Unsupervised Machine Learning for Card Payment Fraud Detection

Mario Parreno-Centeno(✉), Mohammed Aamir Ali, Yu Guan, and Aad van Moorsel

Newcastle University, Newcastle upon Tyne, UK
{m.parreno-centeno1,m.a.ali2,yu.guan,aad.vanmoorsel}@ncl.ac.uk

Abstract. Credit card fraud is one of the most common cybercrimes experienced by consumers today. Machine learning approaches are increasingly used to improve the accuracy of fraud detection systems. However, most of the approaches proposed so far have been based on supervised models, i.e., models trained with labelled historical fraudulent transactions, thus limiting the ability of the approach to recognise unknown fraud patterns. In this paper, we propose an unsupervised fraud detection system for card payments transactions. The unsupervised approach learns the characteristics of normal transactions and then identify anomalies as potential frauds. We introduce the challenges on modelling card payment transactions and discuss how to select the best features. Our approach can reduce the equal error rate (EER) significantly over previous approaches (from 11.2% to 8.55%ERR), for a real-world transaction dataset.

Keywords: Card payments · Fraud detection · Machine learning · Deep learning · Card Not Present · Unsupervised learning

1 Introduction

The value of global non-cash transactions is growing every year and it is estimated to reach beyond 720 billion of dollars in 2020 [8]. Figure 1 breaks down the total transactions value by global growth regions, i.e., North America, Europe, Mature Asia-Pacific (APAC), Emerging Asia, Central Europe Middle East and Africa (CEMEA), and Latin America (LATAM), between 2012 and 2021 (note that values between 2019 and 2021 are estimated). There is a clear increasing trending which is significantly stronger in emerging Asia and CEMEA. In these regions, where the card network development is relatively immature, the proliferation of card use is mainly due to the increase in mobile payments and wallets. On the other hand, in mature markets such as North America, Europe and mature APAC, the adoption of Near Field Communication (NFC)/contactless technology has powered the increment of the card operations.

With the growth of the value of global card payments transactions, fraud activities and losses related to them have increased as well. During the last few

S. Kallel et al. (Eds.): CRiSIS 2019, LNCS 12026, pp. 247–262, 2020.
https://doi.org/10.1007/978-3-030-41568-6_16

years, most of the losses are related to Card Not Present interfaces [32], which refers to online, telephone and mail transactions, in which the card is not physically present at the merchant. The most recent report on card payments fraud of the European Central Bank specified that Card Not Present fraud increased 66% over a period of five years with an approximate 1000 EUR millions of losses in 2016 in Europe [13].

Fighting fraud is a difficult task, and merchants are very sensitive to the fact that overhead associated with security measures (such as PINs) may degrade the customer experience. Moreover, security procedures against online fraud that require extensive personal information can also turn in another source of vulnerability. For example, this information may be exposed after a data breach, and once stolen, it can be used in fraudulent activities.

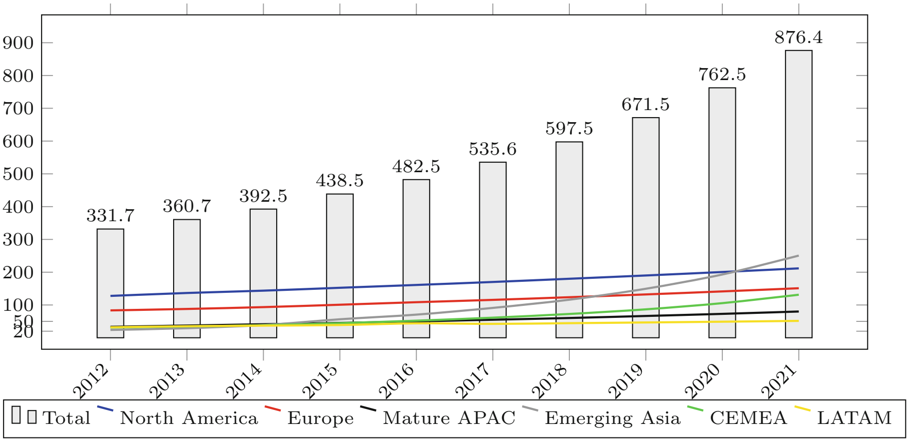

Fig. 1. Estimated value of world wide non-cash transactions from 2012 to 2021 [38].

The first Fraud Detection Systems (FDSs) for Card Not Present (CNP) transactions were based in rules, i.e., a set of thresholds established by experts trigger the alarm. However, card payments ecosystem is fast-changing and rules used in establishing fraudulent activity are likely to become ineffective or obsolete as time passes. More recently, machine learning techniques (ML) have been used to improve detection dynamically [27]. The ML approach learns fraudulent and/or normal patterns from past transactions to inform its fraud detection.

Most of the ML approaches for card payment fraud detection proposed so far are based on *supervised* learning techniques, i.e., the model is trained to find previously known fraud patterns. Thus, the model will not be able to identify *unknown* fraudulent patterns. Furthermore, transactional datasets used to train supervised fraud detection models are often highly skewed toward the number of samples of normal transactions compared to fraudulent ones. Usually, the percentage of fraudulent transactions is between 0.1% and 0.5% [7]. In this scenario, misclassification arises because of the difficulty of the FDS to learn fraud patterns.

In this paper, we propose an unsupervised approach which learns the patterns of normal transactions to detect potentially fraudulent transactions. Thus, it can detect previously undiscovered types of fraud and it does not rely on labeling fraudulent transactions within the data set. We study several Machine Learning and Deep Learning models: an autoencoder, a Multivariate Gaussian distribution and a One Class Support Vector Machine (OC-SVM, proposed already in the literature [17]). We conduct the experiments using a real-world transaction dataset from a European acquirer (the organisation that processes credit card transactions for its merchants). Furthermore, we study the importance of the transactional attributes and show their effect on the detection performance.

In summary, the contributions of this paper are as follows:

- a survey of the state of the art card payment fraud detection systems proposed so far.
- an exhaustive description of the challenges of applying machine learning approaches to detect card payment fraud.
- an evaluation of different unsupervised approaches on real-world card payment transactions dataset.
- an assessment of the effectiveness of feature selection approaches.

This paper is organized as follows. Section 2 introduces a set of well-established performance metrics and Sect. 3 discusses the traditional fraud detection systems and those based on machine learning techniques proposed so far. Section 5 describes the feature selection process and discuss the importance of the transaction's attribute. Section 4 introduces the dataset used to evaluate our approach. Section 6 discusses the performance of the unsupervised approach proposed based on three different algorithms and the trade-off number of attributes-performance. Section 7 concludes the paper.

2 Evaluation Metrics

In this section we introduce a set of well-established performance metrics which will be used throughout this work to evaluate the proposed FDS, and to compare its performance in terms of:

- The false acceptance rate, or FAR, is the measure of the likelihood that the fraud detection system will incorrectly accept a payment (incorrect since it is fraudulent). A system FAR is stated as the ratio of the number of false acceptances divided by the number of transactions considered.
- The false rejection rate, or FRR, is the measure of the likelihood that the fraud detection system will incorrectly reject a legal transaction. A system FRR is stated as the ratio of the number of false recognitions divided by the total number of transactions.

- Equal Error Rate (ERR) is the percentage value when FAR and FRR are equal. The ERR identifies under which parameter settings the proportion of false acceptances is equal to the proportion of false rejections. The lower the equal error rate value, the better the fraud detection system.
- Receiver Operating Characteristic curve (ROC curve), is a graphical plot that illustrates the diagnostic ability of a binary classifier system as its discrimination threshold varies. The ROC curve is created by plotting the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings. The true-positive rate is also known as sensitivity or recall. Furthermore, it can be calculated a 1-FRR. A diagonal (the line with intercept one and slope minus one) can be introduced to divide the ROC space. Points above the diagonal represent good classification results (better than random), points below the line represent poor results (worse than random). The intersection between the curve with the diagonal indicates the ERR.

3 Machine Learning Approaches for Card Fraud Detection

In this section, we discuss some of the machine learning approaches proposed so far. We classify them in supervised and unsupervised systems. The distinction of the group is done based on whether the specific target value to predict is known for the available samples and in the manner that the algorithm is trained.

Table 1. Card payment fraud detection approaches based in unsupervised machine learning techniques

Authors	Year	Techniques	Dataset	Quantitative results
Aleskerov et al. [1]	1997	Auto-associative NN	Synthetic	Yes
Quah et al. [26]	2008	Self Organized Maps	Collected	No
Srivastava et al. [30]	2008	Hidden Markov model	Synthetic	Yes
Bhusari et al. [6]	2011	Hidden Markov model	Synthetic	Yes
KhanT et al. [22]	2011	Hidden Markov model	Synthetic	Yes
Iyer et al. [19]	2011	Hidden Markov model	Synthetic	Yes
Hejazi et al. [17]	2013	One-class SVM	Collected	Yes
Bansal et al. [2]	2014	Self Organized Maps	Collected	Yes
Tech et al. [31]	2014	K-Menas	Synthetic	No

3.1 Supervised Learning

The emphasis on card payments fraud detection systems is on supervised classification methods. It is a discriminative technique trained to find previously known fraud patterns. In classification problems, the system scores the input transaction based in similarities with the attributes of the previously seen fraudulent patterns. Depending on whether the score exceeds a predefined threshold, the transaction will be classified such as legitimate or fraudulent.

Neural Networks (NNs) were one of the first ML techniques use to develop FDS more than 20 years ago and they have become very popular since then. In 1994, [16] developed a fraud detection system based on a 3-layers P-RCE feedforward network. They used a dataset of transactions processed by Mellon Bank during six months of 1991. The original training dataset was sampled to include 3.33% of fraudulent accounts and a feature selection process was applied to the original group of attributes. The results showed that when the system flagged 50 accounts as fraudulent per day, 40% of fraudulent transactions were detected. That meant an improvement of the previous operative FDS based on rules. In [7] an FDS was proposed combining a NN with a rule-based approach. Both modules were combined in a unique sequential system improving the FRR but decreasing the TPR. Reference [24] compared the accuracy of an Artificial Neural Network (ANN) with a Bayesian Belief network. BBN performed better. Reference [15] compared the performance of an FDS based in a NN with four other systems based in an Artificial Immune Systems (AIS), a Naive Bayes (NB), a Bayesian Network (BN) and a Decision Tree (DT) algorithms. The NN and the AIS methods obtained the best accuracy results. [3] compared the performance of FDSs based in two different NNs, a Committed Neural Network and a Clustered Committed Neural Network. The Clustered Committed network architecture showed better detection results. More recently, [14] compared the performance of a NN with a Convolutional Neural Network (CNN), a Random Forest (RF) and a Support Vector Machine (SVM). CNN, RF, and SVM obtained better accuracy results than the approach based on a NN.

In [20] an FDS based on the cardholders profiles was proposed using Recurrent Neural Networks (RNNs). They conclude that a base model based on an RF performed similarly to the proposed deep learning model.

[34] proposed a game-theoretic approach. They model the interaction between an attacker and an FDS such as a multi-stage game between two players both trying to maximize financial gain.

In 2010 [5] compare the accuracy of SVM, RF and Logistic Regression (LR). RF obtained the highest accuracy with a 78% F-score, followed by LR with 70% and SVM with 62%.

In [28] the authors compared the effectiveness of two FDSs based in an SVM and DT algorithms. The dataset was the same used in [5]. DT obtained the best accuracy rate with approximately 95% while SVM 93%.

[37] conducted a study to show whether transaction aggregation may improve the fraud detection rate. The analysis showed that RF, LR, SVM, KNN and Quadratic Discriminant (QDA) improve their accuracy with aggregation. However, DT (CART) did not. They showed the result in two independent datasets from two banks. In both analyses, QDA obtained the highest detection accuracy.

Machine Learning (ML) techniques have demonstrated to be useful to detect fraudulent payments transactions, but keeping a low FAR with a high detection rate is a difficult task. We have seen that FDS has a high FAR when keeping a high detection rate, [4]. FAR has a high impact on the effectiveness of the system. It has associated a cost and customer relations are directly affected.

On the other hand, one characteristic present on all the real card fraud transactional datasets used to train the model is that they are very imbalanced. Percentage of fraudulent transactions is extremely lower than that for legitimate transactions. Usually, the percentage of fraudulent transactions is just between 0.1% and 0.5% [7]. In this scenario, misclassification arises because of the difficulty of the FDS to learn the fraud patterns.

3.2 Unsupervised Learning

One of the main advantages of using unsupervised techniques in card fraud detection system is the possibility of found undiscovered fraudulent patterns. However, approaches for card fraud detection systems based on unsupervised techniques are less common.

In 1997, an FDS based in an auto-associative NN was proposed in [1]. Differently from the FDSs based in Supervised Neural Networks proposed in [16] and [7], this model was trained only with legitimate transactions (300 samples). They test the approach in a synthetic dataset generated with a Gaussian model. Each transaction consists of four attributes and the rate of normal samples was 5:1. The results of the test showed that the system classified correctly all the legitimate transactions and misclassified 15.09% of the fraudulent transactions. The limitation of this system is that they used one network per customer and they tested the approach only in synthetic data simulated from a Gaussian distribution.

In 2008, an FDS based on a Hidden Markov Model (HMM) was proposed in [30]. Same that in [1], this FDS created a spending habit model for each cardholder. The category of items purchased was represented as the underlying finite Markov chain. The transactions were observed through the stochastic process that produces the sequence of the amount of money spent on each transaction. The observation symbols were defined clustering the purchase values of the historical transactions of each cardholder. They were clustered in three price ranges low, medium and high. They tested the system in a synthetic dataset. The test results showed the best result of 80% of accuracy.

In 2014, [2] compared two approaches based on SOM and ID3 algorithms. The approaches clustered the data in four groups low, high, risky and highly risky. Both methods were tested in four datasets including 500, 100, 1500 and 2000 transactions (not more information was specified about the data). SOM had slightly better FPR (23.52% and 28% respectively) and 20% better TPR than ID3 (92.5% and 72.5%). Furthermore, the authors conclude that using the longest dataset, FPR improved 50% and TPR 20%.

In the same year, an unsupervised FDS based on a K-Means algorithm was suggested in [31]. The system was tested in a synthetic dataset. Some of the attributes of the dataset were transaction ID, transaction amount, transaction country, transaction date, credit card number, merchant category id, cluster id and indicative of fraud. The classification classes were the same four groups of the previous approach [2] i.e. low, high, risky and high risky. The authors did not show quantitatively the results.

Table 1 synthesizes the main aspects i.e. authors, technique, type of dataset and analysis of quantitative results for each of the unsupervised approaches reviewed in this section. We can see that only two of the approaches [2,17] were tested in real-world data while showing quantitative results. Between these two approaches, the one based on the OC-SVM model [17] achieved a higher accuracy result i.e. 93%.

4 Dataset

A card transnational payments dataset is a vector of m transactions $\mathbf{t}$:

$$\mathbf{T} = (\mathbf{t}_1, ..., \mathbf{t}_m) \tag{1}$$

Each transaction can be seen as a data tuple of d attributes a:

$$\mathbf{t}_i = (a_1, ..., a_d) \tag{2}$$

In the unsupervised card fraud detection literature, only a few publications use real card payments transactional datasets [15]. It is complicated access to transactional datasets because:

- Anonymity and security reasons [36] i.e. financial institutions usually do not make public the private information of their customers.
- Companies are not in the position to share sensitive information with their competitors.
- Usually, reveal information concerned to fraud detection systems is declared to violate vital security interests.

To show the effectiveness of our approach, we use an anonymised publicly available dataset realized for a leader in electronic transactions [25]. The datasets contain transactions made by credit cards by European cardholders. Each transaction consists of 30 features. To preserve the confidentiality of the customers most of the variables are the principal components transformation of the original values and features name are not specified for most of the attributes. Only features 'Time' and 'Amount' preserve the original value and authors describe the attribute. 'Time' is the seconds elapsed between each transaction and the first transaction in the dataset. The feature 'Amount' is the economic transaction amount. No more extra background information has been given for the rest of the features.

Furthermore, each transaction has associated a label which indicates whether the transaction is either legitimate or fraudulent i.e. equal to 1 if the transaction is fraudulent and equal to 0 otherwise.

However, the authors of the dataset have not specified how they have flagged the fraudulent transaction and they have not given a proof that 100% of fraudulent transactions are detected.

The dataset includes transactions that occurred over two days, where 492 out of 284,807 are fraudulent transactions. Note that the dataset is highly unbalanced, the positive class (frauds) account for 0.172% of all transactions.

We normalize the feature Time and Amount with the max-min technique. Furthermore, we transform the feature Time to indicate the hour of the day which the transaction in the following manner:

$$f(t) = \left[\frac{t}{60 * 60} \% 24 \right].$$

To show the performance of each of the proposed approaches in Sect. 6, we have split the original dataset in a Training dataset including 75% of the legitimate transactions and a testing dataset including the 25% of the legitimate transactions and all the fraudulent transactions and we use 10 folder cross-validation (for the normal samples).

5 Feature Selection

Most of the FDS in the literature use a feature selection process because: - Improve training time: some models are computationally intensive when building the models. If they compute lower-dimensional data, the time to train the model will be lower. - Improve the response of real-time systems: FDS is expected to detect fraudulent transactions in real-time. Detection can be faster if the number of attributes of each transaction is lower. Some authors reduce the number of attributes of the system significantly, for example in [15] the number of attributes was reduced from 33 to 17.

Some of the techniques to reduce the feature dimensional space are GA and PCA [33].

To compare the accuracy between different approaches is common training the system in several datasets, each with a different number of attributes. In [16], the authors compared the performance of an FDS when using two different groups of attributes. One of the groups included payment-related information. The results showed that the model trained without payment-related information increased accuracy.

We have used an extra-Trees algorithm to calculate the importance of the features of the dataset such as in [23]. We use the depth of the node assigned to each of the features to calculate the relative importance of that feature. Features on the top of the tree contribute to a higher rate to the final prediction of the model. To reduce the variance of the estimation, we used the average between several randomized trees.

Figure 2 shows the relevance importance of the features obtained. We can observe that features ‘V17’ and ‘V14’ are relatively much more informative than other features. Later, we will test the accuracy of the different approaches taking into account different groups of features.

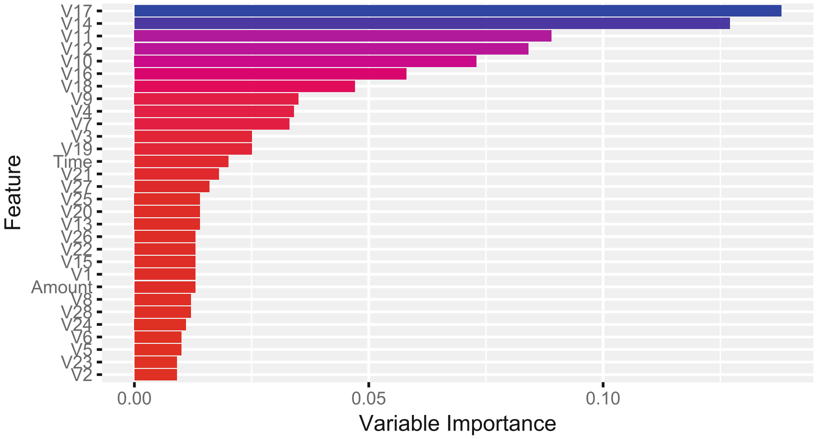

Fig. 2. Feature importance.

6 Proposed Approaches for Card Payments FDS

We propose an unsupervised FDS for card payments transactions. We compare the performance of three systems based on a deep learning technique (autoencoder) and two ML models i.e. multivariate Gaussian distribution model and OC-SVM (the last one previously used in [17] to detect fraudulent payment transactions obtaining the highest accuracy of the all unsupervised approaches reviewed in Sect. 3).

In our system, transactions are collected and recorded i.e. for two days. After that, during a window of time, fraudulent transactions will be flagged manually i.e. after a customer complaint, the same as in previous work showed in Sect. 3. At this point, we will use only normal transactions to train the model. Thus, the approach learns the characteristics of the normal samples. Once the model has been trained, each new transaction is classified as normal or fraudulent depending on how similar they are to the learned patterns according to the ML technique employed what we discuss next.

Deep Learning Autoencoders. Deep Learning is a popular method in image [12,29] and speech recognition [11,18] because of the superior classification performance obtained. It is a class of feature-learning methods, where the input data is transformed into an abstract representation, which has been widely used in pattern recognition and classification. Different levels of abstraction can be achieved by iterating layers.

We use a particular deep learning method called an autoencoder, which consists of an input layer, an output layer of equal size, and one or more hidden layers connecting them. In our model, the number of input units is equal to the number of selected attributes of the transaction. Autoencoders have been used for data representation [39] and more recently for authentication [9].

In this context, the input is the transaction vector $\mathbf{t}_i = (a_1, ..., a_d)$ and the output is:

$$\mathbf{u}(\mathbf{t}) = h_u(\mathbf{W}_u\mathbf{t} + \mathbf{b}_u), \tag{3}$$

where $\mathbf{W}_u \in \mathbb{R}^{d\times s}$ is a weight matrix, $\mathbf{b}_u \in \mathbb{R}^s$ is the bias vector, $a_1, a_2, ...,$ $a_d \in \mathbb{R}^d$ are the attribute of the transaction i and h_u is called the activation function, which in this approach we define such the hyperbolic tangent function [21]. The process of the classification approach is performed in two stages: the encoding and decoding steps. In the encoding step, the input a is mapped to the abstract representation $\mathbf{u}(\mathbf{t})$ according to Eq. 3, and in the decoding step, the transformation is reconstructed to the output representation $\hat{\mathbf{t}}$, which is an approximation of the input transaction, according to the decoder function:

$$\hat{\mathbf{t}} = h_d[\mathbf{W}_d\{\mathbf{u}(\mathbf{t})\} + \mathbf{b}_d],$$

where $\mathbf{W}_d \in \mathbb{R}^{s\times d}$ is the weights decoding matrix, $\mathbf{b}_d \in \mathbb{R}^s$ is the decoding bias vectors, and h_d the decoding activation function. We restrict the degrees of freedom using a tied architecture, where the encoding matrix is the transpose of the decoding matrix, i.e. $\mathbf{W}_d = \mathbf{W}_u^t$ [35].

More than one hidden layer can be applied to achieve higher flexibility (and abstraction) in the model. In a multiple layers architecture, encoders and decoders are stacked symmetrically, where the output from the k^{th} encoder, is the input of the $k + 1^{th}$ encoder.

Once the model has been training using backpropagation, we compute the mean squared error (MSE) between the original transaction t and its representation $\hat{t}$ on the output of the autoencoder, obtaining a validation match score. Here, we classify the instance such as normal or fraudulent based on a decision threshold.

Multivariate Gaussian Distribution. Given the card payments transnational dataset $\mathbf{T} = (\mathbf{t}_1, ..., \mathbf{t}_m)$ we will take into account only those transactions labeled as a normal. We assume that each attribute is normally distributed and we calculate the Gaussian parameters i.e. the mean μ_i and variance σ^2 for each of the features as follow:

$$\mu_i = \frac{1}{m}\Sigma_{j=1}^{m} a_i^{(j)} \tag{4}$$

$$\sigma_i^2 = \frac{1}{m}\Sigma_{j=1}^{m}(a_i^{(j)} - \mu_i)^2 \tag{5}$$

where $i \in \{1, 2, ..., d\}$ and d equal to the number of features.

Given a new transaction, we will calculate the probability to belong to the distribution as follow:

$$P(\mathbf{t}) = P(a_1; \mu_1, \sigma_1^2)P(a_2; \mu_2, \sigma_2^2)...P(a_d; \mu_d, \sigma_d^2) = \\ = \prod_{j=1}^{d} P(\mathbf{a}_j; \mu_j, \sigma_j^2) = \prod_{j=1}^{d} \frac{1}{\sigma_j \sqrt{2\pi}} e^{-(a_j-\mu_j)^2/2\sigma_j^2} \tag{6}$$

And we will consider the transaction as fraudulent if $P(\mathbf{t}) < \epsilon$ where ϵ is the probability threshold.

6.1 Comparison of Unsupervised Approaches for Card Payment Fraud Detection

In this section, we compare the performance of the two proposed approaches i.e. autoencoder and multivariate Gaussian model, with an approach proposed in [17] which was based on an OC-SVM model. So, we compare the performance of these approaches:

- an autoencoder with one hidden layer and 15 hidden units.
- a multivariate Gaussian model.
- a one-class SVM.

And we will consider the transaction as fraudulent if $P(\mathbf{t}) < \epsilon$ where ϵ is the probability threshold.

Table 2 shows the EER obtained by each model. We can see that the autoencoder and Gaussian models get the best EER values, 9.8% and 9.7% respectively. On the other hand, OC-SVM obtains the worst EER value (11.2%).

Figure 3 shows the ROC curve of the three different models. The ROC curve of the autoencoder and Gaussian models are very similar. On the other hand, although the OC-SVM is the model with the highest EER, it keeps a higher True Acceptance Rate ($TAR = 1 - FRR$), when the FAR is very small i.e. approximately $0,1\%$.

Table 2. ERR of three different unsupervised models on the dataset shown previously.

Models	ERR
Autoencoder	9.8%
Gaussian	9.7%
OC-SVM	11.2%

6.2 Feature Importance Experiments

We have seen that autoencoder and Gaussian models obtained very similar accuracy results. However, while deep learning models can manage adequately high dimensional inputs [10], Gaussian models work better on low dimensional space

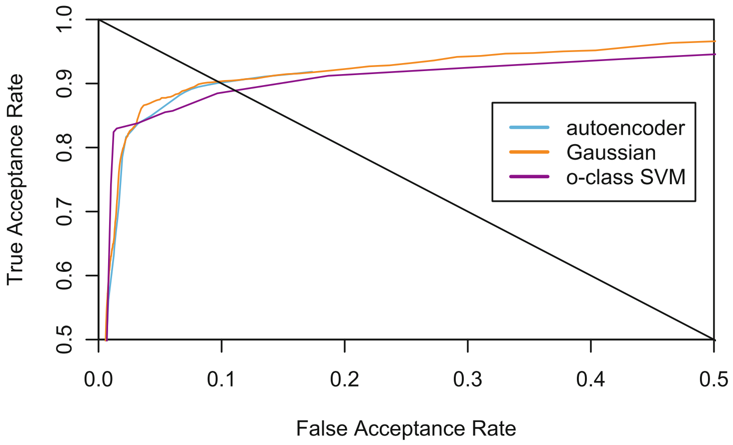

Fig. 3. ROC curves of the three unsupervised approaches i.e autoencoder, Gaussian and oc-svm used to model normal card payment transactions.

problems. Thus, we are going to reduce the number of features of the transactions from 30 to 7 using a five layers autoencoder i.e. the embedded representation of the middle layer of the autoencoder is used as the input of the Gaussian model. Figure 4 shows the ROC curve of the approach and the ROC curve of the Gaussian model for comparison. We can see that EER does not improve.

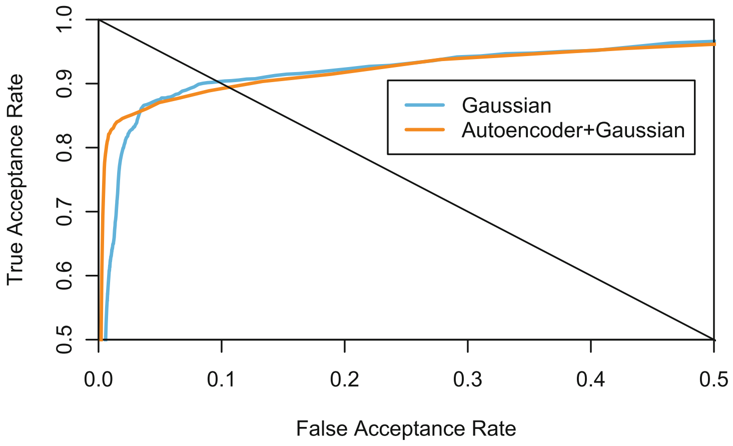

Fig. 4. ROC curve of the model autoencoder+GMM train end to end.

On the other hand, we are going to test the Gaussian model when changing the input vector to take into account different number of attributes. We group the attributes according to the importance calculated in Sect. 5. Figure 5 show the ROC curve of the results. We can observe that the model taking into account the two more informative features has the lowest EER (8.55%) and the model only taken into account the most informative feature has the highest (12.5%).

When the model includes features one by one (by incremental importance), the EER increase constantly until including 8 features, after that the EER increase but not improving the accuracy of the model taking into account four or fewer features (except the model taking into account one feature).

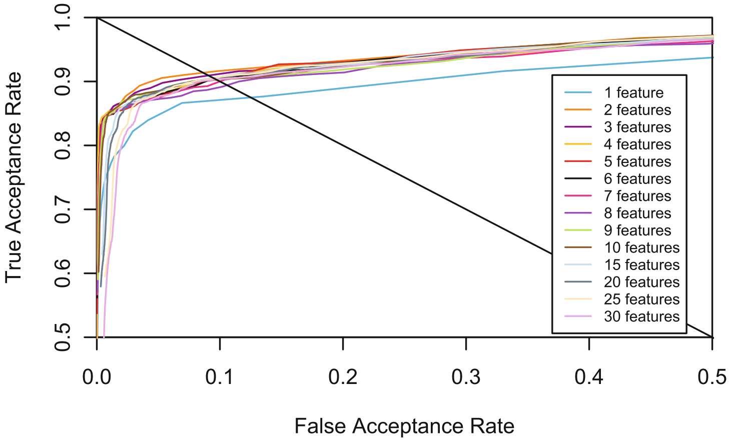

Fig. 5. ROC curves of Gaussian models taking into account different groups of features by importance.

7 Conclusion

In this paper, we proposed two unsupervised ML approaches to model card payments transactions and detect fraudulent activity. The approaches are based on a deep learning technique i.e. an autoencoder and in an ML technique i.e. a Gaussian model. Both systems improve the detection accuracy over a previously proposed approach based on a One-class SVM which was the model with the highest accuracy in the literature and tested on real-world data.

We also have shown that in this case, deep learning feature extraction does not help to improve the accuracy of the Gaussian model. However, taking into account only the two most important attributes selected by a tree model, EER of the Gaussian model improves from 9.7% to 8.5% ERR.

References

1. Aleskerov, E., et al.: 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, pp. 220–226 (1997)

2. Bansal, M.: Credit card fraud detection using self organised map. Int. J. Inf. Comput. Technol. **4**, 1343–1348 (2014)
3. Bekirev, A.S., Klimov, V.V., Kuzin, M.V., Shchukin, B.A.: Payment card fraud detection using neural network committee and clustering. Opt. Mem. Neural Netw. **24**(3), 193–200 (2015). https://doi.org/10.3103/S1060992X15030030
4. Benson Edwin Raj, S., et al.: Analysis on credit card fraud detection methods. In: 2011 International Conference on Computer, Communication and Electrical Technology, pp. 152–156, March 2011
5. Bhattacharyya, S., Jha, S., Tharakunnel, K., Westland, J.C.: Data mining for credit card fraud: a comparative study. Decis. Support Syst. **50**(3), 602–613 (2011). https://doi.org/10.1016/j.dss.2010.08.008, http://www.sciencedirect.com/science/article/pii/S0167923610001326, on quantitative methods for detection of financial fraud
6. Bhusari, V., Patil, S.: Application of hidden Markov model in credit card fraud detection. Int. J. Distrib. Parallel Syst. **2**, 203 (2011)
7. Brause, R., et al.: Neural data mining for credit card fraud detection. In: Proceedings 11th International Conference on Tools with Artificial Intelligence, pp. 103–106 (1999)
8. Capgemini; BNP Paribas: World payments report 2017. Technical report (2017)
9. Centeno, M.P., et al.: Smartphone continuous authentication using deep learning autoencoders. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST), pp. 147–1478, August 2017. https://doi.org/10.1109/PST.2017.00026
10. Centeno, M.P., et al.: Mobile based continuous authentication using deep features. In: Proceedings of the 2nd International Workshop on Embedded and Mobile Deep Learning, EMDL 2018, pp. 19–24 (2018)
11. Deng, L., et al.: New types of deep neural network learning for speech recognition and related applications: an overview. In: 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 8599–8603, May 2013
12. Dong, C., Loy, C.C., He, K., Tang, X.: Learning a deep convolutional network for image super-resolution. In: Fleet, D., Pajdla, T., Schiele, B., Tuytelaars, T. (eds.) ECCV 2014. LNCS, vol. 8692, pp. 184–199. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10593-2_13
13. European Central Bank: Fifth report on card fraud. Technical report (2018)
14. Fu, K., Cheng, D., Tu, Y., Zhang, L.: Credit card fraud detection using convolutional neural networks. In: Hirose, A., Ozawa, S., Doya, K., Ikeda, K., Lee, M., Liu, D. (eds.) ICONIP 2016. LNCS, vol. 9949, pp. 483–490. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46675-0_53
15. Gadi, M.F.A., Wang, X., do Lago, A.P.: Credit card fraud detection with artificial immune system. In: Bentley, P.J., Lee, D., Jung, S. (eds.) ICARIS 2008. LNCS, vol. 5132, pp. 119–131. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85072-4_11
16. Ghosh, S., Reilly, D.L.: Credit card fraud detection with a neural-network. In: 1994 Proceedings of Twenty-Seventh Hawaii International Conference on System Science, pp. 621–630 (1994). https://doi.org/10.1109/HICSS.1994.323314
17. Hejazi, M., et al.: One-class support vector machines approach to anomaly detection. Appl. Artif. Intell. **27**, 351–366 (2013)
18. Hinton, G., et al.: Deep neural networks for acoustic modeling in speech recognition: the shared views of four research groups. IEEE Sig. Process. Mag. **6**, 82–97 (2012)

19. Iyer, D., et al.: Credit card fraud detection using Hidden Markov Model. In: 2011 World Congress on Information and Communication Technologies, pp. 1062–1066, December 2011
20. Jurgovsky, J., et al.: Sequence classification for credit-card fraud detection. Exp. Syst. Appl. **100**, 234–245 (2018). https://doi.org/10.1016/j.eswa.2018.01.037
21. Karlik, B., Olgac, A.: Performance analysis of various activation functions in generalized MLP architectures of neural networks. Int. J. Artif. Intell. Exp. Syst. (IJAE) **1**(4), 111–122 (2010)
22. KhanT, A., et al.: Credit card fraud detection using hidden Markov model **2**, 1062–1066 (2011)
23. Louppe, G.: Understanding random forests: from theory to practice. Ph.D. thesis, October 2014
24. Maes, S., Tuyls, K., Vanschoenwinkel, B., Manderick, B.: Credit card fraud detection using Bayesian and neural networks. In: Maciunas, R.J. (ed.) Interactive Image-Guided Neurosurgery. American Association Neurological Surgeons, pp. 261–270 (1993)
25. Pozzolo, A.D., Caelen, O., Johnson, R.A., Bontempi, G.: Calibrating probability with undersampling for unbalanced classification. In: Proceedings of - 2015 IEEE Symposium Series on Computational Intelligence, SSCI 2015, pp. 159–166 (2015). https://doi.org/10.1109/SSCI.2015.33
26. Quah, J.T., et al.: Real-time credit card fraud detection using computational intelligence. Exp. Syst. Appl. **35**(4), 1721–1732 (2008)
27. Ryman-Tubb, N.F., Krause, P., Garn, W.: How artificial intelligence and machine learning research impacts payment card fraud detection: a survey and industry benchmark. Eng. Appl. Artif. Intell. **76**, 130–157 (2018). https://doi.org/10.1016/j.engappai.2018.07.008, http://www.sciencedirect.com/science/article/pii/S0952197618301520
28. Sahin, Y., Duman, E.: Detecting credit card fraud by decision trees and support vector machines. In: International Multi Conference of Engineers and Computer Scientists, IMECS 2011, vol. 1, pp. 442–447, March 2011
29. Socher, R., et al.: Convolutional-recursive deep learning for 3D object classification. In: Proceedings of the 25th International Conference on Neural Information Processing Systems, NIPS 2012, vol. 1, pp. 656–664 (2012)
30. Srivastava, A., et al.: Credit card fraud detection using hidden Markov model. IEEE Trans. Dependable Secure Comput. **5**, 37–38 (2008)
31. Tech, V.M.: Fraud detection in credit card by clustering approach. Int. J. Comput. Appl. **98**(3), 975–8887 (2014)
32. Bryan, T., et al.: Card-Not-Present Fraud around the World. U.S. Payments Forum 1, March 2017. https://www.uspaymentsforum.org/wp-content/uploads/2017/03/CNP-Fraud-Around-the-World-WP-FINAL-Mar-2017.pdf
33. Ush, A., Khan, S., Akhtar, N., Qureshi, M.N.: Real-time credit-card fraud detection using artificial neural network tuned by simulated annealing algorithm
34. Vatsa, V., Sural, S., Majumdar, A.K.: A game-theoretic approach to credit card fraud detection. In: Jajodia, S., Mazumdar, C. (eds.) ICISS 2005. LNCS, vol. 3803, pp. 263–276. Springer, Heidelberg (2005). https://doi.org/10.1007/11593980_20
35. Vincent, P., et al.: Extracting and composing robust features with denoising autoencoders. In: Proceedings of the 25th International Conference on Machine Learning, ICML 2008, pp. 1096–1103 (2008). https://doi.org/10.1145/1390156.1390294

36. Wang, S.: A comprehensive survey of data mining-based accounting-fraud detection research. In: 2010 International Conference on Intelligent Computation Technology and Automation, vol. 1, pp. 50–53, May 2010. https://doi.org/10.1109/ICICTA.2010.831
37. Whitrow, C., Hand, D.J., Juszczak, P., Weston, D., Adams, N.M.: Transaction aggregation as a strategy for credit card fraud detection. Data Min. Knowl. Discov. **18**(1), 30–55 (2009). https://doi.org/10.1007/s10618-008-0116-z
38. WorldPay: The art and science of global payments a definitive report from Worldpay Global Payments Report, November 2018
39. Yaginuma, Y., et al.: Multi-sensor fusion model for constructing internal representation using autoencoder neural networks. In: Proceedings of International Conference on Neural Networks (ICNN 1996), vol. 3, pp. 1646–1651, June 1996