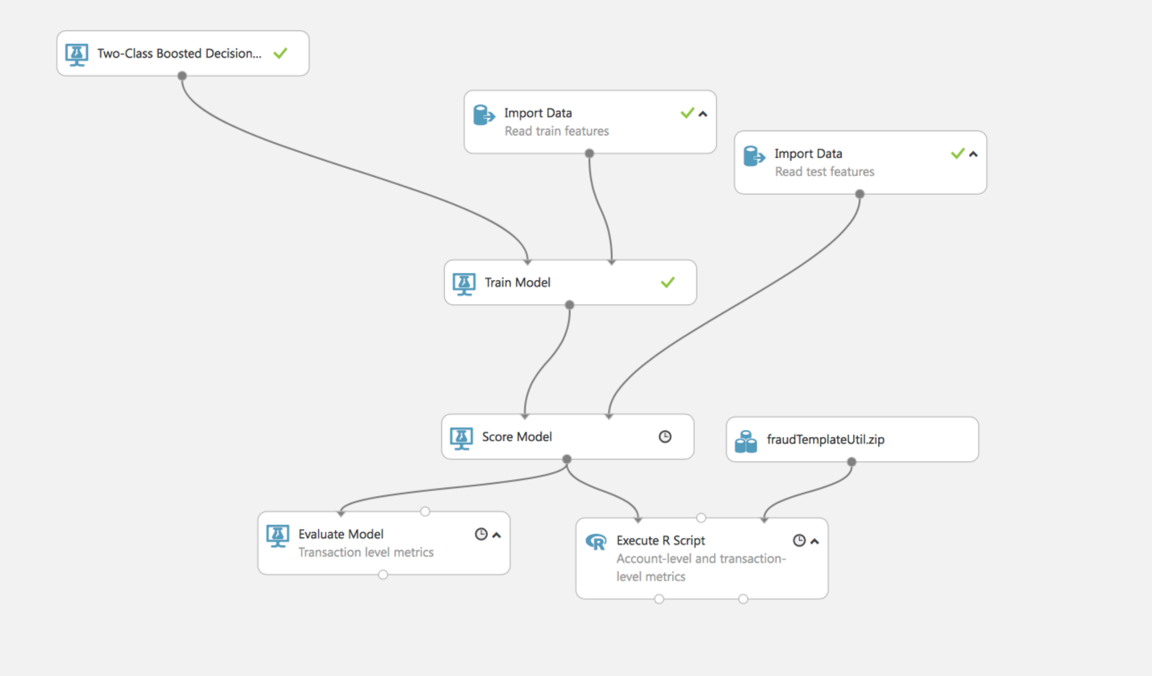


Figure 36: Model Training

Score model is used to predict score for classification and regression model (jeannt).

4.12 Deploying Trained Model

To deploy a model, connect all the data processing, feature engineering, scoring modules, saved transforms, and trained model to form one scoring experiment.

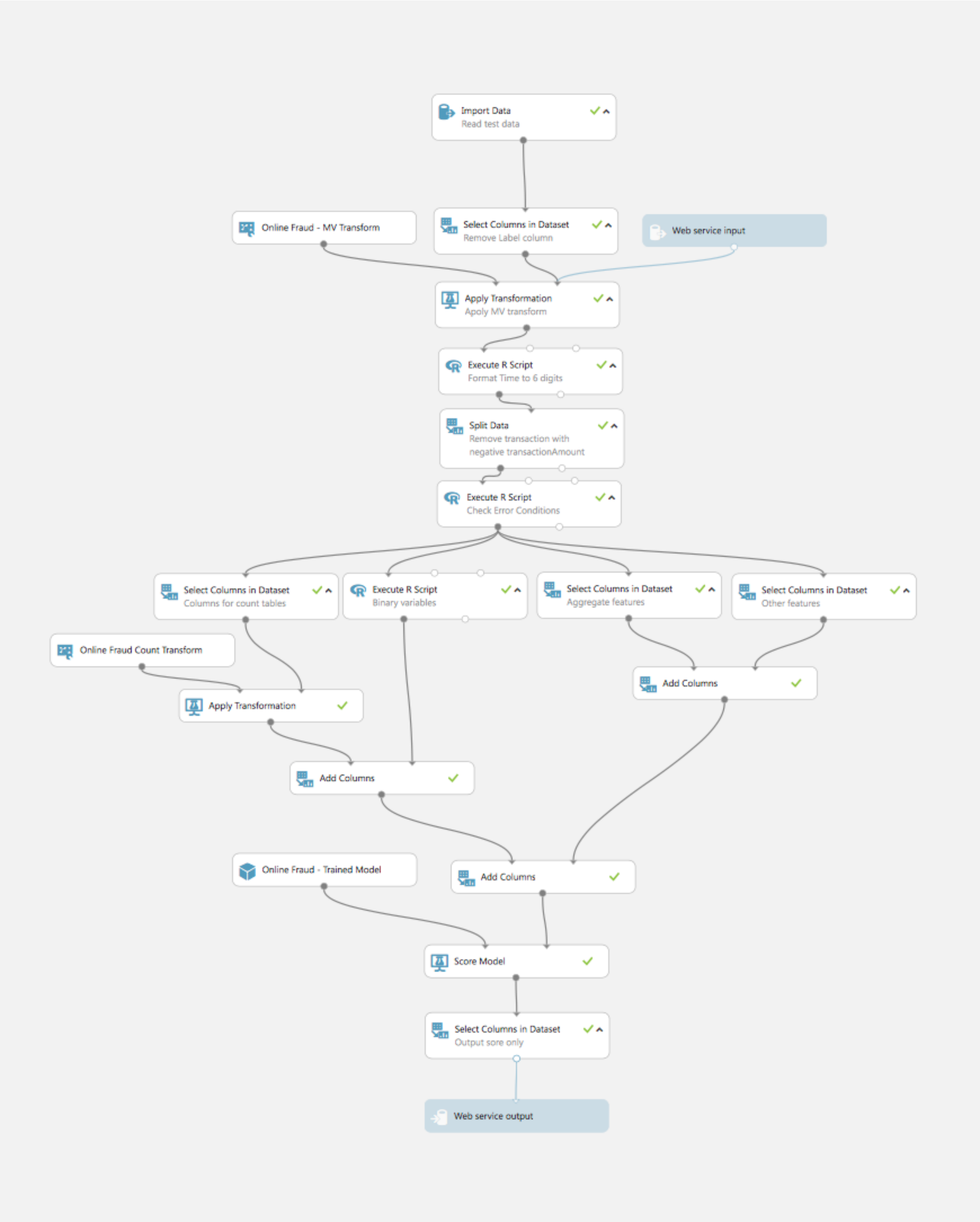
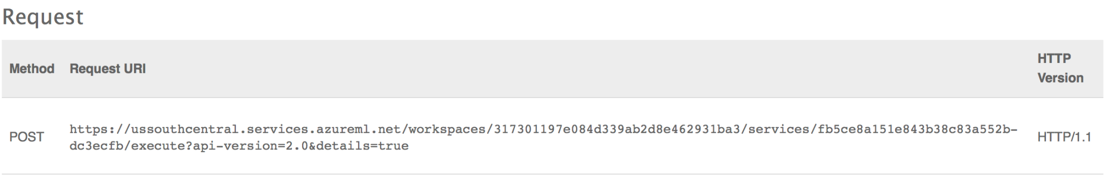


Figure 37: Deployment of trained model

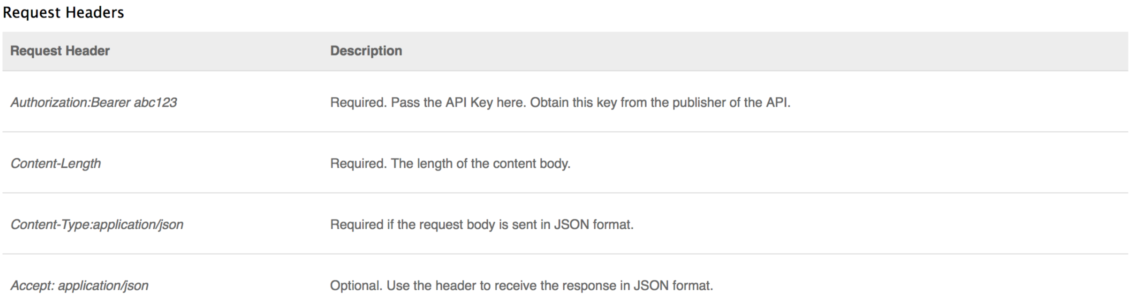
When a model is successfully deployed azure gives us an http end point where we can send post request with our data and get the score for new transactions.



Request

Method	Request URI	HTTP Version
POST	https://ussouthcentral.services.azureml.net/workspaces/317301197e084d339ab2d8e462931ba3/services/fb5ce8a151e843b38c83a552b-dc3ecfb/execute?api-version=2.0&details=true	HTTP/1.1

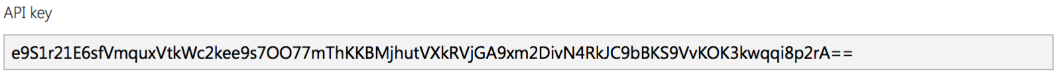
Figure 38: Http end point to get scores from the deployed model



Request Headers

Request Header	Description
Authorization:Bearer abc123	Required. Pass the API Key here. Obtain this key from the publisher of the API.
Content-Length	Required. The length of the content body.
Content-Type:application/json	Required if the request body is sent in JSON format.
Accept: application/json	Optional. Use the header to receive the response in JSON format.

Figure 39: Request Headers



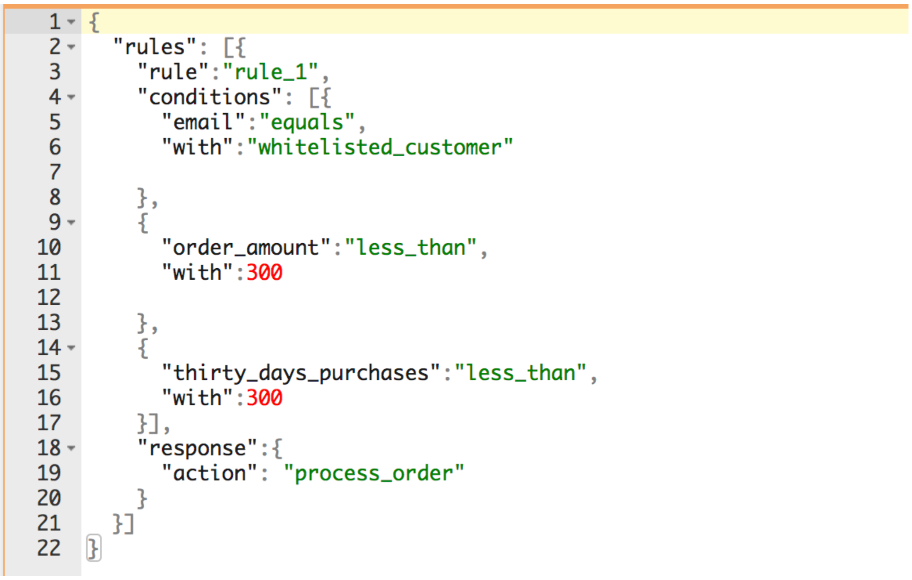
API key

e9S1r21E6sfVmquxVtkWc2kee9s7OO77mThKKBMjhutVXkRVjGA9xm2DivN4RkJC9bBKS9VvKOK3kwqqi8p2rA==

Figure 40: API Key to authenticate http requests

4.13 Implementing Rule Engine

Rule engine is a scripted implemented with “if” and “else” conditions. When a transaction comes in and a score is assigned then it is send to rule engine to take an action. Following screenshot demonstrate how this is implemented in code.



```
{
  "rules": [{
    "rule":"rule_1",
    "conditions": [{
      "email":"equals",
      "with":"whitelisted_customer"

    },
    {
      "order_amount":"less_than",
      "with":300

    },
    {
      "thirty_days_purchases":"less_than",
      "with":300
    }],
    "response":{
      "action": "process_order"
    }
  }]
}
```

Figure 41: Rule engine "if" and "else" statements

Some are the rules configured to work with model are following:

Table 22: A few rules configured in rule engine

Name	**Rules**	**Action**
Rule 1	Payment Method = BitPay	Process Order
Rule 2	Last Order Cancelled	Manual Review
Rule 3	Has Multiple Phone Numbers	Manual Review
Rule 4	Monthly Orders > 3	Manual Review
Rule 5	Payment Method = G2APay && Order Total > 300 && Weekly Order Velocity < 4	Process
Rule 6	Customer Age < 7 (days) && Is Not Direct Traffic && Order Total < 100 && Score < 51 && Phone Country = Billing Country && Monthly Velocity < 2	Process

Rule 7	Customer Age < 7 (days) && Is Not Direct Traffic && Order Total > 100 && Score > 40 && Score < 70 Phone Country = Billing Country && Monthly Velocity < 2	Establish Trust
Rule 8	Customer Age < 30 (days) && Customer Age > 7 (days) && Order Total < 150 && Score < 51 && Phone Country = Billing Country && Monthly Velocity < 2	Process Order
Rule 9	Customer Score > 80	Reject Order

Customer behavior changes and so do the business. It's been noticed that when business drops a strategy to retain older customers a more relaxed rule is required for older customers. Similarly, when a new marketing campaign is up a more relaxed rule is required for new customers.

4.14 Rules Are Effective Business Tools

Rules can be audited to observe and perform tweaks on the fraud control processes for business. When a transaction is passed through a rule its name and score is saved in the database. If a fraud is detected from that specific transaction database is updated and a report is generated this helps to understand the most effective rules and scores are and provides opportunity to fix the bad rules and improve business decisions.

4.15 Auditing Rules

Table 23: Auditing of rules

Name	Decision	Fraudulent	Score	Rejected	Total
Rule 1	Approve	1	0-19	5	145
Rule 2	Reject	0	50-69	450	450
Rule 3	Establish Trust	0	69-79	10	100
Rule 4	Manual Review	15	30-49	30	160

This enables the fraud control model to be optimized and adopt with the changing business dynamics. Following things can be observed from this table:

- Rule 1 is the most effective rule
- Rule 2 needs a tweak because it is rejecting too many orders, which in terms of refunds is a lost business opportunity
- Rule 3 is very good
- Rule 4 is having the most number of fraudulent transactions and needs tweaking

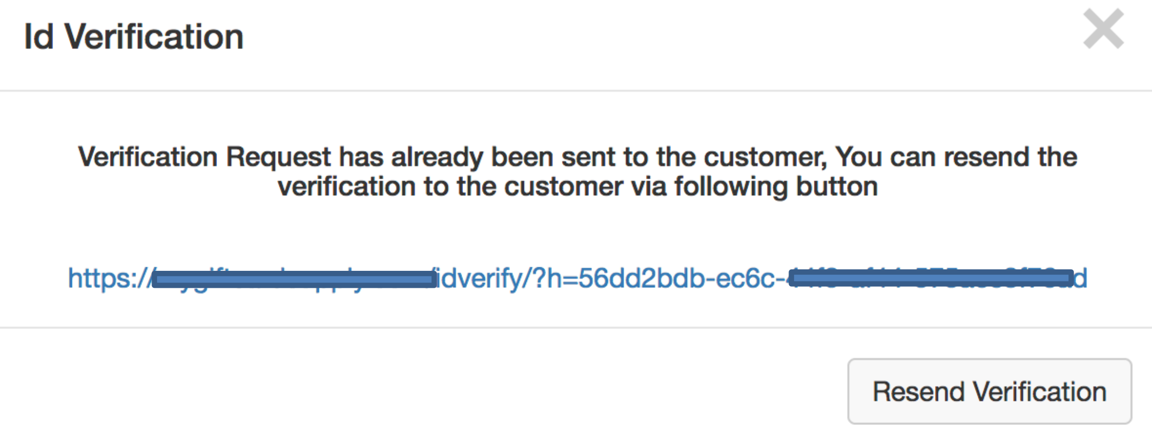
Another interesting fact is that, not just model is learning and improving the human observers are also learning the model which makes it irrelevant that how good the machine learning algorithm is because eventually observers will end up tweaking rules that are best for business.

4.16 Establishing Trust

Trust can be established with a customer by asking for his ID. Adding this step to fraud prevention model has dramatically decreased fraud and makes the future business with the returning customers more efficient.

One important thing to note is that ID verification is already a hectic process. It should only be done as a last line of defense. It means that if customer does not provide his Id the order should not be processed. It should be a user-friendly process and should work on mobile and desktop devices.

Once a rule Identifies that establishing trust is required to system sends an email to the customer to verify his Id.

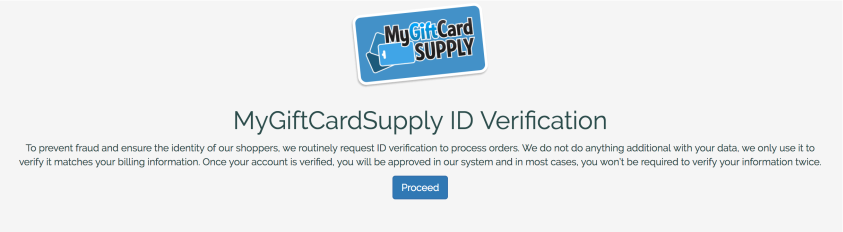


Verification Request has already been sent to the customer, You can resend the verification to the customer via following button

https://[redacted]idverify/?h=56dd2bdb-ec6c-[redacted]d

Figure 42: Id Verification URL

Id verification is a hectic process customer are explained why Id verification is required. This message is also used to take customer in the confidence that their data will be safe.

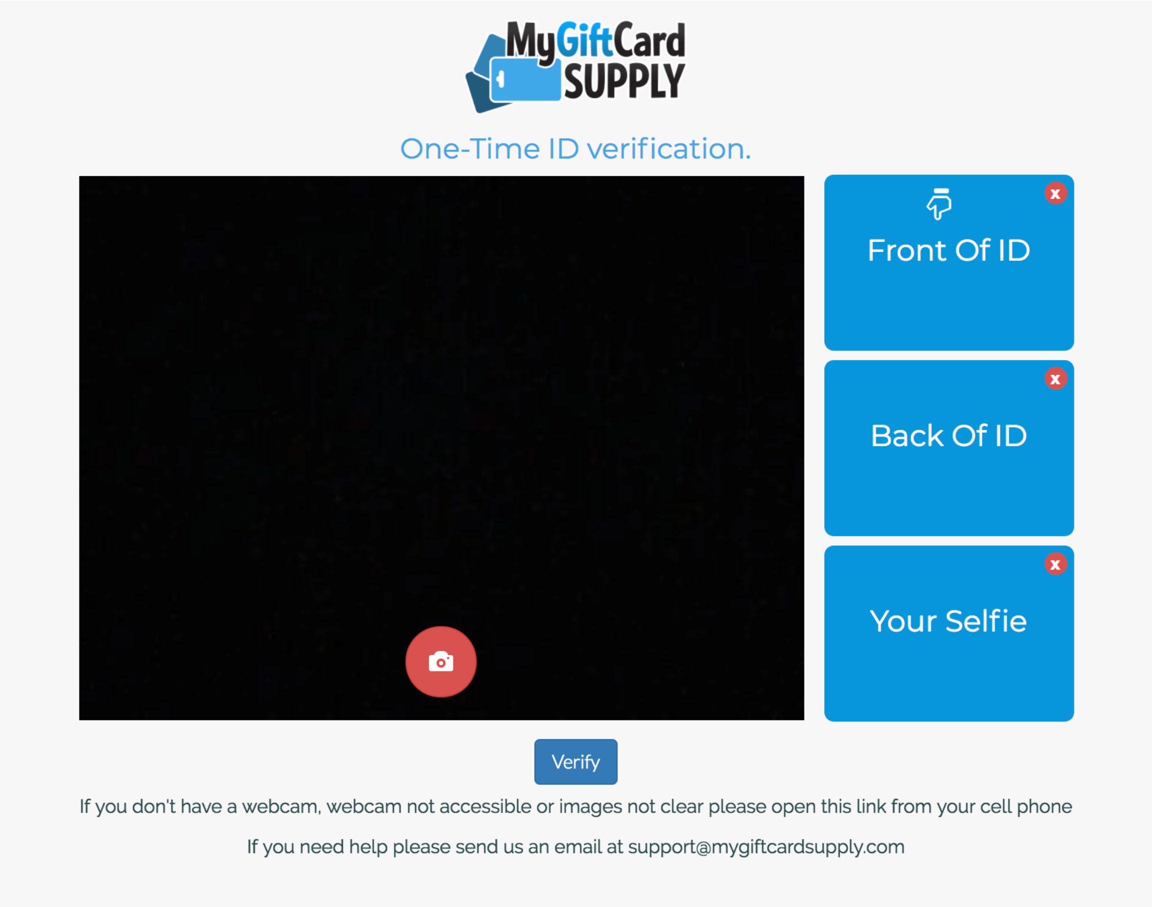


MyGiftCardSupply ID Verification

To prevent fraud and ensure the identity of our shoppers, we routinely request ID verification to process orders. We do not do anything additional with your data, we only use it to verify it matches your billing information. Once your account is verified, you will be approved in our system and in most cases, you won't be required to verify your information twice.

Figure 43: Taking customer in confidence

Id verification must be a user-friendly process.



If you don't have a webcam, webcam not accessible or images not clear please open this link from your cell phone

If you need help please send us an email at support@mygiftcardsupply.com

Figure 44: User friendly interface for customers to upload id

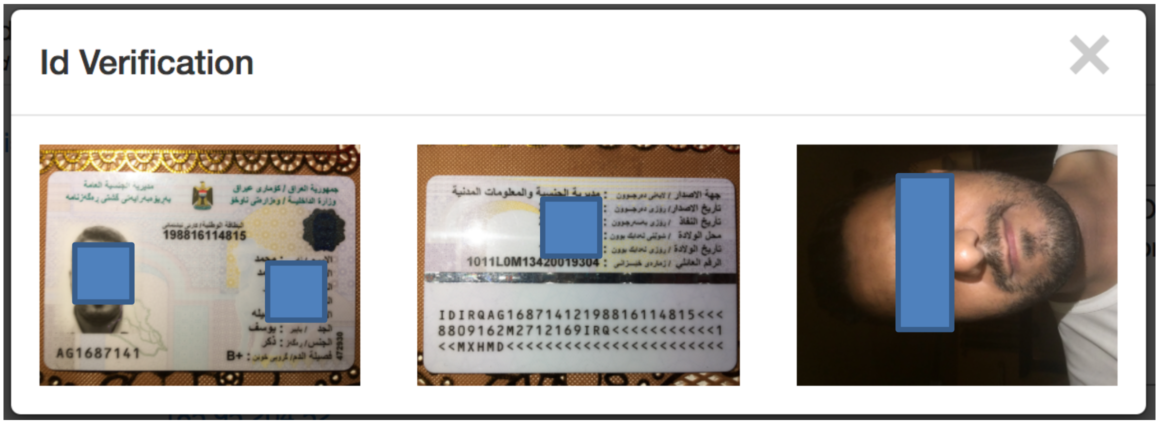
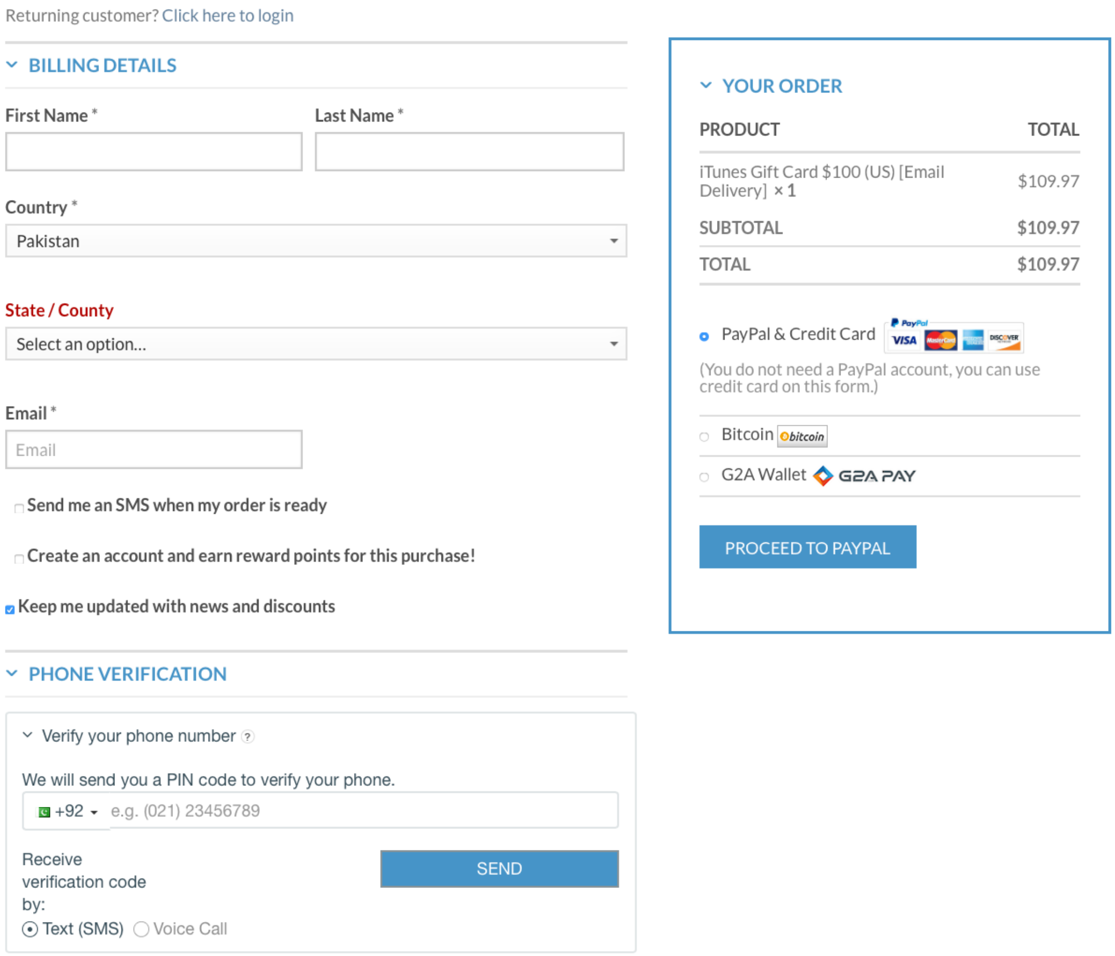


Figure 45: Id Review tool for manually reviewing Id

Once id is verified customer is marked whitelisted and in future not asked to verify id.

4.17 Verifiable Contact Information

Another form of establishing trust is to add verifiable contact information. It adds deterrence and can provide protection from some level of fraud. This is fairly simple and can be achieved by adding a phone verification step on a checkout process



Returning customer? Click here to login

BILLING DETAILS

First Name *

Last Name *

Country *

Pakistan

State / County

Select an option...

Email *

Email

□ Send me an SMS when my order is ready

□ Create an account and earn reward points for this purchase!

☑ Keep me updated with news and discounts

PHONE VERIFICATION

Verify your phone number ?

We will send you a PIN code to verify your phone.

+92 e.g. (021) 23456789

Receive verification code by:

● Text (SMS) ○ Voice Call

YOUR ORDER

PRODUCT	TOTAL
iTunes Gift Card $100 (US) [Email Delivery] × 1	$109.97
SUBTOTAL	$109.97
TOTAL	$109.97

● PayPal & Credit Card

(You do not need a PayPal account, you can use credit card on this form.)

○ Bitcoin

○ G2A Wallet

Figure 46: SMS Verification at checkout

4.18 Results And Conclusions

The fraud prevention model has been deployed and is running for three months. Here are the results.

4.19 Score Analysis.

Table 24: Average Score

Total Transactions Processed	16293
Average Score	25

Score Distribution

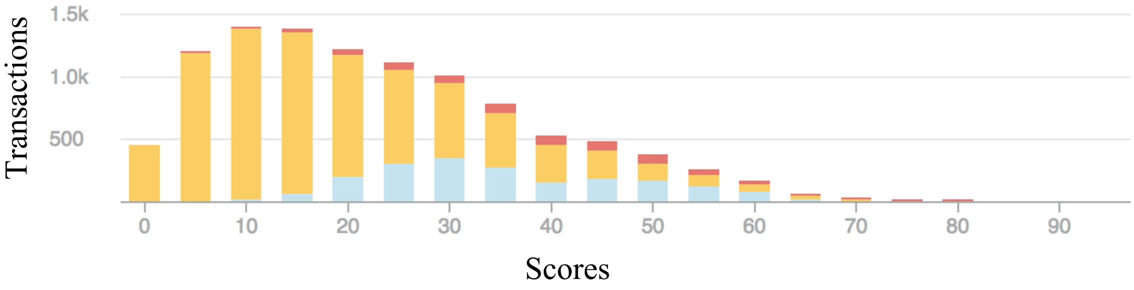


Figure 47: Score distribution

4.20 Manually Reviewed Transaction Vs Approved by Rule Engine

When a transaction is approved automatically by rule engine provides greater efficiency and user experience because there is no delay in processing order. Manual reviews can be slow and can result in the delay of order processing.

Manually Reviewed orders take more time to process and can impact on business efficiency.

Table 25: Manually Reviewed vs Approved by Rule Engine

Total Orders Received	16293
Orders Approved by Rule Engine	6372
Orders Manually reviewed	6997
Refunded	2162
White listed Auto Approved	762

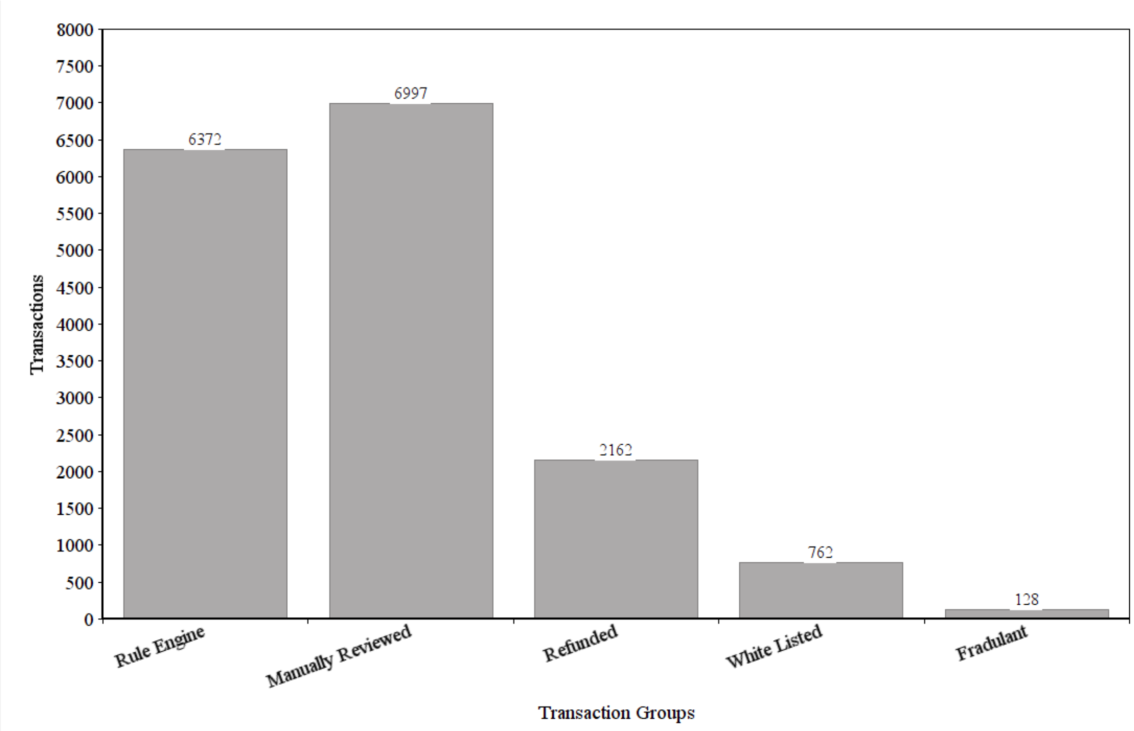


Figure 48: Pie Chart of Manually Reviewed vs Automatically Approved

4.21 Total Transactions Vs Refunded Vs Bad Transactions

Table 26: Total Transactions vs Refunded Transactions vs Fraudulent Transactions

Total Transactions	16293
Refunded Transactions	2162
Fraudulent Transactions	128

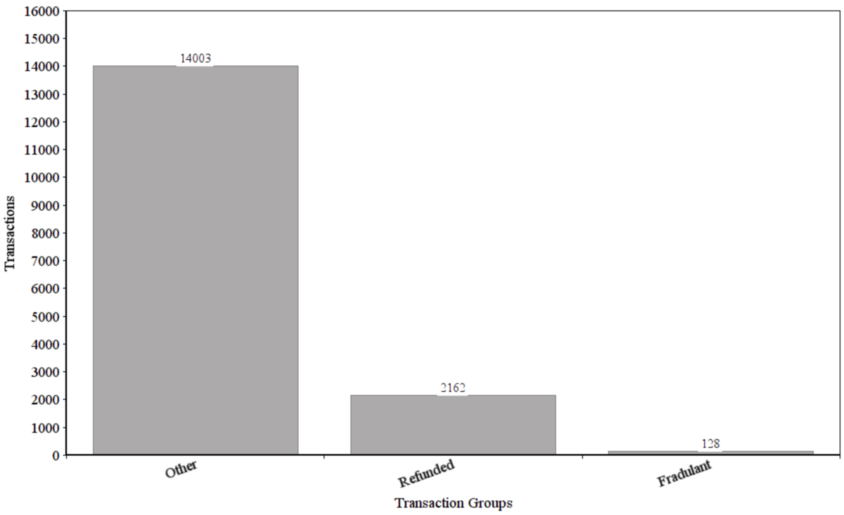


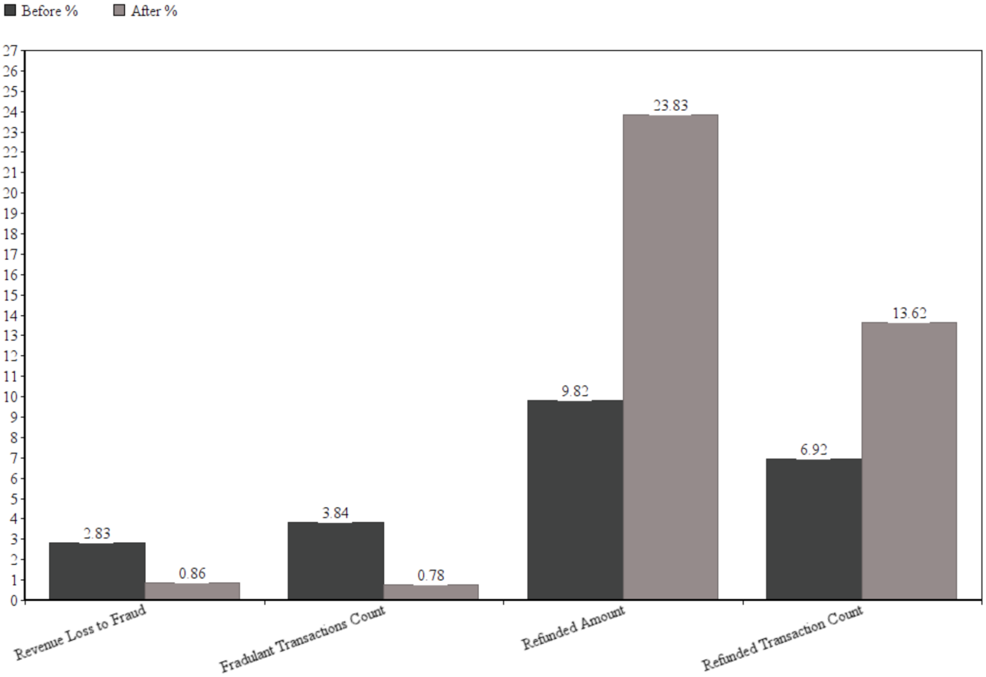
Figure 49: Pie Chart of Total Orders vs Refunded Orders

4.22 Total Revenue Vs Loss to Fraud

Table 27: Revenue Loss to Fraud

Total Revenue	1068486 USD
Refunded Transactions	254622 USD
Loss to Fraud	9201 USD

4.23 Comparison Before and After Implementing Model



4.24 Business Efficiency

When a rule engine approves an order, it’s an instant decision before using this model the processing time was 470 minutes on average after deploying this model the processing time is 58 minutes on average. This model not just reduced the fraud it made business 8 times more efficient.

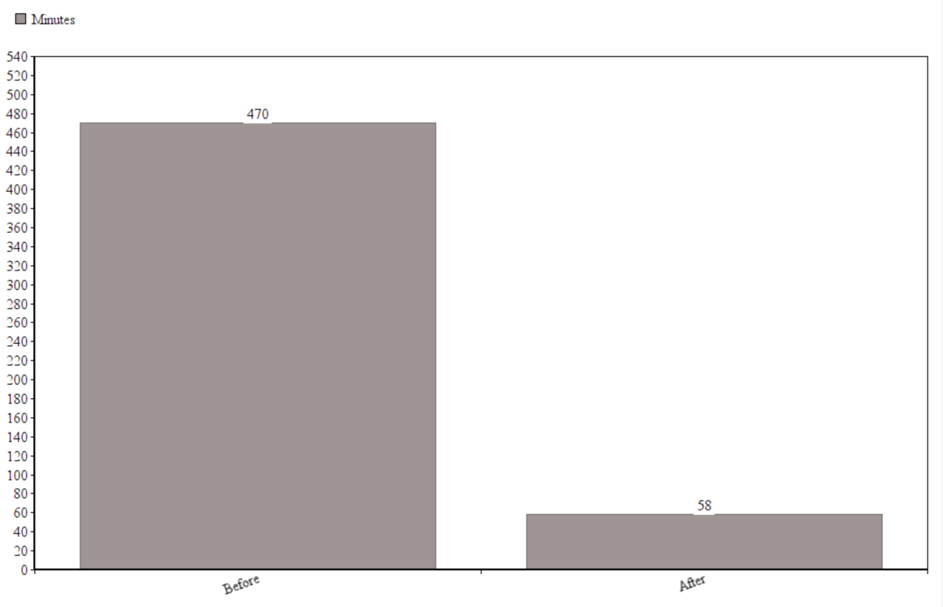


Figure 50: Processing time before and after the model

4.25 Id Verification Statistics

Table 28: Id verification requests vs Id verified

Total Id verification Request	1330
Total Id Verified	1229

92.40 % Customers were ok with providing their Id, while 7.60 percent did not provide their id. This reveals an interesting fact, may be id verification is not as hectic as it sounds if done properly.

4.26 Chapter Summary

In this chapter the proposed model was implemented for a real business and results are shown suggesting that proposed model was highly effective in fraud control. In next chapter the result will be concluded.

5. CONCLUSION

In this study I worked on the prevention of fraud in online transactions and proposed a Machine Learning based multilayer model and implemented it on a real business selling digital products online. The results as shown in chapter 4 suggest that the proposed solution is highly effective in fraud prevention and is able to reduce the fraudulent transaction by more than 50%. Proposed model is also highly adaptive to dynamic business needs and can be configured to tighten or loosen the fraud control strategy of an online business.

This work can further be extended by adding spike and communal detection techniques in the model. A layer for the assessment of economic efficiency of model can also be made part of this model, which can be helpful in reducing the number of refunds a business has to make.

References

Andy Brown and David Divitt Card Fraud Report [Report]. - 2015.

Assis Carlos A. S. [et al.] A Genetic Programming Approach for Fraud Detection in Electronic Transaction [Journal].

BigCommerce Payment fraud: What is it and how it can be avoided? [Report]. - 2016.

Bolton Richard J. and Hand David J. Statistical Fraud Detection: A Review [Journal] // Statistical Science. - 2002. - 2 : Vol. 17. - pp. 235-255.

C. L. Devasena T. Sumathi, V. Gomathi, and M. Hemalatha Effectiveness evaluation of rule based classifiers for the classification of iris data set [Journal] // Bonfring International Journal of Man Machine Interface. - 2011. - No Special Issue : Vol. 1. - pp. 04-09.

Caldeira Evandro, Brandao Gabriel and Pereira Adriano C. M. Fraud Analysis and Prevention in e-Commerce Transactions [Journal].

Caldeira Evandro, Brando Gabriel and Pereira Adriano C. M. Characterizing and Preventing chargebacks in next generation web payment systems [Journal] // Fourth International Conference on Computational Aspects of Social Networks (CASoN). - 2012.

Delamaire Linda, Abdou Hussein and Pointon John Credit card fraud and detection techniques: a review [Journal] // Banks and Bank Systems. - 2004. - Vol. 4.

Gouda I. Salama M.B.Abdelhalim, and Magdy Abd-elghany Zeid Breast Cancer Diagnosis on Three Different Datasets Using Multi-Classifiers [Journal] // International Journal of Computer and Information Technology (2277 – 0764) . - September 2012. - 01 : Vol. 01. - p. 43.

Hayashi Fumiko, Markiewicz Zach and Sullivan Richard J. Chargebacks: Another payment card acceptance cost for merchants [Journal]. - 2016. - p. 72.

Herenj Alka and Mishra Susmita Secure Mechanism for Credit Card Transaction Fraud Detection System [Journal] // International Journal of Advanced Research in Computer and Communication Engineering. - 2013. - 2 : Vol. 2.

jeannt garyericson Data Transformation - Learning with Counts [Online]. - Microsoft. - https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/data-transformation-learning-with-counts.

jeannt garyericson Score Model [Online]. - Microsoft. - https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/score-model.

jeannt garyericson Two-Class Neural Network [Online]. - Microsoft. - https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/two-class-neural-network.

jeannt garyericson Two-Class Support Vector Machine [Online]. - Microsoft. - https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/two-class-support-vector-machine.

jeannt garyerricson Two-Class Boosted Decision Tree [Online]. - Microsoft. - https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/two-class-boosted-decision-tree.

Kou Yufeng [et al.] Survey of Fraud Detection Techniques [Journal] // International Conference on Networking, Sensing & Control. - 2004.

Lee Walter W. and Mesa La Identification and Management of Fradulent Credit/Debit Card Purchases at Merchant Ecommerce Sites [Journal] // United States Patent. - 2007.

Lek Monkol [et al.] Data Mining Prototype For Detecting E-Commerce Fraud [Journal] // Global Co-Operation in the New Millennium. - 2001.

Microsoft Contranaintelligence [Online]. - https://gallery.cortanaintelligence.com.

Microsoft https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/apply-transformation [Online].

Microsoft https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/data-transformation-learning-with-counts [Online].

Microsoft https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/data-transformation-learning-with-counts [Online].

Microsoft Microsoft Documentation [Online]. - https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/clean-missing-data.

Ophir Gottlieb Curt Salisbury, Howard Shek, Vishal Vaidyanathan Detecting Corporate Fraud: An Application of Machine Learning [Journal]. - 2006.

Raghavendra Patidar Lokesh Sharma Credit Card Fraud Detection Using Neural Network [Journal] // International Journal of Soft Computing and Engineering (IJSCE). - May 13, 2011.

Research Microsoft Cortanaintelligence [Online]. - https://azuremlsampleexperiments.blob.core.windows.net/templatedata/Online%20Fraud-%20Untagged%20Transactions.csv.

Research Microsoft Cortanaintelligence [Online]. - https://azuremlsampleexperiments.blob.core.windows.net/templatedata/Online%20Fraud-%20Fraud%20Transactions.csv.

Sevda Soltaniziba Mohammad Ali Balafar The Study of Fraud Detection in Financial and Credit Institutions with Real Data [Journal] // Computer Science and Engineering. - May 02, 2015.

Soumen Chakrabarti Martin Ester, Usama Fayyad, Johannes Gehrke, Jiawei Han, Shinichi Morishita, Gregory Piatetsky-Shapiro, Wei Wang Data Mining Curriculum: A Proposal (Version 1.0) [Journal] // Intensive Working Group of ACM SIGKDD Curriculum Committee. - April 30, 2006.

Statista.com Digital buyer penetration worldwide from 2014 to 2019 [Report]. - 2014.

T. A. Jilani H. Yasin, and M. M. Yasin Article: Pca-ann for classification of hepatitis-c patients [Journal] // International Journal of Computer Applications. - Feburary 2011. - 7 : Vol. 14. - pp. 1-6.

Ward Theresa Strategies for Reducing the Risk of Ecommerce Fraud [Report]. - [s.l.] : First Data, 2010.

Wikipedia Data analysis techniques for fraud detection [Journal]. - 2016.

Wikipedia Machine learning [Journal].

Wikipedia Wikipedia [Online] // WikiPedia. - 09 18, 2105. - https://en.wikipedia.org/wiki/Fraud_deterrence.

Wikipedia Wikipedia [Online] // Wikipedia. - May 5, 2017. - https://en.wikipedia.org/wiki/Profiling_(information_science).
Wikipedia Wikipedia [Online] // Wikipedia. - July 29, 2017. - https://en.wikipedia.org/wiki/Artificial_neural_network.
Wikipedia Wikipedia [Online] // Wikipedia. - Feburary 2014, 2017. - https://en.wikipedia.org/wiki/Labelling.
Wikipedia Wikipedia [Online] // Wikipedia. - July 14, 2017. - https://en.wikipedia.org/wiki/Decision_tree_learning.
Wikipedia Wikipedia [Online] // Wikipedia. - July 16, 2017. - https://en.wikipedia.org/wiki/Statistical_classification.