

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/323157944>

# Ensemble learning for credit card fraud detection

Conference Paper · January 2018

DOI: 10.1145/3152494.3156815

---

CITATIONS

14

---

READS

904

3 authors, including:



**Rameshwar Pratap**

Indian Institute of Technology Mandi

22 PUBLICATIONS 33 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Efficient Sketching Algorithm for Sparse Binary Data [View project](#)

# Ensemble Learning for Credit Card Fraud Detection

Ishan Sohony\*  
Pune Institute of Computer  
Technology,  
ishan.sohony@zensar.com

Rameshwar Pratap†  
rameshwar.pratap@gmail.com

Ullas Nambiar  
Zenlabs, Zensar Technologies, Pune  
ullas.nambiar@zensar.com

## ABSTRACT

Timely detection of fraudulent credit card transactions is a business critical and challenging problem in Financial Industry. Specifically, we must deal with the highly skewed nature of the dataset, that is, the ratio of fraud to normal transactions is very small. In this work, we present an ensemble machine learning approach as a possible solution to this problem. Our observation is that *Random Forest* is more accurate in detecting normal instances, and *Neural Network* is for detecting fraud instances. We present an ensemble method – based on a combination of random forest and neural network – which keeps the best of both worlds, and is able to predict with high accuracy and confidence the label of a new sample. We experimentally validate our observations on real world datasets.

## KEYWORDS

Fraud detection, deep learning, random forest

### ACM Reference Format:

Ishan Sohony, Rameshwar Pratap, and Ullas Nambiar. 2018. Ensemble Learning for Credit Card Fraud Detection. In *CoDS-COMAD '18: The ACM India Joint International Conference on Data Science & Management of Data, January 11–13, 2018, Goa, India*. <https://doi.org/10.1145/3152494.3156815>

## 1 INTRODUCTION

Over last decade, due to rise of e-commerce, the use of credit cards has increased dramatically. This has also increased the risk of fraudulent transactions. Further, credit card transactions are considered as an easy fraud target because of its low risk and high reward nature. Incidence of credit card fraud is limited to about 0.1% of all card transactions, but it may result into huge financial losses as transactions can be of quite large amount. Today's fraud detection systems are designed to prevent one twelfth of one percent of all transactions processed which still translates into billions of dollars in losses. For example, on May 15, 2016, in a coordinated attack, a group of around 100 individuals used the data of 1600 South African credit cards to steal 12.7 million USD from 1400 convenience stores

\*This work was done while pursuing his internship at Zenlabs, Zensar Technologies, Pune.

†This work was done when author was affiliated with Zenlabs, Zensar Technologies, Pune.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](https://permissions.acm.org).

CoDS-COMAD '18, January 11–13, 2018, Goa, India

© 2018 Association for Computing Machinery.

ACM ISBN 978-1-4503-6341-9/18/01...\$15.00

<https://doi.org/10.1145/3152494.3156815>

in Tokyo within three hours. According to a European Central Bank report [1] every day billions of Euros are lost in Europe due to credit card fraud.

There are two possible ways to combat fraud – fraud detection and fraud prevention. Fraud prevention consists of a set of rules, procedures, and protocols put in place to stop fraudulent transactions from occurring. Depending on the domain, there are a number of ways for fraud prevention, for example, use of OTP (one-time-password) on mobile phones, secure payment gateways, security questions for online banking. As, these methods are neither full proof and also they are often inconvenient for the customer, thus it is desirable to have a balance between security and convenience. On the other hand, fraud detection comes into the picture when the fraud prevention systems have been surpassed and a fraudulent transaction has been committed. Once fraudulent transactions has been detected, the goal is to reverse it as soon as possible. In order to accomplish this, fraud detection methods have to be constantly updated to cope with new types of fraud.

It is quite difficult to determine whether an attempt of making a fraudulent transaction has passed the prevention mechanisms. The goal of the fraud detection systems is to check every transaction for the possibility of being fraudulent regardless of the prevention mechanisms, and to identify fraudulent ones as quickly as possible. This problem leads financial institutions to continuously look for better ways to detect fraud. In spite of this, fraudsters constantly change their strategies to deceive of being detected, which makes traditional, rule-based fraud detection systems obsolete very fast. This motivates the applicability of Machine Learning techniques for this problem. In what follows we discuss several challenges associated with using Machine Learning techniques to detect fraudulent usage of cards.

### 1.1 Challenge with credit card fraud detection

Credit card fraud detection is an extremely difficult, but an important problem to solve. However, there are several constraints associated with the problem. In what follows, we mention a few important points:

- **Unavailability of Datasets:** One major challenge associated with the problem is the lack of availability of public datasets [12, 13, 18]. Credit card companies maintain the datasets of their transactions, however, due to privacy and security concerns they are not able to release this data in the public domain. But, any research work in this direction will need such data to build a model. However, there are some results which are performed on synthetically generated data [2, 6]. But none of these previous results disclose the features of the data and the parameters used in classifier models. Due to

this, benchmarking different fraud detection systems is quite difficult. Also, the limited amount of data which is publicly available may not be enough to detect a pattern, as there are millions of possible places and e-commerce sites to use a credit card, which makes this problem extremely hard.

- *Dynamic Fraudulent Behaviour*: Fraudsters often change their behaviour over time so as to beat the current detection systems by modifying their pattern. Due to this, pattern of normal and fraudulent transactions changes constantly. It is quite possible that there exist past fraudulent transactions, which now fit the pattern of normal (legitimate) transactions [16]. As a consequence, the problem becomes very complex in nature and it is difficult to predict even by human experts.
- *Highly Skewed Dataset*: Credit card fraud datasets are highly skewed – where a vast majority of the samples are normal transactions while only a small minority of them are fraudulent transactions. In most of the cases more than 99% of the total transactions are normal, and consequently less than 1% of them are fraudulent [14].
- *Right Evaluation Parameters*: Accuracy is one of the standard measures for determining the effectiveness of any classifier. However, in credit card fraud detection, accuracy may not be the correct measure because, due to skewed nature of the datasets, it is possible that even in a model with high accuracy, most of the fraudulent transactions are being misclassified. Therefore, it is important to evaluate such models on recall - correctly classifying fraudulent transaction - and precision - correctly classifying normal transactions.

## 1.2 Our Approach

The credit card fraud detection problem came to us while co-innovating with a BFSI customer based in US. Due to business confidentiality needs, some aspects of the problem have been masked below. Also, we are using a publicly available dataset that mimics the most important features of the problem raised by the business scenario - skewness of distribution. However, we mimic our experiments on a public dataset [7] which has similar attributes as our original dataset - skewness and distribution. Each feature of the public dataset is of numerical type, and its original features were masked by performing PCA on them. Consequently, the dimension of dataset was significantly reduced, and there was a possibility of features being co-related, we train our model considering every feature. This eliminates the possibility of doing feature engineering on the data.

Ensemble learning is a powerful way to improve the performance of a machine learning model. The core idea of an ensemble is to combine diverse set of classifiers together to improvise the stability and predictive power of the model. We use an ensemble of Random Forests and Neural Networks. Our observation is that Random Forest is able to correctly classify normal transactions, but misclassifies fraud transactions. On the other hand, Neural Networks are able to correctly classify fraudulent transactions, but misclassify some of the normal transactions. Thus, our ensemble method keeps the best of both worlds and is able to predict with high accuracy the label of a new sample. We summarise our approach in Algorithm 1, and illustrate the steps in details in Section 5.

---

### Algorithm 1: Ensemble Machine Learning Algorithm for Credit Card Fraud Detection

---

**Input:** Dataset mentioned in Table 2

**Output:** An ensemble machine learning model for fraud detection

- 1 **Data Preparation:** Split the data into the following three part
    - Training data: 60% normal and 60% fraudulent transactions;
    - Cross Validation data: 20% normal and 20% fraudulent transactions;
    - Test data: 20% normal and 20% fraudulent transactions;
- Model Training:**
- Train a feed-forward Neural Network on the entire Training data;
  - Train another feed-forward Neural Network on under sampled training data – 60% fraudulent transactions and the same number of uniformly sampled normal transactions;
  - Train another feed-forward Neural Network on under sampled training data – 60% fraudulent transactions and half the number of uniformly sampled normal transactions;
  - Train a Random Forest on entire Training data having 300 decision trees;
  - Train a Random Forest on entire Training data having 400 decision trees;
  - Use Cross Validation data for tuning parameters of above three models;
- Model Testing:**
- For model testing use testing data and output the result which is outputted by the majority of classifiers;
- 

## 1.3 Organization of the paper

In Section 2, we present necessary background to understand the paper – we first discuss some standard techniques for handling class imbalance problem, and then we discuss the parameters for evaluating the models. In Section 3, we provide a discription of the dataset and state some challenge associated with the dataset. In Section 4, we present results from our initial attempts to solve the problem which are *via* unsupervised learning and supervised learning. In Section 5, we present our classification model which is an ensemble of Feed-Forward Neural Networks and Random Forests. Finally, in Section 6, we conclude our discussion and state some possible extensions of our work.

## 2 BACKGROUND

### 2.1 Handling class imbalance

As mentioned earlier, the major challenge with credit card fraud detection is the highly imbalanced distribution of normal and fraudulent transactions. Due to this, the ability of any machine learning algorithm to discover the pattern of fraudulent transactions cannot relied upon. Sampling could be a possible approach to overcome this problem. The objective of sampling is to alter the distribution of minority class or the majority class so that the distribution is approximately uniform. But, this may possibly lead to the classifier

overfitting or underfitting the normal transactions and the classifier could potentially classify a fraudulent transaction as normal or vice-versa respectively. There are several ways of sampling to handle the class imbalance problem – oversampling the minority class, undersampling majority class, a combination of these two, and SMOTE [4].

**Oversampling:** Oversampling the minority class replicates the minority class until the number of minority class examples equals the number of examples of majority class. This gives the classifier enough samples of minority class for training. However, there are several problems associated with oversampling approach: a) it doesn't result to more information of being included in the training set, b) it may lead to over-fitting of a model especially in the case of noisy input.

**Undersampling:** Undersampling is contrary to the oversampling approach – we underrepresent the majority class by uniformly sampling points from majority class. There are both advantages and disadvantages to undersampling with respect to oversampling. A major advantage of undersampling is that it creates a model on which data has been observed already, while on the other hand a major disadvantage of undersampling is that amount of training data available to train a model is significantly reduced. Undersampling techniques for learning skewed distributions have been well studied. Japkowicz [11], [10], [5] discussed in detail the applicability of undersampling approach for handling the class-imbalance problem.

**SMOTE:** [4] SMOTE artificially generates data points belonging to the minority class and suggests an approach of handling class imbalance. It is also a type of oversampling approach wherein the minority class is oversampled by creating "synthetic" examples rather than by oversampling with replication.

1

## 2.2 Evaluation Parameters

**Table 1: Confusion Matrix**

	Positive (Fraud)	Negative (Normal)
Positive (Fraud)	True Positive (TP)	False Negative (FN)
Negative (Normal)	False Positive (FP)	True Negative (TN)

In this paper, we use three assessment measures namely – *accuracy*, *recall* and *precision*. They are calculated based on the confusion matrix mentioned in Table 1. A Confusion Matrix quantifies the performance of the classifier while assigning input to different labels. Recall shows the efficiency of classifier in detecting actual fraudulent transaction.

$$\text{Recall} = \frac{TP}{FN + TP}.$$

Precision measures the reliability of the classifier.

$$\text{Precision} = \frac{TP}{FP + TP}.$$

<sup>1</sup>We performed experiments using both oversampling (by replication) of minority class, and SMOTE but we did not get any encouraging results on the dataset.

Finally, accuracy quantifies the total performance of the classifier. It shows that how many of the total experimental records have been classified correctly by the classifier.

$$\text{Accuracy} = \frac{TP + TN}{FP + TP + TN + FN}.$$

## 3 DATASET DESCRIPTION

The dataset [7] contains transactions made with credit cards in September 2013 by European cardholders. This dataset presents transactions that have occurred within a period of two days, where we have 492 fraudulent transactions out of 284,807 total transactions. The dataset is highly imbalanced, the positive class (frauds) account for 0.172% of all transactions. It contains only numerical input variables which are a result of the PCA transformation. Due to confidentiality issues, the original features and more background information about the dataset has not been provided. Features  $V_1, V_2, \dots, V_{28}$  are the principal components obtained with PCA, the only features which have not been transformed with PCA are "Time" and "Amount". Feature "Time" contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature "Amount" is the transaction amount. Feature 'Class' is the response variable and it takes value 1 in case of fraud and 0 otherwise. We describe it in Table 2.

**Table 2: Credit Card Dataset [7]**

Normal	Fraudulent	Features	Instance
284,315	492	30	284,807

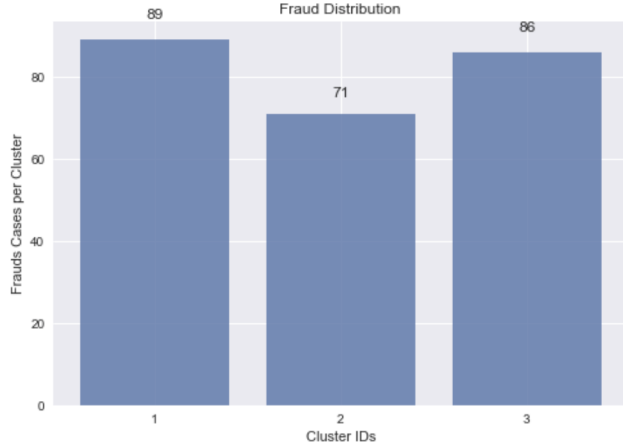
**Challenge with the dataset:** This is a classic example of an unbalanced dataset of credit card fraud. As it has been observed in the dataset description only 0.172% of the transactions are fraudulent, so even a null model (a model which classifies all the transactions as normal) will have an accuracy of 99.928%. Thus, using the accuracy to evaluate the effectiveness of the model is meaningless. Also due to the high degree of imbalance in the dataset, the model must be prevented from overfitting the Normal class. This may lead to high accuracy but at the cost of misclassifying several fraudulent transactions as Normal.

## 4 INITIAL ATTEMPTS

### 4.1 A naive approach via unsupervised learning

We began by using unsupervised learning methods to determine how the fraudulent transactions are distributed in the 30-dimensional space. The main goal of this approach was to determine whether the fraudulent transactions are outliers or clustered in a single or multiple clusters. We used  $k$ -means clustering for the same, and for its implementation we used  $k$ -means++ [3] as an initialization strategy. The reason for selecting  $k$ -means++ is that it gives constant factor approximation with respect to optimal  $k$ -means clustering result. Idea is to cluster the points using  $k$ -means++ and then put the labels of the data to determine the distribution of fraudulent transactions. In Figure 1, we plot the distribution of fraudulent transactions for values of  $k = 3, 5, 10$ .

Thus, our finding was that the fraudulent transactions are neither outliers with respect to  $k$ -means clustering, nor are they isolated in one or more clusters. Rather, they are more or less uniformly distributed in all the clusters. We also attempted other unsupervised clustering techniques such as DBSCAN [8], and a mixture of gaussians [19], but obtained similar results. Due to space limitations we are not able to discuss them in more detail.



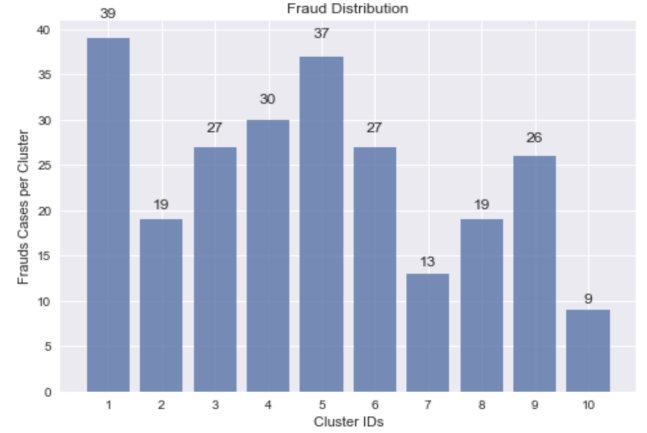
**Figure 1: Distribution of fraudulent transaction after applying  $k$ -mean clustering for values of  $k = 3$**



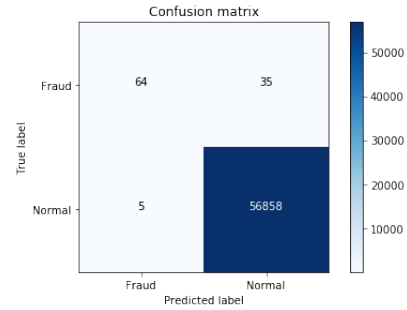
**Figure 2: Distribution of fraudulent transaction after applying  $k$ -mean clustering for values of  $k = 5$ .**

#### 4.2 Another Approach via Supervised Learning – Logistic Regression

We used Binomial Logistic Regression as Fraud Detection is a two class problem. Logistic regression model has been used to study fraudulent behaviour [9],[21]. We used Logistic Regression as prior art and compare our approach with it.



**Figure 3: Distribution of fraudulent transaction after applying  $k$ -mean clustering for values of  $k = 10$ .**



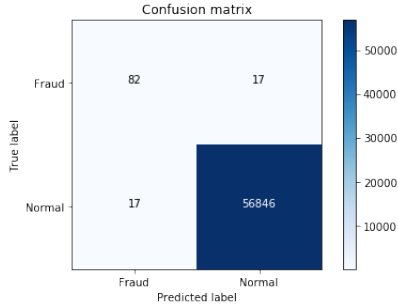
**Figure 4: Logistic Regression Classifier.**

## 5 OUR APPROACH

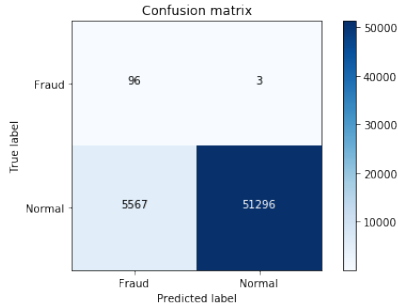
For credit card fraud detection misclassifying even a few normal cases as fraudulent is not tolerable, however, misclassifying even a single fraudulent case as normal is also not tolerable. Therefore, our primary goal is to minimize the misclassification of fraudulent cases and the secondary goal is to minimize the misclassification of normal cases. In order to achieve this goal, we used an ensemble of two types of classifiers, Random Forests and Feed-forward Neural Networks – an ensemble of 3 feed-forward neural networks and 2 random forests. We discuss them in detail below.

*Feed-forward Neural Networks:* Neural Networks are a widely used Machine Learning/ Statistical modelling technique for modelling complex patterns. The basic element of a neural network is a neuron which accepts multiple inputs, aggregates them, applies a (usually nonlinear) activation function, and outputs the result, either as a model prediction or as an input to the next layer. The layered approach allows the neural network to model complex patterns. Neural networks have been used previously to address the credit card fraud problem [20]. We use 3 feed-forward neural networks, which we call  $L_1$ ,  $L_2$  and  $L_3$  in our approach. For the training of all the networks we use the ADAM algorithm [15] and a learning rate of 0.0005.

- $L_1$  has 3 hidden layers with 45, 68 and 102 neurons respectively with the sigmoid activation function. Training Data:  $L_1$  is trained on 60% of normal transactions and 60% of fraudulent transactions.
- $L_2$  has 2 hidden layers with 15, 8 neurons respectively with the sigmoid activation function. Training Data:  $L_2$  is trained on 60% of fraudulent transactions and an equal number of normal transactions.
- $L_3$  has 2 hidden layers with 15, 8 neurons respectively with the sigmoid activation function.  $L_3$  is trained on 60% of fraudulent transactions and half the number of normal transactions.



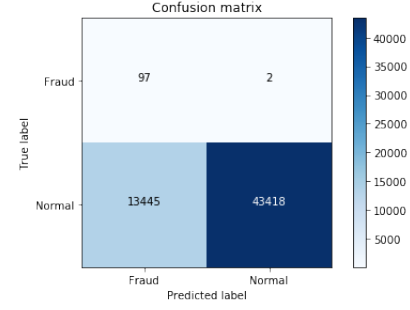
**Figure 5: Confusion Matrix for  $L_1$  Feed-Forward-Neural-Network after training on 60% normal and 60% fraud transactions.**



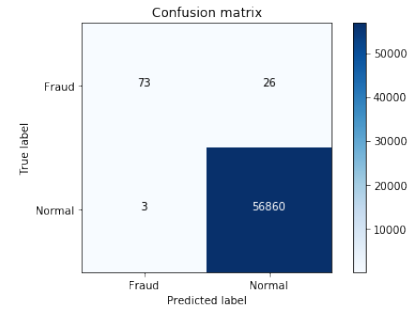
**Figure 6: Confusion Matrix for  $L_2$  Feed-Forward-Neural-Network after training on 60% fraud and equal number of normal transactions.**

*Random forest.* Random Forests have been widely used as the state-of-the-art approach for dealing with imbalanced datasets. Rigorous experimentation showed that this classifier gives optimal results in our case when the number of decision trees is set between 300 and 400, if we increase the number of trees beyond 400, the Random Forest starts to overfit. In our work we use 2 Random Forests namely  $L_4$  and  $L_5$ .

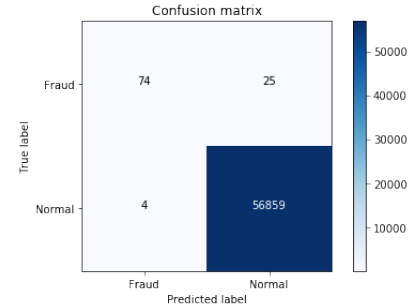
- $L_4$  consists of 300 decision trees.
- $L_5$  consists of 400 decision trees.



**Figure 7: Confusion Matrix for  $L_3$  Feed-Forward-Neural-Network after training on 60% fraud and half the number of normal transactions.**



**Figure 8: Confusion Matrix for Random forest  $L_4$  having 300 decision trees after training on 60% normal and 60% transactions.**



**Figure 9: Confusion Matrix for Random forest  $L_5$  having 400 decision trees after training on 60% normal and 60% transactions.**

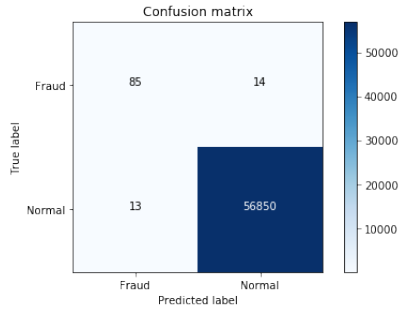
*Ensemble Approach:* We now aggregate the results of individual classifiers  $L_1, L_2, L_3, L_4, L_5$  and present our final classifier  $\mathcal{L}$ <sup>2</sup>. For a new transaction  $x$ , we compute the output value of each individual classifier and output the majority of the result *i.e.*

$$\mathcal{L} = \text{majority}\{L_1(x), L_2(x), L_3(x), L_4(x), L_5(x)\}.$$

<sup>2</sup>We experimentally figured out on the number of classifier to be used. The precision and recall obtained from an ensemble of 5 classifier were better than the precision and recall obtained from 3, and 7 or more classifiers.

**Table 3: Precision, Recall and Accuracy of classifiers**

Classifier	Recall	Precision	Accuracy
Logistic Regression	64.64%	92.75%	99.93%
$L_1$	82.82%	82.82%	99.94%
$L_2$	96.96%	1.69%	90.22%
$L_3$	97.97%	0.71%	76.39%
$L_4$	73.73%	96.05%	99.94%
$L_5$	74.74%	94.87%	99.94%
$\mathcal{L}$	86.73%	85.85%	99.95%

**Figure 10: Confusion Matrix for Ensemble classifier by taking majority of results.**

As we can observe,  $L_1$  has moderately high precision and recall, i.e. it classifies a fair number of fraudulent transactions correctly however, it also misclassifies a fair amount of the transactions.  $L_2$  has a very high recall but low precision, i.e. it is very good at detecting fraudulent transactions however in doing so it also misclassifies a large number of normal transactions. Same is the case with  $L_3$ . In order to balance  $L_2$  and  $L_3$  we introduce random forests  $L_4, L_5$ . Random forests have low recall but high precision, i.e. they misclassify a very low number of normal transactions, but they are not very good detecting fraudulent transactions. Thus we consider a majority approach, we only classify a transaction as fraud or normal if a majority of the classifiers classify it as fraud or normal respectively.<sup>3</sup> Thus we take the best of both worlds and get a classifier whose precision and recall are optimal.

## 6 CONCLUDING REMARKS AND FURTHER DIRECTIONS

In this paper, we look at the critical and complex task of detecting credit card fraud in a highly skewed setting. We propose an ensemble model that combines best of Random Forest and Feed Forward Networks to accurately detect fraud. Our experimental results point to this being a superior method than other popular approaches. An

<sup>3</sup>We also tried boosting approach for ensemble learning – we assigned weights to the outputs of the five classifiers with the logistic regression. However as the results were not encouraging and we discarded that approach. The intuition behind this was that the results of some classifier may be more relevant than the others, i.e. some classifiers may be making more correct predictions than the others. So the results of these classifiers must be given more importance rather.

open direction of our work is to improve the accuracy parameters of the classifier. Although, the scope of our work is limited to the dataset having numerical values, yet in a more general case, for e.g., the datasets having text values it would be interesting to extend our work by including some more sophisticated techniques like word2vec [17].

## REFERENCES

- [1] Second report on card fraud. In *European Central Bank*, 2013.
- [2] Emin Aleskerov, Bernd Freisleben, and Bharat Rao. CARDWATCH: a neural network based database mining system for credit card fraud detection. In *Proceedings of the IEEE/IAFE 1997 Computational Intelligence for Financial Engineering, CIFE 1997*, New York City, USA, March 24-25, 1997, pages 220–226, 1997.
- [3] David Arthur and Sergei Vassilvitskii. K-means++: The advantages of careful seeding. In *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA '07*, pages 1027–1035, Philadelphia, PA, USA, 2007. Society for Industrial and Applied Mathematics.
- [4] Nitesh V. Chawla, Kevin W. Bowyer, Lawrence O. Hall, and W. Philip Kegelmeyer. SMOTE: synthetic minority over-sampling technique. *J. Artif. Intell. Res.*, 16:321–357, 2002.
- [5] Nitesh V Chawla, Nathalie Japkowicz, and Aleksander Kotcz. Special issue on learning from imbalanced data sets. *ACM Sigkdd Explorations Newsletter*, 6(1):1–6, 2004.
- [6] Rong-Chang Chen, Ming-Li Chiu, Ya-Li Huang, and Lin-Ti Chen. *Detecting Credit Card Fraud by Using Questionnaire-Responded Transaction Model Based on Support Vector Machines*, pages 800–806. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.
- [7] Andrea Dal Pozzolo, Olivier Caelen, Reid A Johnson, and Gianluca Bontempi. Calibrating probability with undersampling for unbalanced classification. In *Computational Intelligence, 2015 IEEE Symposium Series on*, pages 159–166. IEEE, 2015.
- [8] Martin Ester, Hans-Peter Kriegel, Jörg Sander, and Xiaowei Xu. A density-based algorithm for discovering clusters a density-based algorithm for discovering clusters in large spatial databases with noise. In *Proceedings of the Second International Conference on Knowledge Discovery and Data Mining, KDD '96*, pages 226–231, 1996.
- [9] D.W. Hosmer and S. Lemeshow. *Applied Logistic Regression*. Wiley-Interscience, Newton, MA, USA, 2000.
- [10] Nathalie Japkowicz. The class imbalance problem: Significance and strategies. In *Proc. of the Int'l Conf. on Artificial Intelligence*, 2000.
- [11] Nathalie Japkowicz and Shaju Stephen. The class imbalance problem: A systematic study. *Intell. Data Anal.*, 6(5):429–449, 2002.
- [12] Sanjeev Jha, Montserrat Guillen, and J Christopher Westland. Employing transaction aggregation strategy to detect credit card fraud. *Expert systems with applications*, 39(16):12650–12657, 2012.
- [13] Chunhua Ju and Na Wang. Research on credit card fraud detection model based on similar coefficient sum. In *First International Workshop on Database Technology and Applications, DBTA 2009, Wuhan, Hubei, China, April 25-26, 2009, Proceedings*, pages 295–298, 2009.
- [14] Piotr Juszczak, Niall M. Adams, David J. Hand, Christopher Whitrow, and David J. Weston. Off-the-peg and bespoke classifiers for fraud detection. *Computational Statistics and Data Analysis*, 52(9):4521–4532, 2008.
- [15] Diederik P. Kingma and Jimmy Ba. Adam: A method for stochastic optimization. *CoRR*, abs/1412.6980, 2014.
- [16] Jesus Mena. *Investigative Data Mining for Security and Criminal Detection*. Butterworth-Heinemann, Newton, MA, USA, 2002.
- [17] Tomas Mikolov, Ilya Sutskever, Kai Chen, Greg Corrado, and Jeffrey Dean. Distributed representations of words and phrases and their compositionality. In *Proceedings of the 26th International Conference on Neural Information Processing Systems, NIPS'13*, pages 3111–3119, USA, 2013. Curran Associates Inc.
- [18] E. W. T. Ngai, Yong Hu, Y. H. Wong, Yijun Chen, and Xin Sun. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3):559–569, 2011.
- [19] Douglas Reynolds. *Gaussian Mixture Models*, pages 659–663. Springer US, Boston, MA, 2009.
- [20] M. Syeda, Yan-Qing Zhang, and Yi Pan. Parallel granular neural networks for fast credit card fraud detection. In *Fuzzy Systems, 2002. FUZZ-IEEE'02. Proceedings of the 2002 IEEE International Conference on*, volume 1, pages 572–577, 2002.
- [21] B.B. Little Y. Jin, R.M. Rejesus. Binary choice models for rare events data: a crop insurance fraud application. *Applied Economics*, 37(7):841–848, 2005.