AUT Jouranl of Modeling and Simulation

AUT J. Model. Simul., 52(1) (2020) 63-76
DOI: 10.22060/miscj.2020.17052.5170

Sequential fraud detection by determining proper sequence length in payment cards using HMM

Ghazaleh Shahidi, Mehrdad Kargari*

Tarbiat Modares University, Industrial and systems engineering, Tehran Jalal AleAhmad Nasr P.O.Box: 14115-111

ABSTRACT: The use of bank cards has increased significantly in recent years. This has resulted in increasing the probability of internet payment card frauds and has highly imposed losses on customers, institutions and banks. The methods used to detect frauds in this area mainly require a huge volume of historical data. On the other hand, these methods usually work well when there are single bank transactions, which means they only have the ability to detect frauds during single bank transactions and do not reveal fraudulent sequence identification.

In this paper, a model is proposed to determine the appropriate sequence length required to evaluate every single customer's spending behavior. Through adding the feature of fraudulent sequence detection in payment cards, the proposed model has been completed. This model automatically creates and updates the Hidden Markov Model of each sequence, and ultimately detects frauds by comparing the Kullback-Leibler divergence between Hidden Markov Model of each sequence. The fraud detection is presented by real semi-supervised payment cards data of an Iranian bank. The obtained F-Score, derived from 7 real fraudulent scenarios created under the supervision of a bank expert, representing 87%. Using the proposed model also leads to a reduction in the fraudulent sequences incidence cost of 81%.

Review History:

Received: Sep. 14,2019
Revised: Apr. 15, 2020
Accepted: May, 27, 2020
Available Online: Jun. 15, 2020

Keywords:

Payment card
Sequential spending behavior
Fraud detection
Hidden Markov Model
KL divergence

1- INTRODUCTION

The incidence of payment card fraud is one of the most considerable challenges facing banks and financial institutions. Payment card fraud inflicts direct financial losses on the organizations, causing customer dissatisfaction and reduces the success rate of organization in retaining its clients.

According to the Nilson Report (2016), the credit card and debit card fraud losses in 2010 were $ 7.6 billion, and it was predicted that by 2020 this number will be quadrupled to $ 31.67 billion. The growth of electronic banking besides having more than 400 million payment cards in Iran have also caused significant financial losses as a result of card fraud (Vosough, Taghavi Fard, and Alborzi 2015).

So far, various methods have been employed to detect credit card and payment card fraud. Kumar and Spafford classified these methods into two general categories; abuse detection which means using a specific pattern obtained from previous known attacks to identify future frauds and anomaly detection which means creating a profile containing user history to identify any deviations of his behavior pattern (Kumar and Spafford 1994). The main advantage of the anomaly detection approach comparing to misuse detection is the potentiality of detecting new attacks that were not identified by the system previously (Kumar and Spafford 1994).

Despite numerous research and studies about card fraud detection, there are still so many unresolved issues in this area. Two of these important issues are addressed in this paper. The first problem is to determine the minimum volume of historical data needed to detect frauds. If all the data is processed, the pace of modeling and fraud detection will be reduced, and in most cases, accessing this volume of data is not possible. On the other hand, if only a part of data is processed, there will be a possibility of reducing the accuracy of modeling. Therefore, a special amount of data must be processed that, in addition to accessibility, has a positive impact on both the speed and accuracy of fraud detection. Detection of sequential fraud is considered as the second unresolved problem. A review of the literature reveals that most of the approaches to payment card fraud focus on single fraudulent transaction and these approaches are less concerned with detecting fraudulent sequences. It is possible that all the single transactions are detected as normal ones, while we are facing a fraudulent sequence which is not detectable by single-transaction-based fraud detection system.

Two main purposes are considered for this work. The first one is to find a solution to determine the appropriate volume of data which needs to be processed. This purpose is achieved by accurate sampling of each payment card data by HMMs, and in such a manner as to indicate the overall and repeatable spending behavior of each customer. The second purpose is also detecting fraudulent sequences in payment cards.

*Corresponding author's email: m_kargari@modares.ac.ir

This problem has been solved by constructing the HMMs of each payment card sequences with a specified length and comparing the degree of KL divergence of these models.

This paper has two main contributions compared to previous works. The first one is determining an adequate sequence length for detecting fraud, which is obtained based on each individual's spending behavior. The main advantage of determining adequate sequence length is using a volume of data which could optimize the pace and accuracy of fraud detection model, and on the other hand to generate a pattern to determine the repetitive spending behavior of the customer. The second contribution of this article is detecting fraudulent sequences in bank card transactions. Nowadays, fraud methods have become more complex in a way that they can avoid the usual rules of fraud detection systems (Van Vlasselaer et al. 2015)the ease of online payment has opened up many new opportunities for e-commerce, lowering the geographical boundaries for retail. While e-commerce is still gaining popularity, it is also the playground of fraudsters who try to misuse the transparency of online purchases and the transfer of credit card records. This paper proposes APATE, a novel approach to detect fraudulent credit card transactions conducted in online stores. Our approach combines (1. One of these complex methods is the incidence of fraudulent sequences. However, most of the studies and systems in bank fraud detection area have only the capability of detecting single fraudulent transactions. Therefore, addressing this significant research gap can be considered as the most important advantage of this study. Totally, the proposed model can be employed as a complementary method to a single-transaction based fraud detection system to increase the accuracy of detecting fraud. In order to evaluate the performance of the proposed model, it was used along with the fraud detection model presented in (Eshghi and Kargari 2019b).

The rest of the paper is organized as follows. First this paper begins with describing the HMMs and addressing the previous works on detection of fraudulent transactions and sequences in payment card in Section 2. Next, in Section 3, the methodology is described in details through 5 different parts. In Section 4, the findings and results are represented. The usage and limitations of proposed model is discussed in Section 5. Finally, Section 6 concludes the paper.

2- RELATED WORKS

Several studies have been carried out in the field of fraud detection based on anomaly detection method. This method is categorized into Unsupervised, Semi-supervised and Supervised anomaly detection proportional to the learning approach (Akhilomen 2013). Supervised anomaly detection needs a labeled data set including "fraud" and "non-fraud" samples. Unsupervised anomaly detection techniques require an unlabeled data set and Semi-supervised anomaly detection involves a small number of labeled samples and a large number of unlabeled samples.

Each of these categories consists of different algorithms and techniques. Decision tree is one of the oldest techniques employed in Supervised anomaly detection (Kokkinaki 1997; Sahin, Bulkan, and Duman 2013; Şahin and Duman 2011; Save et al. 2017; Zareapoor and Shamsolmoali 2015). Artificial neural network is also one of the most common techniques of Supervised anomaly detection (Dorronsoro et al. 1997; Ghosh and Reilly 1994; Guo and Li 2008; Maes et al. 2002; Patidar, Sharma, and others 2011; Syeda, Zhang, and Pan 2002; Wiese and Omlin 2009). Some of the other techniques used for the card fraud detection based on Supervised anomaly detection approach are artificial immune systems (Brabazon et al. 2010; Gadi et al. 2008; Halvaiee and Akbari 2014; Wong et al. 2012), K-nearest neighbors (Ganji and Mannem 2012; Malini and Pushpa 2017), support vector machines (Bhattacharyya et al. 2011; Chen et al. 2004; Chen, Chen, and Lin 2006; Dheepa and Dhanapal 2012; Lu and Ju 2011), genetic algorithms (Duman and Ozcelik 2011; Wu et al. 2007) and hidden Markov models (Falaki et al. 2012; Kumari, Kannan, and Muthukumaravel 2014; Mule and Kulkarni 2014; Robinson and Aria 2018; Abhinav Srivastava et al. 2008)

Two techniques of Fuzzy (Behera and Panigrahi 2017; Bentley et al. 2000; Eshghi and Kargari 2018) and self-organizing maps (Quah and Sriganesh 2008; Zaslavsky and Strizhak 2006) are also used in Unsupervised anomaly detection. Due to the fact that in many cases non-fraud transactions can be accessed, semi-supervised anomaly detection techniques have become more prominent in recent years (Eshghi and Kargari 2019b). Most of the above mentioned studies have worked on single fraudulent transaction. The fact that more complicated fraudsters hide their intention behind a sequence of transactions is neglected in most of the works.

In the year of 2008, Srivastava et al. modeled the sequence of bank card transactions by HMM so that they could detect a single fraudulent transaction (Abhinav Srivastava et al. 2008). In the proposed method of Srivastava et al., HMM is calculated based on the transaction history of each card using the Baum-welch algorithm, and then the probability of generation of the observed transaction sequences with the length of 15 by the HMM is calculated using the forward algorithm. When a new transaction occurs, the initial sequence is updated, and the probability of this observed sequence is also calculated under the condition of HMM. If the probability of observing the second sequence is less than the first sequence, then the last transaction of the second sequence will be considered as fraud. Srivastava et al. have used the concept of sequence in their work but did not detect the fraudulent sequence.

In 2018, Robinson and Aria used Srivastava's work as basis of their study and modeled the sequence of prepaid card transactions on a store-centric approach to detect fraudulent sequences (Robinson and Aria 2018). In their study, the data was windowed and for each sequence with a length of between 100 and 600 transactions, one HMM was obtained, then the divergence of these HMMs was calculated. If the calculated divergence is greater than the threshold obtained by multiple experiments, one encounters a fraudulent sequence.

In general, the HMM is one of the most widely used models for detecting anomalies in different domains. This model has been used to detect anomalies in public areas (Epaillard and

Bouguila 2016), human dynamics (Fuse and Kamiya 2017), Internet user behavior (Xie and Yu 2009)patients health system (Forkan et al. 2015), electronic systems (Dorj, Chen, and Pecht 2013), and in network intrusion detection (Ariu, Tronci, and Giacinto 2011; Bang, Cho, and Kang 2017)Cho, and Kang 2017.

In this paper, HMM analysis and KL Divergence is used to calculate a proper sequence length for each card, which represents the card holder's repeatable spending behavior, and then detects the fraudulent sequences in each card.

3- HIDDEN MARKOV MODEL

HMM is one method among other methods used to detect anomalies in discrete sequences (Chandola, Banerjee, and Kumar 2012). A review of the preceding studies suggests that the HMM is more effective in detecting anomalies in discrete sequences than other methods such as window-based and Markovian techniques (Warrender, Forrest, and Pearlmutter 1999).

The HMM has a finite set of states and a set of transition probabilities. The observation can be created based on the probability distribution. For an external observer, only these results are visible and states are hidden (Rabiner 1989). A HMM can be defined as follows (Rabiner 1989):

$S=\{s_1,s_2,\ldots,s_N\}$ represents a set of states. N shows the number of states in the model and s_i is a state. $V=\{v_1,v_2,\ldots,v_M\}$ is a set of observations and M denotes number of observation symbols per state. $O=O_1,O_2,O_3,\ldots,O_K$ is also the observation sequence. The state transition probability matrix $A=[a_{ij}]$, represents the transition probabilities from one state to the other one. Where $a_{ij}=P(s_j \, at \, t+1 | s_i \, at \, t), 1\le i\le N, 1\le j\le N, t=1,2,\ldots$ and $a_{ij}>0$ for all i, j. we also have $\sum_{j=1}^{N} a_{ij}=1, 1\le i\le N$. The emission probabilities matrix $B=[b_j(k)]$, denotes the probability of different observations in a special state. Where $b_j(k)=P(v_k \, at \, t \mid s_j \, at \, t), 1\le j\le N, 1\le k\le M$, addiyionaly $\sum_{k=1}^{M} b_j(k)=1, 1\le j\le N$. The initial state probability vector $\pi=[\pi_i]$, where $\pi_i=P(s_i \, at \, t=1), 1\le i\le N$ and $\sum_{j=1}^{N}\pi_i=1$.

To illustrate a complete set of model parameters, we use the symbol $\lambda=(A,B,\pi)$, in which as mentioned A is the state transition probability matrix, B is the emission probability matrix and π is the probability vector of the initial state (Rabiner and Juang 1986).

Two types of techniques can be used to detect anomalies using the HMM:

Technique 1. Comparing the acceptance probability of the observation sequence: Srivastava used this technique in his study and thus provided a model for single-transaction fraud detection based on a card-centric approach (A. Srivastava et al. 2008b)the use of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase ,cases of fraud associated with it are also rising .In this paper ,we model the sequence of operations in credit card transaction processing using a hidden Markov model) HMM.

Technique 2. Comparing HMMs generated from the sequences of observation: Robinson and Aria used this technique to detect fraudulent sequences through taking a store-centric approach, and used Kullback-Leibler Divergence to compare the mentioned HMMs (Robinson and Aria 2018).

$$KLD(\mathrm{P}\,\mathrm{Q}) = \sum_i P(i) log \frac{P(i)}{Q(i)} \quad (1)$$

KL Divergence, equation (1) is also known as relative entropy, is used as a measure to calculate the degree of divergence between the two probability distributions in statistics (Kullback 1997).KL divergence completely compare two HMMs and provide accurate information about the degree of divergence of the two models. Besides, the KL divergence is asymmetric, which means that KLD (P || Q) ≠ KLD (Q || P) (Hershey, Olsen, and Rennie 2007). This feature helps us reduce the number of false positives because of the transition from fraud to normal has a different KLD than the transition from normal to fraud (Robinson and Aria 2018).

Robinson and Aria used action on products as the sequence of observation, O^i, to define the parameters of the HMM. Observed symbols were $V=\{product-action_1, product-action_2,\ldots, product-action_M\}$. For example, cash to AT&T 25$ is an observed symbol. Hidden states were also based on sales context, $S=\{normal, weekend, holidays\}$. The transition matrix, A, was generated based on equal probabilities among three mentioned states and the initial state probabilities, π, were also considered equal. In the emission probability matrix, B, each value denoted the sales state x the product types.

The method of mentioned study is generally applied as follows:

1. A HMM, λ_1, is generated for each store from the last sequence, O^i.
2. All the new occurred transactions are added to the next sequence, O^{i+1}, until the specified window size is reached.
3. Then the next HMM, λ_2, is generated from the new sequence, O^{i+1}.
4. The two HMM's are compared, $\Delta\lambda_{2,1} = D_{kl}(\lambda_2, \lambda_1)$.
5. A fraud alert will be raised if $\Delta\lambda$ is greater than the specified threshold.
6. Ultimately, the existing HMM is updated to be the most recent HMM, λ_2.

In the mentioned work, 3 real fraud cases are defined and are injected into the existing data. Then with multiple experiments, parameters such as window size and threshold are determined based on the F-score and the processing time of each experiment.

In this paper the use of HMM analysis and KL Divergence is similar to that of Robinson and Aria; however, significant differences include the following; (i) payment cards rather than stores are modeled, (ii) instead of action on products, clustered transaction amounts are used, (iii) hidden states include channel of transactions (iv) HMM parameters are completely derived from each card transaction history, (v) 7 fraudulent scenarios including 60 fraudulent sequences are modeled, rather than 3 general cases, (vi) proper sequence length is determined for each card by using HMM and KL Divergence, and (vii) for each card, a unique threshold is determined based on its transaction history, rather than obtained F-Score and processing time.

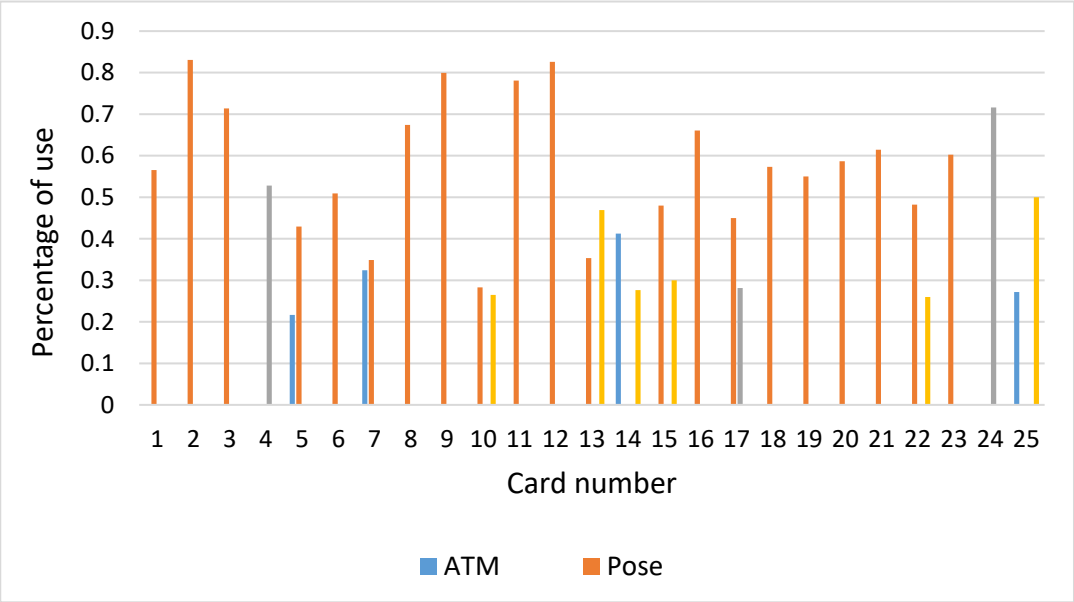

Fig. 1. Most used channels in a sample includes 25 cards

Table 1. The relation between Observations and States

Observation	Dominant channel and the percentage of observation incidence through it
VL (Very Low)	Internet- 52%
L (Low)	POS- 53%
M (Medium)	Internet- 51%
H (High)	ATM- 55%
VH (Very High)	Other- 52%

4- METHODOLOGY

The research methodology consists of four steps. At first, the observations, states HMM parameters are determined. Then, the proper number of transactions is specified, which can illustrate the repeatable spending behavior of each card. In the next step, the threshold of the KL divergence is calculated for each card. Finally, the fraudulent scenarios are defined.

4.1. Determining HMM's parameters

At first, transactions with a zero amount are omitted on each card. Then, to symmetrize and normalize the amount of transactions, the logarithmic amount of them is calculated (Manikandan 2010). Finally, the transactions channels are classified. Generally, transactions can be occurred through seven channels including ATM, POS, Kiosk, PIN pad, Internet, Mobile and Tell. Around 82.7% of all transactions occurred through ATM, POS and Internet; therefore, PIN pad, Kiosk, Mobile, and Tell channels, which together account for about 17.3% of all transactions, are considered as a single channel called "Other". Thus the accuracy of HMM parameters calculation increases.

To define the parameters of the HMM, we must first define the observation symbols and the model states. The transactions of each card are considered as model observations and they are categorized as VL (very low), L (low), M (Medium), H (High) and VH (very high), so the observation symbols are V = {VL, L, M, H, VH} and M = 5. These categories have equal length and exist in the range of the lowest and the highest transactions amount logarithms of each card.

It is important to note that the range for each symbol is determined by the history and spending behavior of each card owner; in this way a unique profile is created for each card. Channels through which the transactions occur are also considered as model states, so S = {ATM, POS, Internet, Other} and N = 4. The reason for choosing channels as model states is that the amount of transactions for each person varies in different and relatively wide range, while the channels that each person uses is limited and more stable.

In Fig. 1., the most frequent use of each channel is shown in different cards. As can be seen the displayed sample contains 25 cards, and in each card one or two channels are used in more than 50% of all transactions. In fact, each card has one or two dominant channels.

Additionally, observations are related to the states, due to the limitation on the transaction amount in different channels. The relation between observation symbols and states is determined by performing calculations and reviews on the used real data. According to Table 1, 52% of transactions with VL symbol is occurred through the Internet channel, 53% of transactions with L symbol is occurred through the Pos channel, 51% of transactions that have been in the M-symbol category are occurred through the Internet, 55%

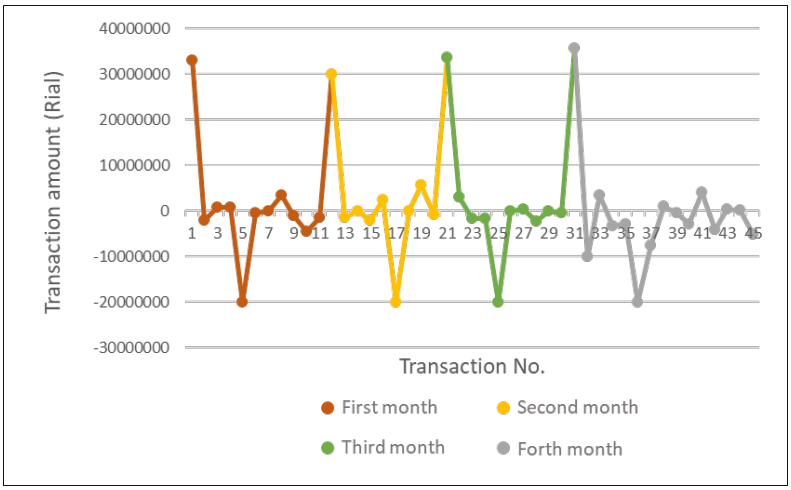

Fig. 1. Sample of an individual's transactions over four months

Fig. 2. Dominant pattern on an individual's transactions sample over four months

of transactions with H symbol are occurred through the ATM channel and finally 52% of VH transactions are performed through other channels. Therefore, for example, knowing that a transaction occurred at H (high) level, it can be said that this transaction was performed through an ATM channel with high probability.

4.2. Determining adequate length of a sequence

After determining the parameters of the HMM, the length of the sequence is calculated according to the spending behavior of each card owner. In general, the purpose of determining this sequence length is to choose the number of transactions that can represent repeatable behavior of the card owner.

Based on the different results obtained in different window sizes in Robinson and Aria's paper, it can be concluded that the length of sequence affects the accuracy of fraud detection model (Robinson and Aria 2018). Therefore, in order to have an accurate fraudulent sequence detection system, a proper sequence length must be considered. On the other hand, since each individual has a different transactional behavior that can depend on his job, the time of receiving a salary, etc., an adequate sequence length is calculated for each person separately. Fig. 1. shows an example of an individual's transactional behavior over four consecutive months, which indicates the dependence of the individual's spending behavior on receiving his monthly salary.

The dominant pattern on the mentioned individual's transactions in each month is shown in Fig. 2.

To determine the appropriate sequence length, the following variables need to be defined:

D: The number of cards

i: The card No. $(1 \le i \le D)$

α_i: The median of the number of i-th card daily transactions

β_i: The average of number of i-th card weekly transactions

j: The sequence length $(\alpha_i \le j \le \beta_i)$

$n_{i,j}$: The number of sequences with the length of j in i-th card

k: The sequence no. $(1 \le k \le n_{i,j})$

k′: The sequence no. $(k+1 \le k' \le n_{i,j})$

$g_{i,j}$: A group of sequences with the length of j in i-th card

$\lambda_{i,j,k}$: The HMM of k-th sequence with the length of j in i-th card

$M_{i,j}$: The average of calculated KL divergence between HMMs of all the sequences with the length of j in i-th card

After defining the above variables, the following steps are taken. The initial step is to calculate and for the existing cards.

In the second step, all the sequences of length $j(\alpha_i \le j \le \beta_i)$ are selected in training data of each card. Sequences of the same length are placed in the group. Therefore, for each card $g_i = \beta_i - \alpha_i + 1$ sequence groups are generated. Next, in each card, $\lambda_{i,j,k}(1 \le i \le D,\ \alpha_i \le j \le \beta_i, 1 \le k \le n_{i,j})$ is calculated according to the second step and separately. Afterwards, in each sequence group of individual card, $KLD(\lambda_{i,j,k+1}, \lambda_{i,j,k'}), (1 \le i \le D, \alpha_i \le j \le \beta_i, 1 \le k \le n_{i,j}, k+1 \le k' \le n_{i,j})$ is calculated between the HMMs of each sequence and all the subsequent sequences.

Then, the average of these KL divergence values is calculated, and $M_{i,j}$ is obtained for different cards and different length of sequences. Finally, in each card, after calculating $\Delta M_i = M_{i,j} - M_{i,j-1}$, the minimum (most negative) ΔM_i is determined and the j-th sequence which is involved in calculating ΔM_i is considered as the sequence length corresponding to the spending behavior for that card.

The basis of the mentioned computational steps is the divergence value between HMMs of transactional sequences. The greater convergence between HMMs of sequences with a certain length or the less calculated KLD value means that the individual's spending behavior is more repeatable with the mentioned sequence length (Robinson and Aria 2018). Based on the calculations performed on our real data, with the smallest sequence length (2 transactions), the average of KLD has the least value, and as the sequence length increases, this value gradually grows, and then it has small fluctuations around a certain value. Then at a unique point (adequate sequence length) suddenly the average of divergence value decreases with a steep gradient. This length of sequence that leads to the most negative gradient of divergence average is actually a relative minimum point. This behavior is observed in all sample cards transactions, and for each card, a relative minimum point is obtained that creates the most negative divergence gradient, which is considered as the adequate sequence length for that card.

Fig. 2. shows the averages of KLDs obtained for a specific card. As can be seen, at the sequence length of 15, the M decreases abruptly. This means that at the sequence length of 15 compared to the other points, the convergence between sequences is greater and the behavior is more repetitive. Therefore, the length of sequence 15 is considered as the adequate sequence length for this card.

Fig. 3. also shows the gradient of the divergence or ΔM. These obtained adequate sequence lengths are used to detect fraud in the next steps, which has ultimately led to the creation of an accurate fraud detection model.

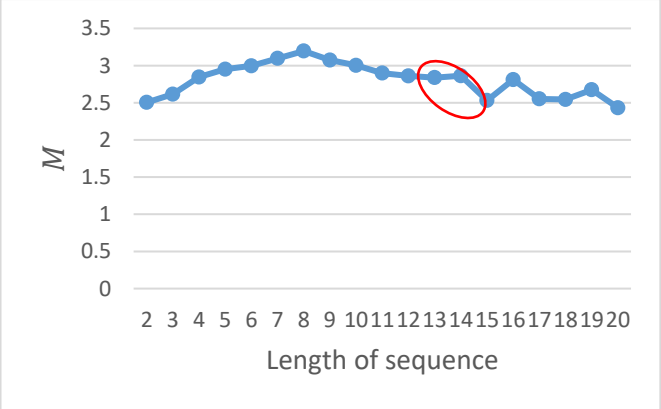

Fig. 2. Obtained Ms for the different lengths of the sequences in the sample card

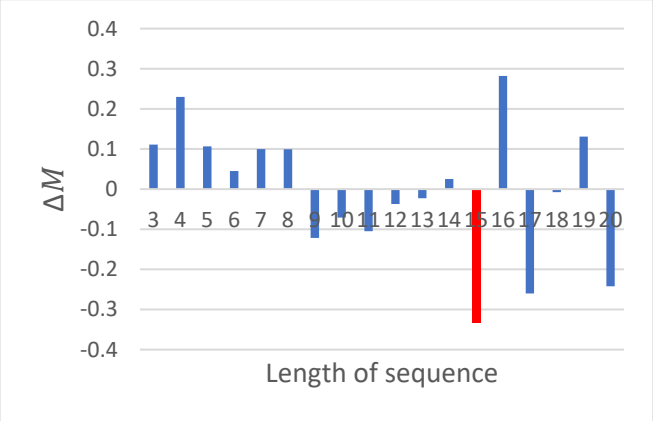

Fig. 3. Obtained ΔMs for the different lengths of the sequences in the sample card

4.3. Calculating threshold

After determining the adequate sequence length for each card, all sequences of proper length are selected in the training data of each card and the KL divergence is calculated between these sequences. The maximum value of the obtained KL divergences in each card is considered to be the divergence threshold of that card, Th_λ. In the mentioned sample card in section 4.2, which has a proper sequence length of 15, the calculated threshold is 5.2. This number is calculated based on the maximum degree of divergence between the HMM of all the sequences with the length of 15 in the training data of this card.

4.4. Fraudulent scenarios

The purpose of determining fraudulent scenarios is to measure the ability of the created system to detect the cardholder's fraudulent behavior. Since the main goal of this study is to establish a system for detecting fraudulent sequences, the fraudulent scenarios are extracted based on the occurrences of fraud in a sequence form. The initial idea behind defining these fraudulent scenarios comes from the fraudulent sequence presented in (Eshghi and Kargari 2019a). After performing reviews on our real bank data and identifying the actual fraudulent sequences in it, and also based on some bank experts opinions, more comprehensive sequences are defined in the form of 7 fraudulent scenarios. It cannot be claimed that the occurrence of these scenarios is certainly equal to the incidence of fraud, but we can say that the occurrence of such transactional behavior is rare with non-fraudulent purposes. In fact, the presence of these scenarios in an individual's transactions increases the probability of fraud incidence.

The length of these fraudulent scenarios varies according to the calculated proper length of the sequence of each card. In our mentioned sample card in section 4.2, all defined scenarios include 15 fraudulent transactions.

Totally 7 scenarios including 60 fraudulent sequences are extracted. In each of these fraudulent sequences, all of the transactions must occur through the same channel. For example, in scenario 1 with one mode, we have 4 fraudulent sequences each of which occurs through one of the possible channels. Each scenario will be described as follows:

Fraudulent scenario 1:

As shown in Fig. 4., scenario 1 is modeled based on the occurrence of a fraudulent sequence of VH amount symbol.

Fraudulent scenario 2:

Scenario 2 is modeled based on the occurrence of a fraudulent sequence of VH and H or M and VH amount symbols. Fig. 5. shows scenario two in its four modes.

Fraudulent scenario 3:

Scenario 3 is modeled based on the occurrence of a fraudulent sequence of VH and H and M amount symbols. Fig. 6. shows scenario three in its two modes.

Fraudulent scenario 4:

As shown in Fig. 7., scenario 4 is modeled based on the occurrence of a fraudulent sequence with an ascending trend which includes, respectively, M, H and VH amount symbols.

Fraudulent scenario 5:

As shown in Fig. 8., scenario 5 is modeled based on the occurrence of a fraudulent sequence with a descending trend which includes, respectively, VH, H and M amount symbols.

Fraudulent scenario 6:

Scenario 6 is modeled based on the occurrence of a fraudulent sequence with an ascending trend which includes, respectively, H and VH or M and H or M and VH amount symbols. Fig. 9. shows scenario six in its three modes.

Fraudulent scenario 7:

Scenario 7 is modeled based on the occurrence of a fraudulent sequence with a descending trend which includes, respectively, VH and H or H and M or VH and M amount symbols. Fig. 10. shows scenario seven in its three modes.

After adjusting each scenario with the proper sequence length of each card, the HMMs of all fraudulent sequences are determined. In each card, the degree of KL divergence between the HMM of each fraudulent sequence and the HMM of the train data last sequence is calculated. If the calculated divergence is greater than or equal to the threshold of each card ($KLD(\lambda_{Sce_i\,(mode_j,channel_k)}, \lambda_N) \geq Threshold_\lambda$), then the system will detect the fraudulent sequence, otherwise the system will not distinguish fraudulent sequences from the normal spending behavior of the cardholder.

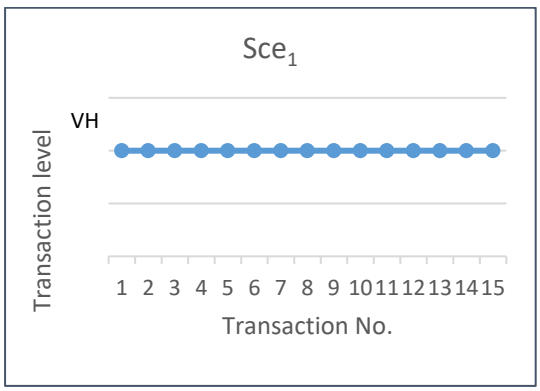

Fig. 4. Fraudulent scenario 1 with one mode

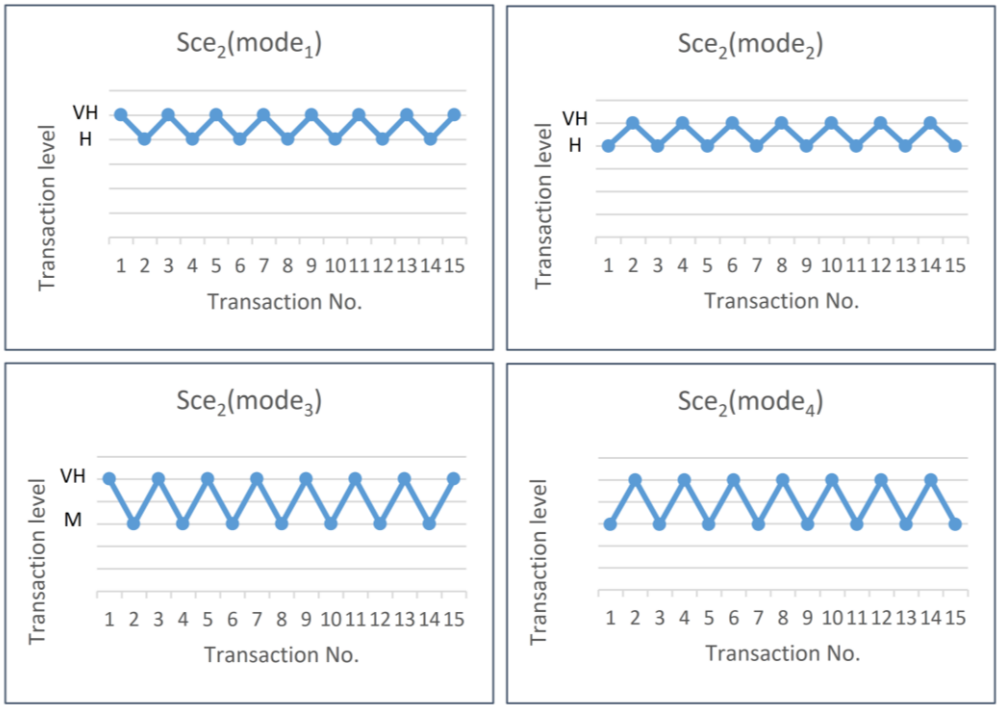

Fig. 5. Fraudulent scenario 2 with four modes

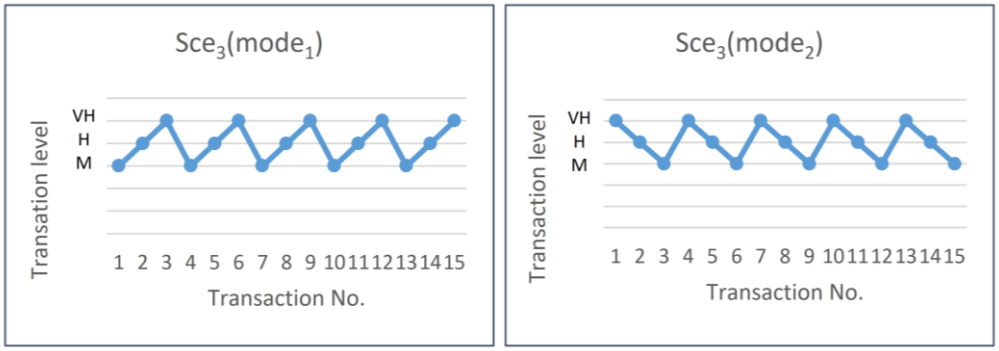

Fig. 6. Fraudulent scenario 3 with two modes

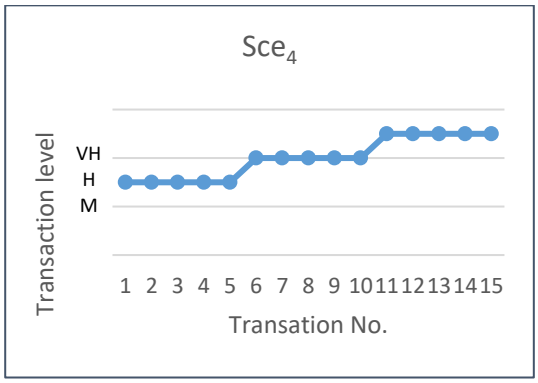

Fig. 7. Fraudulent scenario 4 with one mode

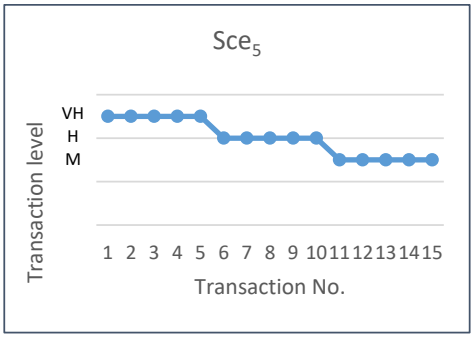

Fig. 8. Fraudulent scenario 5 with one mode

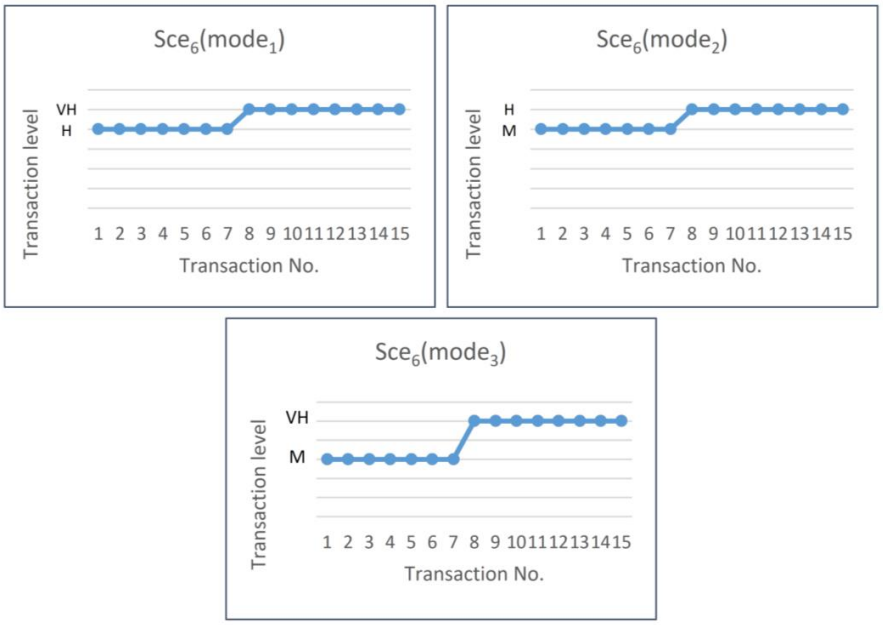

Fig. 9. Fraudulent scenario 6 with three modes

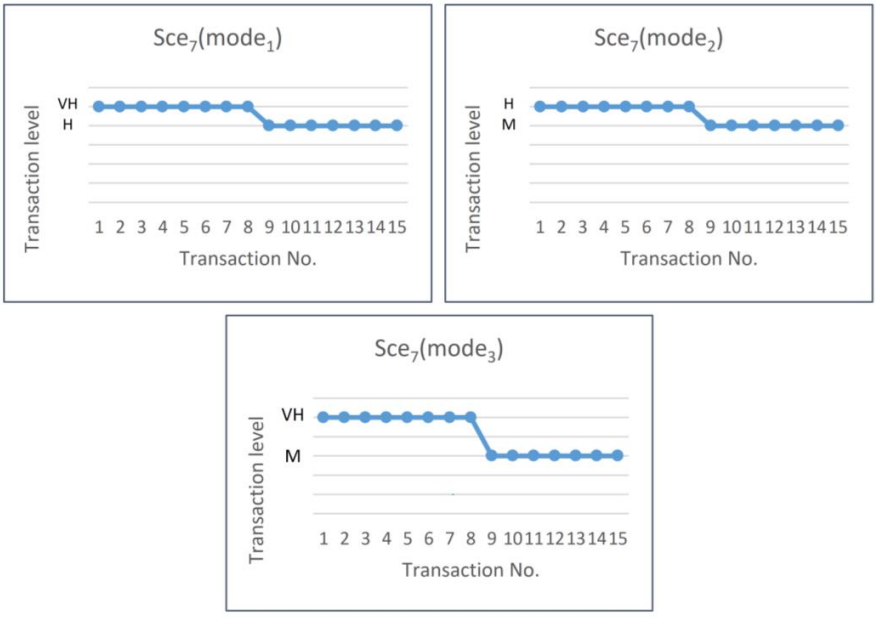

Fig. 10. Fraudulent scenario 7 with three modes

5- EXPERIMENTAL SETTINGS

4.1. Data

The experimental data used is the real payment cards data of a private bank in Iran. This data contains information about around 700 payment cards belonging to different customers. In each card, 70% of the data is considered as trained data and the remaining 30% is considered as test data.

The data driven belongs to a period of one year (2016). For each card, the information is available on three features including the transaction amount, the transaction time, and the channel through which the transaction occurred.

4.2 Measures

In this paper, the common quality measures including $Recall = \frac{TP}{TP+FN}$, $Precision = \frac{TP}{TP+FP}$, $F-Score = 2\times\frac{Precision\times Recall}{Precision+Recall}$ are used to evaluate our proposed fraud detection system. In addition to the mentioned measures, equation (2) is also used to indicate the effect of the proposed model on the cost.

$$Cost = \begin{cases} \alpha_0 Z_0 + \alpha_1 Z_1 + C_0 & Using\ the\ proposed\ model \\ \beta(FN) & Not\ using\ the\ proposed\ model \end{cases} \quad (2)$$

The cost function $Cost = 100\times f_n + 1\times(f_p + t_p)$ has been used in previous works (Gadi et al. 2008). In this paper, the mentioned cost function is improved and localized under the supervision of some bank experts in accordance with the financial process of the considered Iranian bank. The coefficients of the proposed cost function are calculated based on the actual costs in Iran, and for using it in other fraud detection studies, the coefficients can be optimized based on the local costs of the parameters.

According to equation (1), when the proposed model is employed, the cost consists of three parts including the corresponding cost of the 7 identified scenarios, the corresponding cost of an unknown scenario and the fixed cost of the implementation of the model. In the case where the proposed model is not used, the cost function is equal to the cost of occurrence of fraudulent sequences without any alert

Given the fact that the scenarios are modeled under the supervision of bank experts, the experts' opinions and also the obtained cost function are the criteria for evaluating the validity of the model and the results. True positive (TP), true negative (TN), false positive (FP) and false negative (FN) values must be computed to calculate the mentioned measures.

In order to calculate two values of TP and FN:

If $KLD(\lambda_{Sce_i\ (mode_j, channel_k)}, \lambda_N) \geq Threshold_\lambda$, then the sequence $Sce_i\ (mode_j, channel_k)$ will be detected as a fraudulent sequence and the result is recorded as TP.

If $KLD(\lambda_{Sce_i\ (mode_j, channel_k)}, \lambda_N) < Threshold_\lambda$, then the sequence $Sce_i\ (mode_j, channel_k)$ will be detected as a normal sequence and the result is recorded as FN.

In order to calculate the two values of TN and FP, the normal sequences of each card should be examined. Therefore, the test data of each card is used, and sequences of the determined length are selected on this data, and then the HMM of these sequences are calculated. Finally, the KL divergence between the HMM of each sequence and all subsequent sequences are calculated progressively.

If $KLD(\lambda_{k+1}, \lambda_k) \geq Threshold_\lambda$, then the sequence $(K+1)$-th will be detected as a fraudulent sequence and the result is recorded as FP.

If $KLD(\lambda_{k+1}, \lambda_k) < Threshold_\lambda$, then the sequence $(K+1)$-th will be detected as a normal sequence and the result is recorded as TN.

6- RESULT

The results have been obtained by applying the proposed model on the real data. This model compares the normal sequences of each card with the fraudulent scenarios. Table 2 shows the results of each of the seven fraudulent scenarios based on recall, precision and F-score. As can be seen, all the scenarios demonstrate F-score above 85%. By reviewing the experimental findings, it can be concluded that that the proposed model can detect Scenario No.1, which is the sequential occurrence of a VH amount symbol, with the highest F-score (97%).The lowest F-Score (85%) is also related to detecting Scenario No.2, which is the sequential occurrence of VH and H or M and VH amount symbols in four modes.

Another approach for calculating the mentioned measures, is to calculate the overall outcome of applying the model to the existing data, regardless of the distinction between scenarios. In this way, instead of considering each scenario separately and calculating measures for each of them, all 60 fraudulent sequences are applied to the data, and the measures are generally calculated. Thus, according to Table 3, we have one F-score which is equal to 87%.

In the case of examining 60 fraudulent sequences, we developed and used the mentioned cost measure in section 5.2. Generally, cost is an appropriate measure for determining the efficiency of a fraud detection system. The developed cost function in the condition of using the model is $Cost = \alpha_0 Z_0 + \alpha_1 Z_1 + C_0$. This function is based on three hypotheses: (1) there are 7 known scenarios which are described in Section

Table 2. The results of 7 scenarios

	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5	Scenario 6	Scenario 7
Recall	100%	79%	83%	83%	83%	83%	80%
Precision	94%	92%	93%	93%	93%	93%	92%
F-Score	97%	85%	87%	87%	87%	87%	86%

Table 3. The results of all 60 fraudulent sequences

Measure	Value
Recall	83%
Precision	93%
F-Score	87%

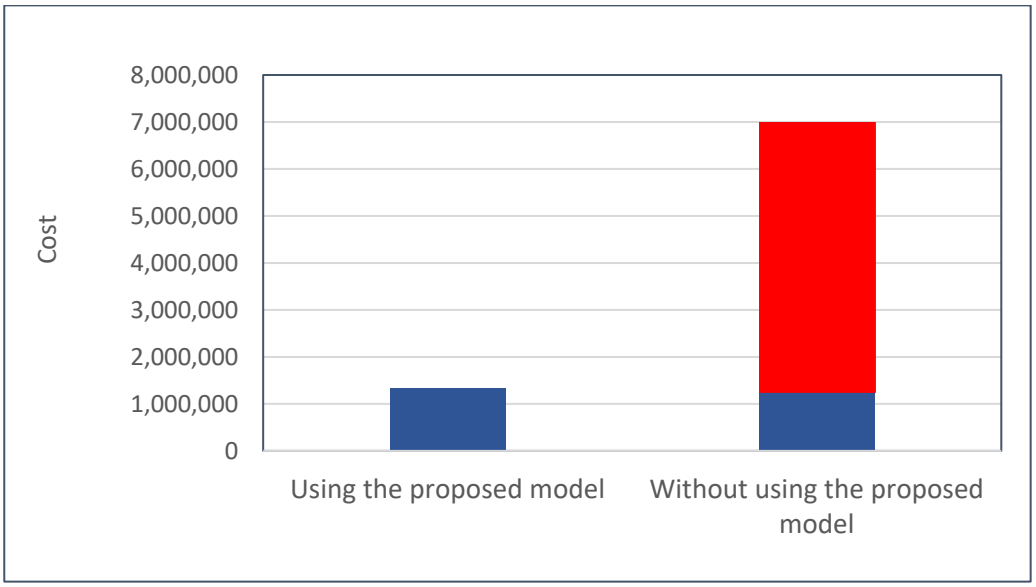

Fig. 11. Comparing the cost of incidence of 60 fraudulent sequences

4.4 and a cost of $\alpha_0 Z_0$ is considered for these seven scenarios. (2) There is 1 unknown scenario which has not been identified in this paper and the cost of $\alpha_1 Z_1$ is considered for this scenario. (3) Setting up the proposed model has a fixed cost, C_0.

To calculate the coefficients α_0 and α_1, we consider the probability of occurrence of each scenario as Uniform (0,1), so α_0 and α_1 are calculated as $7/8$ and $1/8$. Based on the calculations and reviews performed on our real data, $Z_0 = 466,500FN + 100FP + 10TP$ is obtained. According to the formula of Z_0, any fraudulent sequence that occurs and is not identified by the model (FN) generates a cost of 466,500 monetary units. To calculate the FN coefficient, we consider the length of 12 for all seven scenarios, which is the average of the proper lengths of all the cards, and, in each scenario, instead of amount symbols, we place the computed average of each symbol's numeric value. Each false alert (FN) cost includes the expenses of alerting the customer and causing customer dissatisfaction. The number of 100 is calculated based on the experts' opinions, assuming that the cost of sending an alert is positive and the cost of causing customer dissatisfaction is zero. For future processes of any true positive detection (TP), the cost is estimated at 10 units.

Since Z_1 is the cost of using the model in detecting an unknown scenario, it is considered equal to the average of the cost of using the model in detecting a known scenario, $Z_1 = \frac{Z_0}{7}$. The cost of launching the proposed fraud detection model is estimated at 200,000. Therefore, $Cost = \frac{7}{8}Z_0 + \frac{1}{8}\left(\frac{Z_0}{7}\right) + 200,000$ is the cost function in condition of using the model. By replacing FN, FP, and TP values, Z_0 is calculated and consequently the cost in condition of using the model is equal to 1,325,000 units.

Under conditions of not using the model, all 60 fraudulent sequences occur without any alert and $Cost = \beta(FN)$. According to the given explanation, in this condition, the occurrence of any fraudulent sequence generates a cost equivalent to $\beta = 466,500$ units. By replacing β and FN values, we have a cost of 7,000,000 units. As shown in Fig. 11., we can conclude that using the proposed model, caused 81% reduction in the costs of fraudulent sequences.As mentioned earlier, the proposed model is a complementary method to single-transaction based models, so in order to provide a stronger validation for this model, it has been employed along with the MCDM model presented in (Eshghi and Kargari 2019b). After running our proposed model on the data used in the mentioned paper, the F-score obtained from MCDM method with the threshold of 0.8, has increased by 5%. So in this way, the capability of our sequential fraud detection model to cover some of the existing system shortcomings has been indicated.

7- CONCLUSION

In recent years, bank card criminals have become smarter and the types of card frauds are increasingly varied. In this paper, a model is created based on HMM to determine the

adequate data needed to identify the repeatable spending behavior of each payment card owner. Subsequently a model is formed to detect fraudulent sequences by, first using the obtained proper length of the sequences of each payment card and then comparing the existing divergence between the HMMs of sequences.

According to the results obtained, the best performance of the model is related to detecting fraudulent sequences with a steady trend, in which several transactions of a constant amount of symbols occur in a sequential manner through one channel. This model needs a relatively small amount of historical data and has a high accuracy in detecting fraudulent sequences.

This fraud detection system can be used in banks where fraudulent sequences may occur in cards, but the existing fraud detection system only has the capability to detect single-transaction fraud. The best way to apply the proposed model is to use it in parallel with a single-transaction-based fraud detection system to cover the existing system shortcomings.

Totally the injection of more data, associating with the longer period of time can provide more precise patterns and models in which case it would be more appropriate to use the big data approach. Detecting specific fraudulent scenarios for each individual and based on one's spending behavior can also be considered as a prospective study, which may produce better results. The other usage of this sequence matching system in the future is to consider the status of an organization instead of an individual and detect its abnormal situations.

REFERENCES

[1] Akhilomen, John. 2013. "Data Mining Application for Cyber Credit-Card Fraud Detection System." Pp. 218–228 in *Industrial Conference on Data Mining*. Springer.

[2] Ariu, Davide, Roberto Tronci, and Giorgio Giacinto. 2011. "HMMPayl: An Intrusion Detection System Based on Hidden Markov Models." *Computers & Security* 30(4):221–41.

[3] Bang, June-ho, Young-Jong Cho, and Kyungran Kang. 2017. "Anomaly Detection of Network-Initiated LTE Signaling Traffic in Wireless Sensor and Actuator Networks Based on a Hidden Semi-Markov Model." *Computers & Security* 65:108–20.

[4] Behera, Tanmay Kumar, and Suvasini Panigrahi. 2017. "Credit Card Fraud Detection Using a Neuro-Fuzzy Expert System." Pp. 835–843 in *Computational Intelligence in Data Mining*. Springer.

[5] Bentley, Peter J., Jungwon Kim, Gil-Ho Jung, and Jong-Uk Choi. 2000. "Fuzzy Darwinian Detection of Credit Card Fraud." in *the 14th Annual Fall Symposium of the Korean Information Processing Society*. Vol. 14.

[6] Bhattacharyya, Siddhartha, Sanjeev Jha, Kurian Tharakunnel, and J. Christopher Westland. 2011. "Data Mining for Credit Card Fraud: A Comparative Study." *Decision Support Systems* 50(3):602–613.

[7] Bhusari, V., and S. Patil. 2011. "Study of Hidden Markov Model in Credit Card Fraudulent Detection." *International Journal of Computer Applications* 20(5):33–36.

[8] Brabazon, Anthony, Jane Cahill, Peter Keenan, and Daniel Walsh. 2010. "Identifying Online Credit Card Fraud Using Artificial Immune Systems." Pp. 1–7 in *Evolutionary Computation (CEC), 2010 IEEE Congress on*. IEEE.

[9] Chandola, Varun, Arindam Banerjee, and Vipin Kumar. 2012. "Anomaly Detection for Discrete Sequences: A Survey." *IEEE Transactions on Knowledge and Data Engineering* 24(5):823–839.

[10] Chen, Rong-Chang, Tung-Shou Chen, and Chih-Chiang Lin. 2006. "A New Binary Support Vector System for Increasing Detection Rate of Credit Card Fraud." *International Journal of Pattern Recognition and Artificial Intelligence* 20(02):227–239.

[11] Chen, Rong-Chang, Ming-Li Chiu, Ya-Li Huang, and Lin-Ti Chen. 2004. "Detecting Credit Card Fraud by Using Questionnaire-Responded Transaction Model Based on Support Vector Machines." *Intelligent Data Engineering and Automated Learning–IDEAL 2004* 800–806.

[12] Dheepa, V., and R. Dhanapal. 2012. "Behavior Based Credit Card Fraud Detection Using Support Vector Machines." *ICTACT Journal on Soft Computing* 4(4):391–7.

[13] Dorj, E., C. Chen, and M. Pecht. 2013. "A Bayesian Hidden Markov Model-Based Approach for Anomaly Detection in Electronic Systems." Pp. 1–10 in. IEEE.

[14] Dorronsoro, Jose R., Francisco Ginel, C. Sgnchez, and C. S. Cruz. 1997. "Neural Fraud Detection in Credit Card Operations." *IEEE Transactions on Neural Networks* 8(4):827–834.

[15] Duman, Ekrem, and M. Hamdi Ozcelik. 2011. "Detecting Credit Card Fraud by Genetic Algorithm and Scatter Search." *Expert Systems with Applications* 38(10):13057–13063.

[16] Epaillard, Elise, and Nizar Bouguila. 2016. "Proportional Data Modeling with Hidden Markov Models Based on Generalized Dirichlet and Beta-Liouville Mixtures Applied to Anomaly Detection in Public Areas." *Pattern Recognition* 55:125–36.

[17] Eshghi, Abdollah, and Mehrdad Kargari. 2018. "Detecting Frauds Using Customer Behavior Trend Analysis and Known Scenarios." *International Journal of Industrial Engineering & Production Research* 29(1):91–101.

[18] Eshghi, Abdollah, and Mehrdad Kargari. 2019a. "Introducing a Method for Combining Supervised and Semi-Supervised Methods in Fraud Detection." Pp. 23–30 in *2019 15th Iran International Industrial Engineering Conference (IIIEC)*. IEEE.

[19] Eshghi, Abdollah, and Mehrdad Kargari. 2019b. "Introducing a New Method for the Fusion of Fraud Evidence in Banking Transactions with Regards to Uncertainty." *Expert Systems with Applications* 121:382–92.

[20] Falaki, S. O., B. K. Alese, O. S. Adewale, J. O. Ayeni, G. A. Aderounmu, and W. O. Ismaila. 2012. "Probabilistic Credit Card Fraud Detection System in Online Transactions." *Int. J. Softw. Eng. Appl* 6(4):69–78.

[21] Forkan, Abdur Rahim Mohammad, Ibrahim Khalil, Zahir Tari, Sebti Foufou, and Abdelaziz Bouras. 2015. "A Context-Aware Approach for Long-Term Behavioural Change Detection and Abnormality Prediction in Ambient Assisted Living." *Pattern Recognition* 48(3):628–41.

[22] Fuse, T., and K. Kamiya. 2017. "Statistical Anomaly Detection in Human Dynamics Monitoring Using a Hierarchical Dirichlet Process Hidden Markov Model." *IEEE Transactions on Intelligent Transportation Systems* 18(11):3083–92.

[23] Gadi, Manoel Fernando Alonso, Xidi Wang, and Alair Pereira do Lago. 2008. "Credit Card Fraud Detection with Artificial Immune System." Pp. 119–131 in *ICARIS*. Vol. 8. Springer.

[24] Ganji, Venkata Ratnam, and Siva Naga Prasad Mannem. 2012. "Credit Card Fraud Detection Using Anti-k Nearest Neighbor Algorithm." *International Journal on Computer Science and Engineering* 4(6):1035–1039.

[25] Ghosh, Sushmito, and Douglas L. Reilly. 1994. "Credit Card Fraud Detection with a Neural-Network." Pp. 621–630 in *System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on*. Vol. 3. IEEE.

[26] Guo, Tao, and Gui-Yang Li. 2008. "Neural Data Mining for Credit Card Fraud Detection." Pp. 3630–3634 in *Machine Learning and Cybernetics, 2008 International Conference on*. Vol. 7. IEEE.

[27] Halvaiee, Neda Soltani, and Mohammad Kazem Akbari. 2014. "A Novel Model for Credit Card Fraud Detection Using Artificial Immune Systems." *Applied Soft Computing* 24:40–49.

[28] Hershey, John R., Peder A. Olsen, and Steven J. Rennie. 2007. "Variational Kullback-Leibler Divergence for Hidden Markov Models." Pp. 323–328 in *Automatic Speech Recognition & Understanding, 2007. ASRU. IEEE Workshop on*. IEEE.

[29] Kokkinaki, Angelika I. 1997. "On Atypical Database Transactions: Identification of Probable Frauds Using Machine Learning for User Profiling." Pp. 107–113 in *Knowledge and Data Engineering Exchange Workshop, 1997. Proceedings*. IEEE.

[30] Kullback, Solomon. 1997. *Information Theory and Statistics*. Courier Corporation.

[31] Kumar, Sandeep, and Eugene H. Spafford. 1994. "A Pattern Matching Model for Misuse Intrusion Detection."

[32] Kumari, Nitu, S. Kannan, and A. Muthukumaravel. 2014. "Credit Card Fraud Detection Using Hidden Markov Model-a Survey." *Middle-East Journal of Scientific Research* 19(6):821–825.

[33] Lu, Qibei, and Chunhua Ju. 2011. "Research on Credit Card Fraud Detection Model Based on Class Weighted Support Vector Machine." *Journal of Convergence Information Technology* 6(1).

[34] Maes, Sam, Karl Tuyls, Bram Vanschoenwinkel, and Bernard Manderick. 2002. "Credit Card Fraud Detection Using Bayesian and Neural Networks." Pp. 261–270 in *Proceedings of the 1st international naiso congress on neuro fuzzy technologies*.

[35] Malini, N., and M. Pushpa. 2017. "Analysis on Credit Card Fraud Identification Techniques Based on KNN and Outlier Detection." Pp. 255–258 in *Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), 2017 Third International Conference on*. IEEE.

[36] Manikandan, S. 2010. "Data Transformation." *Journal of Pharmacology and Pharmacotherapeutics* 1(2):126.

[37] Mule, Komal, and Madhuri Kulkarni. 2014. "Credit Card Fraud Detection Using Hidden Markov Model (HMM)."

[38] Nilson Report, 2016.

[39] Patidar, Raghavendra, Lokesh Sharma, and others. 2011. "Credit Card Fraud Detection Using Neural Network." *International Journal of Soft Computing and Engineering (IJSCE)* 1(32–38).

[40] Quah, Jon TS, and M. Sriganesh. 2008. "Real-Time Credit Card Fraud Detection Using Computational Intelligence." *Expert Systems with Applications* 35(4):1721–1732.

[41] Rabiner, Lawrence R. 1989. "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition." *Proceedings of the IEEE* 77(2):257–286.

[42] Rabiner, Lawrence R., and Biing-Hwang Juang. 1986. "An Introduction to Hidden Markov Models." *Ieee Assp Magazine* 3(1):4–16.

[43] Robinson, William N., and Andrea Aria. 2018. "Sequential Fraud Detection for Prepaid Cards Using Hidden Markov Model Divergence." *Expert Systems With Applications* 91:235–251.

[44] Sahin, Yusuf, Serol Bulkan, and Ekrem Duman. 2013. "A Cost-Sensitive Decision Tree Approach for Fraud Detection." *Expert Systems with Applications* 40(15):5916–5923.

[45] Şahin, Yusuf G., and Ekrem Duman. ۲۰۱۱. "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines."

[46] Save, Prajal, Pranali Tiwarekar, Ketan N. Jain, and Neha Mahyavanshi. 2017. "A Novel Idea for Credit Card Fraud Detection Using Decision Tree." *International Journal of Computer Applications* 161(13).

[47] Srivastava, A., A. Kundu, S. Sural, and A. Majumdar. 2008a. "Credit Card Fraud Detection Using Hidden Markov Model." *IEEE Transactions on Dependable and Secure Computing* 5(1):37–48.

[48] Srivastava, A., A. Kundu, S. Sural, and A. Majumdar. 2008b. "Credit Card Fraud Detection Using Hidden Markov Model." *IEEE Transactions on Dependable and Secure Computing* 5(1):37–48.

[49] Srivastava, Abhinav, Amlan Kundu, Shamik Sural, and Arun Majumdar. 2008. "Credit Card Fraud Detection Using Hidden Markov Model." *IEEE Transactions on Dependable and Secure Computing* 5(1):37–48.

[50] Syeda, Mubeena, Yan-Qing Zhang, and Yi Pan. 2002. "Parallel Granular Neural Networks for Fast Credit Card Fraud Detection." Pp. 572–577 in *Fuzzy Systems, 2002. FUZZ-IEEE'02. Proceedings of the 2002 IEEE International Conference on*. Vol. 1. IEEE.

[51] Van Vlasselaer, Véronique, Cristián Bravo, Olivier Caelen, Tina Eliassi-Rad, Leman Akoglu, Monique Snoeck, and Bart Baesens. 2015. "APATE: A Novel Approach for Automated Credit Card Transaction Fraud Detection Using Network-Based Extensions." *Decision Support Systems* 75:38–48.

[52] Vosough, Maliheh, Mohammad Taghi Taghavi Fard, and Mahmoud Alborzi. 2015. "Bank Card Fraud Detection Using Artificial Neural Network." *Journal of Information Technology Management* 6(4):721–746.

[53] Warrender, Christina, Stephanie Forrest, and Barak A. Pearlmutter. 1999. "Detecting Intrusions Using System Calls: Alternative Data Models."

[54] Wiese, Bénard, and Christian Omlin. 2009. "Credit Card Transactions, Fraud Detection, and Machine Learning: Modelling Time with LSTM Recurrent Neural Networks." *Innovations in Neural Information Paradigms and Applications* 231–268.

[55] Wong, Nicholas, Pradeep Ray, Greg Stephens, and Lundy Lewis. 2012. "Artificial Immune Systems for the Detection of Credit Card Fraud: An Architecture, Prototype and Preliminary

Results." *Information Systems Journal* 22(1):53–76.

[56] Wu, Chih-Hung, Gwo-Hshiung Tzeng, Yeong-Jia Goo, and Wen-Chang Fang. 2007. "A Real-Valued Genetic Algorithm to Optimize the Parameters of Support Vector Machine for Predicting Bankruptcy." *Expert Systems with Applications* 32(2):397–408.

[57] Xie, Y., and S. Z. Yu. 2009. "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors." *IEEE/ACM Transactions on Networking* 17(1):54–65.

[58] Zareapoor, Masoumeh, and Pourya Shamsolmoali. 2015. "Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier." *Procedia Computer Science* 48:679–685.

[59] Zaslavsky, Vladimir, and Anna Strizhak. 2006. "Credit Card Fraud Detection Using Self-Organizing Maps." *Information and Security* 18:48.

HOW TO CITE THIS ARTICLE

Gh. Shahidi, M. Kargari, Sequential fraud detection by determining proper sequence length in payment cards using HMM, AUT J. Model. Simul., 52(1) (2020) 63-76.

DOI: 10.22060/miscj.2020.17052.5170