A Comparative Study and Performance Analysis of ATM Card Fraud Detection Techniques

Article *in* Journal of Information Security · January 2019

DOI: 10.4236/jis.2019.103011

2 authors, including:

Md. Mijanur Rahman
Jatiya Kabi Kazi Nazrul Islam University
65 PUBLICATIONS **709** CITATIONS

SEE PROFILE

Scientific Research Publishing

Journal of Information Security, 2019, 10, 188-197
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Comparative Study and Performance Analysis of ATM Card Fraud Detection Techniques

Md. Mijanur Rahman*, Anuva Rani Saha

Department of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Mymensingh, Bangladesh
Email: *mijanjkkniu@gmail.com, anuva.knu@gmail.com

How to cite this paper: Rahman, M.M. and Saha, A.R. (2019) A Comparative Study and Performance Analysis of ATM Card Fraud Detection Techniques. *Journal of Information Security*, **10**, 188-197.
https://doi.org/10.4236/jis.2019.103011

Received: June 16, 2019
Accepted: July 28, 2019
Published: July 31, 2019

Abstract

ATM card fraud is increasing gradually with the expansion of modern technology and global communication. In the whole world, it is resulting in the loss of billions of dollars each year. Fraud detection systems have become essential for all ATM card issuing banks to minimize their losses. The main goals are, firstly, to review alternative techniques that have been used in fraud detection and secondly compare and analyze these techniques that are already used in ATM card fraud detection. Recently different card security systems used different fraud detection techniques; these techniques are based on neural network, genetic algorithm, hidden Markov model, Bayesian network, decision tree, clustering method, support vector machine, etc. According to our survey, the most important parameters used for comparing these fraud detection systems are accuracy, speed and cost of fraud detection. This study is very useful for any ATM card provider to choose an appropriate solution for fraud detection problem and also enable us to build a hybrid approach for developing some effective algorithms which can perform properly on fraud detection mechanism.

Keywords

ATM Card, Fraud Detection, Prevention Technology, Supervised and Unsupervised Technique

1. Introduction

An ATM card is the most popular method of payment. Due to the rapid advancement in modern technology, the use of ATM cards has increased and in case of ATM card fraud is also rising. ATM card fraud can be defined as "Unauthorized account activity by a person for whom the account was not intended" [1]. In recent times to reduce the ATM card fraud various fraud detection tech-

nologies are implemented. Fraud detection technology involves identifying Fraud as soon as possible when it has been perpetrated. At present implementation of an efficient fraud detection system is the main challenge. We presented a survey of various modern ATM fraud detection techniques which based on Artificial Intelligence, Data mining, Neural Network, Bayesian Network, Artificial Immune System, Support Vector Machine, and Decision Tree, Machine learning, etc. Most of the Fraud detection and prevention technology include analyzing the spending behavior of users/customer to overcome undesirable behavior. In this paper, we are going to discuss various fraud detection techniques and tools and how these methods properly apply in fraud detection and prevention. The main objective is to review various fraud detection methods used on ATM card and analyze their performance. Most important parameter such as accuracy, speed and cost are used for comparing the system performance.

The organization of this paper is as follows: Section 1 already discussed the introduction and summary of the study. ATM card fraud detection techniques will be presented in Section 2. The performance analysis and result of various methods will be discussed in Section 3. Finally, the conclusion and future scope of this work will be explained in Section 4.

2. ATM Card Fraud Detection Techniques

Fraud risk management in financial organization can be implemented by card fraud detection model. The model is developed by using various fraud detection methods, tools or techniques. Multiple approaches have been available, such as, neural network approach, genetic algorithms, Hidden Markov model, Bayesian network, decision trees, K-means clustering method, support vector machine, artificial immune system, etc.

2.1. Neural Network Based Fraud Detection

Fraud detection system using neural network is totally based on the human brain working principal. As human brain it learns through past experience and uses its knowledge or experience [2] in making the decision about fraudulent or non-fraudulent. It can be configured by supervised and unsupervised learning technique [3]. Supervised learning algorithms are defined as the desired output is known for the input. Back propagation neural network is mostly used supervised technique [4]. Initially the Supervised learning algorithm uses a supervised training data. The training data consists of training examples such as the last one or two year data of particular consumer (occupation, income, large amount of purchased placed, frequencies of large Purchase, location) and the various ATM card fraud face by a particular bank previously. Then it analyzes the training dataset and produces a classifier. When test data is given to the input it Compare the test data with training data. If test data matches with fraudulent record than it will be fraud. Otherwise transaction will be done securely. The layer of neural network in ATM card fraud detection system [2] is shown in **Figure 1**.

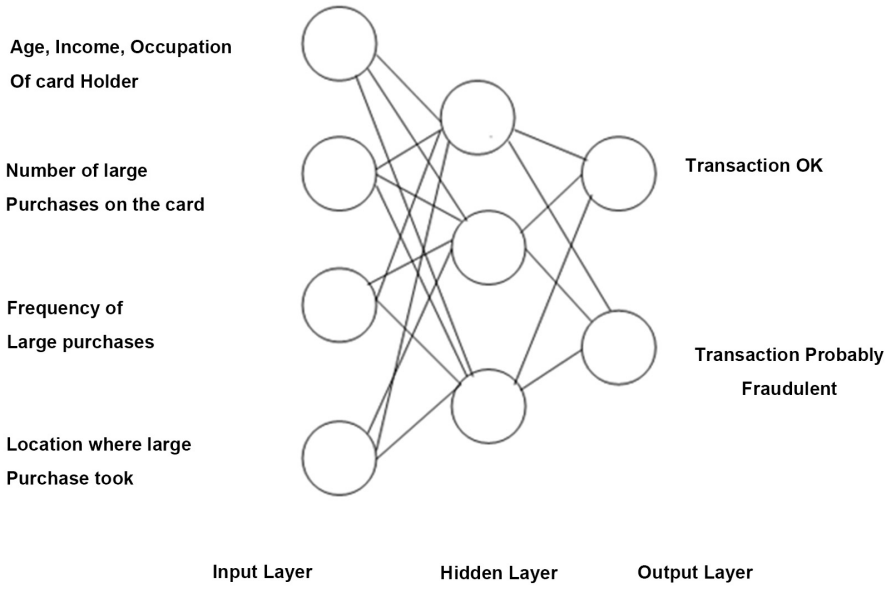

Figure 1. Layers of neural network in ATM card fraud detection.

The unsupervised techniques do not need the previous knowledge of fraudulent and Normal records. These methods raise alarm for those transactions that are most dissimilar from the Normal one. Self-organizing map (SOM) is one of the most popular unsupervised neural networks learning. It operates in two phase: training and mapping [5]. Initially the map is built and weights of the neurons are updated iteratively, based on input samples. Test data is classified automatically into normal and fraudulent classes through the procedure of mapping. After training the SOM, new unseen transactions are compared to normal and fraud clusters. If a new incoming transaction is similar to all previous transactions from genuine set, and then it is considered genuine otherwise it is fraudulent.

2.2. Genetic Algorithm Based Fraud Detection

The Genetic Algorithms are evolutionary algorithms whose main objective is to obtain the better solution to the problem. It detects the fraud in real time and also minimizes the number of false alerts. The fraud that is detected is based on the customers' behavior. The customer confidential information (such as the credit card usage frequency count, credit card usage location, credit card overdraft, current bank balance, average daily spending etc.) is stored in the data warehouse that is exposed to the rule engine which consists of the fraud rule set. The filter and the priority module set's the priority of the information and then send it to the genetic algorithm which performs its function and generates the output. The process [6] is shown in Figure 2 and Figure 3.

2.3. HMM Based Fraud Detection

A hidden Markov model (HMM) is a statistical model in which the system being

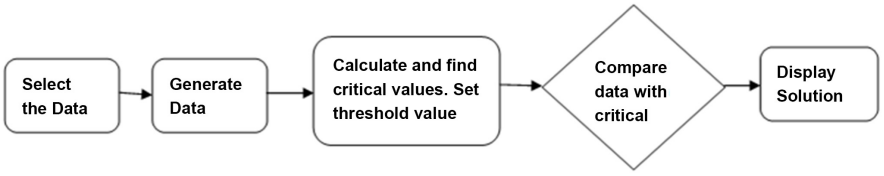

Figure 2. Process of genetic algorithm based method.

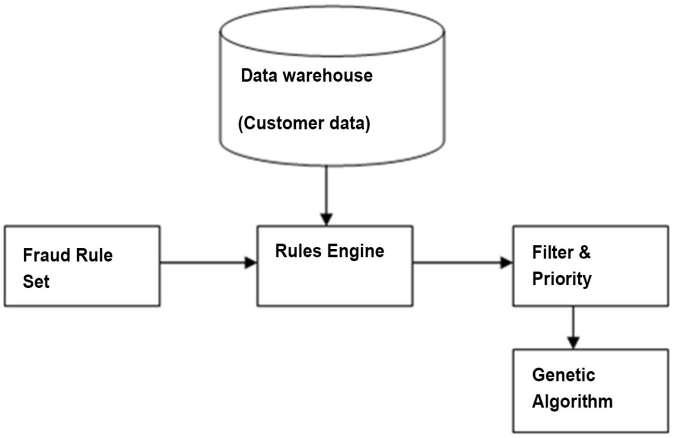

Figure 3. Implementation plan of genetic algorithm based system.

modeled is assumed to be a Markov process with unobserved state [7]. It works on the user spending profiles to detect frauds which can be divided into three types, such as: 1) Lower profile; 2) Middle profile; and 3) Higher profile [2]. The training phase and detection and prevention phase [8] [9] process is given in Figure 4 and Figure 5.

In this model at first start the bank sever and HMM server. When client initiates transaction, HMM starts observing and comparing the operation. It traps the transaction if identified fraud and is blocked .User reply with password on mobile using Bluetooth is same bank ATM else using SMS. Password is verified for authentication and transaction is allowed. Transaction is totally blocked after three failed attempts.

2.4. Bayesian Network Based Fraud Detection

Bayesian networks are statistical techniques in data mining. The goal of Bayesian network is to correctly predict the value of a designated discrete class variable given a vector of predictors or attributes [10]. For the purpose of fraud detection, two Bayesian networks are constructed that describe the behavior of user. First, a Bayesian network is constructed to model behavior under the assumption that the user is fraudulent (F) and another model under the assumption that the user is a legitimate (NF). The "fraud net" is set up by using expert knowledge. The "user net" is set up by using data from non fraudulent users. During operations, user net is adapted to a specific user based on emerging data. By inserting evidence to these networks, the result of any transaction has been classified as fraudulent or non fraudulent behavior. Probability of fraud = P (F) then P (NF)

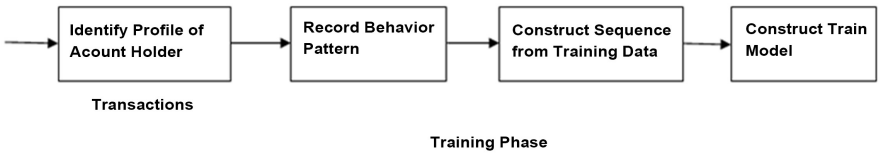

Figure 4. Training phase of process flow diagram in HMM based method.

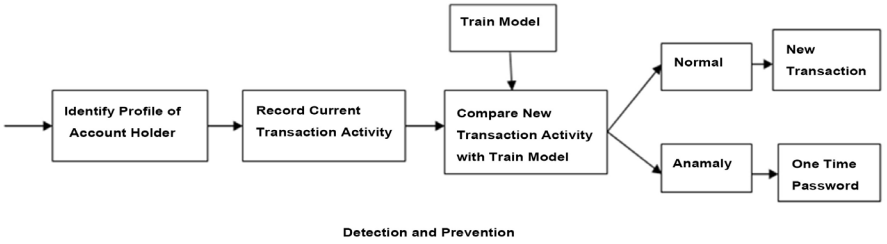

Figure 5. Detection and prevention phase of process flow diagram HMM based method.

= 1 − P (F) in general and by applying Bayes rule, it gives the probability of fraud for any incoming transaction. The fraud probability that has obtained of training can be used as an alarm level.

2.5. Decision Tree Based Fraud Detection

A decision tree is one widely used machine learning technique that has been effective for classification or regression. Its usefulness results from the ability to compensate for missing values and having a highly flexible hypothesis space [11]. First, training sets are generated by selecting a set of measurements from a single smart meter within a particular time period for a particular customer. After the selection of the training dataset, this dataset is used to generate the decision rules representative of the normal energy consumption behavior model for the customer in question. Here, Prediction is achieved by using the generated decision rules to predict the expected energy consumption values based on the feature set (year, day of the week, time) of the validation set. For calculation the Root Mean Squared Error (RMSE) is a widely used statistical method. This calculation is used as an indicator of deviation between the predicted and the actual value in the validation dataset and is calculated [11] as Equation (1).

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}\left(y_t' - y_t\right)^2}{n}} \tag{1}$$

2.6. K-Means Clustering Method Based Fraud Detection

Clustering is a process of arranging data into groups of similar objects. Different grouping results are obtained from various clustering methods available to group the dataset. The choice of a particular method will depend on the desired output [12]. K-Means clustering is a simple and efficient method to cluster the data. The system architecture [13] of the clustering based approach is given in Figure 6.

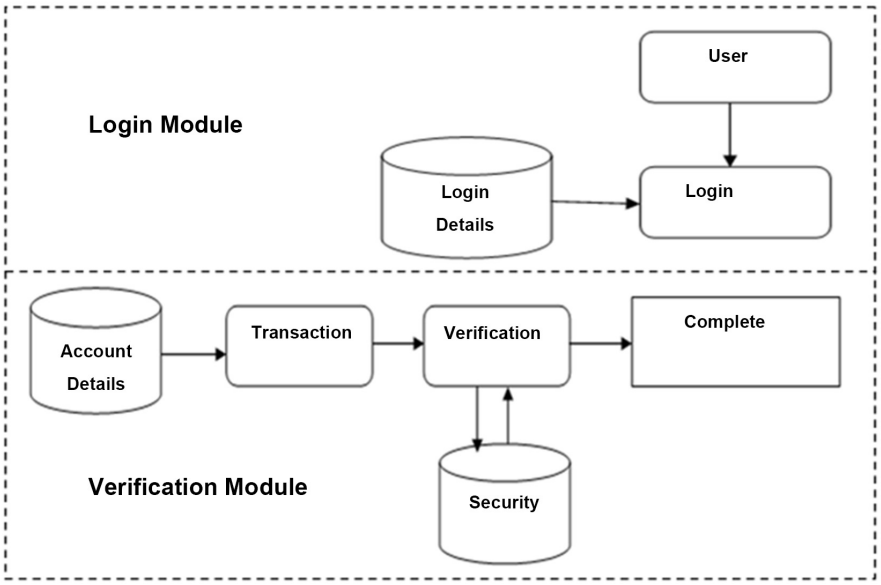

Figure 6. The system architecture of K-Means clustering approach.

First, the variables used in this program are declared such as transaction amount, credit card number, new transaction, transaction date, merchant category id, and transaction type id and transaction country. Then validation process shows the validity of the details required for the transaction. Now the data table that is generated before is entered into the database. Then the data which is removing from the table is now entered to get transaction data. Then an array is used so that the transaction detail will produce row wise. After that clusters are named/labeled as low cluster, high cluster, and middle risky cluster. To detect fraud or genuine transaction now the current transaction details were taken by using k-means clustering algorithm. If it is fraud then the message will display "fraud transaction" or else it will display "legitimate transaction".

2.7. Support Vector Machine (SVM) Based Fraud Detection

The Support Vector Machines (SVM) is statistical learning techniques and has successful application in a range of problems. The basic idea of SVM classification algorithm is to construct a hyper plane as the decision plane which making the distance between the positive and negative mode maximum [10]. SVMs are a popular machine learning method for classification, regression, & other learning tasks. LIBSVM is a library for Support Vector Machines (SVMs). A typical use of LIBSVM involves two steps: first, training a data set to obtain a model & second, using the model to predict information of a testing data set. The main functions carried out by SVM are as 1) At first set up the training data for model creation. 2) Then set up SVM's parameters for the dataset that is created and then send them for SVM training. 3) SVM Trainer, which trains each & every individual data from the large dataset. 4) Once the dataset is trained completely and the SVM Predictor does prediction of that trained data.

2.8. Artificial Immune System Based Fraud Detection

Artificial immune systems (AIS) represent an important strategy inspired by biological systems. The main developments within AIS have focused on three main immunological theories: clonal selection, immune networks and negative selection. The immune system can distinguish between self and non-self [14]. In the concept of credit card fraud detection, self (S) represents all patterns in a finite space that is legitimate and non-self ($\hat{S}$) represents all patterns that are not in self. The AIS consists of artificial lymphocytes (ALCs) that able to classify any pattern as self or non-self by detecting only non-self patterns. For training AIS system only needs positive examples but it can identify items as non-self. The system arbitrarily generates an ALC, test it against the set of self patterns and if it doesn't match any of the self patterns, it is included in the set of mature ALCs. When an ALC does match with any of the self patterns, it is replaced by a new randomly generated ALC which then needs to be tested as well. The ALC becomes mature or adult, by training it with the known self patterns. This training method is known as negative selection. High level model of AIS has been applied for credit card fraud detection. The aim of the AIS system is to have a high anomalous transaction detection rate and a low false positive rate [10].

3. Results Analysis and Discussions

The objectives of the study were to determine the operational response of various fraud detection methods. For result analysis we have done a comparative study on fraud detection methods. We have considered the most important parameter such as, accuracy, speed and cost for comparison. Comparison table is prepared in order to compare various ATM card fraud detection mechanisms. All the techniques of ATM card fraud detection described in this study [10] [15] [16] [17] [18] [19] have its own strengths and weaknesses. The comparison results found from this study are mentioned in **Table 1**.

The performance of various ATM card fraud detection techniques such as neural network, genetic algorithm, Hidden Markov model, Bayesian network, decision tree, clustering method, support vector machine (SVM) and artificial immune system, have been analyzed in this study. As a result every method has both advantages and disadvantages. Neural network has fast processing speed but accuracy is medium, genetic algorithm has good speed of detection but accuracy is medium, HMM has a fast processing speed but it's accuracy is low than any other techniques, speed of detection and accuracy are very good for Bayesian network but it is very expensive, decision tree, clustering method, self organizing map (SOM), all these techniques has good speed of fraud detection but accuracy is medium. At the same time support vector machine has low and artificial immune system has very fast speed of detection [15]. So from the results it can say that the best method among these techniques is AIS, BN, DT, GA, NNSOM, NNBP, and SVM.

Table 1. Comparison of various fraud detection techniques.

Methods	Advantages	Disadvantages	Speed of Detection	Accuracy	Cost	Comments
Neural Network	1) Able to learn from the past. 2) Extract rules and predict future activity based on the current situation. 3) Detect real time credit card fraud.	1) A number of parameter has to be set before any training can begin. There are no clear rules how to set these parameters.	Fast	Medium	Expensive	This method can be used when previous knowledge and past experience is known to the machine.
Genetic Algorithm	1) Works well with noisy data. 2) Easy to integrate with other system. 3) Usually combined into other techniques to increase the performance of these techniques and optimized their parameters.	1) The fraud is detected which is relevant to the customer's behavior. A new classification problem which has inconsistent misclassification cost is introduced. 2) Requires extensive tool knowledge to set up and operate and difficult to understand.	Good	Medium	Inexpensive	This method can be used to detect or predict the fraud in a very short period of time and to minimize the number of false alerts.
Hidden Markov Model	1) Can detect the fraudulent activity at the time of the transaction.	1) Cannot detect fraud with a few transactions. 2) Produces high false alarm as well as high false positive. 3) Not scalable to large size data set.	Fast	Low	High expensive	It has been very effective for more complicated stochastic process.
Bayesian Network	1) Needs training of data to operate and require high processing speed. 2) More accurate and much faster than neural network.	1) Excessive training need. 2) BBNs are slower when applied to new instances.	Very fast	High	Expensive	Very effective for modeling situations where some information is already known and incoming data is unsure or partially unavailable.
Decision Tree	1) High flexibility/Good haleness/Explainable/ Easy to implement/Easy to display and to understand.	1) Requirements to check each condition one by one.	Fast	Medium	Expensive	This method has been effective for classification or regression.
Clustering Method	1) Clustering helps in grouping the data into similar clusters that helps in uncomplicated retrieval of data.	1) There are quite a few non-fraudulent activities which wrongly got detected as frauds. So to detect fraud accurately and efficiently it is necessary that the real data should be available.	High	Medium	Expensive	This method is formed to detect fraud in credit card transaction which are low, high, risky and high risky.
Self-Organizing Map (SOM)	---	---	Fast	Medium	Expensive	This method has been very effective when machine has no previous knowledge.

Continued

Support vector machine (SVM):	SVMs can be robust, even when the training sample has some bias.	Poor in process large dataset.	Low	Medium	Expensive	This method is very effective for large training datasets.
Artificial Immune System (AIS):	Self-Organization/easy in integration with other systems/fault tolerance. This model only needs positive examples to train on, generating detectors (ALCs) with negative selection method.	Need high training time in NSA.	Very fast	Good	Inexpensive	It can be used to distinguish between self and non-self, or more appropriately, between harmful non-self and everything else.

4. Conclusion

The main objective of this work is to review various fraud detection methods on ATM card and analyze their performance. In this paper, we presented a survey of various fraud detection techniques which are most frequently used. We have considered the most important parameters for comparing these fraud detection techniques, such as accuracy, speed and cost. All these techniques of ATM card fraud detection discussed in this survey paper, have its own weaknesses as well as strengths. Some techniques have good speed of detection but medium accuracy. Some techniques have good accuracy but they are very expensive. As a result, although these methods are used for fraud detection, ATM card frauds are still not properly handled by these existing approaches. So we have to build a hybrid approach for developing some effective algorithms which can perform well for the classification problem with variable misclassification costs and with higher accuracy. Our future work is to develop a complete set of pattern recognition technique for fraud detection which overcomes the problem of missing values, handling large data and handling the incomplete dataset.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Suman and Nutan (2013) Review Paper on Credit Card Fraud Detection. *International Journal of Computer Trends and Technology*, **4**, 2206-2215.

[2] Patidar, R. and Sharma, L. (2011) Credit Card Fraud Detection Using Neural Network. *International Journal of Soft Computing and Engineering*, **1**, 32-38.

[3] Paasch, C.A.W. (2008) Credit Card Fraud Detection Using Artificial Neural Network Tuned by Genetic Algorithm. Ph.D. Thesis, Information and Systems Management, Hong Kong University of Science and Technology, Hong Kong.

[4] Mallika, R. (2017) Fraud Detection Using Supervised Learning Algorithms. *International Journal of Advanced Research in Computer and Communication Engineering*, **6**, 6-10. https://doi.org/10.17148/IJARCCE.2017.6602

[5] Sorournejad, S., Zojaji, Z., Atani, R.E. and Monadjemi, A.H. (2016) A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective. ArxiV: abs/1611.06439.

[6] Oberoi, R. (2017) Credit Card Fraud Detection System: Using Genetic Algorithm. *International Journal of Computer & Mathematical Sciences*, **6**, 59-63.

[7] Sonawne, V.D., Gupta, P., Raut, A. and Saudagar, F. (2016) ATM Card Fraud Detection Using Hidden Markov Model. *International Journal of Innovative Research in Computer and Communication Engineering*, **4**, 8742-8747.

[8] Mhamane, S.S. and Lobo, L.M.R.J. (2012) Use of Hidden Markov Model as Internet Banking Fraud Detection. *International Journal of Computer Applications*, **45**, 5-10. https://doi.org/10.1109/ICCCNT.2012.6395910

[9] Bhingarde, A., Bangar, A., Gupta, P. and Karambe, S. (2015) Credit Card Fraud Detection Using Hidden Markov Model. *International Journal of Advanced Research in Computer and Communication Engineering*, **4**, 169-170. https://doi.org/10.17148/IJARCCE.2015.4341

[10] Zareapoor, M., Seeja, K.R. and Alam, M.A. (2012) Analysis of Credit Card Fraud Detection Techniques: Based on Certain Design Criteria. *International Journal of Computer Applications*, **52**, 35-42. https://doi.org/10.5120/8184-1538

[11] Sen, S.K. and Dash, S. (2013) Meta Learning Algorithms for Credit Card Fraud Detection. *International Journal of Engineering Research and Development*, **6**, 16-20.

[12] Vaishali (2014) Fraud Detection in Credit Card by Clustering Approach. *International Journal of Computer Applications*, **98**, 29-32. https://doi.org/10.5120/17164-7225

[13] Sonawane, Y.B., Gadgil, A.S., More, A.E. and Jathar, N.K. (2016) Credit Card Fraud Detection Using Clustering Based Approach. *International Journal of Advance Research and Innovative Ideas in Education*, **2**, 1773-1776.

[14] Tripathi, K.K. and Pavaskar, M.A. (2012) Survey on Credit Card Fraud Detection Methods. *International Journal of Emerging Technology and Advanced Engineering*, **2**, 721-726.

[15] Kumari, S. and Choubey, A. (2017) A Review on Various Techniques and Approaches for Credit Card Fraud Detection. *International Journal of Scientific Research Engineering & Technology*, **6**, 485-489.

[16] Bhatia, S., Bajaj, R. and Hazari, S. (2016) Analysis of Credit Card Fraud Detection Techniques. *International Journal of Science and Research*, **5**, 1302-1307. https://doi.org/10.21275/v5i3.NOV162099

[17] Singh, P. and Singh, M. (2015) Fraud Detection by Monitoring Customer Behavior and Activities. *International Journal of Computer Applications*, **111**, 23-32. https://doi.org/10.5120/19584-1340

[18] Pumsirirat, A. and Liu, Y. (2018) Credit Card Fraud Detection Using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. *International Journal of Advanced Computer Science and Applications*, **9**, 18-25. https://doi.org/10.14569/IJACSA.2018.090103

[19] Gupta, S. and Malsa, N. (2017) Credit Card Fraud Detection and Prevention—A Survey. *International Journal for Innovative Research in Science & Technology*, **4**, 1-7.