Credit Card Fraud Detection in Payment Using Machine Learning Classifiers

Maad M. Mijwil[1] and Israa Ezzat Salem[2]

[1] Computer Techniques Engineering Department, Baghdad College of Economic Sciences University
Baghdad, Iraq
Email: mr.maad.alnaimiy [AT] baghdadcollege.edu.iq

[2] Computer Techniques Engineering Department, Baghdad College of Economic Sciences University
Baghdad, Iraq
Email: israa.ezzat [AT] baghdadcollege.edu.iq

ABSTRACT— ***The fraud detection in payment is a classification problem that aims to identify fraudulent transactions based individually on the information it contains and on the basis that a fraudster's behaviour patterns differ significantly from that of the actual customer. In this context, the authors propose to implement machine learning classifiers (Naïve Bayes, C4.5 decision trees, and Bagging Ensemble Learner) to predict the outcome of regular transactions and fraudulent transactions. The performance of these classifiers is judged by the following ways: precision, recall rate, and precision-recall curve (PRC) area rate. The dataset includes more than 297K transactions via credit cards in September 2013 and November 2017 that have been collected from Kaggle platform, of which 3293 are frauds. The performance PRC ratio of machine learning classifiers is between 99.9% and 100%, which confirms that these classifiers are very good at identifying binary classes 0 in the dataset. The results of the tests have proved that the best classifier is C4.5 decision trees. This classifier has the best accuracy of 94.12% in prediction of fraudulent transactions.***

Keywords— Fraud Detection, Machine Learning, Payment, Predict, Classifiers, Credit Card.

1. INTRODUCTION

Card operations are carried out with credit or debit cards, which are used to buy goods and services, both in physical establishments and on the Internet [1]. Fraud in this type of operation occurs generally when the cards are copied since, in the event of theft, the customer usually notices the loss before the fraudster can act [2]. The most common way to clone cards is to install devices in-store terminals or ATMs, which save the information of the magnetic strip when performing a regular operation. In the case of Internet purchases, fraud is even easier since knowing the card details is enough without the need for it to be present [3]. Figure 1 shows some of the cartoon images of credit card information theft (download from Google).

At the present time, payment cards are one of the most popular and widely used methods by many citizens around the world. This is why so many frauds occur, and it is one of the most common problems faced by banks and payment service providers (PSP) [4]. Fraud occurs when it is not the legitimate customer who performs the operation but a third party who has managed to operate as if it were the real customer, having already saved all the bank's security mechanisms. By presenting the credit card or by announcing the credit card details (ID card, expiration date and security code) on the Internet, it is easy to perform card payments on the merchant side. The result of the low level of security card payment is the effect of fraudulent abuse. In addition, another major reason is the increase in the use of mobile devices for payment initialization. In 2015, universal payment cards lost $21.84 billion due to fraudulent transactions [6].

Figure 1: Cartoon images of credit card information theft.

For clarity, the principal contribution of our research is the application of three machine learning classifiers : (Naïve Bayes, C4.5 decision trees, and Bagging Ensemble Learner) to detect fraud operations on 28 credit cards. Our dataset includes 297,467 transactions in September 2013 and November 2017 that have been collected from the Kaggle platform, of which 3293 are frauds. This study assists in finding the best classifier out of the three classifiers used by evaluating their performance based on precision, recall rate, and precision-recall curve (PRC) area rate.

The rest of the paper is constructed as follows. Section 2, reviews some prior arts between 2017-2020. In Section 3, introduces the machine learning classifiers that will be applied in this study. In contrast, section 4 demonstrates the results obtained from these three classifiers and compares them with the results of one of the previous studies. Finally, conclusions are extracted in Section 5.

2. LITERATURE SURVEY

Many authors use machine learning classifiers to deal with the problem of card payment fraud detection. Actually, there are admittedly a large number of published papers, but in this section, we only elected six studies because they are very close to our current research. We start by Awoyemi et. al [7]. This study applies three classifiers: (Logistic Regression, K-Nearest Neighbour, and Naïve bayes) for the dataset of credit card transactions from European cardholders, containing more than 284K transactions. The results of this study show the greatest accuracy according to Naïve Bayes of over 97%. Yee et al. [8], discusses the application of machine learning classifiers (Naïve Bayes, Bayesian network classifiers, Tree Augmented Naïve Bayes, logistics and J48 classifiers). The results of this study achieve an accuracy of 100.0% through the J48 classifier and logistics. In the literature by Safa and Ganga [9], classifiers are implemented: Naïve Bayes, K-nearest neighbour, and Logistic Regression. The research results show that the highest accuracy rate is obtained by using Logistic regression classifier, which is 97.69%. In another study, Trivedi et al. [10] point out that seven machine learning classifiers are applied, such as Decision Tree, Random Forest, Naïve Bayes, Gradient Boosting, Super Vector Machine, k-Nearest Neighbour and Logistic Regression. The dataset for this study comprises more than 284K transactions. In this study, the best accuracy is obtained by the random forest classifier exceeded 95%. The study by Husejinović from BiH [11], suggests three machine learning classifiers (Naive Bayes, C4.5 decision tree and Bagging Ensemble) for dataset contains more than 284K transaction where 492 are fraud. The results of this study achieve more than 92% by C4.5 decision tree. This study is the closest to our current study, as its results will be compared with ours. In a study conducted by Najadat et. al from Jordan [12], they discuss the application of six machine learning classifiers: Voting, Ada boosting, Random Forest, Decision Tree, Logistic Regression and Naïve Base. The results of this study show that the classifier with the best accuracy is the Naive bayes, which has scored over 91%.

3. THE CLASSIFIERS

In this paper, we examine the performance of Naïve Bayes, C4.5 decision tree, and Bagging ensemble method to pass the precision, recall rate, and PRC area rate test performance. Figure 2 illustrates the mechanism of this paper. The mechanism consists of three parts. The left side is the dataset, the middle is the applied classifiers, and the last position on the right is the outputs of these classifiers. In this section, we will briefly review each of the classifiers applied in this study. We expect it is valuable to readers.

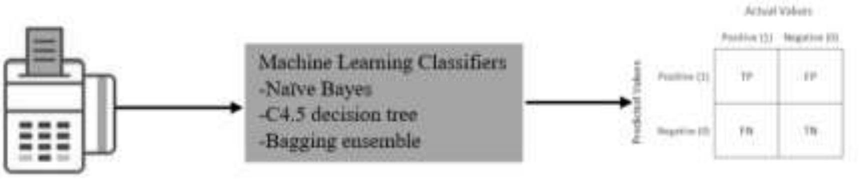

Figure 2: The mechanism of this paper [Designed by Authors].

3.1 The first classifier is Naïve Bayes

Naïve Bayes [13][14] is a probabilistic machine learning algorithm that can be applied to a variety of classification tasks. This classifier is created by English mathematician Thomas Bayes. Figure 3 shows the main equation for the Naïve Bayes classifier with an explanation of each variable.

In addition, this classifier is based on Bayes' theorem and it is an idle learning model. It can also handle unstable dataset. This classifier works mathematically, that is, calculating the probabilities of all variables and classifying them according to the variable with the highest probability value. On the other hand, even with little training data, the classifier can be very successful. Its advantage is that it gives a value of zero as the probability value in case the test data has a value that is not observed in the training data, because the result cannot be predicted. These conditions are commonly referred to as zero frequency. Therefore, the correction method can be used to solve such problems, such as the application of Laplace estimation.

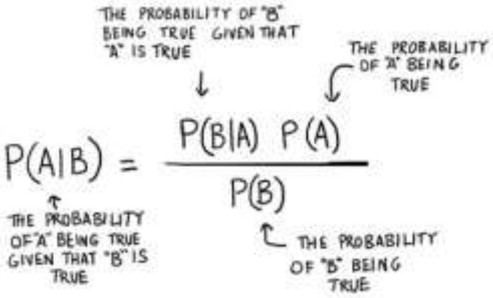
THE PROBABILITY OF "B" BEING TRUE GIVEN THAT "A" IS TRUE
THE PROBABILITY OF "A" BEING TRUE
P(A|B) = P(B|A) P(A) / P(B)
THE PROBABILITY OF "A" BEING TRUE GIVEN THAT "B" IS TRUE
THE PROBABILITY OF "B" BEING TRUE

Figure 3: Naïve Bayes equation [15].

3.2 *The second classifier is C4.5 Decision Tree*

The C4.5 Decision Tree [16][17] is one of the most popular machine learning classifiers in data classification. It creates a tree structure model consisting of decision nodes and terminal nodes. No matter how big the decision is, this classifier can predict the correct decision well. It is updated by dividing the data set into small parts, making it easier to use. The important note in this classifier is that a decision node can contain one or more branches (see Figure 4). The first node in any diagram is called a root node. Data in the decision tree can consist of different sections, such as categorical and numerical data. This classifier is developed in the early 1980s by the American computer scientist J. Ross Quinlan.

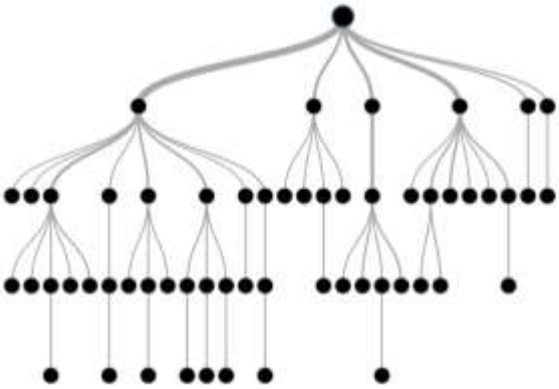

Figure 4: Example of C4.5 Decision Tree [from Google]

The dataset applied in the classification problem using the decision tree algorithm should be divided into two main parts (training data and testing data). The algorithm uses training data to build a model. The success of the model in problem-solving is calculated by applying the model to test data.

3.3 *The third classifier is Bagging Ensemble Learning*

The Bagging Ensemble [18][19] is developed by Breiman in 1996. A collection is created by applying estimators to boot samples obtained from the original dataset. The bootloader is used here to generate refundable random selections and sub-samples. The sub-samples will be the same as the number in the original dataset. Therefore, some observations are not included in the samples created as a result of the boot, while some may be seen two or more times.

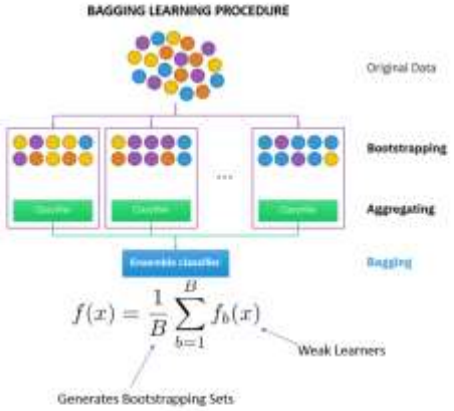
BAGGING LEARNING PROCEDURE
Original Data
Bootstrapping
...
Aggregating
Ensemble classifier
Bagging
$f(x) = \frac{1}{B}\sum_{b=1}^{B} f_b(x)$
Weak Learners
Generates Bootstrapping Sets

Figure 5: An example of Bagging Ensemble [20].

In the consolidation of estimates stage, the averages are taken for the regression trees, while the results are determined by voting in the classification trees. Bagging can also improve the predictive effectiveness of inconsistent predictors. They can be made more convenient by using variables with small deviations but large variances. Figure 5 shows an example of Bagging Ensemble.

4. EXPERIMENTS

In order to verify the success of the proposed classification models, several experiments are conducted on the dataset to select the best classifier. To determine the performance of the classifiers, we rely on only three outputs: Precision, Recall, and PRC Area. Where the higher the accuracy results, then this classifier is the best among these experiments. In addition, the confusion matrix provides a complete description of the performance of the classifier. Through this matrix, we can distinguish the correct classifier implementation from the wrong classifier implementation. Confusion Matrix consists of two classes which are actual class and predicted class, as presented in Table 1.

Table 1*:* Confusion Matrix

		Predicted class	
		0	1
Actual class	0	True positive (TP)	False negative (FN)
	1	False positive (FP)	True negative (TN)

Now, we calculate the Precision and Recall by formula (1) and (2), respectively:
Precision is a ratio of true positives (*TP*) and actual positives (*TP+FP*), by formula (1)

$$Precision = \frac{TP}{TP+FP} \quad (1)$$

Recall is a ratio of true positives (*TP*) and actual positives (*TP+FN*). Measures the fraction of actual positives that are correctly recognized so, by formula (2)

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

The area under the PR curve is applied to measure the overall ability of the test to identify binary classes. It is a basic tool for judging models of unbalanced datasets with binary classes. The graphical visualization of the PRC is described by the recall rate on the X-axis and the precision on the Y-axis. The higher the number, the better the performance of the classifier is. The original dataset is unbalanced because only 0.19% of the data is classified as fraud. If we predict that all data inputs will be classified as class 1, then we will gain 99.81% accuracy. This work is performed using Weka software v3.6 with the latest update in October 2020 with a computer: CPU: Intel® 4 Cores-2.40GHz-Core i5-9300H, Graphics Cards: AMD Radeon XR, RAM: 8GB, and running on Ubuntu 18.04.4 LTS 64-bit. Table 2 presents the performance results of all applied classifiers. These results are applied to get precision, recall and PRC rates.

Table 2: Performance Rates

Classifiers	Precision		Recall		PRC Area	
	Class 0	Class 1	Class 0	Class 1	Class 0	Class 1
Naïve Bayes	99.9%	65.6%	96.5%	81.2%	100%	81.0%
C4.5	100%	94.1%	100%	78.9%	99.9%	75.6%
Bagging	100%	91.6%	99.9%	80.7%	100%	83.8%

From the table above, we note the following: The PRC area in class 0 is between 99.9% and 100%, this means that these classifiers are very well at distinguishing binary classes 0 in our dataset. While the PRC area in class 1, we found that the results in this column are different. The Naïve Bayes classifier is 81%, the C4.5 classifier is 75.6%, and the Bagging Ensemble classifier is 83.8%. This experiment proves that the performance of the C4.5 Decision Tree classifier is good, while the Bagging classifier is perfect, and the Naïve Bayes classifier is acceptable. This column is a key indicator because it tells us the prediction results of the classifiers, whether it is a regular or a fraudulent transaction. The precision of class 1, in this column, means the precision of the predicted value of the negative value of class 1. For all predicted fraudulent transactions, 94.12% will be perfectly predicted with the best achievement of the C4.5 Decision Tree classifier.

A comparison of the current work is made with previous work conducted by Husejinović [11]. Table 3 illustrates the comparison between these two studies. Through this table, we notice the success of the current work on the previous research in the accuracy of predicting fraudulent transactions. Also, the dataset employed in our work is more than the previous study.

Table 3: Comparison between current study and previous study

Studies	Dataset	Fraud transactions	History	Precision
Husejinović [11]	284.807	492	Sep. 2013	92.74%
Our Work	297,467	3293	Sep.2013 & Nov.2017	94.12%

5. CONCLUSIONS

In recent years, fraud transactions have become widespread and have become one of the most critical problems facing banks all over the world. In this paper, three classifiers of machine learning are applied to predict regular or fraudulent transactions. The best performance is C4.5 Decision Tree with 94.1% precision and 78.9% recall. The acceptable performance is Bagging Ensemble with 91.6% precision and 80.7% recall. As for the worst performance, it is the Naïve Bayes classifier. The results through this classifier are not convincing, as it gives a precision of 65.6% and a recall of 81%. In the future, other classifiers will be used and applied to a set of local data that will be collected from banks in Iraq.

6. REFERENCES

[1] Gupta S. and Johari R., "A New Framework for Credit Card Transactions involving Mutual Authentication between Cardholder and Merchant," In Proceedings of International Conference on Communication Systems and Network Technologies (CSNT), pp: 22-26, Katra, India, 13-15 July 2011. https://doi.org/10.1109/CSNT.2011.12.

[2] Budhram T., "A New Framework for Credit Card Transactions Involving Mutual Authentication between Cardholder and Merchant, South African Crime Quarterly," vol.40, pp:31-37, June 2012. https://doi.org/10.17159/2413-3108/2012/v0i40a843

[3] Ermatita and Sutedja I., "Detection of Frauds for Debit Card Transactions at Automated Teller Machine in Indonesia Using Neural Network," IOP Conference Series Conference- Journal of Physics: Conference Series, Palembang, Indonesia, pp:1-10, 26–27 November 2018. https://doi.org/10.1088/1742-6596/1196/1/012076

[4] DeVries P. D., "The problem of fraud in the banking industry: Are biometrics the answer?," International Journal of Services and Standards, vol.7, no.3, pp:310-327, January 2011. https://doi.org/10.1504/IJSS.2011.045055

[5] Ogundele O., Zavarsky P., Ruhl R., and Lindskog D., "Fraud Reduction on EMV Payment Cards by the Implementation of Stringent Security Features," International Journal of Intelligent Computing Research, vol.3, no.3, pp:328-348, September 2012. https://doi.org/10.20533/ijicr.2042.4655.2012.0031

[6] Robertson D., "Top Card Issuers in Asia-Pacific," The Nilson Report, pp:1-12, October 2016. PDF link: https://nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf

[7] Awoyemi J. O., Adetunmbi A. O., and Oluwadare S. A., "Credit card fraud detection using machine learning techniques: A comparative analysis," In Proceedings of International Conference on Computing Networking and Informatics (ICCNI), pp:1-6, Lagos, Nigeria, 29-31 October 2017. https://doi.org/10.1109/ICCNI.2017.8123782

[8] Yee O. S., Sagadevan S., and Malim N. H. A. H., "Credit Card Fraud Detection Using Machine Learning as Data Mining Technique," Journal of Telecommunication, Electronic and Computer Engineering, Vol. 10 No.4, pp:23-27, August 2018.

[9] Safa M. U., and Ganga R. M., "Credit Card Fraud Detection Using Machine Learning," International Journal of Research in Engineering, Science and Management, vol. 2, no.11, pp: 372-374, November 2019

[10] Trivedi N. K., Simaiya S., Lilhore U. K., and Sharma S. K., An Efficient Credit Card Fraud Detection Model Based on Machine Learning Methods, International Journal of Advanced Science and Technology, vol.29, no.5, pp: 3414 - 3424, April 2020.

[11] Husejinović A., "Credit Card Fraud Detection Using Naive Bayesian And C4.5 Decision Tree Classifiers," Periodicals of Engineering and Natural Sciences, vol.8, no.1, pp:1-5, January 2020.

https://doi.org/10.21533/pen.v%25vi%25i.300

[12] Najadat H., Altiti O., Aqouleh A. A., and Younes M., Credit Card Fraud Detection Based on Machine and Deep Learning, In Proceedings of International Conference on Information and Communication Systems (ICICS)-IEEE, pp:1-6, Irbid, Jordan, 7-9 April 2020. https://doi.org/10.1109/ICICS49469.2020.239524

[13] Chen S., Webb G. I., Liu L., and Ma X., "A Novel Selective Naïve Bayes Algorithm," Knowledge-Based Systems - Elsevier, Vol.192, March 2020. https://doi.org/10.1016/j.knosys.2019.105361

[14] Salmi N. and Rustam Z., "Naïve Bayes Classifier Models for Predicting the Colon Cancer," IOP Conference Series Conference- Materials Science and Engineering, Malang, Indonesia, pp-1-9, 20-21 March 2019. https://doi.org/10.1088/1757-899X/546/5/052068.

[15] Sammit, "#MLMuse—Naivety in Naive Bayes' Classifiers," Clairvoyant Soft. Available online: https://blog.clairvoyantsoft.com/mlmuse-naivety-in-naive-bayes-classifiers-9c7f6ba952bf

[16] Hsian B., Merbouha A., Ezzikouri H., And Erritali M., "A comparative study of decision tree ID3 and C4.5," International Journal of Advanced Computer Science and Applications Special Issue on Advances in Vehicular Ad Hoc Networking and Applications, pp:13-19, July 2014. http://dx.doi.org/10.14569/SpecialIssue.2014.040203

[17] Oujdi S., Belbachir H., and Boufares F., "C4.5 Decision Tree Algorithm for Spatial Data, Alternatives and Performances," Journal of Computing and Information Technology, vol.27, no.3, pp:23-29, May 2020. https://doi.org/10.20532/cit.2019.1004651

[18] Gaikwad D. P., and Thool R. C., "Intrusion Detection System Using Bagging Ensemble Method of Machine Learning," In Proceedings of International Conference on Computing Communication Control and Automation-IEEE, pp:1-6, Pune, India, 26-27 February 2015. http://doi.org/10.1109/ICCUBEA.2015.61

[19] Tuysuzoglu G. and Birant D., "Enhanced Bagging (eBagging): A Novel Approach for Ensemble Learning," The International Arab Journal of Information Technology, Vol. 17, No. 4, pp:515-528, July 2020, https://doi.org/10.34028/iajit/17/4/10

[20] Singhal G., "Ensemble Methods in Machine Learning: Bagging Versus Boosting," Pluralsight, June 2020. Available online: https://www.pluralsight.com/guides/ensemble-methods:-bagging-versus-boosting