IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 10, No. 3, September 2021, pp. 698~706
ISSN: 2252-8938, DOI: 10.11591/ijai.v10.i3.pp698-706

Human behavior scoring in credit card fraud detection

Imane Sadgali, Nawal Sael, Faouzia Benabbou
Laboratory of Modelling and Information Technology, Faculty of sciences Ben M'SIK, University Hassan II, Casablanca, Morocco

Article Info

Article history:

Received Dec 19, 2020
Revised May 6, 2021
Accepted May 21, 2021

Keywords:

Behavior score
Credit card fraud
Fraud detection
Rules extraction
Transaction scoring

ABSTRACT

Now days, the analysis of the behavior of cardholders is one of the important fields in electronic payment. This kind of analysis helps to extract behavioral and transaction profile patterns that can help financial systems to better protect their customers. In this paper, we propose an intelligent machine learning (ML) system for rules generation. It is based on a hybrid approach using rough set theory for feature selection, fuzzy logic and association rules for rules generation. A score function is defined and computed for each transaction based on the number of rules, that make this transaction suspicious. This score is kind of risk factor used to measure the level of awareness of the transaction and to improve a card fraud detection system in general. The behavior analysis level is a part of a whole financial fraud detection system where it is combined to intelligent classification to improve the fraud detection. In this work, we also propose an implementation of this system integrating the behavioral layer. The system results obtained are very convincing and the consumed time by our system, per transaction was 6 ms, which prove that our system is able to handle real time process.

Corresponding Author:

Imane Sadgali
Laboratory of Modelling and Information Technology, Faculty of sciences Ben M'SIK
University Hassan II
Casablanca, Morocco
Email: sadgali.imane@gmail.com

1. INTRODUCTION

In the virtual world, like that of banking transactions, knowing the user of a card, return to an authentication, a code or a phone number combined. However, each person has habits, preferences or even limits in his use of the credit card. For this, several researches are focused on the study of the behavior of the client or consumer to establish a known profile. In the field of fraud detection, the use of machine learning techniques (ML) is attractive for many reasons. First, they allow the discovery of patterns in large data streams, i.e. transactions arrive as a continuous stream and each transaction is defined by many variables. Second, fraudulent transactions are often correlated both in time and in space. For example, scammers usually attempt to commit fraud in the same store with cards within a short period of time. Third, machine-learning techniques can be used to detect and model existing fraudulent strategies and identify new strategies associated with cardholder behaviors.

In credit card fraud detection system (CCFD), it is important in the analysis of a transaction to compute its risk factor in order to know which kind of analysis to carry out, whether deep or light. In a previous work we proposed an architecture of a credit card fraud detection system and we proposed a multi-level strategy for transaction classification [1]. Notably, we proved the performance of the support vector machine (SVM) and bidirectional GRU (BiGRU) [2], [3] models at the classification level. Also the problems of unbalanced data were raised and dealt with in another work. The scope of this work of scoring

cardholder's behavior is not limited to an analysis of the customer profile, to give a score but also to evaluate the integration of the behavior layer in the whole process of credit card fraud detection system.

The rest of the paper is structured is being as; section 2 presents the different works of customer behavior. Section 3 details the background. Section 4 presents the approach. Section 5 provides a summary of the experiments and finding. Section 6, presents the framework implementation. Finally, we conclude in section 7.

2. RELATED WORKS

In this section, we will take a deep look on different works concerning our objective, which aim to generate rules using cardholder behavior to detect and prevent credit card fraud. Behera and Panigrahi presented [4], in 2015, a hybrid approach for credit card fraud detection, first the initial authentication, then behavior analyze by using fuzzy C-means clustering and at last the learning phase using neural network. They got 93.90% correctly classified transactions and 6.10% incorrectly one. In 2017, they proposed an improvement of their solution, a neuro-fuzzy expert system, divided into four components: authentication, pattern matching, fuzzy rules and neural network [5]. In 2017, Askari and Hussain proposed a fraud detection algorithm based on fuzzy logic and iterative dichotomiser 3 (ID3), test results showed that the detection rate achieved was 89% [6]. Kho and Vea investigated in credit card fraud detection based on transaction behavior [7], in 2017, there was a non-disclosure agreement (NDA) between the participating bank and the proponent of this work, that why we have just the results, the best accuracy was achieved by, classifier for evaluating the proposing method, random tree, with rate 94.32%. In 2019, Li and Xie proposed behavior-cluster based imbalanced classification method [8]; the main idea is to divide user behaviors into many group behaviors, remove behavior noise then hierarchical sampling. Moreover, results showed 98.50% accuracy rate. Sanchez *et al*. had proposed to use association rules to extract knowledge so that normal behavior patterns [9]. This technique as results overcomes the difficulties of minimum support and confidence, reduces the excessive generation of rules, optimizes the execution times, and helps make the results more intuitive, all of this make the work of fraud analysts easier.

In another context of switching bank services depending on customer behavior, Marvi and Ioannou proposed a survival analyze based on data collected from customers and using life tables [10], a hazard proportional model was built to determine the risk of churn behavior. In era of the smart grid, when Meng *et al*. proposed a learning model based on multiple linear regression to learn the consumption pattern of customers [11]. The results showed it big potential to help the utility companies in making marketing decisions and designing efficient pricing models, which benefit both the customers and the utility companies themselves. Roderguz *et al*. proposed a fuzzy ontology for semantic modelling and recognition of human behavior [12], and the main contribution was to help modeling and treating uncertain, vague, incomplete, or imprecise information. Leon *et al*. used learning and clustering of fuzzy cognitive maps to describe travelers' behavior and change trends in different abstraction levels [13], the results of this work help transportation policy decision makers in better understanding of people's needs. Dai and al. developed a new algorithm, in 2020, combined association rules and multivalued discrete features, association rules (AR) are used to calculate the jaccard distance (ARJD). Then, based on the K-mode clustering algorithm, a user behavior-clustering algorithm ARJDKM combining ARJD and this method is proposed [14]. This solution can solve the problem of improper processing of multi-valued discrete features and improve the accuracy of user's similarity calculation.

Bhukya and Sadanandam suggested a rough-set associative classification rules extraction process for the MapReduce framework to process big data [15]. The suggested solution has two levels, the generation of base item sets for the MapReduce base class label and rules generation for the rough set based classification. This proposed approach tested on the standard data set achieved 83.91% significant performance compared to naive-bayes 81.69% and C4.5 81.91%. Pan *et al*. presented an improved top down approach to efficiently mine all rare item sets and their association rules. This method uses paths in a directed graph to represent every item sets in the database, generates a pattern matrix, and stores each metavector and its corresponding support count in a hash table. It solves a serious problem of Rarity algorithm that its full combination tree is too large to store in the memory [16]. Bian *et al*. presented a novel method called NAR-Miner, to automatically extract negative association programming rules from large-scale systems. This method reduced the number of uninteresting rules and mitigated the rule explosion problem to a certain degree [17].

From Table 1, we conduct that the higher accuracy was achieved by the behavior-clustering technique. In addition, all these works used a particular or generated dataset none of these was standard. The fuzzy logic was the most applied technique and achieved a good result in different fields. In addition, in the context of intrusion detection the rough set theory improved the classification rate. In our context, we propose a hybrid model based on fuzzy logic and rough set to analyze cardholder behavior. Inspiring from

result of a rough-set and associative classification rules in [15], we aim to combine rough set, fuzzy and association rules, for behavior scoring of credit card transactions. Based on generated rules, our system for credit card fraud detection CCFD, will assign a score for transactions before classifying them as fraudulent or not.

Table 1. Synthetise of works

Paper	Technique	Dataset	Accuracy
[4]	Fuzzy Clustering & Neural Network	Generated	93.90%
[5]	Neuro-fuzzy expert system	Generated	-
[6]	Fuzzy- iterative dichotomiser 3 (ID3)	-	89.00%
[7]	Confidently	Particular bank	97.58%
[8]	behavior-cluster based imbalanced classification method	Financial institution and 18 UCI data sets	98.50%
[9]	Fuzzy Association rules	Retail companies	-
[10]	Life tables	European financial services data	-
[11]	Multiple linear regression	Particular bank	-
[12]	ontology + Fuzzification of the ontology + Fuzzy reasoning	http://www.duslab.de/cosdeo/	-
[13]	Fuzzy cognitive maps + PSO	Particular data	-
[14]	ARJDKM: association rules (AR) + Jaccard distance (ARJD). + K-mode clustering (KM)	Tencent advertising algorithm competition	-
[15]	a rough-set + associative classification rules	KDD-96 UC-Census dataset	83.91%
[16]	Rare Association Rules Mining	Particular data	-
[17]	NAR-Miner: Negative association rules	private data	-

3. BACKGROUND

In this section, we give a brief introduction of different proposed techniques in our approach for the credit card fraud detection based on cardholder's behavior. We emphasize, that our approach operates in the continuous learning approach to discover a new fraud pattern.

3.1. Credit card fraud detection system

This work is part of a project to build a credit card fraud detection system [1]. This system is structured in four levels: -authentication level: which executes all system controls and create a profile for the incoming transaction and he cardholder; -behavioral level: that computes the risk factor, which is the scope of this paper; -smart level: that classifies the transaction either with SVM or BiGRU models based on transaction risk. In addition to a transverse background processing level, to ensure the updating and guarantee the evolution of the system. In our previous work [2], [3] we have shown the efficiency of the proposed SVM and BGRU models for the classification of transactions. By analyzing behavior, we aim to improve the performance of our system by incorporating a co-behavioral layer integrating business expertise and the power of machine learning, which will first make it possible to assess the severity of transactions before their classification.

3.2. Association rules

By definition, association rules are defined on transaction sets. Given that it is more common to work with tuples rather than transactions in a database, various solutions have been proposed to this problem. When working with relational databases, it is usual is to consider each item to be a pair of (attribute, value) and each transaction to be a tuple in a table. An association rule, as introduced by Agrawal *et al*. [18], is said to be an ''implication" of the form A => C denoting the presence of item sets A and C in some of the T transactions, assuming that A, C $\subset$ I, A $\cap$ C =Ø; and A, C $\neq$ Ø. This is for a given an item set I, and a transaction set T, where each transaction is a subset of I. The usual measures proposed by Agrawal *et al*. for establishing an association rule's fitness and interest are:

- Confidence (X→Y) = P (X|Y) = Support (X∪Y) /Support (X)
- Support (X→Y) = Support (X∪Y) = P (X∪Y)
- Lift (X→Y) = Confidence / expected confidence = Confidence (X→Y)/ Support (X)

3.3. Fuzzy logic

In 1965, Zadeh invented the fuzzy logic [19], for representing the cognitive uncertainties, measuring the intensity of the truth-values for unquantifiable measures or probabilistic measures within the range of 0 and 1. Let D be the collection of examples or instances or objects represented in set theoretic notion as $\{e_1, e_2 ..... e_n\}$, where the D is called the universe of discourse and the e_i is the individual example or object (element) of D. A fuzzy set A in the universe of D is described by a membership function $\mu_A(e)$: D $\rightarrow$ [0, 1], which quantifies the intensity or grade of membership of the element in the fuzzy set A. The membership

crisp value $\mu_A(e) = 1$ means that e is 100% a member of A and $\mu_A(e) = 0$ means that e is 100% not a member of A, and in case of fuzzy logic $0 \leq \mu_A(e) \leq 1$ which means that e is partially member of A. Hence, as the membership values goes closer to 1, the intensity of membership of e in A becomes stronger.

3.4. Rough set theory

Rough set theory is a new mathematical approach to imperfect knowledge, proposed by Pawlak [20], [21] presents yet another attempt at this problem. Rough assemblies have been proposed for a very wide variety of applications. In particular, the rough set approach appears to be important for artificial intelligence and cognitive science, especially in machine learning, knowledge discovery, data mining, expert systems, rough reasoning, and pattern recognition. The concept of rough set can be defined by means of topological, interior, and closing operations, called approximations.

Let X be a subset of U, i.e. X ⊆ U. Our goal is to characterize the set X with respect to R. To do this, we need some additional notation and some basic concepts of rough set theory, which presented below. By R(x), we denote the equivalence class of R determined by the element x. The indistinguishable relation R describes-in a sense-our ignorance of the universe U. The equivalence classes of the relation R, called granules, represent an elementary portion of knowledge that we are able to perceive thanks to R. In using only, the indistinguishable relation, in general, we are not able to observe individual objects from U but only the accessible granules of knowledge described by this relation. The definitions of set approximations presented above can be expressed in terms of granules of knowledge is being as. The lower approximation of a set is the union of all the granules that are fully included in the set; the upper approximation-is the union of all the granules which have a non-empty intersection with the set; the limit region of a set is the difference between the upper and lower approximation of the set [22].

4. PROPOSED APPROACH

In this paper, our main goal to propose an approach for behavior scoring for credit card fraud detection. The principle of scoring is to propose an evaluation of the risk of the transaction. Through our state of art [23], we noticed that fuzzy association rules are more suitable for the behavior layer than other techniques. That was confirmed in our pervious study and argute our choice [24]. The use of rough set theory model with fuzzy association rules technique will be a plus, since in other contexts it improves detection rate [15].

4.1. Processing flow

Figure 1 describes the follow of the processing for the rule's generation. First, we use feature engineer to complete the cardholder profile information, like the frequency of purchase the timing, and the merchant type. Second, we apply a feature selection with rough set theory, to select the best and more significant feature for rules generation.

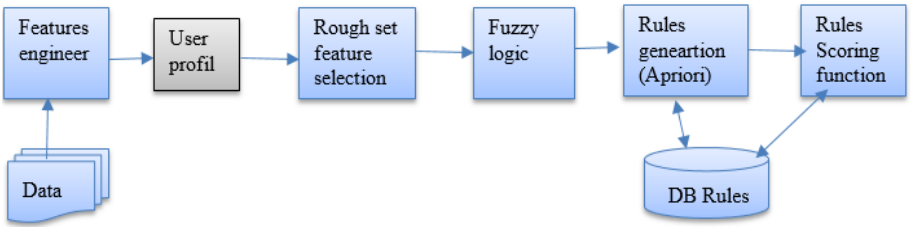

Figure 1. Approach processing flow

Then, we applied fuzzy logic to have a fuzzification of our chosen dataset. After this, we used association rules algorithm to generate rules and store them in rules database. For this purpose, we choose Apriori algorithm. The last component, it is a rules scoring function, which is described above, in the next paragraph.

4.2. Behaviour scoring

To ensure a good behavior scoring we analyze the user profile. The feature engineer will define the client profile through his card transaction habits. Therefore, for each client we have the information of frequency of transaction by type, time range of purchases, number of transactions and the usual inter-

transaction time gap. All of this information will be extracted from system database and stored in a duplicate database, to be used in our behavior analysis. The 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 an automatic terminal machine (ATM) in foreign country, perhaps with an amount not expected. We will check the rules of our database and label this transaction as suspicious. We, note that the stored rules concerns the suspicious transaction behave. For each incoming transaction, we will check all stored rules, and a counter incremented for every respected rule, that mean suspected transaction, so the expression of score is:

Score=number of rules respected/number of all rules

If the score is equal 0, that mean the risk of the transaction behavior is null, but if the score is reaches 1, that mean this transaction behave have a high risk to be fraudulent.

5. EXPERIMENTS

5.1. Dataset

This study is based on a generated dataset, composed of 60.000 transactions across 12 attributes, as decribed in Table 2. The attributes include transaction and cardholder information. Table 3 shows the distribution of legitimate and fraudulent transactions of our chosen dataset of kaggle. To construct this dataset, we try to have a randomly 200 transactions with two transactions status, genius and fraudulent, and data susceptible to be fraudulent transactions. The rest of dataset was generated with only the legitimate status.

Table 2. Dataset description

Features	Description
Transaction amount.	the amount of transaction adjusted in bank currency.
Transaction type.	National, international or e-commerce.
Transaction date and time.	Date and time of transaction in YYMMDDHHMMSS format.
Transaction channel.	The channel of incoming transaction (Terminal of electronic payment or point of sale (POS), automatic terminal machine (ATM), e-commerce or merchant application)).
Billing address	Address of billing for the customer and Shipping address: address of merchant or point of service for the purchase, address of ATM for withdrawal.
Merchant type.	hotels, transport, food, healthcare.
Inter transaction gap time.	Time between the current transaction and the last one.
Number of transaction per day.	The average number of transactions done by the cardholder in one day.
Number of transactions per week.	The average number of transactions done by the cardholder in one week.
Number of transactions per month.	The average number of transactions done by the cardholder in one month.
Frequency of transaction type.	The average frequency of transaction type done by the cardholder.

Table 3. Transaction distribution

	Number of transactions	Percentage of transactions
Genuine	59832	99.72%
Fraudulent	168	0.28%

5.2. Method

First, we will pre-process our dataset to be able to generate the association rules, we will start with the selection of the attributes, with rough set theory, that will help define the client's profile and emerge the mining rules. Then, a data fuzzification step is done, to make place for the Apriori algorithm to generate the rules. The chosen features for this study, which selected by rough, a set selector, are:

- Transaction channel: ATM, E-commerce, POS.
- Transaction type: National, International, E-commerce.
- Time range purchase: weekend, evening, holiday, other.

For the fuzzification, we will have a dataset with eight variables instead of only three; therefore, the value will be 0 or 1: automatic teller machine (ATM), point of sale (POS), electronic commerce (E-commerce), national, international, weekend, evening and holiday. Thus, our dataset is built and ready to be used, for the generation of association rules with Apriori, and stored in rules dataset. For each incoming transaction, the behaviour scoring have the responsibility to check stored rules, and return a behaviour score. We remind that the background processing, using database view, which generates these rules. A counter incremented for every missed rule, so the expression of score is:

Score=number of rules not respected/number of all rules

If the score is equal 0, that mean the risk of the transaction behave is null, but if the score is equal 1 or approaching 1, that mean this transaction behave have a high risk to be fraudulent. After calculating the behaviour score, the transaction goes to a prediction function to decide if it considered as fraudulent or genuine one.

5.3. Results

In this part we will present, the finding of the proposed approach. We consider transaction from our dataset, the feature selection was done in data preprocessing step, which is guaranteed by the background level, when we constructed the dataset, we will calculate the score and the risk for giving parameters, for simulation, and we will pass our transaction into classifying algorithm based on these rules. The rules will be generated as described before by the back-processing part. The Table 4 presents the results obtained by applying our selected approach, which is a hybrid solution that combined the three well-known methods; rough set, fuzzy logic and association rules and comparison with others approaches from baseline.

Table 4. Results of behavioral layer

Techniques	Number of generated rules	Detection rate
Apriori + rough set + Fuzzy	13	39%
Apriori + rough set	8	24%
Apriori	2	6%
Association rules	2	6%
FP-grouth	5	15%

The given results is about different implementation of association rules: efficient-apriori application programming interface (API); an efficient pure Python implementation of the Apriori algorithm, machine learning extensions (MLxtend) API which is a Python library of useful tools for the day-to-day data science tasks, and pyfpgrouth API; a Python implementation of the frequent pattern growth algorithm. As we can see, our approach outperforms other methods in number of generated rules, and the detection rate. We notify that the number of rules is not important and the low detection rate. This is due to the fact that the nature of the fraudulent transaction which are few compared to no fraudulent ones. The fraudulent transactions rules are rare and the fraud detection dataset are always unbalanced data problems. That is why the generated rules are not quite appropriate for the subset of the tests, but in a standard environment, this concern will be resolved because of the volume of the data and their resemblance.

6. CCFD FRAMEWORK IMPLEMENTATION

In this section, we propose a global evaluation of our CCFD by integrating the different levels and in particular the behavioural level as shown in Figure 2. Note that the proposed system is updated, and able to stand on real time world of credit card fraud detection. This is insured by a complementary background processing. This process discovers new rules of associations, emerged from new data when updating the database from the financial system database. In addition, it is responsible of pre-processing data before generation of rules (balancing data/feature selection), updating latest status of previous treated transactions. These entire tasks are periodically done. We can see that; this processing is a part of our approach for cardholder's behaviour analysis for credit card fraud detection. By analysing the user's profile rules stored in database to check the behaviour of this user and report any derivation of normal habits.

6.1. Dataset experiment process

In this experience, first the background process balances the data, split it for across validation and train our too models (SVM, BGRU), this layer also generates new rules and store them in the rules database. Secondly, the authentication layer constructs the transaction and cardholder profile for each transaction in the data set. Then, the behavior layer checks the rules for the cardholder and calculate a score based on stored rules. Finally, the smart layer calculates the risk given by the transaction profile and make the decision of which model to use. This decision is the sum of score behavior and transaction risk. This test was applied on a generated dataset, composed of 14924 transaction across 13 features. The lake of clear real data pushes us to use a generated dataset. Our previous work [2], [3] gives result on the well-known dataset of kaggle [25], but for behavior part, we have to get a clear data to analyze each cardholder profile.

6.2. Performance metric

For performance metrics, several commonly used classification performance measures based on the confusion matrix are employed in this paper to evaluate the performance of fraud detection architecture:

- Accuracy: (TP + TN)/ (TP + FP + TN + FN)
- Recall (or Sensitive/True positive rate): TP/ (TP + FN))
- Precision: TP/ (TP + FP)
- F1-score: 2 (Precision x Recall)/ (Precision + Recall)

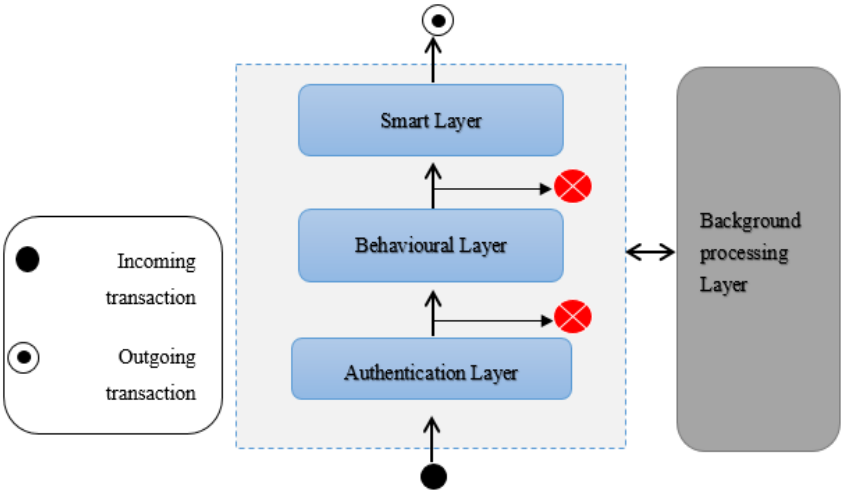

Figure 2. CCFD system architecture

6.3. Experiment results

For Simulation, we consider some rules as described below; P=3: the number of risk parameters;

- X_1: Transaction amount (1: high/ 0: low),
- X_2: Transaction country (1: zone 1/ 0: zone: 2),
- X_3: Transaction channel (1: type 1,0: type 2)
- High amount if > 10000, else it is low.
- Zone 1 countries in: Africa, South America. Zone 2, when not in zone 1.
- Transaction channel type 1: ATM, E-commerce, type 2 : POS, Merchant application.
- β_1 : - 0.10, β_2: - 0.20, β_3: - 0.30, Threshold = 1.7

The risk equation, as describe in our previous work [2], using the logistic model:

$$R = 1 + e^{-\Sigma_{i=0}^{p} X_i \beta_i} \quad (1)$$

To synthetize our finding, we display in Figure 3 (see in appendix) the number of transactions classified by BiGRU or SVM, the consumed time for whole transaction treatment, and the performance metrics obtained by classification report function. By using transaction score, our system has classified 27.25% of transaction by SVM and 82.75% by BiGRU. The time consumed by the smart layer to treat 14924 transactions was 90.10s, as described in Table 5 of classification report, an average of 6ms per transaction, which is quite good. These results prove that our system respects the real-time processing, and the background processing in the fourth level of our CCFD system guarantees its adaptability. In addition, the system's performances are very promising; this on our generated dataset but the results obtained on our recent work [2] showed that, BiGRU deep neural network classifier had very promising results with an accuracy rate of 97.16%. Moreover, that on a standard dataset from Kaggle with real transactions is even better and the results exceed all those reported in previous works.

Table 5. Classification report

	Accuracy	Precision	Recall	F1-score
Genuine	80%	81%	100%	89%
Fraudulent		56%	2%	4%
Test of 14924 transactions took: 90.10s				
BGRU Counter		10857 transactions		
SVM Counter		4067 transactions		

7. CONCLUSION

Fraud analysis is of critical importance in the banking industry and the biggest challenge remains the cost of fraud, whether to analyze it, detect it or prevent it. Since transactions take place in realtime, require a process that consumes little time and is as efficient as the size and infrastructure of the financial institute that adapts it. In this paper, we presented our behavioral analysis to credit card fraud detection based on a hybrid methods using Apriori, rough set and fuzzy techniques that gave a prominsing results. The comparative study proved that our approach is the best combinaison to generate rules in a context where fraud remains low compared to legitimate transactions. We also proposed an implementation of the whole CCFD system and gave results of transaction classification based on the score given by behavior layer. Even if the classification results do not reach the results obtained with SVM and BiGRU in our last paper, we consider that the behavior layer can improve the financial fraud detection system, not only by generating rules but also we can benefit from human expertise to integrate a new rules in this layer. We also proved that our system is able to work in real time; the average time consumed per transaction was 6 ms, which is a very satisfying running time. In our future work, we will focus on the impact of the dataset quality on classification and improve the confidence of rules generated to improve the performance of the whole CCFD system.

APPENDIX

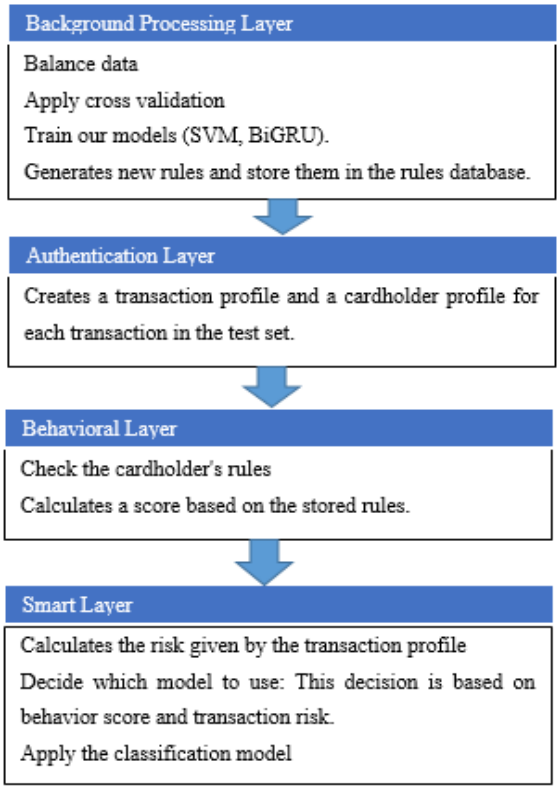

Figure 3. CCFD processing flow

REFERENCES

[1] I. Sadgali, N. Sael, and F. Benabbou, "Adaptive Model for Credit Card Fraud Detection," *International Journal of Interactive Mobile Technologies (IJIM)*, vol. 14, no. 3, pp. 54-65, 2020.

[2] I. Sadgali, N. Sael, and F. Benabbou, "Bidirectional Gated Recurrent Unit for improving classification in credit card fraud detection," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 15, no. 3, pp. 1704-1712, 2021, doi: 10.11591/ijeecs.v21.i3.pp1704-1712.

[3] I. Sadgali, N. Sael, and F. Benabbou, "Fraud detection in credit card transaction using machine learning techniques," *2019 1st International Conference on Smart Systems and Data Science (ICSSD)*, 2019, pp. 1-4, doi: 10.1109/ICSSD47982.2019.9002674.

[4] T. K. Behera and S. Panigrahi, "Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering and Neural Network," *2015 Second International Conference on Advances in Computing and Communication Engineering*, 2015, pp. 494-499, doi: 10.1109/ICACCE.2015.33.

[5] T. K. Behera and S. Panigrahi, "Credit Card Fraud Detection Using a Neuro-Fuzzy Expert System," *International Journal of Computational Intelligence in Data Mining*. *Advances in Intelligent Systems and Computing*, vol. 556, pp. 835-843, May 2017, doi: 10.1007/978-981-10-3874-7_79.
[6] S. M. S. Askari and M. A. Hussain, "Credit card fraud detection using fuzzy ID3," *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 446-452, doi: 10.1109/CCAA.2017.8229897.
[7] J. R. D. Kho and L. A. Vea, "Credit card fraud detection based on transaction behavior," *TENCON 2017-2017 IEEE Region 10 Conference*, 2017, pp. 1880-884, doi: 10.1109/TENCON.2017.8228165.
[8] Q. Li and Y. Xie, "A Behavior-cluster Based Imbalanced Classification Method for Credit Card Fraud Detection," *Proceedings of the 2019 2nd International Conference on Data Science and Information Technology*, July 2019, pp. 134-139, doi: 10.1145/3352411.3352433.
[9] D. Sanchez, M. A. Vila, L. Cerda, and J. M. Serrano, "Association rules applied to credit card fraud detection," *Expert Systems with Applications*, vol. 36, no. 2, pp. 3630-3640, March 2009, doi: 10.1016/j.eswa.2008.02.001
[10] M. Mavri and G. Ioannou, "Customer switching behavior in Greek banking services using survival analysis," *International journal of Managerial Finance*, vol. 34, no. 3, pp. 186-197. 2008, doi: 10.1108/03074350810848063.
[11] F. Meng, X. Zeng, and Q. Ma, "Learning Customer Behaviour under Real-Time Pricing in the Smart Grid," *2013 IEEE International Conference on Systems, Man, and Cybernetics*, 2013, pp. 3186-3191, doi: 10.1109/SMC.2013.543.
[12] N. D. Rodríguez, M. P. Cuéllar, J. Lilius, and M. D. Calvo-Flores, "A fuzzy ontology for semantic modelling and recognition of human behavior," *International jornal of Knowledge-Based Systems*, vol. 66, pp. 44-60, August 2014, doi: 10.1016/j.knosys.2014.04.016.
[13] M. León, L. Mkrtchyan, B. Depaire, D. Ruan, and K. Vanhoof, "Learning and clustering of fuzzy cognitive maps for travel behavior analysis," *International journal of Knowledge and Information Systems*, vol. 39, pp. 435-462, 2014, doi: 10.1007/s10115-013-0616-z.
[14] J. Dai, H. Yin, and P. Zhang, "A User Behavior Clustering Algorithm Combines Association Rules and Multi-valued Discrete Features," *2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, 2020, pp. 23-27, doi: 10.1109/ICCCBDA49378.2020.9095685.
[15] B. Hanumanthu and M. Sadanandam, "Rough Sets Base Associative Classification Rules Extraction from Big Data," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9, no. 1, November 2019, doi: 10.35940/ijitee.A9140.119119.
[16] Q. Pan, L. Xiang, and Y. Jin, "Rare Association Rules Mining of Diabetic Complications Based on Improved Rarity Algorithm," *2019 IEEE 7th International Conference on Bioinformatics and Computational Biology (ICBCB)*, 2019, pp. 115-119, doi: 10.1109/ICBCB.2019.8854639.
[17] P. Bian, B. Liang, W. Shi, J. Huang, and Y. Cai, "NAR-Miner: Discovering Negative Association Rules from Code for Bug Detection," In *Proceedings of the 26th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'18)*, October 2018, pp. 411-422, doi: 10.1145/3236024.3236032.
[18] R. Agrawal, T. Imielinski, and A. Swami, "Mining association rules between set of items in large databases," In *Proceedings of the 1993 ACM SIGMOD conference*, pp. 207-216 June 1993, doi: 10.1145/170035.170072.
[19] L. A. Zadeh, "Information and control," *Fuzzy sets*, vol. 8, no. 3, pp. 338-353, 1965.
[20] Z. Pawlak and A. Skowron, "Rudiments of rough sets," *Information sciences*, vol .177, no. 11, pp. 3-27, 2007, doi: 10.1016/j.ins.2006.06.003.
[21] Z. Pawlak, "Rough sets: Theoretical aspects of reasoning about data," *Springer Science and Business Media*, vol. 9, 2012.
[22] Z. Suraj, "An Introduction to Rough Set Theory and its applications," *ICENCO*, Cairo, Egypt, vol. 3, no. 80, 2004, doi: 10.1.1.488.192.
[23] I. Sadgali, N. Sael, and F. Benabbou, "Detection of credit card fraud: State of art," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 18, no. 11, pp. 76-83, 2018.
[24] I. Sadgali, N. Sael, and F. Benabbou, "A Review of anomaly detection based on association rules techniques," *Proceedings of the 5th International Conference on Smart City Applications*, 2021, pp. 1155-1166, doi: 10.1007/978-3-030-66840-2_88.
[25] Source file dataset of kaggle for credit card fraud. [Online]. Available: https://www.openml.org/d/1597.