

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 7, July 2018

## Credit Card Fraud Detection Techniques for Modified Genetic Algorithm

Kritika Joshi<sup>1</sup>, Dr. (Mrs) Ani Thomas<sup>2</sup>

M. Tech. Scholar, Department of IT (E-Security), Bhilai Institute of Technology, Durg, India<sup>1</sup>

Professor & HOD, Department of IT, Bhilai Institute of Technology, Durg, Durg, India<sup>2</sup>

**ABSTRACT:** The use of credit cards for online purchases has increased recently thereby causing credit card fraud. Thus there is a need to detect and prevent credit card frauds. In this paper, we propose a method to detect fraud in credit card transactions using Genetic Algorithms. The aim is to develop a search heuristic method of generating test data and to generate useful solutions to optimization and search problems. A credit card payment system is developed which is a user friendly system. It allows utilization of all the facilities provided by an online banking system including online shopping. This system also stores all the user details in a secure manner. Thus using this system a user can perform banking operations and purchase items online without credit card fraud.

**KEYWORDS:** Genetic algorithm, data mining, heuristic approach, fraudulent transactions

### I. INTRODUCTION

The increase usage of credit cards for online purchases as well as common purchases causes a credit card fraud. In the electronic payment system mode, fraud transactions are climbing on the regular basis. The users need to wait for hours at the bank. Instead they can just take the service of Online Credit Card Fraud Detection System. This paper is to propose a credit card fraud detection system using genetic algorithm. Genetic algorithms are evolutionary algorithms which aim at obtaining better solutions as time progresses and technically to eliminate the fraud, a high importance has given to develop efficient and secure electronic payment system to detect whether a transaction is fraudulent or not.

Credit card fraud detection payment system presents to find the detection of credit card fraud mechanism and examines the result based on the principles of genetic algorithm. The advantage of detecting fraud is to increase security for both credit card companies and their clients. The prevention of fraud transactions are not performed from being cleared; the company must accept the financial cost of that transaction. The aim is to develop a method of generating test data and to detect fraudulent transaction with this algorithm. This algorithm is an different technique and acceptable based on the principles of genetic and natural selection, heuristic used to solve high complexity computational problem. This algorithm is a different technique and evolutionary search based on the principles of genetic and natural selection are used to solve high complexity computational problems.

A credit card is a thin handy plastic card that contains identification information such as a signature or picture, and authorizes the person named on it to charge purchases or services to his account - charges for which he will be billed periodically. Today, the information on the card is read by automated teller machines (ATMs), store readers, bank and is also used in online internet banking system. They have a unique card number which is of utmost importance. Its security relies on the physical security of the plastic card as well as the privacy of the credit card number. There is a rapid growth in the number of credit card transactions which has led to a substantial rise in fraudulent activities. Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card as a fraudulent source of funds in a given transaction. Generally, the statistical methods and many data mining algorithms are used to solve this fraud detection problem. Most of the credit card fraud detection systems are based on artificial intelligence, Meta learning and pattern matching. The Genetic algorithms are evolutionary algorithms which aim to obtain the better solutions in eliminating the fraud. A high importance is given to develop efficient and secure electronic payment system to detect

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 7, July 2018

whether a transaction is fraudulent or not. In this paper, we will focus on credit card fraud and its detection measures. A credit card fraud occurs when one individual uses other individuals' card for their personal use without the knowledge of its owner. When such kind of cases takes place by fraudsters, it is used until its entire available limit is depleted. Thus, we need a solution which minimizes the total available limit on the credit card which is more prominent to frauds. And, a Genetic algorithm generates better solutions as time progresses. The complete emphasis is given on developing efficient and secure electronic payment system for detecting the fraudulent.

## II. DIFFICULTIES OF CREDIT CARD FRAUD DETECTION

Fraud detection systems are prone to several difficulties and challenges enumerated below. 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 causes 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 as fraud 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 [8].

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].  
Ukraine 19% Indonesia 18% Yugoslavia 18% Malaysia 6% Turkey 9% United States 1% other country 29%  
Statistical Classification of Credit Card Fraud Occurrence  
Ukraine Indonesia Yugoslavia Malaysia Turkey United States other country 5.

Lack of standard metrics: there is no standard evaluation criterion for assessing and comparing the results of fraud detection systems.

## III. PROBLEMS WITH CREDIT CARD FRAUD DETECTION

There are lots of issues that make this procedure tough to implement and one of the biggest problems associated with fraud detection is the lack of both the literature providing experimental results and of real world data for academic researchers to perform experiments on. The reason behind this is the sensitive financial data associated with the fraud that has to be kept confidential for the purpose of customer's privacy. Now, here we enumerate different properties a fraud detection system should have in order to generate proper results:

- The system should be able to handle skewed distributions, since only a very small percentage of all credit card transactions is fraudulent.
- There should be a proper means to handle the noise. Noise is the errors that is present in the data, for example, incorrect dates. This noise in actual data limits the accuracy of generalization that can be achieved, irrespective of how extensive the training set is.

# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 7, July 2018

- Another problem related to this field is overlapping data. Many transactions may resemble fraudulent transactions when actually they are genuine transactions. The opposite also happens, when a fraudulent transactions appears to be genuine. The systems should be able to adapt themselves to new kinds of fraud. Since after a while, successful fraud techniques decreases in efficiency due to the fact that they become well known because an efficient fraudster always find a new and inventive ways of performing his job.
- There is a need for good metrics to evaluate the classifier system. For example, the overall accuracy is not suited for evaluation on a skewed distribution, since even with a very high accuracy; almost all fraudulent transactions can be misclassified.
- The system should take care of the amount of money that is being lost due to fraud and the amount of money that will be required to detect that fraud. For example, no profit is made by stopping a fraudulent transaction that is way lesser than the amount of money that will be required to detect it.

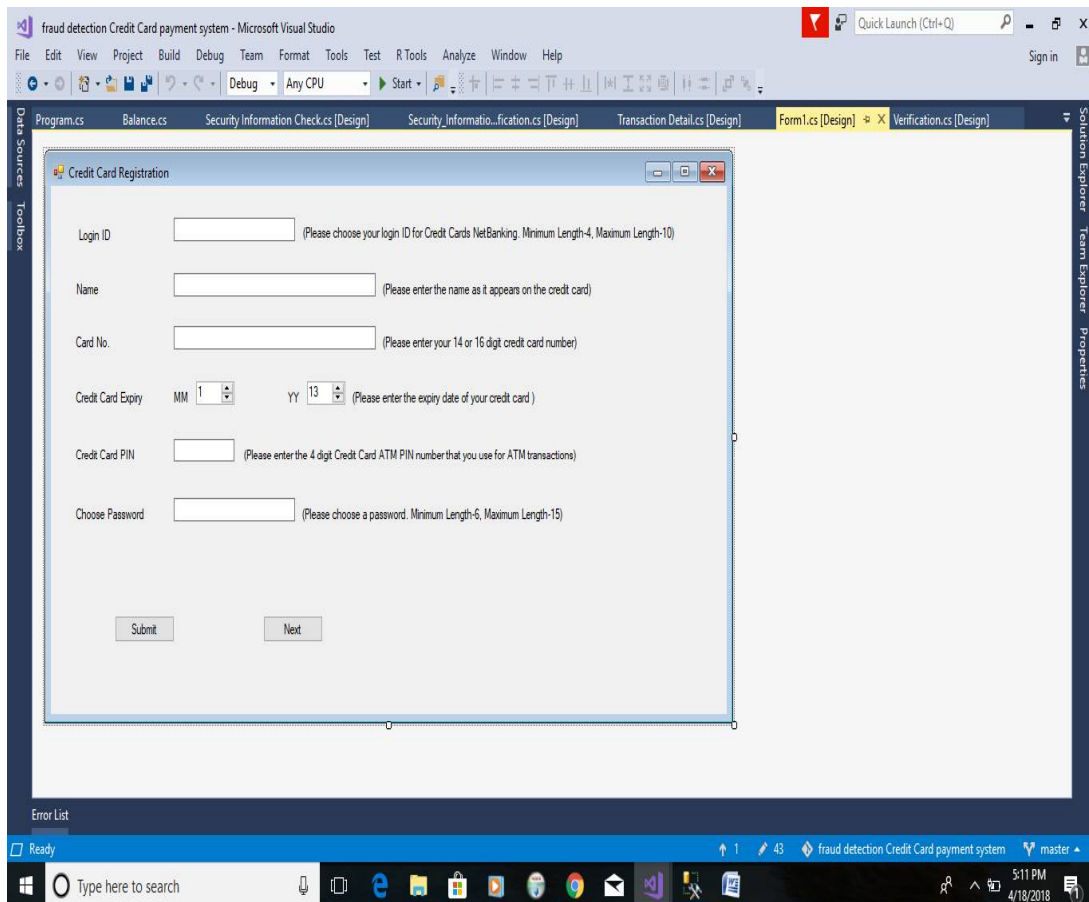
## IV. METHODOLOGY & RESULT

### Fraud Detection System Using Genetic Algorithm

The flow of fraud detection system:

Form for Sign In and Sign up

We go for Sign Up and we register



The screenshot shows a Windows application window titled "Credit Card Registration" running in Microsoft Visual Studio. The form contains the following fields and controls:

- Login ID:  (Please choose your login ID for Credit Cards NetBanking. Minimum Length-4, Maximum Length-10)
- Name:  (Please enter the name as it appears on the credit card)
- Card No.:  (Please enter your 14 or 16 digit credit card number)
- Credit Card Expiry: MM  YY  (Please enter the expiry date of your credit card)
- Credit Card PIN:  (Please enter the 4 digit Credit Card ATM PIN number that you use for ATM transactions)
- Choose Password:  (Please choose a password. Minimum Length-6, Maximum Length-15)

At the bottom of the form, there are two buttons: "Submit" and "Next". The background shows the Visual Studio IDE with various toolbars and a taskbar at the bottom.

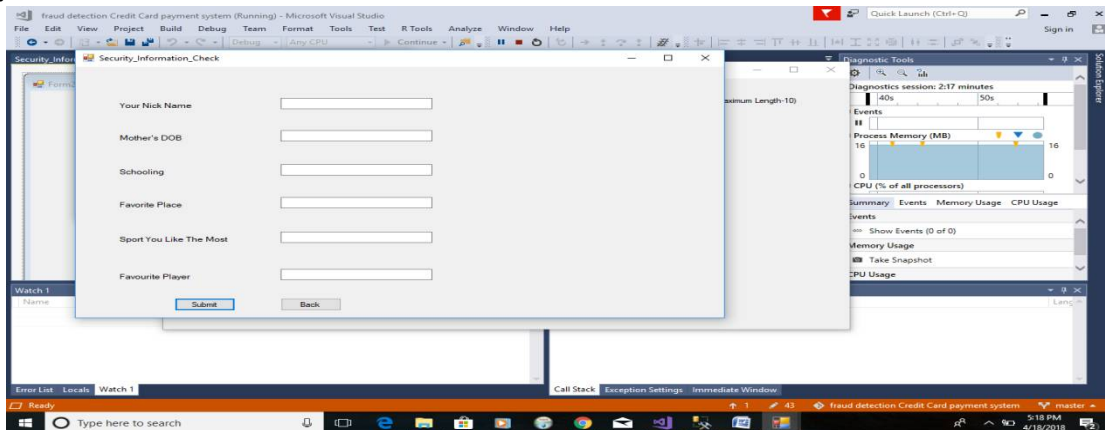
# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

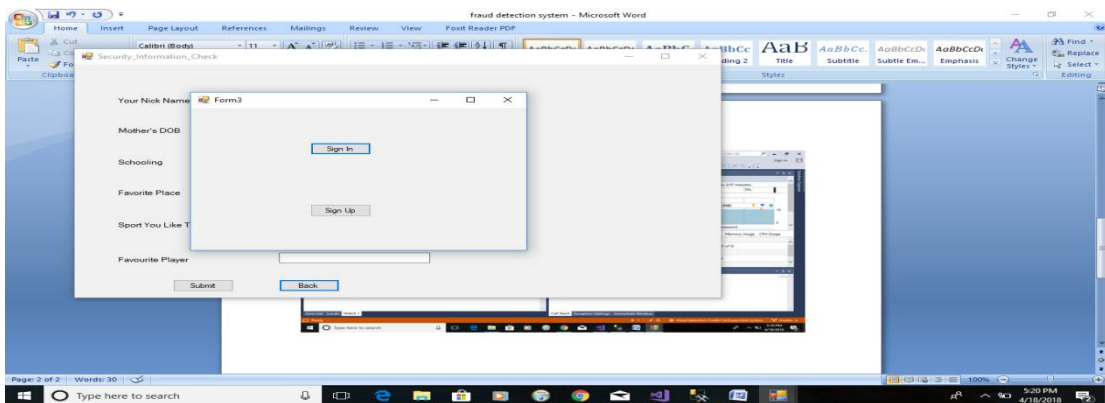
Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 7, July 2018

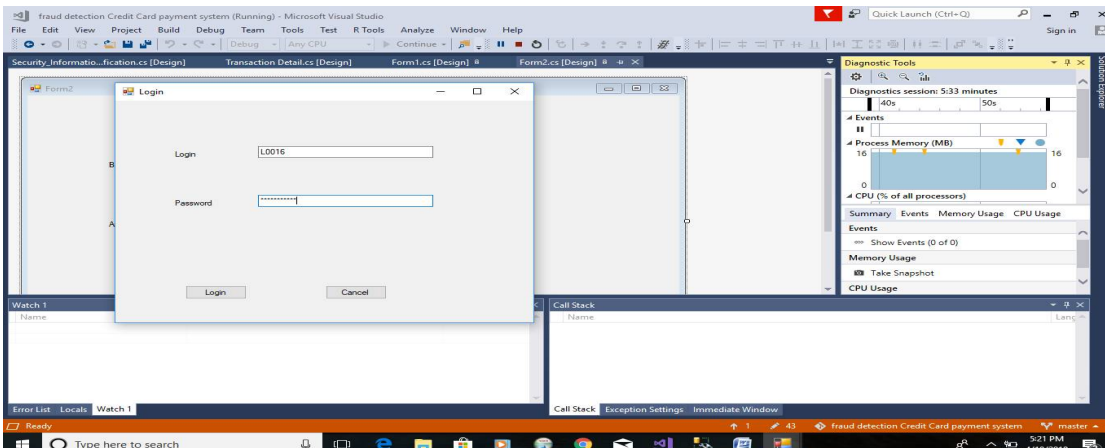
## Security Information Check:



## Back To Sign In:



## Login:



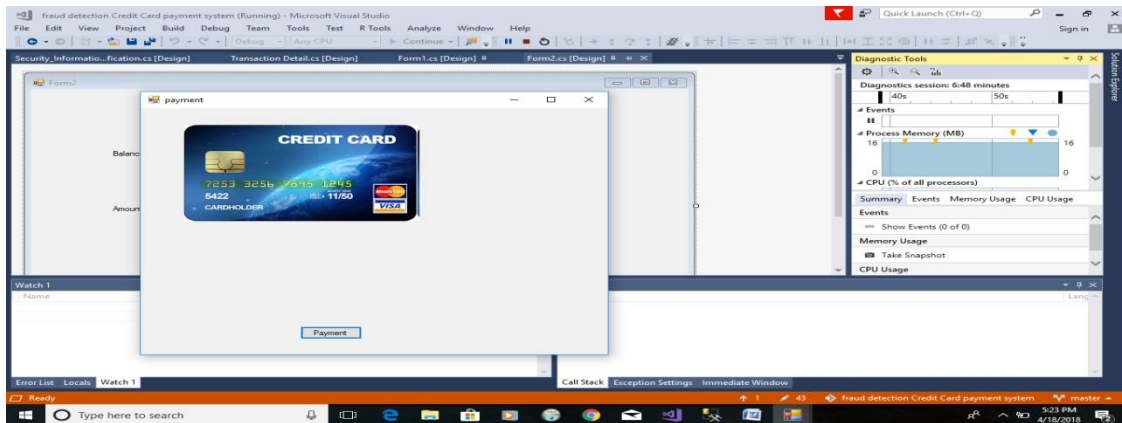
# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

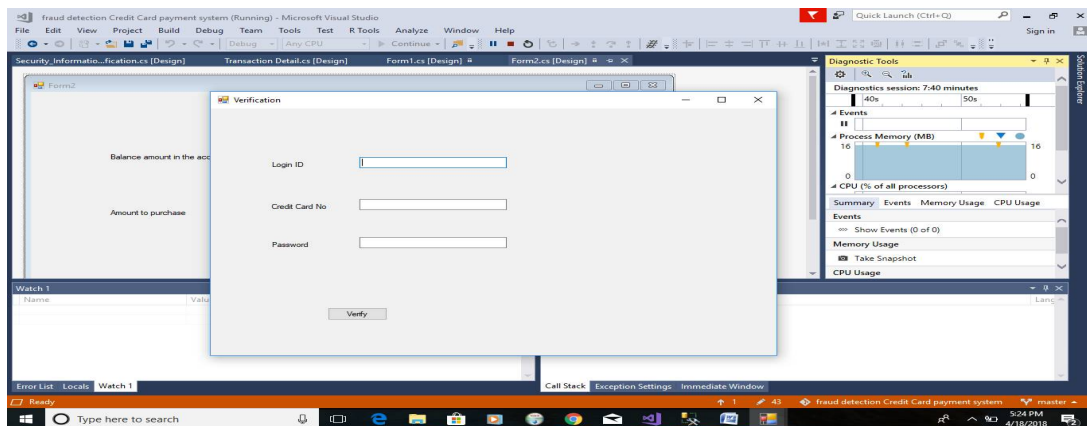
Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 7, July 2018

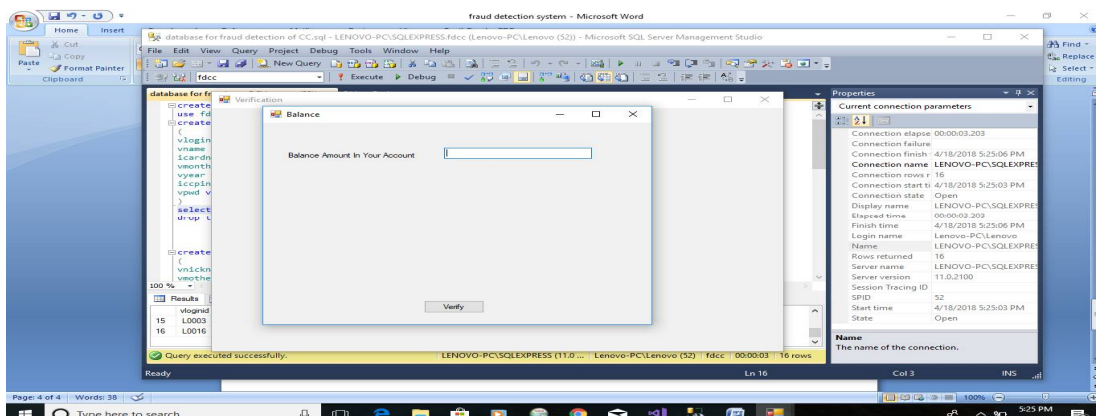
## Payment Form:



## Verification:



## Balance:



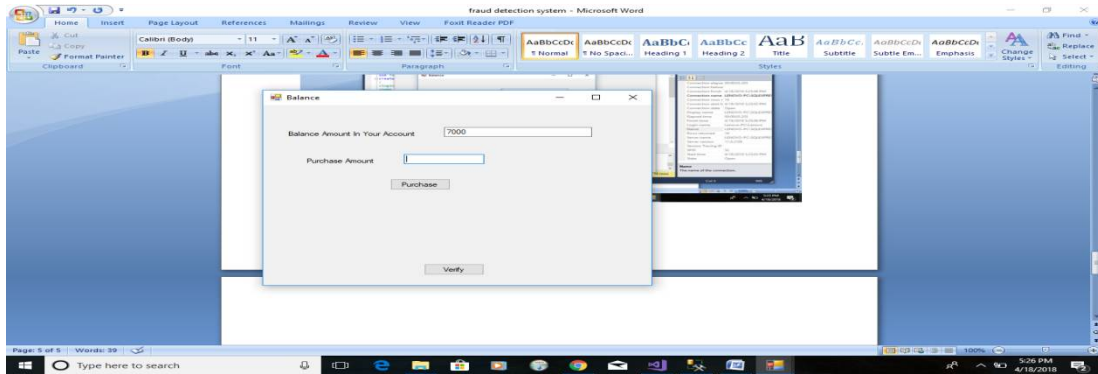
# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

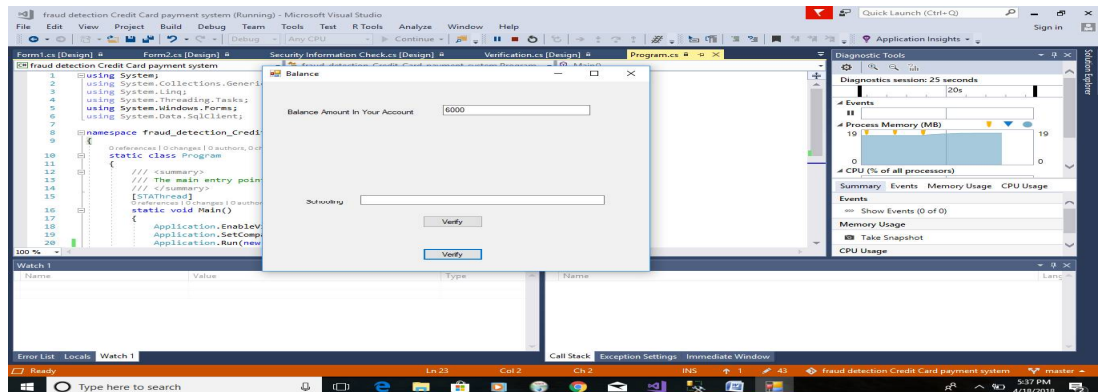
Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 7, July 2018

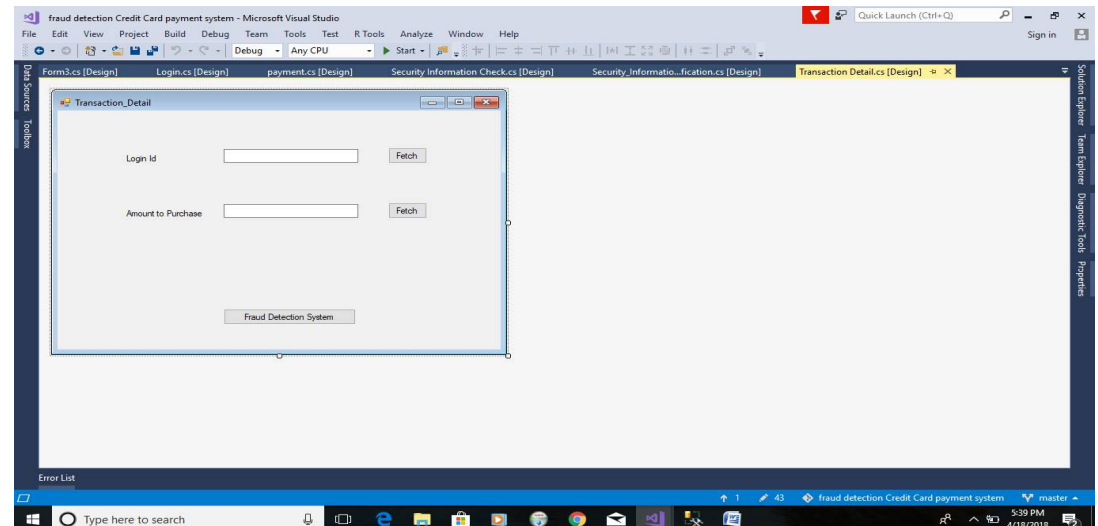
## Purchase Amount:



## If the Balance amount is not correct



## Transaction Detail:



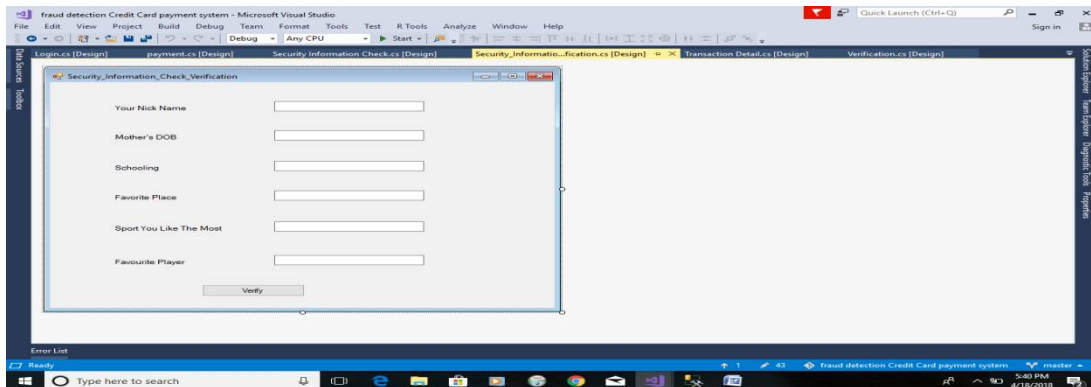
# International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: [www.ijirset.com](http://www.ijirset.com)

Vol. 7, Issue 7, July 2018

## Security Information Check Verification:



This is the last verification to check whether there is fraud.

## Update Form:

We can update the registration if needed for example if there is any mistake in entering the name we can update.

## Delete Form:

We can delete the registration details if the card is not in use.

## V. CONCLUSION

In recent years, topics such as fraud detection and fraud prevention have received a lot of attention on the research front, in particular from payment card issuers. The reason for this increase in research activity can be attributed to the huge annual financial losses incurred by card issuers due to fraudulent use of their card products. A successful strategy for dealing with fraud can quite literally mean millions of dollars in savings per year on operational costs.

Analyzing every transaction is legitimate or not is very expensive. Moreover it is also time consuming, hence it is not practically possible. Confirming whether a transaction was done by a client or a fraudster is a better option, but by phoning all card holders is cost prohibitive if it is check in all transactions. Further it might also lead to customer dissatisfaction.

## REFERENCES

- [1] K. Rama Kalyani, D. Uma Devi, "Fraud Detection of Credit Card Payment System by Genetic Algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 7, July-2012.
- [2] Vishal Vatsal, Shamik Sural, and A.K. Majumdar, "A Game-Theoretic Approach to Credit Card Fraud Detection", ICISS 2005, LNCS 3803, pp. 263– 276, 2005, Springer-Verlag Berlin Heidelberg 2005.
- [3] E. Aleskerov, B. Freisleben, B. Rao, CARDWATCH: "A Neural Network Based Database Mining System for Credit Card Fraud Detection," Proc. Computational Intelligence for Financial Engineering (CIFEr), 220-226, 1997.
- [4] P.K. Chan, W. Fan, A.L. Prodromidis, S.J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," IEEE Intelligent Systems, 67-74, 1999.
- [5] M. Syeda, Y.Q. Zhang, Y. Pan, "Parallel Granular Neural Networks for Fast Credit Card Fraud Detection", Proc. FUZZ-IEEE 2002 Int. Conference, 572- 577, 2002.
- [6] Min-Jung Kim and Taek-Soo Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection", H. Yin et al. (Eds.): IDEAL 2002, LNCS 2412, pp. 378-383, 2002. © Springer-Verlag Berlin Heidelberg 2002.
- [7] Yuchun Tang, Member, IEEE, Yan-Qing Zhang, Member, IEEE, V. Nitesh. Chawla, Member, IEEE, and Sven Krasser, Member, "SVMs Modeling for Highly Imbalanced Classification", IEEE 2009.
- [8] PiyapholPhoungphol, Yanqing Zhang, YichuanZha, and BismitaSrichandan, "Multiclass SVM with Ramp Loss for Imbalanced Data Classification", IEEE International Conference on Granular Computing, (2012).

## International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

Visit: [www.ijirset.com](http://www.ijirset.com)

**Vol. 7, Issue 7, July 2018**

- [9] J. Buhl, D. J. T. Sumpter, I. D. Couzin, J. J. Hale, E. Despland, E. R. Miller, and S. J. Simpson, "Reports from disorder to order in marching locusts," *Science*, vol. 312, pp. 1402-1406, 2006.
- [10] SuvasiniPanigrahi, AmlanKundu, Shamik Sural, A.K. Majumdar, "Credit Card Fraud Detection: A Fusion Approach Using Dempster-Shafer Theory And Bayesian Learning", *Information Fusion*, 10, 354–363, (2009).
- [11] Arturo Elías, Alberto Ochoa-Zezzatti, Alejandro Padilla, and Julio Ponce, "Outlier Analysis for Plastic Card Fraud Detection a Hybridized and Multi Objective Approach", Springer-Verlag Berlin Heidelberg, (2011).
- [12] Estabrooks, A., Jo, T., Japkowicz, N. "A Multiple Resampling Method for Learning from Imbalances Data Sets", *Computational Intelligence* 20(1) (2004)
- [13] J.Stolfo, J., D.W Fan, W. Lee, A.L Prodromidis, "Credit card fraud detection using meta-learning: Issues and initial results", In: *AAAI Workshop on AI Approaches to Fraud Detection and Risk Management*, AAAI Press, pp. 83– 90., Menlo Park, CA (1997)
- [14] C. Phua, A.Damminda,,V. Lee, "Minority Report in Fraud Detection: Classification of Skewed Data." *Sigkdd Explorations* 6(1) (2004) Dynamic passcode authentication.
- [15] V. Srikanth, Dr. R. Dhanapal, "A Business Review of E-Retailing in India" ,*International Journal of Business research and Management (IJBRM)*,Vol 1,Issue 3,PP 105-121 ,2011.
- [16] A Shamir, A. Secureclick, "A web payment system with disposable credit card numbers" In: Syverson, P.F. (ed.) *FC 2001. LNCS*, Springer, vol. 2339, pp. 232–242., Heidelberg (2002)
- [17] A. Singh, A.L.M dos Santos, "Grammar based off line generation of disposable credit card numbers" In: *SAC 2002: Proceedings of the 2002 ACM symposium on Applied computing*, ACM Press, pp. 221–228., New York (2003).