TEST Engineering & Management

May- June 2020
ISSN: 0193-4120 Page No. 6868 - 6874

Credit Card user Classification based on Cash-out Loop Hole

Shreya Patel, Nileshkumar Kakade, Ankit Chauhan
Assistant Professor, Information Technology Department, Parul University,Gujarat, India
Assistant Professor, Computer Department, Parul University, Gujarat, India
Assistant Professor, Computer Department, Parul University, Gujarat, India

Article Info
Volume 83
Page Number: 6868 - 6874
Publication Issue:
May-June 2020

Article History
Article Received: *19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *18 May 2020*

Abstract:
Extensive development and fluctuations in the meantime advancement of economy in 1991 were observed in the National monetary zone. Although the fiscal trade is usually versatile in achievement and direction, the division involves its self-structuring of challenges when it comes to ethical conducts, economic pain and commercial supervision. This analysis attempts to amplify focus on disputes, for instance, financial firm swindlers and elevated credit card requirement. Investigation emphasizes on supplementary evidence (writing audit and case approach) covering all economic troupes dealing with delegating financial wrongdoing. Moreover, bank and organization face colossal misfortunes not only by credit card misrepresentation conducts but also deceitful cash-out makes. Besides, such associations need successful techniques to identify fake money out. To identify deceitful Loophole precisely, we develop several parameters which are not measured before like location based marking, POS (Point of sale) machine identification etc.. We additionally build a benchmark include set dependent on the customary methodology. We look at these example sets utilizing a genuine informational index containing genuine exchanges of charge cards with various ML (Machine Learning) techniques such as, Random Forest (RF). The outcomes uncover that our proposed framework, which think about both proviso and dynamic standards of conduct of cardholders, to discover misrepresentation movement of future exchange.

Keywords*: Credit card fraud, PoS machine, Sequence of Purchase, Suppost Vector Machine, Decision Tree, Random Forest, Start end Time, PoS location, Fix amount.*

I. INTRODUCTION:

Money related misrepresentation has been expanding with the predominance of present day advances, bringing about many billions of dollars of misfortune every year. There are numerous sorts of economic swindles and credit card frauds, which leads to loss of billions of dollars annually. As per The Nilson Report, misfortunes from charge card extortion landed up to 21billion dollar globally in the year 2015 and expected same figure to get amplified up to 31 billion dollar by the year 2020.ACI Worldwide evaluated that in any event 46% of Americans were casualties of Visa misrepresentation in 2012–2016. MasterCard extortion in china is likewise on the pinnacle. Contrasted and the quantity of similar issues in the year 2015, the quantity of such incidents in China expanded by 3.8% in the year 2016 when it comes to announced charge card extortion incidents. Hence, it is menial for financial and plastic money related organizations to look forward to conduct pre-emptive strike to defeat such cheats. [1]

There are several types of credit card frauds, each having different purpose to be achieve here by we have describe some of the most frequent credit card frauds.

1. Card Not Present Fraud (CNP)

Nowadays with huge use of internet CNP is being very popular, someone can use your fund if he/she has account no, CVV code and expiry date of your card via phone, email or internet. Without having physical card they can easily access your money. [17, 2]

2. Counterfeit Card Fraud

This fraud is also done if the fraudulent have your card details. This implies a phony attractive swipe card embraces entirely card subtleties. The fake strip at that point used to make a bogus card that is totally useful.[18,4]

3.Card ID Theft

This type of fraud steal identification of the cardholder, it is very vulnerable if the ID is disclose by the criminal.it is quite difficult one since it requires some investment period towards recognize it as well as it takes a long time for recovering too.[19]

4.Mail Non-Receipt Card Fraud

This fraud is also known as not received card issue, where an authorized user has requested for a card but in between the traffic it is interrupt by fraudulent user and used by the same unauthorized party to make fake transaction in future. [20, 12]

5.Cash out fraud

False Cash-out mentions an extraction of money from Credit Card over a phony buy exchange that sidesteps the premium interest rates and credit-card cutoff points of loans set by the giving bank. [10]

Our examination centers on an empathy of falsified cash-out, one of the significant kind of Credit Card Swindle. It includes utilization credit-cards at PoS (point-of-sales) machine and outside virtual payment schemes. Dissimilar to furthermost credit card misrepresentation, right now the cardholder and vendor plot in the false money outs. In a regular false exchange, a dealer with such machines manufactures imaginary exchanges for a card user, on behalf of instance for offer of products. As opposed to getting products in the exchange, the cardholder gets money straightforwardly from the dealer. During the procedure, the shipper takes a little segment of the exchange cost as commission expense .mean While the cardholder take pleasure to utilizing a premium allowed "fund" for various days just as fail to pay high premium installments on legitimate loans on their credit card.

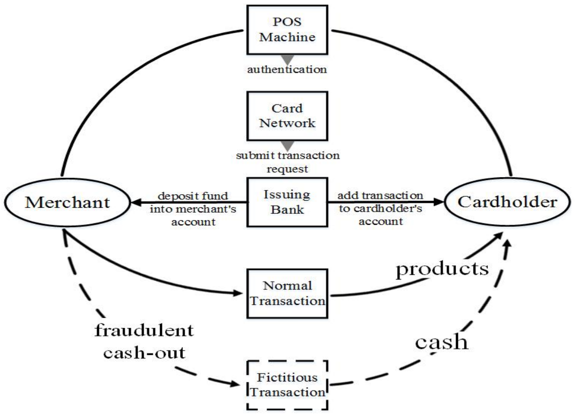


Fig. 1.The graphical Representation of fraudulent cash-out.[10]

The figure shows actual fraudulent cash advances practices steps. A distinctive run-through in credit card extortion identification is, to develop a structures from transaction records and fabricate a prototypical model to anticipate the misrepresentation hazard. In this study we are focusing on some real life parameters which supports to the dynamic behavior of fraudulent like sequence of parameter, PoS machine number, Location, Start and end time, Fix amount(pattern) etc. They are tested through various classification procedures like DT (Decision Tree, SVM (Support Vector Machine) and RF(Random Forest) Using a dataset containing real transactions of MasterCard in India.

II. RELATED WORKS

Yunjie X, Jiaoyang L,and Yue W (2019), has develop highlights utilizing a useful information investigation calculation to catch the time-subordinate personal conduct standards of cardholders in their paper. Also develop a standard feature set depends on conventional methodology of Whitlow’s approach. It makes several features and makes combinations of it, than compares these several feature set using a genuine data set with tangible transaction of 25,000 swipe credit cards with machine learning approaches alike SVM(support vector machine),extreme gradient boosting etc. It uses Standard Deviation and Mean to find out the total amount. The limitation is it depends on traditional parameter like transaction amount and time only. [1]

Yiheng S, Noshir C, Yuan L (2017), has proposed to explore the recognition of deceitful cash-out further down the consequences wherever only the labels of a tiny set of customers and merchants are available. It constructs a semi-regulated learning calculation that consequently tunes the earlier and constraints in Markov irregular field whereas gathering names for each hub in the diagram.it uses JD dataset of china. The limitation is works under the labelled data, which may be not suitable for every situation. [10]

Dr Jamal A, Nana G (2018) has been discover Bank Loophole is achieved only by using SVM(Support Vector Machine).SVM could assistance to diminish hazard as well as expand the nature of administration reached out to client's so as to prevail in business. The target of this work is to give extortion location engineering that will empower bank to identify false exchanges progressively with sparkle dependent on machine learning technique support vector machine.They have demonstrated that SVM-S is better arrangement as contrast with BPN ((Back Propagation Networks) [15]

Aswini E., Soundarya V.,SureshKumar M. ,.Kavitha S. (2019), They have utilize RF(Random Forest) Algorithm to verdict the fake exchanges in addition precision of those exchanges. These calculation depends on supervise knowledge calculation wherever it utilizes DT for grouping of dataset. Later that the confusion matrix is acquired. Presentation of RFA is assessed dependent scheduled the confusion matrix. The consequences got after setting up the dataset gives precision around ninety percentage. [13]

Shiwani L, Olawale A ,Hemaint J, Julius W (2019), has assesses execution of, Logistic Regression, KNN(K-Nearest Neighbor), NB(Naive Bayes), and SVM(Support Vector Machine) on especially mutilated information on Credit card extortion. Besides, the after impacts of this undertaking were confined by the little information scope of deceitful issues specified by the dataset. But it is useful for small size data only, it cannot supported by real life huge sized dataset [11]

III. METHODOLOGY

a. *Input Data*

Dataset is contain 1000 user transactions behavior in that 365 day period and 365 night time transactions (total 730 column). Highlight “Class” is the reaction variable and it takes esteem 1 if there should arise an occurrence of extortion and 0 in any case. [1]

b. *Feature Extraction*

TABLE I. BASIC FEATURES[1]

Features	Function
Amount	Total Transaction done in year
No	No of Transaction
STD	Standard Deviation
Min	Minimum of Transaction
Max	Maximum of Transaction
Average	Average of Transaction

c. *SVM(Support Vector Machine Classification)*

SVM is a Supervise machine model that utilizes characterization calculations for two-bunch grouping issues. In the wake of giving a SVM model arrangements of named preparing information for both of two classifications, they're ready to sort new models. [15]. Support-vectors are data focuses that are contiguous to hyper plane, and the determinations of the informational index is, on the off chance that it is evacuated, it would adjust the circumstance of the apportioning hyperplane. Thusly, they can be seen as the essential segments of a data set. [11]

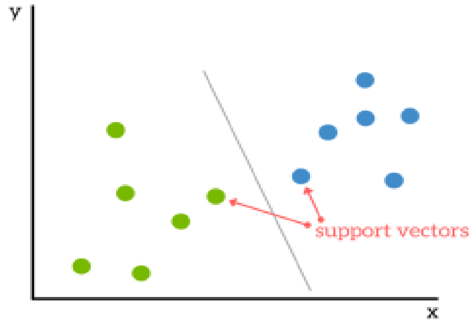


Fig. 2.SVM Hyper plane [16]

As an essential model, to a game plan undertaking for best two Characteristics (like those image above), you should seriously think over the hyperplane Concerning representation an understanding that is straightly separates and commands an arranged around data. Instinctively, the additional from hyperplane our information centers untruth, that is just a glimpse of something larger certain we need help that they bring been viably organized. We In need our data centers with make Concerning outline much out beginning with those hyperplane Similarly as could reasonably be expected, same time at present on the right side from affirming it. Thusly at new-fangled difficult information is included, whatsoever adjacent of the hyper plane, it shows up would be pick those classes those we dispatch to it.

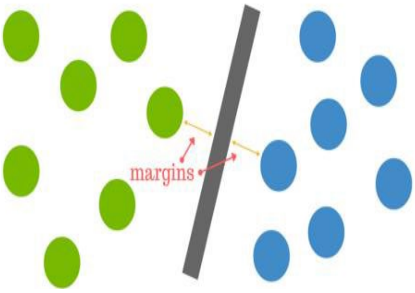


Fig. 3.Margins [16]

Those division the center of the hyper-plane and the closest information point from whichever set might be acknowledged as an edge. Those target will be ought to choose a hyperplane with the best could sensibly be normal edge between the hyperplane Also At whatever side of the point inside the planning set, accommodating A progressively awesome chance of new data being requested successfully.

IV. Proposed System

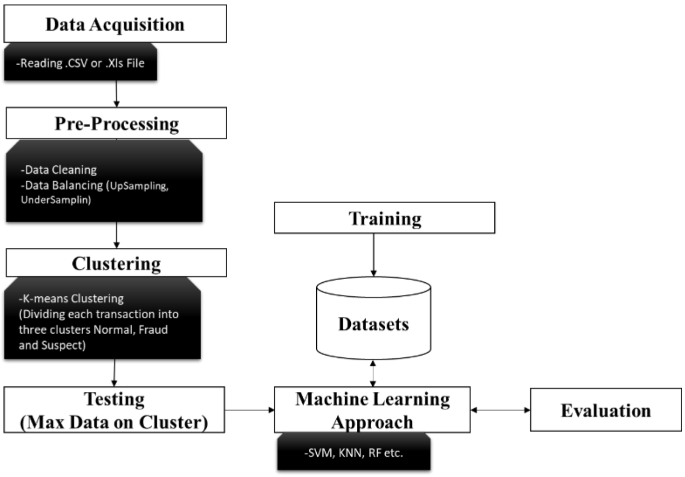

Data Acquisition
-Reading .CSV or .Xls File
Pre-Processing
-Data Cleaning
-Data Balancing (UpSampling, UnderSamplin)
Clustering
-K-means Clustering (Dividing each transaction into three clusters Normal, Fraud and Suspect)
Testing (Max Data on Cluster)
Training
Datasets
Machine Learning Approach
-SVM, KNN, RF etc.
Evaluation

Fig. 4.Proposed System

Data Acquisition

In this part different datasets are use from different sources. The datasets contains transactions made by Master Card users. This dataset presents 1500 Transactions.

Pre-process

In this part we will divide transaction on month, year or half year basics. And remove the unwanted data, missing column and doing data balancing.

Clustering pattern (k means)

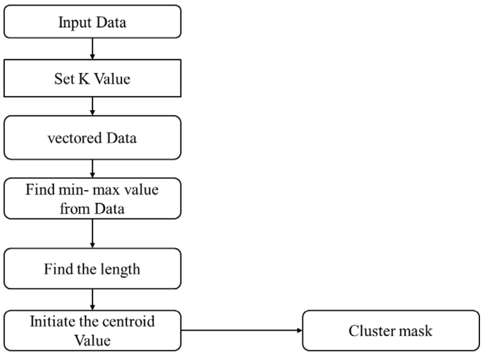


Fig. 5.K-means Clustering

Proposed Features

TABLE II. PROPOSED FEATURES

Features	Function
Sequences of purchases	In this part user purchase are monitoring based on try using credit card with same amount in multiple time.
start-end time	Some users use the card in every month starting date and pay on ending

	day that can be monitor.
POS machine	Some Business holders give offer to use credit card and give cash money by taking 1-5 % charge and fraud user take cash and invest in market for more gain.
Location	Every time made purchase with same place of same amount
Fix amount (pattern)	Same amount in every bill cycle and paying other CC bill and rotating this process.

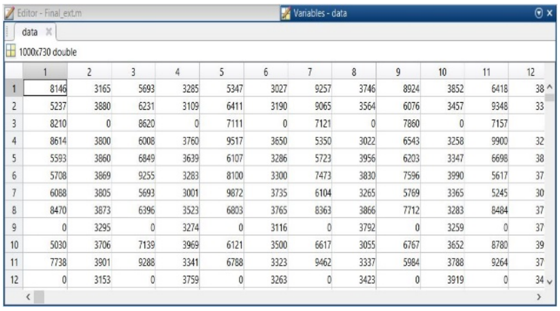
DT (Decision Tree Classification)

DT algorithm is derives from the grouping of supervise learning. It tends to be utilized to illuminate both regression and classification difficulties. DT uses the tree demonstration to crack the challenge in which each and every child node resembles to a class tag and characteristics are exemplified on the internal node of the tree. We can epitomize any Boolean function on separate attributes using the decision tree. It is also called rule based testing.

Random Forest

Alike its name proposes, contains a gigantic amount of dispersed decision trees that fill in as a gathering work. Each separate tree in RF lets out a class desire and the class with the maximum divisions transforms into prototypical forecast [9][13][3]. A huge amount of respectably uncorrelated models (trees) filling in as a board of trustees shall outflank several of specific integral models

V. Result and Analysis

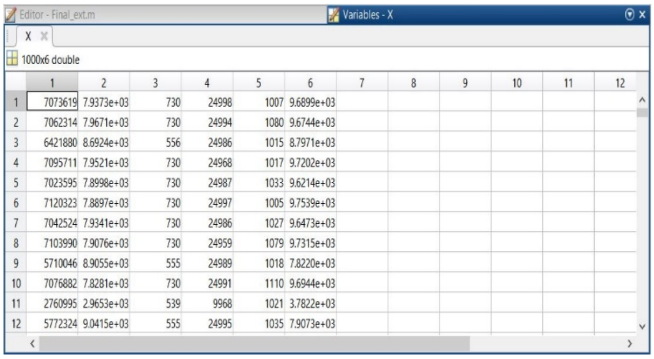

Editor - Final_ext.m | Variables - data

data

1000x730 double

	1	2	3	4	5	6	7	8	9	10	11	12
1	8146	3165	5693	3285	5347	3027	9257	3746	8924	3852	6418	38
2	5237	3880	6231	3109	6411	3190	9065	3564	6076	3457	9348	33
3	8210	0	8620	0	7111	0	7121	0	7860	0	7157	
4	8614	3800	6008	3760	9517	3650	5350	3022	6543	3258	9900	32
5	5593	3860	6849	3639	6107	3286	5723	3956	6203	3347	6698	38
6	5708	3869	9255	3283	8100	3300	7473	3830	7596	3990	5617	37
7	6088	3805	5693	3001	9872	3735	6104	3265	5769	3365	5245	30
8	8470	3873	6396	3523	6803	3765	8363	3866	7712	3283	8484	37
9	0	3295	0	3274	0	3116	0	3792	0	3259	0	37
10	5030	3706	7139	3969	6121	3500	6617	3055	6767	3652	8780	39
11	7738	3901	9288	3341	6788	3323	9462	3337	5984	3788	9264	37
12	0	3153	0	3759	0	3263	0	3423	0	3919	0	34

Fig. 6. Input data


Editor - Final_ext.m | Variables - X

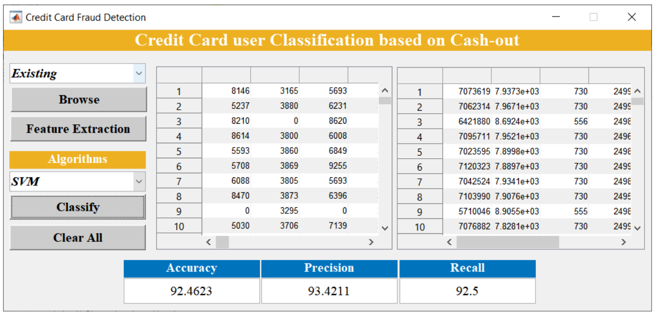
X

1000x6 double

	1	2	3	4	5	6	7	8	9	10	11	12
1	7073619	7.9373e+03	730	24998	1007	9.6899e+03						
2	7062314	7.9671e+03	730	24994	1080	9.6744e+03						
3	6421880	8.6924e+03	556	24986	1015	8.7971e+03						
4	7095711	7.9521e+03	730	24968	1017	9.7202e+03						
5	7023595	7.8998e+03	730	24987	1033	9.6214e+03						
6	7120323	7.8897e+03	730	24997	1005	9.7539e+03						
7	7042524	7.9341e+03	730	24986	1027	9.6473e+03						
8	7103990	7.9076e+03	730	24959	1079	9.7315e+03						
9	5710046	8.9055e+03	555	24989	1018	7.8220e+03						
10	7076882	7.8281e+03	730	24991	1110	9.6944e+03						
11	2760995	2.9653e+03	539	9968	1021	3.7822e+03						
12	5772324	9.0415e+03	555	24995	1035	7.9073e+03						

Fig. 7. Existing Features

As shown in figure 8, it displays the Final feature set of Amount, STD, No, Max, Min, Avg in every column.


Credit Card Fraud Detection

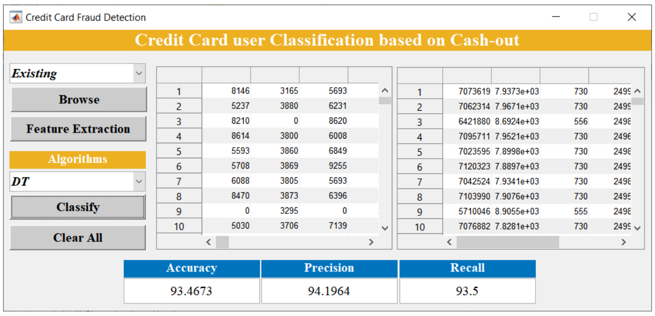
Credit Card user Classification based on Cash-out

1	8146	3165	5693
2	5237	3880	6231
3	8210	0	8620
4	8614	3800	6008
5	5593	3860	6849
6	5708	3869	9255
7	6088	3805	5693
8	8470	3873	6396
9	0	3295	0
10	5030	3706	7139

1	7073619	7.9373e+03	730	2499
2	7062314	7.9671e+03	730	2499
3	6421880	8.6924e+03	556	2498
4	7095711	7.9521e+03	730	2496
5	7023595	7.8998e+03	730	2498
6	7120323	7.8897e+03	730	2499
7	7042524	7.9341e+03	730	2498
8	7103990	7.9076e+03	730	2495
9	5710046	8.9055e+03	555	2498
10	7076882	7.8281e+03	730	2499

Accuracy	Precision	Recall
92.4623	93.4211	92.5

Fig. 8. Existing Features with SVM classification


Credit Card Fraud Detection

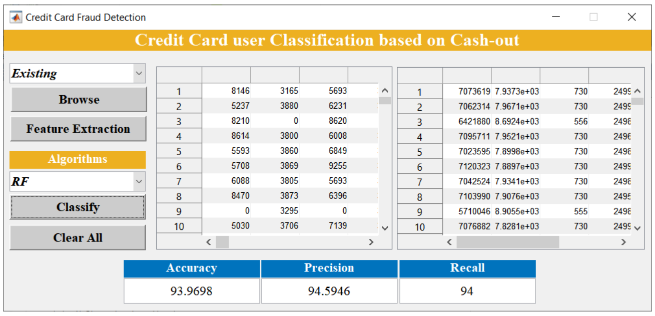
Credit Card user Classification based on Cash-out

1	8146	3165	5693
2	5237	3880	6231
3	8210	0	8620
4	8614	3800	6008
5	5593	3860	6849
6	5708	3869	9255
7	6088	3805	5693
8	8470	3873	6396
9	0	3295	0
10	5030	3706	7139

1	7073619	7.9373e+03	730	2499
2	7062314	7.9671e+03	730	2499
3	6421880	8.6924e+03	556	2498
4	7095711	7.9521e+03	730	2496
5	7023595	7.8998e+03	730	2498
6	7120323	7.8897e+03	730	2499
7	7042524	7.9341e+03	730	2498
8	7103990	7.9076e+03	730	2495
9	5710046	8.9055e+03	555	2498
10	7076882	7.8281e+03	730	2499

Accuracy	Precision	Recall
93.4673	94.1964	93.5

Fig. 9. Existing Features with DT classification


Credit Card Fraud Detection

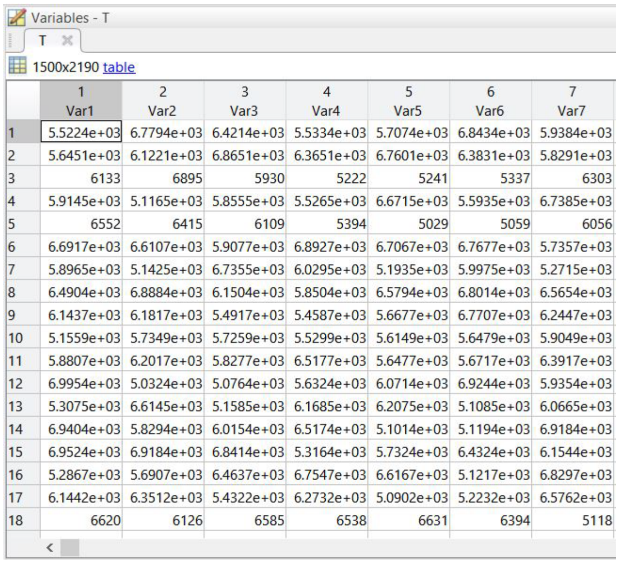
Credit Card user Classification based on Cash-out

1	8146	3165	5693
2	5237	3880	6231
3	8210	0	8620
4	8614	3800	6008
5	5593	3860	6849
6	5708	3869	9255
7	6088	3805	5693
8	8470	3873	6396
9	0	3295	0
10	5030	3706	7139

1	7073619	7.9373e+03	730	2499
2	7062314	7.9671e+03	730	2499
3	6421880	8.6924e+03	556	2498
4	7095711	7.9521e+03	730	2496
5	7023595	7.8998e+03	730	2498
6	7120323	7.8897e+03	730	2499
7	7042524	7.9341e+03	730	2498
8	7103990	7.9076e+03	730	2495
9	5710046	8.9055e+03	555	2498
10	7076882	7.8281e+03	730	2499

Accuracy	Precision	Recall
93.9698	94.5946	94

Fig. 10. Existing Features with RF classification



Variables - T

T

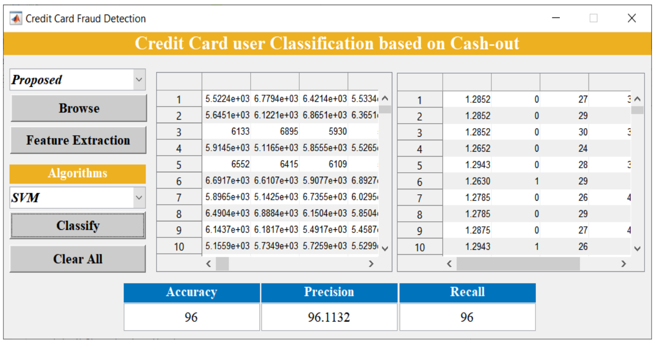
1500x2190 table

	1 Var1	2 Var2	3 Var3	4 Var4	5 Var5	6 Var6	7 Var7
1	5.5224e+03	6.7794e+03	6.4214e+03	5.5334e+03	5.7074e+03	6.8434e+03	5.9384e+03
2	5.6451e+03	6.1221e+03	6.8651e+03	6.3651e+03	6.7601e+03	6.3831e+03	5.8291e+03
3	6133	6895	5930	5222	5241	5337	6303
4	5.9145e+03	5.1165e+03	5.8555e+03	5.5265e+03	6.6715e+03	5.5935e+03	6.7385e+03
5	6552	6415	6109	5394	5029	5059	6056
6	6.6917e+03	6.6107e+03	5.9077e+03	6.8927e+03	6.7067e+03	6.7677e+03	5.7357e+03
7	5.8965e+03	5.1425e+03	6.7355e+03	6.0295e+03	5.1935e+03	5.9975e+03	5.2715e+03
8	6.4904e+03	6.8884e+03	6.1504e+03	5.8504e+03	6.5794e+03	6.8014e+03	6.5654e+03
9	6.1437e+03	6.1817e+03	5.4917e+03	5.4587e+03	5.6677e+03	6.7707e+03	6.2447e+03
10	5.1559e+03	5.7349e+03	5.7259e+03	5.5299e+03	5.6149e+03	5.6479e+03	5.9049e+03
11	5.8807e+03	6.2017e+03	5.8277e+03	6.5177e+03	5.6477e+03	5.6717e+03	6.3917e+03
12	6.9954e+03	5.0324e+03	5.0764e+03	5.6324e+03	6.0714e+03	6.9244e+03	5.9354e+03
13	5.3075e+03	6.6145e+03	5.1585e+03	6.1685e+03	6.2075e+03	5.1085e+03	6.0665e+03
14	6.9404e+03	5.8294e+03	6.0154e+03	6.5174e+03	5.1014e+03	5.1194e+03	6.9184e+03
15	6.9524e+03	6.9184e+03	6.8414e+03	5.3164e+03	5.7324e+03	6.4324e+03	6.1544e+03
16	5.2867e+03	5.6907e+03	6.4637e+03	6.7547e+03	6.6167e+03	5.1217e+03	6.8297e+03
17	6.1442e+03	6.3512e+03	5.4322e+03	6.2732e+03	5.0902e+03	5.2232e+03	6.5762e+03
18	6620	6126	6585	6538	6631	6394	5118

Fig. 11. Input MasterCard dataset

Fig. 12. Proposed Feature

As shown in figure 10, it displays the Final feature set of Sequence Purchase, day/night transaction, Pattern, Location, POS in every column.



Credit Card Fraud Detection

Credit Card user Classification based on Cash-out

Proposed

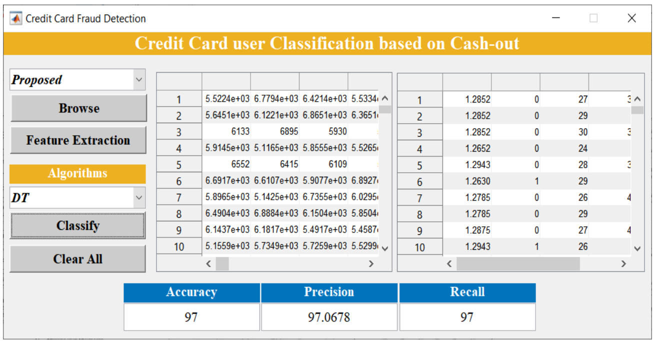
SVM

1	5.5224e+03	6.7794e+03	6.4214e+03	5.5334
2	5.6451e+03	6.1221e+03	6.8651e+03	6.3651
3	6133	6895	5930	
4	5.9145e+03	5.1165e+03	5.8555e+03	5.5265
5	6552	6415	6109	
6	6.6917e+03	6.6107e+03	5.9077e+03	6.8927
7	5.8965e+03	5.1425e+03	6.7355e+03	6.0295
8	6.4904e+03	6.8884e+03	6.1504e+03	5.8504
9	6.1437e+03	6.1817e+03	5.4917e+03	5.4587
10	5.1559e+03	5.7349e+03	5.7259e+03	5.5299

1	1.2852	0	27	3
2	1.2852	0	29	
3	1.2852	0	30	3
4	1.2652	0	24	
5	1.2943	0	28	3
6	1.2630	1	29	
7	1.2785	0	26	4
8	1.2785	0	29	
9	1.2875	0	27	4
10	1.2943	1	26	

Accuracy	Precision	Recall
96	96.1132	96

Fig. 13. Proposed Features with SVM Classification



Credit Card Fraud Detection

Credit Card user Classification based on Cash-out

Proposed

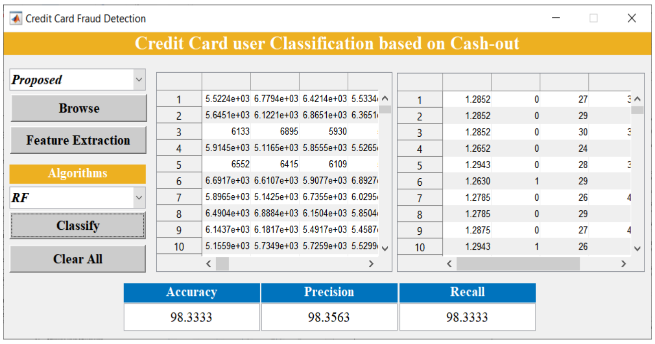
DT

1	5.5224e+03	6.7794e+03	6.4214e+03	5.5334
2	5.6451e+03	6.1221e+03	6.8651e+03	6.3651
3	6133	6895	5930	
4	5.9145e+03	5.1165e+03	5.8555e+03	5.5265
5	6552	6415	6109	
6	6.6917e+03	6.6107e+03	5.9077e+03	6.8927
7	5.8965e+03	5.1425e+03	6.7355e+03	6.0295
8	6.4904e+03	6.8884e+03	6.1504e+03	5.8504
9	6.1437e+03	6.1817e+03	5.4917e+03	5.4587
10	5.1559e+03	5.7349e+03	5.7259e+03	5.5299

1	1.2852	0	27	3
2	1.2852	0	29	
3	1.2852	0	30	3
4	1.2652	0	24	
5	1.2943	0	28	3
6	1.2630	1	29	
7	1.2785	0	26	4
8	1.2785	0	29	
9	1.2875	0	27	4
10	1.2943	1	26	

Accuracy	Precision	Recall
97	97.0678	97

Fig. 14. Proposed Features with DT Classification



Credit Card Fraud Detection

Credit Card user Classification based on Cash-out

Proposed

RF

1	5.5224e+03	6.7794e+03	6.4214e+03	5.5334
2	5.6451e+03	6.1221e+03	6.8651e+03	6.3651
3	6133	6895	5930	
4	5.9145e+03	5.1165e+03	5.8555e+03	5.5265
5	6552	6415	6109	
6	6.6917e+03	6.6107e+03	5.9077e+03	6.8927
7	5.8965e+03	5.1425e+03	6.7355e+03	6.0295
8	6.4904e+03	6.8884e+03	6.1504e+03	5.8504
9	6.1437e+03	6.1817e+03	5.4917e+03	5.4587
10	5.1559e+03	5.7349e+03	5.7259e+03	5.5299

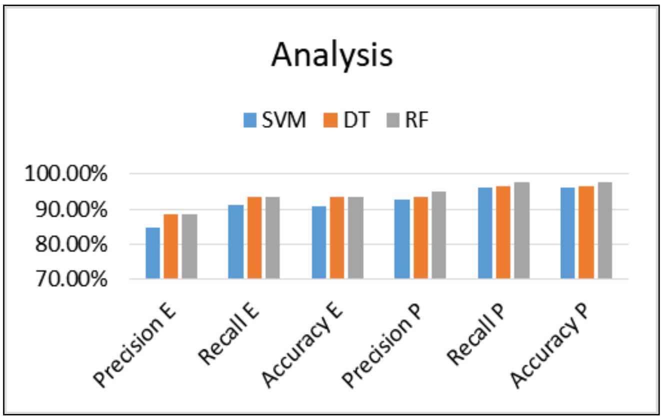
1	1.2852	0	27	3
2	1.2852	0	29	
3	1.2852	0	30	3
4	1.2652	0	24	
5	1.2943	0	28	3
6	1.2630	1	29	
7	1.2785	0	26	4
8	1.2785	0	29	
9	1.2875	0	27	4
10	1.2943	1	26	

Accuracy	Precision	Recall
98.3333	98.3563	98.3333

Fig. 15. Proposed Features with RF Classification

TABLE III. RETRIEVAL ANALAYSIS

Parameters	Existing		
	Precision	Recall	Accuracy
SVM	93.42%	92.05%	92.46%
DT	94.19%	93.05%	93.46%
RF	94.59%	94.00%	93.96%
Parameters	Proposed		
	Precision	Recall	Accuracy
SVM	96.11%	96.00%	96.00%
DT	97.00%	97.067%	97.00%
RF	98.35%	98.33%	98.33%



Analysis graph

CONCLUSION

The exhibition of the proposed framework will be tried on the standards like, due Data, made as similar to credit card statements database. As an enhance the research by updating data balancing using clustering, include parameters sequences of purchases, start-end time and fix amount (pattern) transactions and testing with more multi-classification algorithms like SVM, DT and RF. RF gives 98.33% Accuracy which is batter for future credit card fraud prediction.

REFERENCES

1. Yue Wu, Yunjie Xu, Jiaoyang Li," Feature construction for fraudulent credit card cashout detection,Elsevier-September,2019.
2. C. Singh and K. Antony, "Frauds in the Indian Banking Industry", IIMB-2016 -IIMB-WP N0. 505
3. S. Xuan S. Wang ,Z.Li,L.Zeng,S.Wang,C.Jiang" Random Forest for Credit Card Fraud Detection", IEEE-2018
4. Anuveeta Datta Chowdhury," Critical Analysis of Credit Card Frauds in India", 2019 IJLSI| Volume 1, Issue 2.
5. R. Di Clemente, M. C. González, M. Luengo-oroz, M. Travizano, S. Xu, and B. Vaitla ," Sequences of purchases in credit card data reveal lifestyles in urban populations",Nature Communications-2018.
6. J. O. Awoyemi and S. A. Oluwadare ," Credit card fraud detection using Machine Learning Techniques",IEEE-2017.
7. Mary Frances Zeager, Aksheetha Sridhar, Nathan Fogal, Stephen Adams, Donald E. Brown, and Peter A. Beling," Adversarial Learning in Credit Card Fraud Detection",IEEE-2017.
8. Alejandro Correa Bahnsen,Djamila Aouada,Aleksandar Stojanovic,Björn Ottersten ," Feature Engineering Strategies for Credit Card Fraud Detection", ELSEVIER - 2016
9. F. Fadaei Noghani and M.- H. Moattar*," Ensemble Classification and Extended Feature Selection for Credit Card Fraud Detection", Journal of AI and Data Mining-2017
10. Yuan Li,Yiheng Sun, Noshir Contractor,"Graph mining assisted semi-supervised learning for fraudulent cash-out detection",IEEE-2017.
11. Olawale Adepoju, Julius Wosowei, Shiwani Lawte, Hemaint Jaiman," Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques",Global Conference for Advancement in Technology-2019.
12. Anuruddha Thennakoon, Chee Bhagyani, Sasitha Premadasa, Shalitha Mihiranga, Nuwan Kuruwitaarachchi," Real-time Credit Card Fraud Detection Using Machine Learning",IEEE-2019.
13. M.Suresh Kumar,V.Soundarya ,S.Kavitha ,E.S.Keerthika , E.Aswini," Credit Card Fraud Detection Using Random Forest Algorithm",IEEE-2019.
14. Pawan Kumar, Fahad Iqbal," Credit Card Fraud Identification Using Machine Learning Approaches",IEEE-2019.
15. Nana Kwame Gyamfi, .Dr Jamal-Deen Abdulai," Bank Fraud Detection Using Support Vector Machine",IEEE-2018.
16. https://www.kdnuggets.com/2016/07/support-vector-machines-simple-explanation.html.
17. https://www.investopedia.com/terms/c/cardnotpresent-fraud.asp
18. https://www.bpfi.ie/customer-assist/personal-customers/counterfeit-card-skimming-prevention/
19. https://www.consumerprotect.com/crime-fraud/11-types-of-credit-card-fraud-scams/
20. https://www.professionalsecurity.co.uk/news/case-studies/mail-non-receipt-fraud-warning/