*Grenze International Journal of Engineering and Technology, January Issue*

# A Review of Credit Card Fraud Detection Methods: An Approach Focused on Data and Technique

Ravi Bhushan[1] and Dr. Vineeta khemchandani[2]
[1]School of Computer Science and Engineering, Galgotias University, Gr.Noida
Email: ravi.bhushan_phd2019@galgotiasuniversity.edu.in
[2]School of Computer applications and Technology Galgotias University, Gr.Noida
Email: vineetakh05@gmail.com

***Abstract*— A crucial rule in the modern economy is the use of credit cards. It turns become an inevitable aspect of domestic, commercial, and international operations. Even while there are many advantages to using credit cards when done properly and cautiously, fraudulent activity can result in serious credit and financial harm. To address the rise in credit card fraud, numerous strategies have been put forth. Nevertheless, preventing credit card theft is the common objective of all these strategies; each has unique disadvantages, benefits, and traits. After looking into the challenges of detecting credit card fraud, we aim to cover the most recent methods, datasets, and assessment standards for credit card fraud detection in this paper. A list and comparison of the benefits and drawbacks of fraud detection techniques are provided. Additionally, the methodologies provided are categorised into two primary ways for detecting fraud: supervised misuse and unsupervised anomaly detection. Once more, the capacity to process both numerical and categorical datasets is used to classify the strategies. The useful and common characteristics of various datasets used in literature are then extracted for future use once they have been described and classified into real and synthesised data. Also gathered and addressed are evaluation criteria used in the literature. Thus, unresolved problems in detecting credit card fraud are described as recommendations for novice researchers.**

***Keywords*— Fraud Detection Techniques, Fraud Classification, Credit Card.**

## I. INTRODUCTION

At the current state of the world, financial organizations expand the availability of financial facilities by employing of innovative services such as credit cards, Automated Teller Machines (ATM), internet and mobile banking services. Besides, along with the rapid advances of e-commerce, the use of credit card has become a convenience and necessary part of financial life. Credit card is a payment card supplied to customers as a system of payment. There are lots of advantages in using credit cards such as:

### *A. Ease of purchase*

Credit cards can make life easier. They allow customers to purchase on credit in arbitrary time, location and amount, without carrying the cash. Provide a convenient payment method for purchases made on the internet, over the telephone, through ATMs, etc.

*Grenze ID: 01.GIJET.12.1.55_2*

*B. Keep customer credit history*

Having a good credit history is often important in detecting loyal customers. This history is valuable not only for credit cards, but also for other financial services like loans, rental applications, or even some jobs. Lenders and issuers of credit mortgage companies, credit card companies, retail stores, and utility companies can review customer credit score and history to see how punctual and responsible customers are in paying back their debts.

*C. Protection of Purchases*

Credit cards may also offer customers, additional protection if the purchased merchandise becomes lost, damaged, or stolen. Both the buyer‟s credit card statement and company can confirm that the customer has bought if the original receipt is lost or stolen. In addition, some credit card companies provide insurance for large purchases.

In spite of all mentioned advantages, the problem of fraud is a serious issue ine-banking services that threaten credit card transactions especially. Fraud is an intentional deception with the purpose of obtaining financial gain or causing loss by implicit or explicit trick. Fraud is a public law violation in which the fraudster gains an unlawful advantage or causes unlawful damage. The estimation of amount of damage made by fraud activities indicates that fraud costs a very considerable sum of money.

Although, credit card fraud detection has gained attention and extensive studies pecially in recent years and there are lots of surveys about this kind of fraud such as [1], [2], [3], neither classify all credit card fraud detection techniques with analysis of datasets and attributes. Therefore in this paper, we attempt to collect and integrate a complete set of researches of literature and analyze them from various aspects. The main contributions of this work are highlighted as follows:

- To the best of our knowledge, the absence of complete and detailed credit card fraud detection survey is an important issue, which is addressed by analyzing the state of the art in credit card fraud detection.
- The state of the art fraud detection techniques are described and classified from different aspects of supervised/unsupervised and numerical/categorical data consistent.
- In credit card fraud research each author has used its own dataset. There is no standard dataset or benchmark to evaluate detection methods. We attempt to gather different data sets investigated by researchers, categorize them into real and synthetized groups and extract the common attributes affects the quality of detection.

The rest of the paper is organized as follows: a general description of types of fraud is presented in Section2.Challengesof credit card fraud detection are identified in Section3. Section4describes the credit card fraud detection techniques, their advantages and disadvantages and classification of them. In section 5 the dataset used by researchers and corresponding evaluation criteria are explained; another classification upon data types is also drawn in this section. Finally open issues of credit card fraud detection are presented in Section6.

## II. CREDIT CARD FRAUD

TABLE I. KEY FRAUD STATISTICS FY 2025

| Fraud Type | Cases | Amount (₹ crore / ₹) | Notes |
|---|---|---|---|
| Internet & credit-card fraud (bank-reported) | 13,516 | ₹520 crore (↓ 64 % from ₹1,457 crore FY 23–24) | Over 50% drop in volume and value |
| All digital financial frauds (incl. UPI, cards) | 2.4 million | ₹4,245 crore (Apr 2024–Jan 2025) | +67 % in value YOY |
| Total banking frauds (cards, loan, advances) | 23,953 | ₹36,014 crore | Primarily from high-value loan/advance fraud |
| High-value cyber fraud cases (>₹1 lakh) | 29,082 | – | Approx. 4x increase from FY23–24 |
| Digital arrest scams (Jan–May 2025) | 21 cases | ₹9.21 crore | |

Credit card fraud Illegal use of credit card or its information without the knowledge of the owner is referred to as credit card fraud. Different credit card fraud tricks belong mainly to two groups of application and behavioral fraud [3]. Application fraud takes place when, fraudsters apply new cards from bank or issuing companies using false or other‟s information. Multiple applications may be submitted by one user with one set of user details (called duplication fraud) or different user with identical details (called identity fraud).

Behavioral fraud, on the other hand,has four principal types: stolen/lost card, mail theft, counterfeit card and „„card holder not present.

Here's the latest snapshot of credit card (and wider digital) fraud in India for FY 2024–25 (April 2024–March 2025), broken down into key metrics and trends:

## III. Difficulties of Credit Card Fraud Detection

Fraud detection systems are prune to several difficulties and challenges enumerated bellow. An effective fraud detection technique should have abilities to address these difficulties in order to achieve best performance.

- Imbalanced data: The credit card fraud detection data has imbalanced nature. It means that very small percentages of all credit card transactions are fraudulent. This cause the detection of fraud transactions very difficult and imprecise.
- Different misclassification importance: in fraud detection task, different misclassification errors have different importance. Misclassification of a normal transaction asfraud is not as harmful as detecting a fraud transaction as normal. Because in the first case the mistake in classification will be identified in further investigations.
- Overlapping data: many transactions may be considered fraudulent, while actually they are normal (false positive) and reversely, a fraudulent transaction may also seem to be legitimate (false negative). Hence obtaining low rate of false positive and false negative is a key challenge of fraud detection systems[4, 5, and 6].
- Lack of adaptability: classification algorithms are usually faced with the problem of detecting new types of normal or fraudulent patterns. The supervised and unsupervised fraud detection systems are inefficient in detecting new patterns of normal and fraud behaviors, respectively.
- Fraud detection cost: The system should take into account both the cost of fraudulent behavior that is detected and the cost of preventing it. For example, no revenue is obtained by stopping a fraudulent transaction of a few dollars [5, 7].
- Lack of standard metrics: there is no standard evaluation criterion for assessing and comparing the results of fraud detection systems.

## IV. Credit Card Fraud Detection Techniques

Table II. Advantages and Disadvantages of Fraud Detection Methods

| Techniques | | Advantages | Disadvantages |
|---|---|---|---|
| **Artificial Neural Network (ANN)** | | Ability to learn from the past/lack of need to be reprogrammed/ Ability to extract rules and predict future activities based on the current situation/ High accuracy/ Portability/ high speed in detection/ the ability to generate code to be used in real-time systems/ the easiness to be built and operated/ Effectiveness in dealing with noisy data, in predicting patterns, in solving complex problems, and in processing new instances/Adaptability /Maintainability /knowledge discovery and data miming | Difficulty to confirm the structure/high processing time for large neural networks and excessive training/ poor explanation capability/ difficult to setup and operate/high expense/ non numerical data need to be converted and normalized/Sensitivity to data format. |
| **Artificial Immune System (AIS)** | | High capability in pattern recognition/powerful in Learning and memory/Self-organization/ easy in integration with other systems/dynamically changing coverage/ self Identity/ multilayered/ has diversity/ noise tolerance/ fault tolerance/ predator-prey dynamics/ Inexpensive / no need to training phase in DCA. | Need high training time in NSA/ poor in handle missing data in ClonalG and NSA |
| **Genetic Algorithm** | | Works well with noisy data/easy to integrate with other systems/ usually combined into other techniques to increase the performance of those techniques and optimize their parameters/ easy in build and operate/In expensive/fast in detection/ Adaptability/Maintainability/knowledge discovery and data miming | Requires extensive tool knowledge to set up and operate and difficult to understand. |
| **Hidden Markov Model (HMM)** | | Fast in detection | Highly expensive/ low accuracy/not scalable to large size data sets |
| **Support Vector Machines (SVM)** | | SVMs deliver a unique solution, since the optimality problem is convex/by choosing an appropriate generalization grade, SVMs can be robust, even when the training sample has some bias. | Poor in process largedataset/expensive/has low speed of detection/ medium accuracy/lack of transparency of results |
| **Bayesian Network** | | High processing and detection speed/high accuracy | Excessive training need/ expensive |
| **Fuzzy Logic Based System** | **Fuzzy Neural Network** | Very fast in detection/good accuracy | Expensive |
| | **Fuzzy Darwinian System** | Very high accuracy/ Maintainability | Has very low speed in detection/ High expensive |

| | | |
|---|---|---|
| **Expert System** | Easy to modify the KB/ easy to develop and build the system/ easy to manage complexity or missing information/high degree of accuracy/ explanation facilities/good performance/Rules from other techniques such as NN and DT can be extracted, modified, and stored in the KB. | Poor in handling missing information or unexpected data values/poor in process different data types /knowledge representation languages do not approach human flexibility/ poor in build and operate/ poor in integration |
| **Inductive logic programming (ILP)** | Powerful in process different data types/ powerful modeling language that can model complex relationships/powerful in handle missing data | Has low predictive accuracy/extremely sensitive to noise/ their performance deteriorates rapidly in the presence of spurious data. |
| **Case based reasoning (CBR)** | Useful in domain that has a large number of examples/ has the ability to work with incomplete or noisy data/effective/ flexible/ easy to update and maintain/ can be used in a hybrid approach. | May suffer from the problem of incomplete or noisy data. |
| **Decision tree (DT)** | High flexibility/good haleness/ explainable/easy to implement/easy to display and to understand | Requirements to check each condition one by one. In fraud detection condition is transaction. |

The credit card fraud detection techniques are classified in two general categories: fraud analysis (misuse detection) and user behavior analysis (anomaly detection).

The first group of techniques deals with supervised classification task in transaction level. In these methods, transactions are labeled as fraudulent or normal based on previous historical data. This dataset is then used to create classification models which can predict the state (normal or fraud) of new records. There are numerous model creation methods for a typical two class classification task such as rule induction [1], decision trees [2] and neural networks [3]. This approach is proven to reliably detect most fraud tricks which have been observed before [4], it also known as misuse detection. The second approach deals with unsupervised methodologies which are based on account behavior. In this method a transaction is detected fraudulent if it is in contrast with user‟s normal behavior. This is because we don‟t expect fraudsters behave the same as the account owner or be aware of the behavior model of the owner [5].To this aim, we need to extract the legitimate user behavioral model (e.. user profile) for each account and then detect fraudulent activities according to it. Comparing new behaviors with this model, different enough activities are distinguished as frauds. The profiles may contain the activity information of the account; such as merchant types, amount, location and time of transactions, [6].This method is also known as anomaly detection. In this section we will introduce main advantage and disadvantage of each approach.

In order to best comprise in fraud detection techniques we have been summarizes the advantages and disadvantages of the mentioned techniques, which demonstrated in Table 1. It is important to make a point that primary version of this Table presented in [19]. Finally, Fig. 2 shows a complete classification of fraud detection techniques.

## V. DATA SET AND EVALUATION

The mentioned methods in any field definitely need a creditable data set to test upon it, and examine efficiency in compare to other‟s related work. The lack of publicly available database has been a limiting factor for the publications on financial fraud detection [21], particularly credit card transactions. On the other hand, credit card is inherently private so, creating a proper data set for this purpose is very difficult and there are no standard techniques to do this.

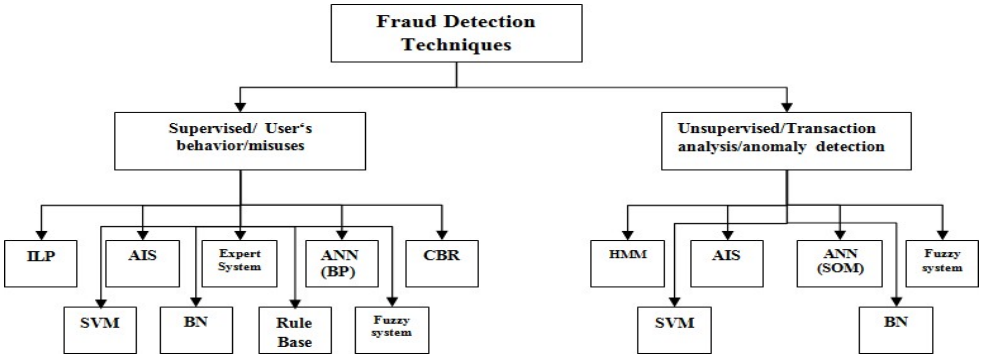


Fig 1. A complete classification of credit card fraud detection techniques

Also, there is no universal corpus for credit card. Altogether, some works build their own data set for evaluation [22], [24]. However others use data sets which are gains by certain banks or financial institutions in a specific time window [21], [20], [25], [23], [26], and [27].
Table2 will be present some credit card fraud detection research which had used real or synthetically generated dataset

TABLE III. DETAILS OF DATASET USED BY RESEARCHERS

| Collection form | Amount | Used in | Methods |
|---|---|---|---|
| Large Brazilian bank, with registers within time window between Jul/14/2004 through Sep/12/2004. (Real Data set) | 41647 transactions/ 3.14% fraudulent transactions | Manoel Fernando, Alonso Gadi et al. (2008) | AIS |
| Financial institute in Ireland (WebBiz) (Real Data set) | 4 million transactions from 462279 unique customers/ 5417 fraudulent transactions | Anthony Brabazon et al. (2010) | AIS |
| Hong kong bank, with registers within time window between January 2006 to January 2007 (13 month) (Real Data set) | 50 million credit card transactions on about one million (1,167,757 credit cards) credit cards from a single country | C. Paasch (2007) / Siddhartha Bhattacharyya et al. (2010) | ANN tuned by genetic algorithm/ Data mining techniques |
| Chase Bank and First Union Bank (Real Data set) | Each bank supplied 500,000 records spanning one year with/ 20% fraud and 80% non fraud distribution for Chase Bank/ 15% versus 85% for First Union Bank | Philip K. Chan (1999) | Data mining techniques |
| Major US bank (Real Data set) | 6000 credit card data with 64 predictor variables plus 1 class variable, 84% of the data are normal accounts and 16% are fraudulent accounts | G. Kou, et al. (2005) | Multiple criteria linear programming |
| Large Australian bank (Real Data set) | 640361 total transactions, with 21746 credit cards | Nicholas Wong et al.(2012) | AIS |
| Vesta Corporation (Vesta corporation is an innovator and worldwide leader in virtual commerce with headquarter in Portland, Oregon, USA) (Real Data set) | 206,541 transactions, 204,078 transaction are normal and 2463 are fraudulent | John Zhong Lei (2012) | ANN |
| Mellon Bank (Real Data set) | 1,100,000 transactions/ authorized in two month period | SushmitoGhosh(1994) | ANN |
| Synthetically generated Data | 320000000 transactions/ 1050 credit card/ 42 features | M. Hamdiozcelik et al. (2010) | GA |
| Synthetically generated Data | 1000000 transactions/ 20 features | K.RamaKalyani et al. (2012) | GA |
| Synthetically generated Data | 10000 transactions | Tao guo et al. (2008) | Data mining techniques |
| Synthetically generated data | The data are extracted into a flat file from SQL server database containing sample Visa Card transactions and then preprocessed. | MubeenaSyeda et al. (2002) | ANN |

TABLE IV. THE COMMON ATTRIBUTES IN MOST DATASET

| Row | Attribute Name | Description |
|---|---|---|
| 1 | Posting date | Date when transaction was posted to the accounts |
| 2 | Merchant Category Code (MCC) | a code devote to each goods |
| 3 | Transaction Date and Time | Date and Time which the transaction was actually performed |
| 4 | Transaction status | status of transaction success/fail |
| 5 | Transaction Place | place of transaction (usually determine by IP Address) |
| 6 | Money Amount | Amount of Money |
| 7 | Transaction Type | Type of transaction payment/deposit/transfer and etc |
| 8 | customer identification | The identification code which advocate to each customer |
| 9 | Scheme | The type of credit card used, e.g. MasterCard, Visa, etc. |

Primary attributes are attributes of credit card transactions which are available in the most datasets. We present these mentioned attributes in Table3.
The volume of fraud in every dataset is different. This might be because of the different security protocols used by different organizations and banks and so on. Whatever the reason is, this fact causes different fraud characteristics on each dataset, which affects the performance of the fraud detection system.

Therefore considering the dataset‟s characteristics will help the system having more precise results.
A proper data set is a data set which covers various fraud and several attributes of customer profile or behavior. We believe that the contribution of attributes is a critical factor that should be considered.

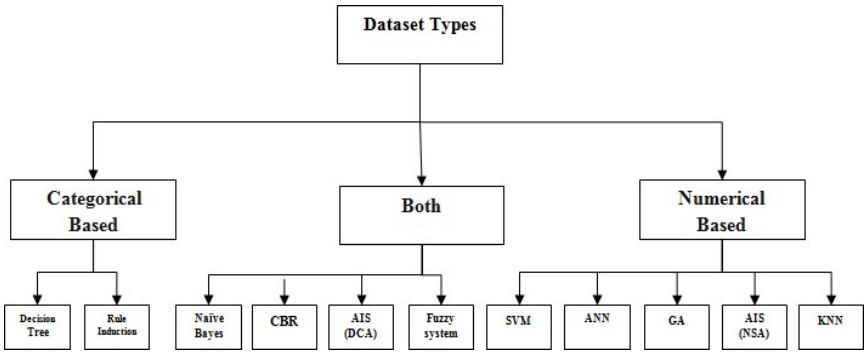


Fig. 2 A complete classification of the dataset‟s attribute

Also, a proper data set should be able to reflect the real world of credit card. Credit card transaction datasets usually divided in to two types: numerical and categorical attributes. In statistics, categorical data is a statistical data type consisting of categorical variables, used for observed data whose value is one of a fixed number of nominal categories, or for data that has been converted into that form, for example as grouped data. However numeric data are numbers like age, cost, etc. In fraud detection applications customer‟s gender and name are the typical numerical attribute, and categorical attributes are those like merchant category code, date of transaction, amount of transaction and etc. Some of these categorical variables can, depending on the dataset, have hundreds and thousands of categories. Finally, Fig. 3shows a complete classification in two groups: numerical and categorical attributes which is suitable for each algori

*Evaluation*

There are a variety of measures for various algorithms and these measures have been developed to evaluate very different things. So it should be criteria for evaluation of various proposedmethod. False Positive (FP), False Negative (FN), True Positive (TP), and True Negative (TN) and the on between them are quantities which usually adopted by credit card fraud detection researcher to compare the accuracy of different approaches. The definitions of mentioned parameters are presented below:

- FP: the false positive rate indicates the portion of the non-fraudulent transactions wrongly being classified as fraudulent transactions.
- FN: the false negative rate indicates the portion of the fraudulent transactions
- wrongly being classified as normal transactions.
- TP: the true positive rate represents the portion of the fraudulent transactions correctly being classified as fraudulent transactions.
- TN: the true negative rate represents the portion of the normal transactions correctly being classified as normal transactions.

Table 4shows the details of the most common formulas which are used by researchers for evaluation of their proposed methods. As can be seen in this table some researchers had been used multiple formulas in order to evaluated their proposed model.
The aim of all algorithms and techniques is to minimize FP and FN rate and maximize TP and TN rate and with a good detection rate at the same time.

## VI. OPEN ISSUES

While credit card fraud detection has gained wide-scale attention in the literature, there are yet some issues (a number of significant open issues) that face researchers and have not been addressed beforeadequately. Wehope this overview focuses the direction of future research to provide more efficient and trustable fraud detection systems. These issues are as follow:

*Nonexistence of standard and comprehensive credit card benchmark or dataset*

Credit card is inherently private property, so creating a proper benchmark for this purpose is very difficult. Incomplete datasets can cause fraud detection system to learn fraud tricks or normal behavior partially. On the

other hand, lack of a standard dataset makes comparison of various techniques problematic or impossible. Many researchers used datasets that are only permitted to authors and cannot be published in order to privacy considerations.

TABLE IV. EVALUATION CRITERIA FOR CREDIT CARD FRAUD DETECTION

| Measure | Formula | Description | Used in |
|---|---|---|---|
| Accuracy (ACC)/Detection rate | TN + TP/TP + FP + FN + TN | Accuracy is the percentage of correctly classified instances. It is one the most widely used classification performance metrics | Nicholas Wong et al. (2012) [30], Manoel Fernando, et al. (2008)[21], soltani et al. [8],A. Brabazon et al. (2011) [35], Siddhartha et al. (2008) [23], P. Ravisankar et al. (2011) [31], AbhinavSrivastava et al. (2008) [29], John Zhong et al. (2012) [26], Qibei Lu et al. (2011) [32], AmlanKundu (2006) [28] |
| Precision/Hit rate | TP/TP + FP | Precision is the number of classified positive or fraudulent instances that actually are positive instances. | Manoel Fernando, et al. (2008)[36], Siddhartha et al. (2008) [50], John Zhong et al. (2012) [26], Qibei Lu et al. (2011) [32], AmlanKundu (2006) [28] |
| True positive rate/Sensitivity | TP/TP + FN | TP (true positive) is the number of correctly classified positive or abnormal instances. TP rate measures how well a classifier can recognize abnormal records. It is also called sensitivity measure. In the case of credit card fraud detection, abnormal instances are fraudulent transactions. | Maes S. et al. (2002) [5], Siddhartha et al. (2008) [23], Tao guo et al. (2008) [24], P. Ravisankar et al. (2011) [31], AbhinavSrivastava et al. (2008) [29], John Zhong et al. (2012) [26], Qibei Lu et al. (2011) [32], AmlanKundu (2006) [28] |
| True negative rate /Specificity | TN/TN + FP | TN (true negative) is the number of correctly classified negative or normal instances. TN rate measures how well a classifier can recognize normal records. It is also called specificity measure. | Siddhartha et al. (2008) [23], Philip K. Chan (1999) [26], Tao guo et al. (2008) [24], P. Ravisankar et al. (2011) [31], John Zhong et al. (2012) [26], Maes S. et al. (2002) [5], Qibei Lu et al. (2011) [32], AmlanKundu (2006) [28] |
| False positive rate (FPR) | FP/FP+TN | Ratio of credit card fraud detected incorrectly | Nicholas Wong et al. (2012) [30], soltani et al. [8], Maes S. et al. (2002) [5], Philip K. Chan (1999) [26], AbhinavSrivastava et al. (2008) [29], John Zhong et al. (2012) [26], Qibei Lu et al. (2011) [32], AmlanKundu (2006) [28] |
| ROC | True positive rate plotted against false positive rate | Relative Operating Characteristic curve, a comparison of TPR and FPR as the criterion changes | Manoel Fernando, et al. (2008)[36], Maes S. et al. (2002) [5], Tao guo et al. (2008) [24],John Zhong et al. (2012) [26], Qibei Lu et al. (2011) [32],AmlanKundu (2006) [28] |
| Cost | Cost = 100 * FN + 10 * (FP +TP) | | Manoel Fernando, et al. ,(2008)[36], soltani et al. [8], Philip K. Chan (1999) [26], Qibei Lu et al. (2011) [32] |
| F1-measure | 2 × (Precision ×Recall)/(Precision +Recall) | Weighted average of the precision and recall | Siddhartha et al. (2008) [23] |

*A. Nonexistence of standard algorithm*

There is not any powerful algorithm known in credit card fraud literature that outperforms all others.Eachtechnique hasits own advantages and disadvantages as stated in previous sections. Combining these algorithms to support each other‟s benefits and cover their weaknesses would be of great interest.

*B. Nonexistence of suitable metrics*

The limitation of good metrics in order to evaluate the results of fraud detection system is yet an open issue. Nonexistence of such metrics causes incapability of researchers and practitioners in comparing different approaches and determining priority of most efficient fraud detection systems.

*C. Lack of adaptive credit card fraud detection systems*

Although lots of researches have been investigated credit card fraud detection field, there are none or limited adaptive techniques which can learn data stream of transactions as they are conducted. Such a system can update

its internal model and mechanisms over a time without need to be relearned offline. Therefore, it can add novel frauds (or normal behaviors) immediately to model of learn fraud tricks and detect them afterward as soon as possible.

## REFERENCES


[1] KhyatiChaudhary, JyotiYadav, BhawnaMallick, " A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications Volume 45– No.1 2012.

[2] Michael Edward Edge, Pedro R, Falcone Sampaio, "A survey of signature based methods for financial fraud detection", journal of computers and security, Vol. 28, pp 3 8 1 – 3 9 4, 2009.

[3] Linda Delamaire, Hussein Abdou, John Pointon, "Credit card fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2, 2009.

[4] Salvatore J. Stolfo, David W. Fan, Wenke Lee and Andreas L. Prodromidis; "Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results"; Department of Computer Science- Columbia University; 1997.

[5] Maes S. Tuyls K. Vanschoenwinkel B. and Manderick B.; "Credit Card Fraud Detection Using Bayesian and Neural Networks"; Vrije University Brussel – Belgium; 2002.

[6] Andreas L. Prodromidis and Salvatore J. Stolfo; "Agent-Based Distributed Learning Applied to Fraud Detection"; Department of Computer Science- Columbia University; 2000.

[7] Salvatore J. Stolfo, Wei Fan, Wenke Lee and Andreas L. Prodromidis; "Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAM Project"; 0-7695-0490-6/99, 1999 IEEE.

[8] Soltani, N., Akbari, M.K., SargolzaeiJavan, M., "A new user-based model for credit card fraud detection based on artificial immune system," Artificial Intelligence and Signal Processing (AISP), 2012 16th CSI International Symposium on., IEEE, pp. 029-033, 2012.

[9] S. Ghosh and D. L. Reilly, "Credit card fraud detection with a neural-network", Proceedings of the 27th Annual Conference on System Science, Volume 3: Information Systems: DSS/ Knowledge- Based Systems, pages 621-630, 1994. IEEE Computer Society Press.

[10] MasoumehZareapoor, Seeja.K.R, M.Afshar.Alam, "Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria", International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, 2012.

[11] Fraud Brief – AVS and CVM, Clear Commerce Corporation, 2003, http://www.clearcommerce.com.

[12] All points protection: One sure strategy to control fraud, Fair Isaac, http://www.fairisaac.com, 2007.

[13] Clear Commerce fraud prevention guide, Clear Commerce Corporation, 2002, http://www.clearcommerce.com.

[14] RaghavendraPatidar, Lokesh Sharma, "Credit Card Fraud Detection Using Neural Network", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, 2011.

[15] Holland, J. H. "Adaptation in natural and artificial systems." Ann Arbor: The University of Michigan Press. (1975).

[16] E. Aleskerov, B. Freisleben, B. Rao, „CARDWATCH: A Neural Network-Based Database Mining System for Credit Card Fraud Detection", the International Conference on Computational Intelligence for Financial Engineering, pp. 220-226, 1997.

[17] SushmitoGhosh, Douglas L. Reilly, Nestor, "Credit Card Fraud Detection with a Neural- Network", Proceedings of 27th Annual Hawaii International Conference on System Sciences, 1994.

[18] Moody and C. Darken, "Learning with localized receptive fields." in Proc. of the 1988 Connectionist Models Summer School, D.S. Touretzky, G.E. Hinton and T.J. Sejnowski, eds., Morgan Kaufmann Publishers, San Mateo, CA, 1989, pp. 133-143.

[19] Adnan M. Al-Khatib, "Electronic Payment Fraud Detection Techniques", World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 4, 137-141,2012

[20] V. Cutello, G. Narzisi, G. Nicosia, M. Pavone, "Clonal Selection Algorithms: A Comparative Case Study Using Effective Mutation Potentials", proceeding of International Conference on ArtificialImmune Systems (ICARIS), pp. 13-28, 2005.

[21] M. Gadi, X. Wang, A. Lago, "Credit Card Fraud Detection with Artificial Immune System", Springer, 2008.

[22] EkremDuman, M. HamdiOzcelik," Detecting credit card fraud by genetic algorithm and scatter search", Expert Systems with Applications 38 (2011) 13057–13063.

[23] Siddhartha Bhattacharyya, SanjeevJha, KurianTharakunnel, J. Christopher Westland "Data mining for credit card fraud: A comparative study". Elsevier, Decision Support Systems (2011), 50; (602–613).

[24] T. Guo, G.yang LI, "neural data mining for credit card fraud detection", Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, 2008.

[25] C. Paasch, Credit Card Fraud Detection Using Artificial Neural Networks Tuned by Genetic Algorithms, Hong Kong University of Science and Technology (HKUST), Hong Kong, DoctoralDissertation, 2007.

[26] Philip K. Chan, Wei Fan, Andreas L. Prodromidis, and Salvatore J. Stolfo," Distributed DataMining in Credit Card Fraud Detection", international conference on intelligent systems",1999.

[27] G. Kou, Y. Peng, Y. Shi, M. Wise, W. Xu, Discovering credit cardholders" behavior by multiple criteria linear programming, Annals of Operations Research 135, (2005) 261–274.

[28] AmlanKundu, ShamikSural, and A.K. Majumdar, “Two-Stage Credit Card Fraud DetectionUsing Sequence Alignment”, ICISS 2006, LNCS 4332, pp. 260–275, 2006.
[29] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar. “Credit Card Fraud Detection using Hidden Markov Model”, IEEE Transactions on dependable and secure computing, Volume 5; (2008) (37-48).
[30] Nicholas Wong, Pradeep Ray, Greg Stephens & Lundy Lewis (2012). “Artificial immune systems for the detection of credit card fraud: an architecture, prototype and preliminary results”,International journal of information systems, Volume 22, pp 53–76.
[31] P. Ravisankar, V. Ravi, G. RaghavaRao, I. Bose, “Detection of financial statement fraud and Feature selection using data mining techniques” , Decision Support Systems 50 (2011) 491–500.
[32] Qibei Lu, ChunhuaJu, “Research on Credit Card Fraud Detection Model Based on Class Weighted Support Vector Machine”, Journal of Convergence Information Technology, Vol. 6, Number 1, 2011.