Adaptive Model for Credit Card Fraud Detection

https://doi.org/10.3991/ijim.v14i03.11763

Imane Sadgali (✉), Nawal Sael, Faouzia Benabbou
University Hassan II, Casablanca, Morocco
sadgali.imane@gmail.com

Abstract—While the flow of banking transactions is increasing, the risk of credit card fraud is becoming greater particularly with the technological revolution that we know, fraudulent are improve and always find new methods to deal with the preventive measures that financial systems set up. Several studies have proposed predictive models for credit card fraud detection based on different machine learning techniques. In this paper, we present an adaptive approach to credit card fraud detection that exploits the performance of the techniques that have given high level of accuracy and consider the type of transaction and the client's profile. Our proposition is a multi-level framework, which encompasses the banking security aspect, the customer profile and the profile of the transaction itself.

Keywords—Fraud Detection, Machine-Learning, Credit Card Fraud, customer profile, transaction profile.

1 Introduction

Customers all over the world, more inclined to abandon the use of cash, and opt for e-wallets or credit cards, this for security reasons, resource management and to enjoy the benefits of the online bank services. According to the interbank electronic banking center (CMI) [2], the electronic banking activity during the period of the last quarter of 2018 was characterized by a strong growth, compared to 2017, in the Payment activity (+26.6% in transaction number and +19.0% in amount of payment transactions). For this purpose, the banking institutions have implemented various techniques to prevent credit card frauds, but as we will see, they remain insufficient and limited [4].

Small businesses sometimes use manual transaction verification, through physical review of customer details and orders, or call back a customer to confirm transaction. However, it is a slow and expensive process, and can only be operational for a small number of transactions.

Other techniques are used to secure transaction with credit cards based on information included in the card, here below someone.

Credit card numbers that must be conform to Luhn's Algorithm. This acts as a checksum that facilitates the detection of single-digit errors or transposition errors. It

does not offer a real defense against credit card fraud but rather helps validate client-side data entry.

To prevent and stop Cyber Attacks. The online marketplace must ensure that their website compliance to industrial recognized security standard such as PCI. One common method is using SSL to encrypt sensitive data such as credit card and login details [24].

The Card Verification Code 2(CVC2) is used by most card systems. An additional three-digit code is printed on a tamper signature tape, and merchants who accept non-card transactions require this code for the transaction to be approved. CVC2 helps to prevent credit card fraud but it does not protect against fraud when the credit card has been physically compromised or stolen, or when the details have been copied.

The Address Verification Service is an electronic service used to prevent fraud without a card by checking the details of a customer's delivery address. This method does not protect against false fraudulent applications, the details contained in the files of the issuing bank.

The Virtual ATM, as proposed lastly [25], a new system is introduced that provides ATM service without traditional booths but two-layer authentications with a tiny OS independent device.

Another techniques used are the MasterCard Secure Code and Verified by VISA, which adds an additional verification factor for Internet purchases. These programs are effective at prevent only electronic card fraud and are only applied in optimal conditions.

This said, securing this form of payment, needs to perform intelligent data processing techniques to check the patterns and characteristics of suspicious and non-suspicious transactions in real time as possible. Machine learning techniques play a big role in this regard. Models that identify fraudulent transactions make the task easier for the financial institution, avoiding the loss of large sums of money. Recent studies, conducted on specific institutions or generic data, have shown that several machine-learning techniques have revealed a good rate of success in detecting fraudulent transactions [1]. Not all these techniques offer real-time analysis, but they improve the rate of false alarms. However, the client’s profile is rarely used.

The aim of this paper is to propose a hybrid model for credit card fraud detection, with three level of security and it is based on profile of customer and transaction. The proposition is adapted to real time transaction and to reduce the rate of false alarm.

The rest of this paper is organized as follows. The section 2 contains the state of art analysis. In section 3, the framework background is described. The section 4 detailed the proposed framework. Finally, we conclude and propose our future work in Section 5.

2 State of Art and Analysis

From our previous work [1], we have observed that, practically, almost all of techniques focus on online frauds, because it considered as the most critical and spreader one. The systems proposed use several machine-learning techniques, especially those

of artificial intelligences and combine them with optimization techniques such as aggregation. However, most of them give a result based on a particular dataset, which is itself characterized by unbalanced data.

The complex networks can be used to improve data mining models. They may be integrated as complementary tools, to improve the clustering rates obtained by classical data mining algorithms. In addition, the huge challenge in several works was the imbalanced dataset problem.

As result, we found that the One-Class Support Vector Machine (OCSVM) method outperform other techniques in all fields of comparison [3] with 96.6% as accuracy and low false alarm rate. The Results based on accuracy, reveal that, Self-Organization Map SOM Clustering helps in identifying new hidden patterns in input data, outperforms other techniques and works well in real time. The Outliner Detection (OD) and Fuzzy Logic FL models work fast and well on online large datasets, while Neural Network (NN) requires a high computing power for learning and functioning, which makes it not adapted to operate in real time. In addition, the Neuro-fuzzy inference system's (NFIS) training time increases as the number of samples increases but time taken for testing after the initial training is very less.

The main challenges identified for credit card fraud detection system are cited bellow:

- To detect frauds in a huge dataset where the legal transactions rate is more important than the fraudulent rate ones, which can be negligible.
- To minimize false alarms.
- To learn the behaviour of users and update it dynamically.
- To improve detection accuracy.

This system must be able to adapt to different transaction profiles, to improve it performances.

3 Framework Background

In this section, we present the fraud detection techniques related to our proposed framework.

3.1 Support Vector Machines (SVM)

SVM uses a linear model to implement nonlinear class boundaries by mapping input vectors nonlinearly into a high-dimensional feature space. In the new space, an optimal separating hyperplane is constructed. Bhattacharyya and al. evaluated SVM and Random Forests approaches [5], with the Logistic Regression. The results showed that, while sensitivity and accuracy decreased with lower proportions of fraud in the training data, precision showed an opposite trend.

Hejazi and al. [6] investigated two-class and one-class SVM for detection of fraudulent credit card transactions and shown the interest of one-class SVM (OCSVM) for the anomaly detection problem. Phuongand present a Real Time Data-Driven ap-

proaches [3] for Credit Card Fraud Detection using OCSVM with the optimal kernel parameter selection and shown that the proposed approach achieved a high-level of detection accuracy and a low false alarm rate.

From the result of our comparative study [23], we have done to confirm our state of art finding, and to help us in the choice of framework techniques, we found that SVM gives the best results in terms of accuracy and MSE and outperform DT, KNN and RF for fraud credit card detection.

3.2 Fuzzy Association Rules (FAR)

The Fuzzy Logic (FL) is used for representing the cognitive uncertainties, measuring the intensity of the truth-values for unquantifiable measures or probabilistic measures within the range of zero and one. In [7] the authors propose a novel methodology based on Fuzzy Association Rules (FAR) to detect credit card fraud. The applied methodology overcomes the difficulties of minimum support and confidence, optimizes the execution times, reduces the excessive generation of rules, and makes the results more intuitive, thereby facilitating the work of fraud analysts. In addition, Askari [8] proposed fraud detection algorithm based on Fuzzy-ID3.

3.3 Deep Learning (DL)

DL presents a promising solution to the problem of credit card fraud detection by enabling institutions to make optimal use of their historic customer data as well as real-time transaction [9]. In a comparative study between DL, LR and Gradient Boosted Tree [10], the authors found that deep learning has the largest value for the majority of the feature sets, such as: frequency of transaction, number of transactions, transaction amount, In [11] the authors evaluated different DL algorithms and showed that, the Long Short-term Memory (LSTM) and Gated Recurrent Units (GRUs) model significantly outperformed the baseline ANN. This indicates that order of transactions for an account contains useful information in differentiating between fraud and non-fraudulent transactions.

4 Hybrid Model Description

In this section, we describe the proposed architecture for the automatic detection of financial fraud. The proposed solution operates in the continuous learning approach to discover a new fraud pattern. Which focuses on the human factor considered as an essential element, and works in parallel with the usual controls of the financial system.

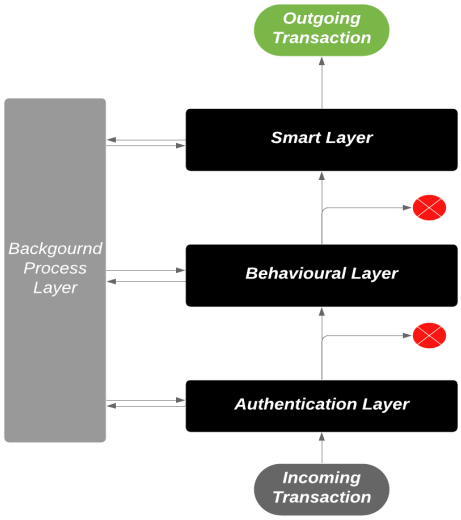

Fig. 1. Architecture of proposed solution

The fig.1, present the architecture of our proposed solution. We divide our model into four components; authentication layer, behavioral layer smart layer and background-processing layer. We choose each time to use a hybrid solution by using different algorithms with higher accuracy.

4.1 Authentication Layer (AL)

The authentication of the transaction, by passing the usual security level of the financial system. This filter is responsible of establishing the profile of the incoming transaction. We use also the feature engineer to identify the client profile. For example, if we have a client that had never made an international transaction, and start to use his credit card in a suspicious website or retrieving money from a country with a high degree of fraud, we have to give a score of risk with this parameters to take decision of considering the current transaction as fraudulent or not.

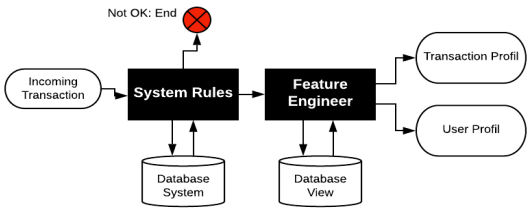

Fig. 2. Architecture of authentication layer

The fig.2, present the architecture of authentication layer. In this section, we will describe each bloc of this architecture.

Incoming Transaction. Any transaction coming from different channel: merchant application, terminal of payment electronic (TPE), automatic terminal machine (ATM)

System rules: This process contains all rules defined by the financial system, such as PIN verification, CVC2 for internet payment, address and expiry date, the initial authentication screen for cardholder. The system can also check black list for credit card depending on financial system strategy and Handle some plafond of card and account (number of transactions per day, total amount of transaction per day, maximum and minimum amount for each transaction).

Feature engineer: The creation of domain expertise functions participates significantly in the construction of predictive models of credit card fraud detection; since financial systems manage a huge flow of information about card accounts, customers and transactions [12]. However, not all of these data reveal important predictors such as consumer consumption patterns over time, or a client's travel abroad, etc. Many such predictors can be derived from all of the original data. This research identifies and creates some important and commonly used predictors.

For this study, the following predictors were created and added to the data:

- Inter-transaction time gap
- Number of transactions per: day, week, and month
- Frequency of transaction by type, including national or international
- Time range of purchases (Weekend, evening, holidays)

Each of these attributes to a weight according to their importance for prediction.

Transaction profile: Each incoming transaction will be ranked on two level of transaction: prioritized or normal one. As parameters for risk scoring, to classify the incoming transaction, we have the most important [1]: the transaction amount, transaction localization (if it's made in a country with a high degree of fraud), used channel (ATM, TPE, E-commerce) and the merchant type.

For this, we choose the risk estimate based on the logistic model [22]:

$$1 + e^{-\sum_{i=0}^{p} x_i \beta_i} \quad (1)$$

Where Xi is one of our chosen parameters, and βi is the weight of the Xi parameter, the value of βi will be defined by the financial system administrator. P is the number of used parameters.

If the result R of equation (1) exceeds a threshold defined by the financial system administrator, the incoming transaction is considered prioritized, else it is a normal transaction.

User profile: The feature engineer will allows as defining the user profile by known the habits of this client. Therefore, for each client we have the information of time range of purchases, frequency of transaction by type, number of transactions and the usual inter-transaction time gap. All of this information will be extracted from system database and stored in the duplicate database, to be used in second layer.

Not ok: End. If this layer goes to the Not ok, that mean the system rules found this transaction suspicious, we have to exit the framework of credit card fraud detection, insert transaction in our view database annotated as fraudulent one. The financial system can manage the fraud according to his policies.

Database system: Refer to the financial system database. In our framework, we will simply consult and update from this database and never insert in or update it.

Database view: Refer to our locale database; it is a duplicate of transaction data from database of system, with annotated transactions and additional predictors from feature engineer.

4.2 Behavioral Layer (BL)

In the second layer, we apply a feature selection and Fuzzy association rules (FAR). The fig.3; present the architecture of behavioral layer.

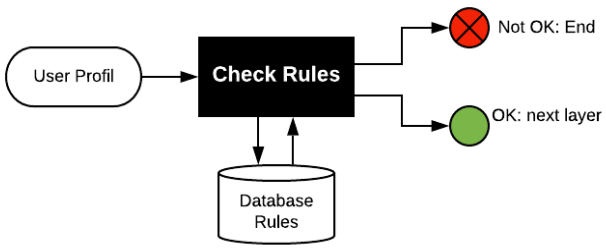

Fig. 3. Architecture of behavioral layer

Rules database: Refer to special database of extracted rules and update by the fourth component the batch training as described below. Check rules. This function has the ability to validate a transaction depending on user's profile of incoming transaction, basing on stored rules from BPL, if the transaction is suspected, we go to "Not ok: End" else, we continue to the SL.

On this layer, our main goal is to check if the user's profile is compatible with the behavior rules already stored in the rules database. For example, if the user has never been abroad and we receive a transaction from a distributor in another country, perhaps with an amount not expected. We will check the rules of our database and label this transaction as suspicious.

4.3 Smart Layer (SL)

In this component, we divide the transactions according to their profile and need, in two categories to classify them as fraudulent or genuine. The choice of these techniques was based on our latest a comparative study [1].

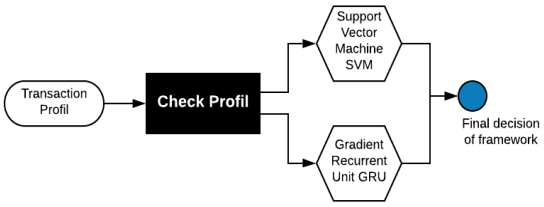

Fig. 4. Architecture of Smart layer

The fig.4, present the architecture of smart layer. We give a description of architecture bloc's in details.

Check transaction profile: As previously described, we divide transactions into two types: normal and priority. At this level, we decide the type of the current transaction and send it to the appropriate model:

Support Vector Machine (SVM): For all normal transaction (as defined in transaction profile predictor), we use SVM, which is most performant MLT for the anomaly detection problem [6][16][17][18], that achieves a high-level of detection accuracy and a low false alarm rate [1]. The choice was made to satisfy the transaction need in real time.

Gradient Recurrent Unit (GRU): If the transaction is prioritized, we will use another technique that can handle the sensitivity in this case, even if it perhaps consume more time. A gated recurrent unit makes each recurrent unit adaptively so allows capture dependencies of different time scales. GRU has gating units that modulate information flow into the unit, however, GRUs do not have separate memory cells [15], and significantly outperformed other machine learning techniques [10][11][19][20].

Final decision of framework. The process of ending the framework is responsible for inserting the transaction with the genuine annotation, in our duplicate database, and delivering the current transaction to the financial system, for continuing its normal processing.

4.4 Background Processing Layer (AL)

To maintain our solution updated a background processing is periodically done, to train the models and discover new rules of associations emerged from these models.

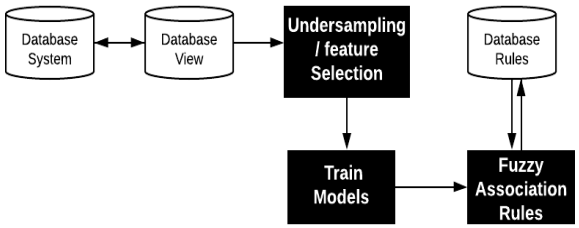

Fig. 5. Architecture of Background processing layer

The fig.5, present the architecture of background processing layer. This component will be responsible of:

Updating the database: View from the system database, to have the latest status of previous treated transactions.

Training our two models: Using our annotated database view.

Inserting new discovered rules: Emerged from the database view into rules database.

Under sampling: Over sampling and under sampling are two popular sampling techniques to address the problem or imbalanced data. A sub-sampling technique removes some occurrences from the majority class and an over-sampling method replicates additional subjects from the minority class. In our case, we choose the under-sampling method, which proved its performance for credit card fraud detection [14].

Feature selection: Is the process of selecting a subset of relevant features [13], from our duplicate database, depending on the type of transaction and the incoming channel. We use the most relevant predictors. In addition, the user's profile rules are stored in this database to analyze the behavior of this user and report any derivation of normal habits.

Fuzzy association rules (FAR): A large analysis of the state of the art in the techniques and methods used in fraud detection and prevention, and a review of various relevant publications over the last years confirms the effort employed to obtain useful knowledge from the transaction databases or repositories using different techniques and methodologies [1]. In the light of the results obtained, we have decided to use fuzzy logic-based data mining techniques in order to obtain non-explicit, useful information from large repositories. It overcomes the difficulties of minimum support and confidence, optimizes the execution times, reduces the excessive generation of rules, and helps make the results more intuitive, there by facilitating the work of fraud analysts, for a scoring risk. According to the profile of the user and the rules, we decide whether the transaction is non-fraudulent and if the framework can continue to the next [7] [8] [21].

5 Conclusion and Future Work

The present paper, proposes a conceptual framework, to detect credit card fraud. Compared to the classic model proposed in literature, this framework, makes a significant contribution by taking into account human behavior factors, and imbalanced data, and allow detecting unusual transactions that would have not been considered using traditional methods. The collected data are examined and used to train and maintain the model adaptive. Our framework uses different detection algorithms to improve accuracy and four-component design to handle data storage, making decision, analyze behavior and guaranty a good authentication filter.

Future work will have as its main objective the implementation and evaluation of the framework as a tool for credit card fraud detection.

6 References

[1] I. Sadgali, N. Sael, F. Benabbou (2018), "Detection of credit card fraud: State of art", International Journal of computer science and network security, Vol.18, No.11, pp.76-83.

[2] https://www.cmi.co.ma

[3] P.Hanh Tran, K.Phuc Tran, T. Thu Huong (2018), "Real Time Data-Driven Approaches for Credit Card Fraud Detection", Proceedings of International Conf.On E-Business and Applications, Da Nang, Vietnam, pp.6-9. https://doi.org/10.1145/3194188.3194196

[4] N. Wong, P. Ray, G. Stephens and L.Lewis (2012), "Artificial immune systems for the detection of credit card fraud: an architecture, prototype and preliminary results", Information Systems Journal, Vol.22, No.1, pp.53-76.https://doi.org/10.1111/j.1365-2575.2011.00369.x

[5] S. Bhattacharyya, S. Jha, K. Tharakunnel, J.C. Westland (2011), "Data mining for credit card fraud: A comparative study", Elsevier, Decision Support Systems, Vol.50, No.3, pp.602-613. https://doi.org/10.1016/j.dss.2010.08.008

[6] M. Hejazi (2013), "One-class support vector machines approach to anomaly detection", Applied Artificial Intelligence Journal, Vol.27, No.5, pp.351-366. https://doi.org/10.1080/08839514.2013.785791

[7] D. Sanchez, M.A. Vila, L. Cerda, J.M. Serrano (2009), "Association rules applied to credit card fraud detection", Elsevier, Expert Systems with Applications, Vol.36, No.2, Part.2, 2009, pp.3630-3640. https://doi.org/10.1016/j.eswa.2008.02.001

[8] S. Askari, A. Hussain (2017), "Credit Card Fraud Detection Using Fuzzy ID3", Proceedings of International Conf. On Computing, Communication and Automation (ICCCA), Greater Noida, India, pp.446-452. https://doi.org/10.1109/CCAA.2017.8229897

[9] Schmidhuber,Jürgen (2015), "Deep learning in neural networks: An overview". Neural networks, Vol.61, pp.85-117. https://doi.org/10.1016/j.neunet.2014.09.003

[10] G. Rushin, C. Stancil, M. Sun, S. Adams, P. Beling (2017), "Horse Race Analysis in Credit Card Fraud—Deep Learning, Logistic Regression, and Gradient Boosted Tree", Proceedings of International Conference Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, pp.117- 121. https://doi.org/10.1109/SIEDS.2017.7937700

[11] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, P. Beling (2018), "Deep Learning Detecting Fraud in Credit Card Transactions", Proceedings of International Conference Sys-

tems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, pp.129- 134. https://doi.org/10.1109/SIEDS.2018.8374722

[12] Barker, Katherine J., J. D'amato, P. Sheridon (2008), "Credit card fraud: awareness and prevention", Journal of Financial Crime, Vol.15, No.4, pp.398-410. https://doi.org/10.1108/13590790810907236

[13] M. Alshawabkeh, J.A.Aslam , J. Dy, D. Kaeli (2011), "Feature Selection Metric Using AUC Margin for Small Samples and Imbalanced Data Classification Problems", Proceedings of International Conference on Machine Learning and Applications (ICMLA), Honolulu, HI, USA, pp.145-150. https://doi.org/10.1109/ICMLA.2011.70

[14] R. Blagus, L. Lusa (2015), "Joint use of over- and under-sampling techniques and cross-validation for the development and assessment of prediction models", BMC Bioinformatics, Vol.16, No.1, pp.362-371. https://doi.org/10.1186/s12859-015-0784-9

[15] J. Chung, C. Gulcehre, K. Cho, Y. Bengio (2014), "Empirical evaluation of gated recurrent neural networks on sequence modeling". arXiv preprint arXiv:1412.3555.

[16] C. Whitrow, D. J. Hand, P. Juszczak.P, D. Weston, N. M. Adams (2009), "Transaction aggregation as a strategy for credit card fraud detection", Springer, Data Mining and Knowledge Discovery, Vol.18, No.1, pp.30-55. https://doi.org/10.1007/s10618-008-0116-z

[17] Y. Sahin, S. Bulkan, E. Duman (2013), "A cost-sensitive decision tree approach for fraud detection", Elsevier, Expert Systems with Applications, Vol.40, No.15, pp.5916-5924. https://doi.org/10.1016/j.eswa.2013.05.021

[18] L. Dhanabal,Dr. S. P. Shantharajah (2015), "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms", International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, No.6, pp.446-452.

[19] A. S. Davis, I. Arel (2016), "Faster Gated Recurrent Units via Conditional Computation", Proceedings of International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, pp.920-924. https://doi.org/10.1109/ICMLA.2016.0165

[20] Xu, Congyuan; Shen, Jizhong; Du, Xin; Zhang, Fan (2018), "An Intrusion Detection System Using a Deep Neural Network with Gated Recurrent Units", IEEEAccess, Vol. 6, pp.48697-48707. https://doi.org/10.1109/ACCESS.2018.2867564

[21] J. Shaji, D. Panchal (2017), "Improved Fraud Detection in eCommerce Transactions", Proceedings of International Conf.IEEE, Communication Systems, Computing and IT Applications (CSCITA), Mumbai, India, pp.121-126.https://doi.org/10.1109/CSCITA.2017.8066537

[22] L.M. Sullivan, J. M. Massaro and R, B, D'Agostino (2004), "TUTORIAL IN BIOSTATISTICS Presentation of multivariate data for clinical use: The Framingham Study risk score functions", Statistics in medicine, Vol.23, No.10, pp1631-1660. https://doi.org/10.1002/sim.1742

[23] I. Sadgali, N. Sael, F. Benabbou (2018), "Fraud detection in credit card transaction using machine learning techniques", Proceedings of International Conf. on Smart Systems and Data science 2019: ICSSD'19, Rabat, Morocco.https://doi.org/10.1145/3368756.3369082

[24] O. Ghazali, C. Yang Leow, S. Qaiser, N. Pattabiraman (2019), "Cloud-Based Global Online Marketplaces Review on Trust and Security", International Journal of Interactive Mobile Technologies (iJIM), Vol.13, No.4, pp 96-116.https://doi.org/10.3991/ijim.v13i04.10523

[25] S. Shahreen Sifat, A. Shihab Sabbir (2015), "Virtual ATM: A Low Cost Secured Alternative to Conventional Mobile Banking", International Journal of Interactive Mobile Technologies (iJIM), Vol.9, No.2, pp 44-49. https://doi.org/10.3991/ijim.v9i2.4314

7 Authors

Imane Sadgali received the engineer degree in software engineering from INPT, Morocco, in 2009, and worked for eight years for a payment system company. Currently, she is preparing her PhD in computer Science in faculty of Science Ben M'sik. Her research interests card fraud detection and prevention using machine learning. Email: sadgali.imane@gmail.com

Nawal Sael is a professor of Computer Science and member of Computer Science and Information Processing laboratory at faculty of science Ben M'sik (Casablanca, Morocco). She received her Ph.D. in Computer Science from the Faculty of Sciences, University Hassan II Casablanca, Morocco, 2013 and her engineer degree in software engineering from ENSIAS, Morocco, in 2002. Her research interest include data mining, educational data mining, machine learning and Internet of things. Email: saelnawal@hotmail.com

Faouzia Benabbou is a professor of Computer Science and member of Computer Science and Information Processing laboratory. She is Head of the team "Cloud Computing, Network and Systems Engineering (CCNSE)". She received his Ph.D. in Computer Science from the Faculty of Sciences, University Mohamed V, Morocco, 1997. His research areas include cloud Computing, data mining, machine learning, and Natural Language Processing. She has published several scientific articles and book chapters in these areas. Email: Faouzia.benabbou@univh2c.ma

Article submitted 2019-09-24. Resubmitted 2019-11-15. Final acceptance 2019-11-17. Final version published as submitted by the authors.