Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks

Article · January 2021

DOI: 10.12720/jait.12.2.113-118

3 authors:

Ibtissam Benchaji
Mohammed V University of Rabat
7 PUBLICATIONS **40** CITATIONS
SEE PROFILE

Samira Douzi
La Faculté de Médecine et de Pharmacie de Rabat
21 PUBLICATIONS **87** CITATIONS
SEE PROFILE

Bouabid Ouahidi
Mohammed V University of Rabat
57 PUBLICATIONS **312** CITATIONS
SEE PROFILE

Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks

Ibtissam Benchaji, Samira Douzi, and Bouabid El Ouahidi
Faculty of Sciences IPSS, University Mohammed V, Rabat, Morocco
Email: ibtissam_benchaji@um5.ac.ma, {samiradouzi8, Bouabid.ouahidi}@gmail.com

***Abstract*—With the increasing use of credit cards in electronic payments, financial institutions and service providers are vulnerable to fraud, costing huge losses every year. The design and the implementation of efficient fraud detection system is essential to reduce such losses. However, machine learning techniques used to detect automatically card fraud do not consider fraud sequences or behavior changes which may lead to false alarms. In this paper, we develop a credit card fraud detection system that employs Long Short-Term Memory (LSTM) networks as a sequence learner to include transaction sequences. The proposed approach aims to capture the historic purchase behavior of credit card holders with the goal of improving fraud detection accuracy on new incoming transactions. Experiments show that our proposed model gives strong results and its accuracy is quite high.**

***Index Terms*—credit card, fraud detection, sequence learning, recurrent neural networks, LSTM**

I. Introduction

In recent years, credit card transactions have been set as the most popular payment mode thanks to the improvement of technology and the emergence of new e-service payment solutions, such as e-commerce and mobile payments. However, credit card fraud has also increased with the advent of these new technologies.

The security of card payments and the trust of consumers in making card payments is a matter of concern for any bank in the world. According to the statistics published by the Nilson Report site in 2017 [1], the financial losses caused by credit card fraud were amounted to $24.71 billion in 2016 and $27.69 billion in 2017. It is also reported that the actual amount of losses will increase by 2020.

Despite developing advanced technologies to prevent fraud, such as the use of chip and pin verification, 3-D Secure for online transactions and security questions for internet banking, traditional machine learning models used to automate detection of fraud are inadequate, as they fail to predict whether a transaction is fraudulent or not for the following raisons:

- Fraudsters invent new fraud patterns and continuously change their strategies to avoid being detected.
- Machine learning models that are never updated are inadequate as they do not adapt to new fraud strategies.
- Static machine learning models do not take account of changes and trends in consumer spending behavior, for example during holiday seasons and geographical regions.

In these situations, the implementation of an accurate fraud detection system that adapts to new fraud behaviors and evolves continuously is of crucial importance for financial institutions in order to prevent fraud before it occurs, protect consumers' interests and reduce the damages caused by fraud [2], [3].

In this paper, we propose a new credit card fraud detection system based on Long Short-Term Memory (LSTM) networks to predict the fraudulent behavior of credit card transactions and deliver good fraud detection performance. We provide the experimental results to validate the effectiveness of our approach.

The structure of this work is as follows. Section II gives a general introduction to sequence classification. Section III presents a review of credit card fraud literature. In Section IV, the structure of our proposed method is described. Section V details the dataset used in this study and discusses the results obtained. Finally, the paper is concluded in Section VI and suggested ideas for future research.

II. Sequence Classification for Credit Card Fraud Detection

In credit card fraud detection, traditional fraud detection systems aim to identify transactions with a high probability of being fraud, based only on individual transaction information such as amount, time and transaction location. Such systems are inadequate, since they do not consider the consumer spending behavior, which is useful to discover relevant fraud patterns [4].

A fraud is not just a property of the transaction itself, but a property of both the transaction and the particular context in which it occurred i.e. the account and the merchant. Therefore, identical buying behaviors may at the same time represent either entirely legitimate behavior in the context of some customers or obvious anomalies in the context of others [5].

To construct such a context that defines consumers' profile, it is very important to summarize the history of

Manuscript received August 1, 2020; revised February 8, 2021.

doi: 10.12720/jait.12.2.113-118

consumer spending patterns, in order to capture the sequential dependency between consecutive credit card transactions. The objective is to allow a classifier to better detect very dissimilar transactions within the purchases of a consumer.

Therefore, in the following section, we construct such a context by using the sequence learner LSTM recurrent neural networks as a dynamic pattern recognition classifier to model long term dependencies within transaction sequences.

III. Literature Review

Credit card fraud detection is a challenging problem that attracts the attention of machine learning and artificial intelligence communities for several reasons. For instance, credit card fraud data sets are highly imbalanced since the number of fraudulent transactions is much lower than the legitimate ones. Thus, many of traditional classifiers fail to detect minority class objects for these skewed data sets [4], [6], [7]. On the other hand, credit card fraud detection system has to respond in very short times to become useful in real scenarios. Another critical aspect is the data conditional distribution that evolves over time because of seasonality and new attack strategies [8].

Therefore, many modern techniques based on supervised learning, unsupervised learning, anomaly detection and ensemble learning have been devoted to payment card fraud detection [9]. In particular, supervised classification techniques demonstrated to be extremely effective for facing this challenge, where pre-classified datasets containing labeled historical transactions are used for training a classifier that builds a detection model capable to predict whether a new transaction is fraudulent or genuine. Some of these algorithms are support vector machines [10], [11], hidden Markov models [11], [12], logistic regression algorithms [10], [13], decision trees [14], [15], random forests [10], [16]-[19], and k-nearest neighbors [20], [21].

Unsupervised classification methods are used to detect unusual behavior of a system and to identify transactions that do not conform to the model as potential fraudulent cases [22]-[24]. It can help to detect some new patterns of fraud that have not been detected before.

However, most of these approaches handle each transaction as a single object and neglect the relationship between them. This sequential information between transactions may have major impact on the outcome of credit card fraud detection model.

Recently, deep learning methods based on Recurrent Neural Networks (RNN) have been used in fraud detection field given their reputation as one of the most accurate learning algorithms in sequence analysis work [25]-[27]. RNN is a dynamic machine learning approach capable of analyzing the dynamic temporal behaviors of various bank accounts by modeling the sequential dependency between consecutive transactions of credit card holders.

In this paper, we propose a novel sequence learner for credit card fraud detection by using LSTM recurrent neural networks to model long term dependencies within transaction sequences.

IV. Proposed Model

In this section, we describe our proposed model based on LSTM architecture for credit card fraud detection. The steps of this model are detailed below.

A. Data Preparation

The values and types of the dataset's features that will ultimately be used as input to neural networks are different. Such differences can vary widely, affecting the performance of the classifier. Data normalization is then done by fine-tuning the input features to align the entire probability distribution of values. In addition, all categorical features must be converted to numerical values in order to use neural networks and other classifier algorithms that deal only with numerical data. Thus, each input data is normalized to the range values [0, 1]. We choose the Min-Max normalization technique because it reduces noise effects and ensures that neural networks efficiently update parameters and accelerate network training [28]. We use the following formula (1):

$$x(t)^{'} = \left(\frac{x(t) - x(t)_{\min}}{x(t)_{\max} - x(t)_{\min}} \right) \quad (1)$$

where $x(t)^{'}$ is the normalized value of $x(t)$ and $x(t)_{\max}$ and $x(t)_{\min}$ are the maximum and minimum values of the whole sequence respectively.

The neural network is trained by using the historical credit card data that includes details about the card holder's purchases. Using these data, the neural network compares the transaction information with the previously stored information. If the data fits the pattern, then the card is definitely used by its owner. If there is no match, the probability of fraud is then high.

In order to group the observations and transform them into sequences that are appropriate for network presentation and classification, we follow the steps below:

- Group the transactions by account and count the number of transactions for each account.
- Split the accounts into different sets according to their transaction counts.
- Order the transactions by time for each account in each set.

Therefore, each transaction i at time t can be then extended into a sequential vector $X_i = \{x_{i1}, x_{i2}, x_{i3}, ..., x_{i(t-1)}, x_{it}\}$.

B. Long Short Term Memory Networks

Long Short-Term Memory (LSTM) is a special type of artificial Recurrent Neural Network (RNN) architecture used to model time series information in the field of deep learning (Fig. 1).

In contrast to standard feedforward neural networks, LSTM has feedback connections between hidden units that

are associated with discrete time steps, which allow long-term sequence dependencies to be learned and a transaction label to be predicted given the sequence of past transactions. LSTMs were developed to overcome the problem of vanishing and exploding gradient that can be observed during the training of traditional RNNs [29].

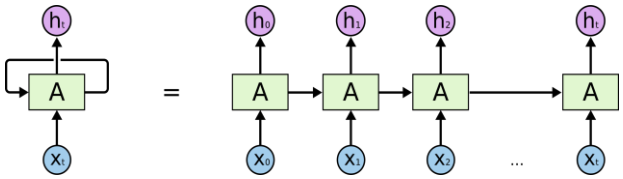


Figure 1. An unrolled recurrent neural network.

LSTM unit consists of a memory cell that stores information which is updated by three special gates: the input gate, the forget gate and the output gate. The cell remembers values over arbitrary time intervals and the three gates regulate the flow of information into and out of the cell. Fig. 2 depicts the LSTM unit structure.

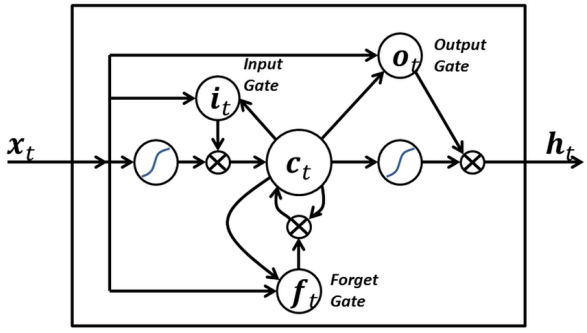


Figure 2. LSTM unit structure.

At time t, x_t is the input data of the LSTM cell, h_{t-1} is the output of the LSTM cell at the previous moment, c_t is the value of the memory cell, h_t is the output of the LSTM cell.

The LSTM unit calculation method can be divided into the steps below:

- The first step according to Eq. (2) is to calculate the candidate's memory cell value $\tilde{c}_t$, W_c is the weight matrix, b_c is the bias.

$$\tilde{c}_t = \tanh\left(W_c \cdot \left[h_{t-1}, x_t\right] + b_c\right) \tag{2}$$

- Calculate the value of the input gate i_t, the input gate controls the update of the current input data to the state value of the memory cell, σ is sigmoid function, W_i is the weight matrix, b_i is the bias. The equation for the input gate is given by (3):

$$i_t = \sigma\left(W_i \cdot \left[h_{t-1}, x_t\right] + b_i\right) \tag{3}$$

- Calculate the value of the forget gate f_t, the forget gate controls the update of the historical data to the state value of the memory cell, W_f is the weight matrix, b_f is the bias. The equation for the forget gate is given by (4):

$$f_t = \sigma\left(W_f \cdot \left[h_{t-1}, x_t\right] + b_f\right) \tag{4}$$

- Calculate the value of the current moment memory cell c_t, and c_{t-1} is the state value of the last LSTM unit. We use the following Eq. (5):

$$c_t = f_t * c_f + i_t * \tilde{c}_t \tag{5}$$

Here dot product is represented by "*".

The memory cell update depends on the state value of the last cell and the candidate cell and is controlled by the input gate and the forget gate.

- Calculate the value of the output gate o_t, the output gate controls the output of the memory cell's state value, W_o is the weight matrix, b_o is the bias. The equation for the output gate is given by (6):

$$o_t = \sigma\left(W_o \cdot \left[h_{t-1}, x_t\right] + b_o\right) \tag{6}$$

- Finally, calculate the output of LSTM unit h_t according to Eq. (7).

$$h_t = o_t * \tanh(c_t) \tag{7}$$

Benefit from three control gates and memory cell, LSTM can easily retain, read, reset and update information over long periods of time.

In this paper, we employed long short term memory networks to model the sequential dependency between consecutive transactions of credit card holders. The hidden state architecture of LSTM allows establishing connections between neural networks' nodes across time steps. Therefore, the model can retain information from past inputs, allowing it to identify temporal associations between events that may be dispersed in the input sequence. LSTM is an adequate model of succession patterns in sequential data points where the occurrence of one event may depend further back in time on the presence of several other events.

V. Experimental Results

This section describes the dataset and provides the evaluation metrics used in this work. The results of the experiments of the proposed method are then presented.

A. Dataset Description

Datasets provide a way to train and validate the efficacy of the proposed methods, hence playing an important role in motivating research. One of the challenges with studying credit card fraud detection systems is that it is considered highly confidential and not publicly disclosed [30], [31]. Researchers have therefore suggested using synthetic data that is modeled after a real data set to contain similar patterns. For this work, we use BankSim software, a simulation tool specifically designed to emulate fraud data

[32]. BankSim generated data is obtained from the Kaggle website.

BankSim uses a multi-agent-based simulation methodology based on a sample of aggregated real transaction data that a bank in Spain offers. The original bank data is made up of thousands of transactional data records from November 2012 to April 2013. BankSim uses multiple agents of three different categories to mimic this original bank data: traders, customers, and fraudsters. These agents communicate with each other over a sequence of simulated days, resulting in a purchase transaction log closely resembling the original bank data.

The data set used in these experiments contains details of 594,643 different transactions across a six-month time period. There is a significant class imbalance problem associated with our dataset. Only 7,200 transactions (≈1,2%) are labeled as "Fraud", while the remaining 587,443 transactions are labeled as "Genuine". Fig. 3 illustrates the class distribution of the dataset used in our experiments.

The dataset used in this work contains transactions corresponding to card purchases made during 180 simulated days and consists of 594,643 different transactions, among which 7,200 (≈1,2%) are labeled as "Fraud", while the remaining 587,443 are labeled as "Genuine". Raw data provides information about transaction and account details. Each transaction message is represented as a feature vector composed of 10 features described in Table I.

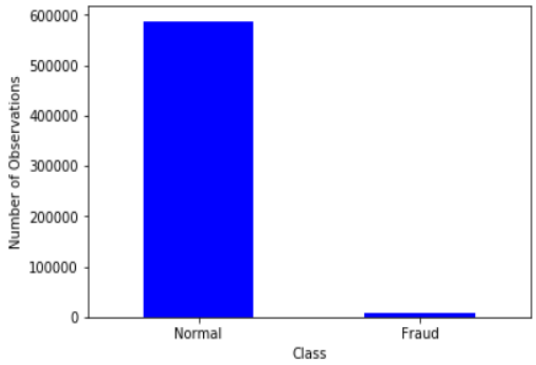


Figure 3. Class distribution of credit card DataSet.

TABLE I. FEATURE VECTORS DESCRIPTION

Name	Description
Step	The day the transaction took place from 1 to 180
Customer ID	A number identifying the customer account involved in the transaction
Age Category	A categorical value putting the customer into one of 8 different age groups
Gender	A categorical variable indicating the gender of the customer
Zip Code of account	The zip code associated with the customer
Merchant ID	A number identifying the merchant involved in the transaction
Zip Code of Merchant	The zip code of the merchant
Category purchase	A categorical variable indicating what type of good or service was purchased
Amount of purchase	The total amount that the transaction cost
Fraud status	A binary variable indicating if the transaction was fraudulent of not

B. Building the Model

We build a pattern recognition LSTM networks with 9 input neurons since each input feature present in our dataset will be represented by its input neuron. Feature 'Fraud status' is used as output neuron. One hidden layer with 15 neurons was used to analyze the structure of the networks. Table II presents the parameter values used in the proposed LSTM model.

TABLE II. LSTM TRAINING PARAMETERS

Parameters	LSTM values
Number of features	9
LSTM memory size	15
Epoch number	100
Learning rate	[0.1, 0.4]
Loss function	Cross Entropy
Optimiser	Adam Optimiser

This model is based on Keras deep learning framework. The implementation steps of the proposed model are detailed below:

- Reshape dataset into three-dimensional tensor (samples, number of timesteps, number of features).
- Define learning parameters (memory size, learning rate, batch size and epochs).
- Define LSTM cell.
- Set tensor variables for weight and bias vectors.
- Divide dataset into training, validation, and testing.
- Compute the output based on softmax activation function.
- Define cross entropy loss function.
- Add Adam optimization function to minimize the cross-entropy loss function.
- Repeat:
  Compute training error.
  Compute validation error.
  Update weights and biases using back propagation.
- Predict for testing dataset using trained LSTM.

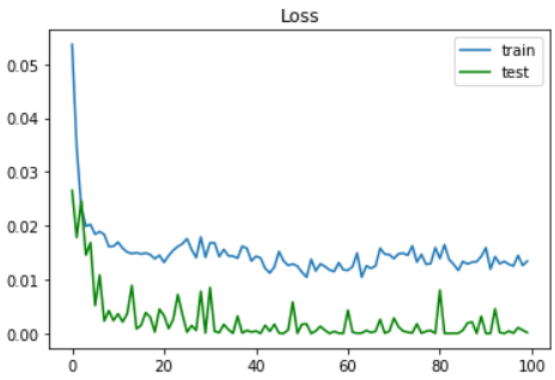


Figure 4. LSTM loss function.

The loss function used for the pattern recognition network is Cross-entropy. Fig. 4 shows the performance plot of train and validation data subsets. In our case the network is well trained since that the loss function decreases for both training and validating data.

C. Performance Metrics

In this study, we trained the feedforward networks with our dataset divided into three sets. The first subset 70% of data is the training set, the second subset 15% of data is the validation set and the last test subset 15% of data is used to test the network generalization.

To assess the performance of our model with more accuracy, we introduce the following evaluation metrics represented by Eqs. (8), (9) and (10):

- The Mean Square Error (MSE):

$$MSE = \frac{1}{N}\sum_{n=1}^{N}\left(y_n - y'_n\right)^2 \tag{8}$$

where y_n is the original value associated to the nth sample and y'_n is the value predicted.

- The Mean Absolute Error (MAE):

$$MAE = \frac{1}{N}\sum_{t=1}^{N}\left|y_t - y'_t\right| \tag{9}$$

- The Root Mean Square Error (RMSE):

$$RMSE = \sqrt{\frac{1}{N}\sum_{t=1}^{N}\left(y_t - y'_t\right)^2} \tag{10}$$

In the above formula, y_t represents the original value of the t moment, y'_t represents the predicted value of the t moment, and N is the total number of the test samples. If the value of MAE, RMSE, and MAPE is smaller, then the deviation between the predicted value and the original value is also smaller. Table III lists the results obtained for LSTM model over the last 10 epochs.

TABLE III. LIST OF 10 LAST EPOCHS RESULTS

Epoch	AUC	MSE	MAE
1	0.9953	0.0037	0.0067
2	0.9949	0.0042	0.0078
3	0.9956	0.0034	0.0063
4	0.9951	0.0039	0.0069
5	0.9955	0.0036	0.0066
6	0.9951	0.0038	0.0069
7	0.9953	0.0037	0.0067
8	0.9954	0.0036	0.0065
9	0.9951	0.0038	0.0069
10	0.9955	0.0035	0.0065

VI. CONCLUSION

In this study, we have proposed a sequence classifier based on the LSTM networks to catch the consumer behavior of individual cardholders when constructing a credit card fraud detection model. Future work will be dedicated to the study of other variants of RNN and compare their performances with our approach.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Ibtissam Benchaji conducted the research and wrote the paper, Samira Douzi and Bouabid El Ouahidi directed, guided, and provided suggestions for each stage of research. All authors had approved the final version.

REFERENCES

[1] The Nilson Report, Trade Publication on Consumer Payment Systems, issue 1118, October 2017.

[2] T. P. Bhatla, V. Prabhu, and A. Dua, "Understanding credit card frauds," *Cards Business Review*, pp. 1-15, June 2003.

[3] J. L. Liu, C. Chen, and H. Yang, "Efficient evolutionary data mining algorithms applied to the insurance fraud prediction," *International Journal of Machine Learning and Computing*, vol. 2, no. 3, pp. 308-313, June 2012.

[4] J. T. Quah and M. Sriganesh, "Real-Time credit card fraud detection using computational intelligence," *Expert Systems with Applications*, vol. 35, pp. 1721-1732, November 2008.

[5] J. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P. E. Portier, L. He-Guelton, and O. Caelen, "Sequence classification for credit-card fraud detection," *Expert Systems with Applications*, vol. 100, pp. 234-245, June 2018.

[6] M. Hlosta, R. Stríž, J. Kupčík, J. Zendulka, and T. Hruška, "Constrained classification of large imbalanced data by logistic regression and genetic algorithm," *International Journal of Machine Learning and Computing*, vol. 3, no. 2, pp. 214-218, April 2013.

[7] I. Benchaji, S. Douzi, and B. E. Ouahidi, "Novel learning strategy based on genetic programming for credit card fraud detection in big data," in *Proc. International Conference Big Data Analytics, Data Mining and Computational Intelligence*, July 2019, pp. 3-10.

[8] A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: A realistic modeling and a novel learning strategy," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3784-3797, August 2018.

[9] A. Abdallah, A. M. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90-113, June 2016.

[10] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602-613, February 2011.

[11] S. S. Dhok and G. R. Bamnote, "Credit card fraud detection using hidden Markov model," *International Journal of Advanced Research in Computer Science*, vol. 3, no. 3, pp. 816-820, 2012.

[12] A. Srivastava, A. Kundu, S. Sural, and S. Member, "Credit card fraud detection using hidden Markov model," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1, pp. 37-48, February 2008.

[13] A. D. Pozzolo, R. A. Johnson, O. Caelen, S. Waterschoot, N. V. Chawla, and G. Bontempi, "Using HDDT to avoid instances propagation in unbalanced and evolving data streams," in *Proc. International Joint Conference on Neural Networks*, July 2014, pp. 588-594.

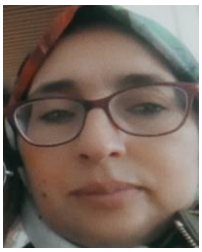
[14] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," arXiv: 1009.6119, 2010.

[15] Y. Sahin, S. Bulkan, and E. Duman, "A cost-sensitive decision tree approach for fraud detection," *Expert Systems with Applications*, vol. 40, no. 15, pp. 5916-5923, November 2013.

[16] A. D. Pozzolo, O. Caelen, Y. A. L. Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a

practitioner perspective," *Expert Systems with Applications*, vol. 41, no. 10, pp. 4915-4928, August 2014.
[17] A. C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature engineering strategies for credit card fraud detection," *Expert Systems with Applications*, vol. 51, no. 1, pp. 134-142, June 2016.
[18] A. C. Bahnsen, A. Stojanovic, and D. Aouada, "Cost sensitive credit card fraud detection using Bayes minimum risk," in *Proc. the 12th International Conference on Machine Learning and Applications*, December 2013, pp. 333-338.
[19] V. V. Vlasselaer, C. Bravo, O. Caelen, T. Eliassi-Rad, L. Akoglu, M. Snoeck, and B. Baesens, "APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions," *Decision Support Systems*, vol. 75, pp. 38-48, July 2015.
[20] V. R. Ganji and S. N. R. Mannem, "Credit card fraud detection using anti-k nearest neighbor algorithm," *International Journal on Computer Science and Engineering*, vol. 4, no. 6, pp. 1035-1039, June 2012.
[21] J. Pun and Y. Lawryshyn, "Improving credit card fraud detection using a meta-classification strategy," *International Journal of Computer Applications*, vol. 56, no. 10, pp. 41-46, October 2012.
[22] F. T. Liu, K. M. Ting, and Z. H. Zhou, "Isolation forest," in *Proc. the Eighth IEEE International Conference on Data Mining*, 2008, pp. 413-422.
[23] X. Zhao, J. Zhang, and X. Qin, "Loma: A local outlier mining algorithm based on attribute relevance analysis," *Expert Systems with Applications*, vol. 84, no. 30, pp. 272-280, October 2017.
[24] C. S. Hemalatha, V. Vaidehi, and R. Lakshmi, "Minimal infrequent pattern based approach for mining outliers in data streams," *Expert Systems with Applications*, vol. 42, no. 4, pp. 1998-2012, March 2015.
[25] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," *Nature*, vol. 323, no. 6088, pp. 533-536, 1986.
[26] J. L. Elman, "Finding structure in time," *Cognitive Science*, vol. 14, no. 2, pp. 179-211, June 1990.
[27] A. Graves and N. Jaitly, "Towards end-to-end speech recognition with recurrent neural networks," in *Proc. the 31st International Conference on Machine Learning*, June 2014, pp. 1764-1772.
[28] I. A. Basheer and M. Hajmeer, "Artificial neural networks: Fundamentals, computing, design, and application," *Journal of Microbiological Methods*, vol. 43, no. 1, pp. 3-31, December 2000.
[29] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735-1780, November 1997.
[30] A. D. Pozzolo, O. Caelen, Y. A. L. Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," *Expert Systems with Applications*, vol. 41, no. 10, pp. 4915-4928, August 2014.
[31] E. A. Lopez-Rojas and S. Axelsson, "A review of computer simulation for fraud detection research in financial datasets," in *Proc. Future Technologies Conference*, December 2016, pp. 932-935.
[32] G. Vaughan, "Efficient big data model selection with applications to fraud detection," *International Journal of Forecasting*, June 2018.

Ibtissam Benchaji received the engineer's degree from the National School of Applied Sciences of Tangier, Morocco in 2009. She is currently a predoctoral researcher at the Computer Science Department of the Faculty of Sciences Rabat Agdal at the University Mohammed V, Rabat, Morocco under the supervision of Prof. El Ouahidi Bouabid. Her current research interests include machine learning techniques for anomaly and fraud detection.



Samira Douzi received the master degree in development quality in 2013, from the Department of Computer Science at the Faculty of Sciences Rabat Agdal. Since 2016 she is a predoctoral researcher in the Department Computer Science at the Faculty of Sciences Rabat Agdal where she is pursuing a Ph.D. degree. Her main researches interests include big data, deep learning and cyber security.

Bouabid El Ouahidi is a university professor and ex head of the Computer Science Department. He received Ph.D. Degree in computer security from the University of Caen-France. His research interests include open distributed systems, quality of services of distributed applications, big data, cyber security and machine learning.