International Journal of Advanced Science and Technology
Vol. 29, No. 6, (2020), pp. 4344 – 4352

Detection of Fraudulence Activity Using Smart Cards

S. Sathyavathi[1], R. Dhaaraani[2], S. Kavitha[3], G. Prema Arokia Mary[4]
[1] *Assistant Professor, SRG, Department of Information Technology, Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India*
[2]*PG Scholar, M.Tech (Data Science), Department of Information Technology,Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India*
[3]*Assistant Professor II, Department of Information Technology, Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India*
[4]*Assistant ProfessorI, Department of Information Technology, Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India*
[1]*sathyavathi.s.it@kct.ac.in,*
[2]*dhaaraani.18mds@kct.ac.in,*
[3]*kavitha.s.it@kct.ac.in,*
[4]*premaarokiamary.g.it@kct.ac.in*

Abstract

Credit card fraud is a major issue in budgetary administrations. Enormous measure of cash is lost because of the credit card each year. The loss of cash creates more turmoil to the two shippers and clients. To maintain a strategic distance from this circumstance, in this task, another methodology has been proposed to distinguish atypical conduct dependent on heterogeneous data and a data fusion strategy. There are four kinds of datasets applied in this undertaking including credit card, steadfastness card, GPS and picture data. Each dataset has various modalities. In proposed framework we utilize Random Forest Algorithm (RFA) for finding the fraudulent exchanges and the precision of those exchanges. This calculation depends on administered learning calculation where it utilizes decision trees for classification of the dataset. So each dataset must be handled independently. In that, initial step is pre-processing and the subsequent stage is highlight choice. Machine learning calculations are utilized for classification in these four kinds of datasets. After classification, the halfway outcome must be put away. All the middle of the road results are blended and investigated utilizing Data fusion strategy to wind up with legitimate outcomes.

Keywords: *Data Fusion, Credit card fraud, Random forest, classification.*

1. Introduction

Money related fraud is a reliably creating risk with clearing results in the areas of budgetary administrations, business and government associations. Trick is named as unlawful misleading with the expectation of acquiring financial benefit [1]. Credit card fraud is a generally expanding issue in the credit card industry, especially in the online segment. These criminal operations that expect to acquire products without paying, or to increase ill-conceived assets from a record, have made serious harm the clients and the specialist organization [2]. Strategies to recognize credit cards successfully, rapidly and precisely has become an intriguing issue in late research. As of now, the data digging calculations are utilized for identifying credit card fraud hazard [8].

Data fusion may be the way towards incorporating numerous data resources to create gradually steady, precise, and useful data compared to that offered by anybody data

ISSN: 2005-4238 IJAST

source. Info fusion types are frequently sorted since, moderate, or even high, broker upon the actual processing phase at which running happens. Low-level data blend joins several wellsprings associated with crude information to create brand new crude info. The desire is the fact that melded files is more instructional and designed than the very first info. Individuals are a prime situation of Data fusion.

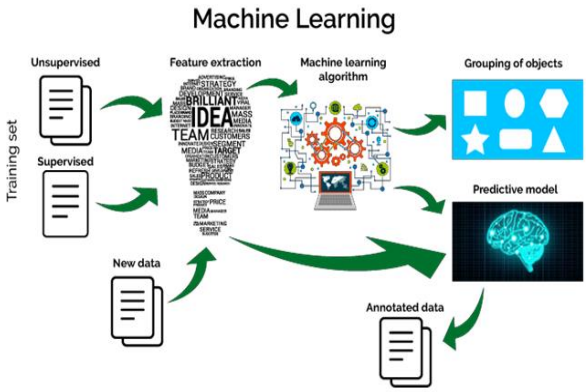


Fig 1: Machine learning architecture

Figure 1. Machine Learning Architecture

Generally, such a methodology needs to think about the current sorts of fraud to make models by learning the different fraud designs. Abnormality recognition is to construct the profile of ordinary swap conduct of the cardholder determined by his/her verifiable exchange information, and select a recently trade as a possible fraud within the off opportunity that it veers off from the normal exchange carry out. Notwithstanding, a peculiarity identification strategy needs enough progressive example data to describe the typical exchange conduct of a cardholder [7].

There are numerous fraud exchanges which can't be effectively recognized by the client and furthermore by the financial position which prompts loss of touchy data [4]. There are different models which are utilized for identifying the fraud exchanges dependent on the conduct of the exchanges and these techniques can be named two general classes, for example, regulated learning and unaided learning calculation. In existing framework for finding the exactness of the fraudulent actuates they have utilized techniques, for example, Cluster Analysis, Support Vector Machine, Naïve Bayer's Classification and so forth [6]. The point of this paper is to identify the exactness of the fraudulent exchanges by utilizing Random Forest Algorithm.

The paper is composed as follows. Segment II portrays some related work about credit card fraud. Segment III presents the strategies utilized in our trial. The analyses and execution measures are examined in Segment IV. At last, Segment V conclusion and future work are presented.

2. Foundation Study

Adepoju, O., et al. [1] if the dataset together with decoded job areas were introduced to individuals while all has been said in completed the veritable segments which is often followed regarding charge card blackmail recognizable resistant can realize. In addition , typically the eventual results of this commencing were restricted by the tiny data scale fraudulent circumstances given by often the dataset. Using a greater dataset with an more and more imperative quantity of fraudulent conditions, the calculations can be willing to

ISSN: 2005-4238 IJAST

make needs for steadily significant accurate. To look for following these goals, all the in addition processing push may be necessary.

Benchaji, I., et al. [2] yet another technique for facts age of unbalanced data set's minority category was planned to improve fraudulence identification throughout e-banking by making use of K-Means bunching and innate calculation as being an oversampling system. Albeit anatomical calculations are actually applied in several regions, each of our application place plans to manage imbalanced details set matter by generating new small section class cases to increase brand-new preparing pieces. Applying this kind of calculation straight into bank credit card scams location system means to minimize fraudulent change and decline the quantity of spurious, fake, caution.

Ghobadi, F., et al. [3] piled up a Cost Hypersensitive credit card fraud spot framework to create CSNN. Ju, C., et al. [4] offers another credit card scams recognition style dependent on evaluation coefficient total to determine whether the mastercard exchange can be fraud substitute or not. Typically the explore demonstrates the version can acknowledge fraud transaction precisely, plus the outcome surpasses oddity breakthrough discovery by group when the anomaly data is certainly far less when compared with ordinary files. In the event that typically the calculation can be employed in bank's credit card fraud identification framework, it is not easy to design the likelihood of bamboozling not long soon after exchange.

Lucas, Y., et al. [5] offer a procedure to assess the covariate move in your transient dataset. This procedure consists of in characterizing the deals of every moment against every single different days to weeks: If the group is fruitful then the days or weeks are exclusive and there is a good covariate transfer between them. However ,, if the class isn't efficient, the days are generally comparative. Wang, C., et al. [8] provides the benefits of BP neural program calculation as well as whale computation, and suggests another credit card scams identification calculations utilizing whale calculation to enhance BP nerve organs system working out.

3. Framework Model

The primary goal is to discover the fraudulence happened in credit card utilizing the data fusion method. At the point when at least one datasets are intertwined, it gives more data than the data from single dataset. The underlying procedure for each dataset must be done independently because of the modalities of data. Right off the bat, the credit card data are gathered and pre-prepared. At that point the characteristic which are required for the fraud location must be chosen. After the element choice, the classification must be finished. Classification is finished utilizing the machine learning calculation.

Anomaly on Credit Card Detection

Using card payment transforming in the broadest way of installments both equally over the website and head to head, the credit card scams will on the whole quicken speedily. Recognizing bogus exchange applying ordinary procedures for manual unique proof are generally monotonous along with off bottom part, thusly the emergences of enormous files has taken customary method procedures slowly ridiculous. Company associations get changed to willing techniques, at any rate with smart strategies relying on fake mastering.

ISSN: 2005-4238 IJAST

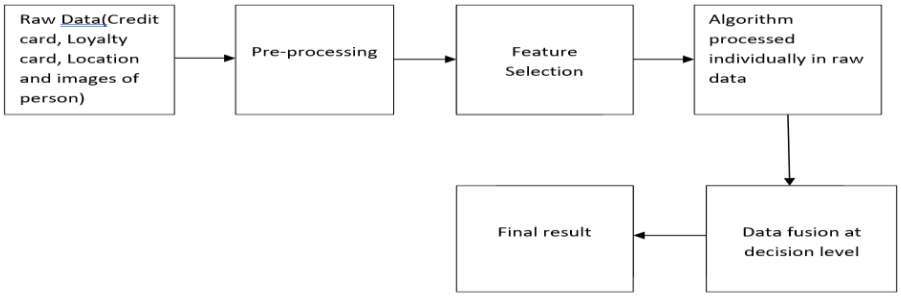


Figure 2. Flow Diagram Process

The figure 2 represents the work stream of the proposed framework. The initial step includes data assortment. The crude data of credit card, faithfulness card, GPS and face pictures are gathered. The gathered dataset comprises of the subtleties of clients. The gathered dataset must be stacked and pre-handled utilizing python libraries. All the four datasets needs to splitted into preparing and testing data independently. In the wake of stacking the dataset, the element choice is the following procedure. In this procedure, which adds to the conclusive outcome are chosen. In light of the highlights, the outcome can be found without any problem. The classification procedure must be performed for all the datasets. Machine learning calculations like Random Forest was utilized for classification in credit card dataset. In like manner, the best classification calculations will be executed for different datasets. The outcomes which are gotten from classification procedure will be put away as middle of the road result for all the four datasets. Data fusion is the decision making step in the framework. At that stage, all the halfway outcomes will be consolidated and examined. With the assistance of examined result, the event of frauds can be identified precisely.

Data Collection

The dataset of credit card subtleties was gathered from the kaggle site. It contains the data over a particular timeframe. In like manner, the other crude data for dependability card, GPS and Face pictures will be gathered. The crude data contains the subtleties of the credit card clients. The credit card data contains of the subtleties like Cardholder name, card number, sum, and so forth.

Time	ATM_PIN_	CARD_NA	USER_SIGI	CCV_NO	BANK_NA	BANK_CO	BANK_IFS	BANK_PIN	BANK_AD	CARD_VAI	ACCOUNT	USER_PHC	USER_PIN
51435	1.19749	-0.35212	-0.1359	0.2221	0.231128	1.086617	-0.42036	0.391464	0.672499	-0.05812	-0.57469	-0.27234	-1.63818
78049	0.976047	-0.28995	1.465321	1.300002	-1.38289	-0.47959	-0.63257	0.064533	0.710743	-0.09367	-0.22983	0.169038	-0.05085
157168	-1.3953	0.478266	-0.58491	-1.20153	0.928544	-0.74362	0.755504	-0.1414	-2.1185	0.182768	1.304131	-0.56024	-0.13508
69297	1.276014	-0.6727	-0.42549	-0.7774	-0.58209	-0.8804	-0.1035	-0.20304	-1.24165	0.849479	0.995417	-0.58712	-0.93091
144504	-0.31275	-1.20256	2.249806	-0.29721	-0.96339	1.207532	-0.83778	-0.05765	1.121421	0.744263	-2.05854	-0.13717	0.325085
43843	-0.15206	-3.30944	-0.8751	-0.35432	-1.28107	0.57596	0.241441	-0.07576	-0.50341	0.214609	-1.43046	-1.55325	-0.6374
124531	-0.88491	-0.40874	1.796732	-0.63774	-0.56537	1.693424	0.287936	0.623672	0.892499	-1.32559	-0.6587	-0.18949	-0.7173

Figure 3. Credit card Dataset

Processing Data of Our Framework

The gathered crude data for Credit card, steadfastness card, GPS and Face pictures are first stacked. At that point the pre-processing step will be executed. In this progression, the dataset will be checked for missing data. The missing qualities can either be erased or loaded up with data utilizing python orders.

ISSN: 2005-4238 IJAST

Checking Missing Values

	Time	ATM_PIN_NO	CARD_NAME	...	RECEIVER_IFSC_NO	Amount	Class
0	False	False	False	...	False	False	False
1	False	False	False	...	False	False	False
2	False	False	False	...	False	False	False
3	False	False	False	...	False	False	False
4	False	False	False	...	False	False	False
..	...	...	...	...	...	...	...
585	False	False	False	...	False	False	False
586	False	False	False	...	False	False	False
587	False	False	False	...	False	False	False
588	False	False	False	...	False	False	False
589	False	False	False	...	False	False	False

[590 rows x 31 columns]

Figure 4. Preprocessing credit card data

Training Data and Testing Data

Train_test_split() is utilized to part all the gathered dataset into preparing and testing data. 70% of the all out dataset is utilized for preparing the calculation. 30% of the picked dataset is utilized for testing. After the parting of preparing and testing data, the model must be manufactured. In that model, the calculations will be actualized.

X-train & X-test

[590 rows x 31 columns]

	Time	ATM_PIN_NO	CARD_NAME	...	RECEIVER_ADDRESS	RECEIVER_IFSC_NO	Amount
0	51435	1.197490	-0.352125	...	-0.031160	-0.013680	39.95
1	78049	0.976047	-0.289947	...	0.059639	0.061220	92.98
2	157168	-1.395302	0.478266	...	-0.662353	-0.161005	29.57
3	69297	1.276014	-0.672705	...	-0.054869	-0.000007	92.68
4	144504	-0.312745	-1.202565	...	-0.221374	-0.136090	40.00
..	...	...	...	...	...	...	...
585	149640	0.754316	2.379822	...	0.304703	-0.044362	2.00
586	69394	1.140431	1.134243	...	0.071993	0.113684	1.00
587	139117	-3.975939	-1.244939	...	0.877424	0.667568	8.30
588	148028	-1.053840	4.362801	...	0.847220	0.531932	0.00
589	135314	-3.158990	1.765452	...	-0.235477	0.018129	84.28

[590 rows x 30 columns]

	Time	ATM_PIN_NO	CARD_NAME	...	RECEIVER_ADDRESS	RECEIVER_IFSC_NO	Amount
285	88029	-1.489450	1.464234	...	-0.224106	0.051787	1.00
113	97466	-0.507070	0.710443	...	-0.548975	0.212319	15.95
18	36346	-0.634011	0.555985	...	-0.120555	0.128903	40.00
76	166152	-1.860363	0.308274	...	-0.022718	-0.140742	340.00
206	79914	-1.631201	1.030757	...	0.554988	0.354009	29.99
..	...	...	...	...	...	...	...
277	154158	-1.165732	1.410133	...	-1.272036	-0.473882	1.98
9	23413	1.197664	0.184014	...	-0.071034	0.001532	5.49
359	65385	-2.923827	1.524837	...	1.510206	-0.324706	1354.25
192	156944	-1.726626	-0.181792	...	0.146527	-0.156524	0.89
559	102489	-2.296987	4.064043	...	0.969582	0.335041	104.00

[413 rows x 30 columns]

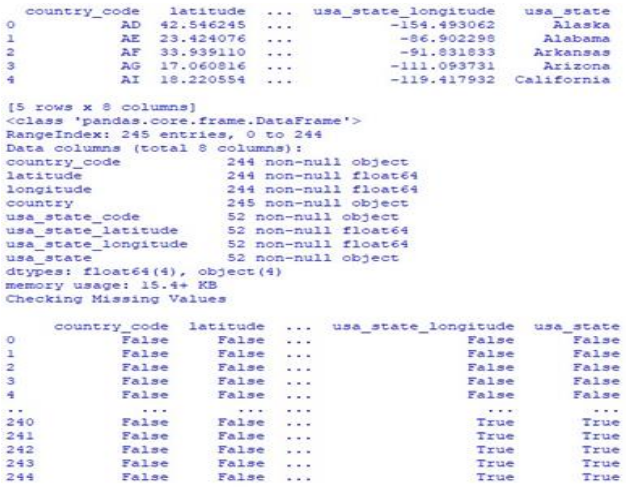
Figure 5: X training and test data

Y-train, Y-Test

```
[177 rows x 30 columns]
285    0
113    0
18     0
76     0
206    0
      ..
277    0
9      0
359    1
192    0
559    1
Name: Class, Length: 413, dtype: int64
225    0
14     0
85     0
418    1
132    0
      ..
346    1
369    1
140    0
533    1
171    0
Name: Class, Length: 177, dtype: int64
```

Figure 6: Y training and test data

ISSN: 2005-4238 IJAST



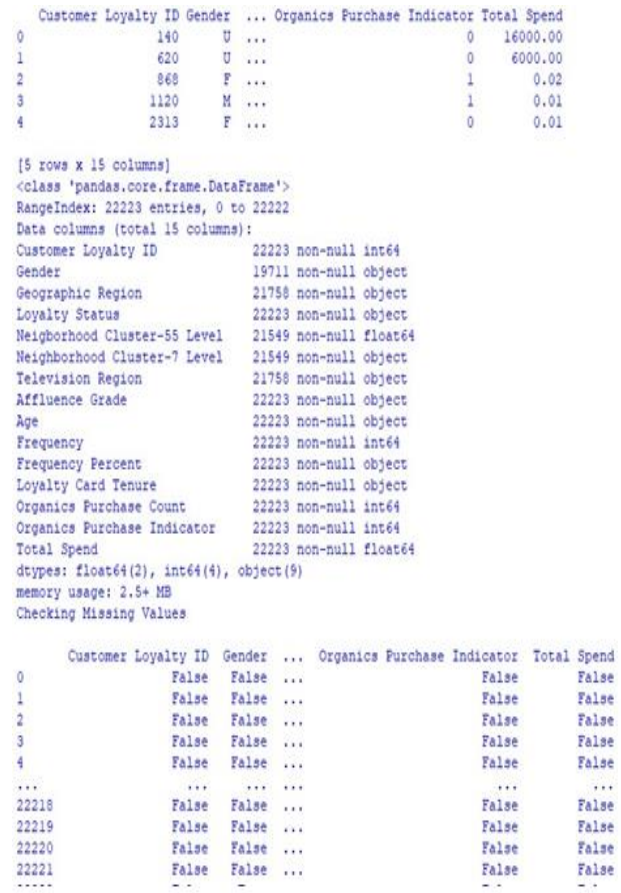
```
  country_code   latitude  ...  usa_state_longitude   usa_state
0           AD  42.546245  ...          -154.493062      Alaska
1           AE  23.424076  ...           -86.902298     Alabama
2           AF  33.939110  ...           -91.831833    Arkansas
3           AG  17.060816  ...          -111.093731     Arizona
4           AI  18.220554  ...          -119.417932  California

[5 rows x 8 columns]
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 245 entries, 0 to 244
Data columns (total 8 columns):
country_code            244 non-null object
latitude                244 non-null float64
longitude               244 non-null float64
country                 245 non-null object
usa_state_code          52 non-null object
usa_state_latitude      52 non-null float64
usa_state_longitude     52 non-null float64
usa_state               52 non-null object
dtypes: float64(4), object(4)
memory usage: 15.4+ KB
Checking Missing Values

     country_code  latitude  ...  usa_state_longitude  usa_state
0           False     False  ...                False      False
1           False     False  ...                False      False
2           False     False  ...                False      False
3           False     False  ...                False      False
4           False     False  ...                False      False
..            ...       ...  ...                  ...        ...
240         False     False  ...                 True       True
241         False     False  ...                 True       True
242         False     False  ...                 True       True
243         False     False  ...                 True       True
244         False     False  ...                 True       True

[245 rows x 8 columns]
```

Figure 7. GPS Result



```
   Customer Loyalty ID Gender  ... Organics Purchase Indicator Total Spend
0                  140      U  ...                          0    16000.00
1                  620      U  ...                          0     6000.00
2                  868      F  ...                          1        0.02
3                 1120      M  ...                          1        0.01
4                 2313      F  ...                          0        0.01

[5 rows x 15 columns]
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 22223 entries, 0 to 22222
Data columns (total 15 columns):
Customer Loyalty ID           22223 non-null int64
Gender                        19711 non-null object
Geographic Region             21758 non-null object
Loyalty Status                22223 non-null object
Neigborhood Cluster-55 Level  21549 non-null float64
Neighborhood Cluster-7 Level  21549 non-null object
Television Region             21758 non-null object
Affluence Grade               22223 non-null object
Age                           22223 non-null object
Frequency                     22223 non-null int64
Frequency Percent             22223 non-null object
Loyalty Card Tenure           22223 non-null object
Organics Purchase Count       22223 non-null int64
Organics Purchase Indicator   22223 non-null int64
Total Spend                   22223 non-null float64
dtypes: float64(2), int64(4), object(9)
memory usage: 2.5+ MB
Checking Missing Values

       Customer Loyalty ID  Gender  ...  Organics Purchase Indicator  Total Spend
0                    False   False  ...                        False        False
1                    False   False  ...                        False        False
2                    False   False  ...                        False        False
3                    False   False  ...                        False        False
4                    False   False  ...                        False        False
...                    ...     ...  ...                          ...          ...
22218                False   False  ...                        False        False
22219                False   False  ...                        False        False
22220                False   False  ...                        False        False
22221                False   False  ...                        False        False
```

Figure 8. Steadfastness card result

Random Forest Classification Algorithm

Random forests or maybe random determination forests can be a group mastering technique for category, relapse and various errands functions by building a large number of00 decision forest at implementing time and glorious the class this is the method of typically the classes (classification) or indicate prediction (relapse) of the specific trees. Purposeful decision forested acres right for final decision trees' tendency for over installation to their prep set.

ISSN: 2005-4238 IJAST

Algorithm:
Input: Info set M and the quantity of trees t.
Output: A random forest classification.
Initialize a = 1 to t:

1) Design a bootstrap trial M_i from the training set m whose size is n.
2) Build a binary tree of the bootstrapped data recursively from root node. Replicate the upcoming steps until all records of present node belong to a label.

a) Select a subset of √s traits.
b) For b = 1 to √s:
i) Calculate *left middle[b]* and *right middle[b]*.
c) For c= 1 to $|M_{ic}|$:
i) Compute the space L_k and R_k between the $data_k$ and each center.
ii) Suppose $L_k \leq R_k$ Allocate d_k to the left child of the present node. Otherwise allocate d_k to the right child of the present node.
d) Divide the node into a left and a right child. Where M_{ic} is the subgroup of M_i in the present node

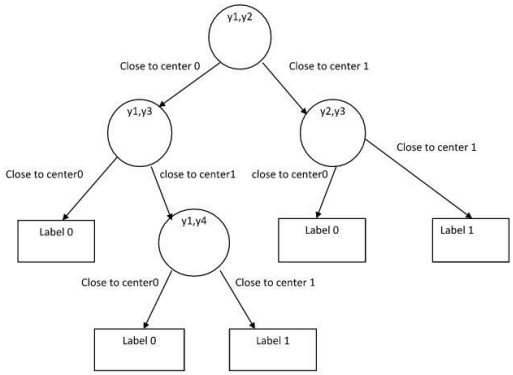


Figure 9: Random Forest Tree

A simple trial of random tree is shown in Fig. 9. The internal nodes are represented by circles. The variables in a circle are traits casually chosen from Y= {y1, y2, y3, y4}. The decisions are made according to their values. Each end node is represented by a rectangle and corresponds to a label.

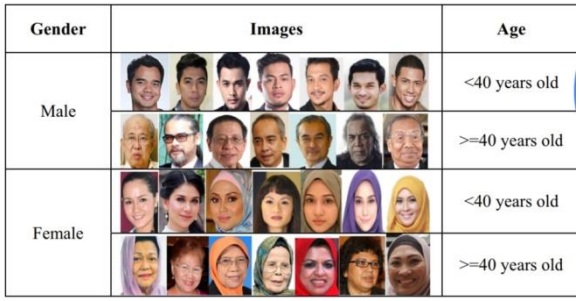


Figure 10: Face image Output

In figure 10 represents the face image output using Recurrent Neural Network.

Out of the normal language space, specialists have RNNs to show client practices in comparable web server logs, particularly in meeting based suggestion errands.

Data Fusion Techniques Of Our Framework

(i) Normalize the info set

ISSN: 2005-4238 IJAST

(ii) Determine the eccentricity of credit card,

$$\varepsilon(x)=1+\frac{||\mu-x||^2}{X-||\mu||^2} \quad (1)$$

(iii) Calculate degree of suspicion based on eccentricity result,

$$\gamma_k^{cc}=1-\frac{1}{\varepsilon_k} \quad (2)$$

(iv) Identify the disagreement of credit card and steadfastness card,

1.Find difference between credit and steadfastness card,

$$\delta_k=\left||cc_k-lc_k|\right| \quad (3)$$

Suppose (3) becomes 0,there is no chance of suspicion otherwise use (4),

$$\gamma_k^{dis}=1-\frac{1}{1+_{\delta_k^2}} \quad (4)$$

(v)Detect degree of suspicion based on distance between card holder car and store location,

$$\gamma_k^{loc}=e\frac{-d_k^2}{2\sigma_k^2} \quad (5)$$

(vi)Compute suspicion in face pictures,

$$\gamma_k^{gen}\,or\,\gamma_k^{age}=1-classification\ accuracy \quad (6)$$

If uncertainity occurs, use (7)

$$\gamma_k^{gen}\,or\,\gamma_k^{age}=classification\ accuracy \quad (7)$$

(vii)Finally fuse info set using (8) with weight w,

$$\gamma_k^{total}=\frac{\sum_{i=1}^{N}w_i\gamma_i}{\sum_{i=1}^{N}w_i} \quad (8)$$

4. Results and Discussion

This region shows the exact subtleties plus aftereffects about investigations. From the very beginning, a concept correlation is manufactured on a identical subset. Appears to fall apart we check to see the connection involving a model's exhibition plus the proportion associated with lawful and even fraud deals in a subsection, subdivision, subgroup, subcategory, and subclass. At long last, the idea shows the very exhibitions regarding models when using a lot increased dataset and that is progressively turn to the legitimate outcome. Considering that exactness pace isn't satisfactory to know the production of a hit-or-miss forest type when the files is totally imbalanced. For instance, a default auguration of all circumstances into the principal part category will moreover have a high opinion of excellence.

ISSN: 2005-4238 IJAST

Table 1. Degree of suspension with distance

Table 1: Degree of Suspicion

Sno	Credit card	Steadfastness card	Lifetime	Gender	Distance	Total
1	0.99899765	0.980309478	0.8015	0.0975	0.887860	0.753233
2	0.66403396	0.017881954	0.1984	0.0975	0.888817	0.373326
3	0.01149939	0.020377667	0.8015	0.0975	0.762443	0.375343
4	0.70626717	0.738609143	0.1984	0.0975	0.976795	0.543514
5	0.14545314	0.368776080	0.1984	0.0975	0.888876	0.339801
6	0.38384978	0.115812439	0.1984	0.0975	0.888763	0.336865
7	0.55700852	0.566584475	0.1984	0.0975	0.78933	0.441764
8	0.60546674	0.117871994	0.1984	0.0975	0.976585	0.399217
9	0.3605588	0.425790072	0.1984	0.0975	1.83E-04	0.582449
10	0.43059378	0.135402063	0.1984	0.0975	2.88E-04	0.748379

5.Conclusion

This particular paper explains the plausibility of credit card scams recognition determined by anomaly mining applies exclusion discovery exploration dependent on splitting up whole in to credit card fraud area and offers this identity techniques as well as its observational process. Lastly this course demonstrates class utilizing arbitrary forest classer utilizing trades through abnormality mining imitating investigation associated with credit card swap data group of one specific business financial institution. The evaluation shows that exemption mining may identify credit card scams better than anomaly recognition influenced by bunching whenever abnormalities tend to be far not quite typical information. In the event that this particular calculation is actually applied directly into bank credit card scams recognition platform, the likelihood of scams exchanges could be predicted soon after charge card exchanges through the banks. Additionally, an advancement of towards fraud methods can be obtained to prevent banking institutions from amazing misfortunes formerly and reduce dangers. Upcoming work can easily concentrate on the actual accompanying: 1) Using carry out profile with regard to peculiarity detection. 2) Utilizing metaheuristic computation for planning neural techniques and bodyweight determination.

References

[1] Adepoju, O., Wosowei, J., lawte, S., &Jaiman, H. (2019), " Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques", Global Conference for Advancement in Technology (GCAT), pp.13-23.
[2] Benchaji, I., Douzi, S., &ElOuahidi, B. (2018), " Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection", Cyber Security in Networking Conference (CSNet), pp.4-13.
[3] Ghobadi, F., &Rohani, M. (2016), "Cost sensitive modeling of credit card fraud using neural network strategy", 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), pp.34-45.
[4] Ju, C., & Wang, N. (2009), " Research on Credit Card Fraud Detection Model Based on Similar Coefficient Sum", First International Workshop on Database Technology and Applications, pp.11-19.
[5] Lucas, Y., Portier, P.-E., Laporte, L., Calabretto, S., He-Guelton, L., Oble, F., &Granitzer, M. (2019), "Dataset Shift Quantification for Credit Card Fraud Detection", 2019 IEEE Second International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), pp.22-29.
[6] Mareeswari, V., &Gunasekaran, G. (2016), "Prevention of credit card fraud detection based on HSVM", International Conference on Information Communication and Embedded Systems (ICICES), pp.39-48.
[7] Yu, W.-F., & Wang, N. (2009), "Research on Credit Card Fraud Detection Model Based on Distance Sum", International Joint Conference on Artificial Intelligence, pp.1-11.
[8] Wang, C., Wang, Y., Ye, Z., Yan, L., Cai, W., & Pan, S. (2018), "Credit Card Fraud Detection Based on Whale Algorithm Optimized BP Neural Network", International Conference on Computer Science & Education (ICCSE), pp.16-24.

ISSN: 2005-4238 IJAST