ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 12, December 2019

Credit Card Fraud Detection

Aditi Kulkarni[1], Pooja Nangare [2], Saba Latif[3], Rani Molkire[4]

Department of Computer, NBN Sinhgad school of Engineering, Savitribai Phule Pune University, Pune, Maharastra, India

ABSTRACT: Due to the rise and rapid growth in credit card transaction the amount of credit card fraud increases day by day. Large amount of fake users do transaction using credit card details. There is no facility to track the fake users after completion of transactions. There is a lot of money wastage of users while such type of transaction is done. So to avoid such type of transaction we develop the smart application who can prevent the type of credit card fraud transaction. User adds the credit data, bank data to the MySQL central database. This is all valid data captured by users from appropriate bank and credit card. Three stage security systemsis added in this system to avoid fraud transaction. Amount verification, face recognition and pin system is designed to do all type of verification. Location tracking is also provided to track the fraud users in this system.

KEYWORDS: Data mining, MySQL database, Gps, Authentication, image processing, open CV

I. INTRODUCTION

In current system, which does not require fraud manner and yet is able to detect frauds by considering a cardholder's spending habit.The details of items purchased in Individual written account are usually not known to any Fraud Detection System running at the bank that issues credit cards to the cardholders henceaddressing this problem. Another important advantage of this application -based approach is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine. An FDS runs at a credit card issuing bank. User has to submit all the relevant data in the system database so it will be easily accessible by next transaction system. Credit card details such as credit card number, credit card type, pin number, holder name, transaction id all the information collected by system admin. Bank details also required to handle all transaction process with the specific users. Amount verification done by users through sending SMS. If users detect that transaction done by other users it has the option to block the account. Face recognition done by system to detect proper user if fraud user detected system will not provide next access to user. Credit card pin validation is provided to final stage security validation. If fraud is done by any users the location tracking system is used using GPS technology to track the fraud user location. Overall system is designed to handle all the fraud related task[6][11].

II. LITERATURE SURVEY

Fraud act as the wrongful or criminal deception intended to result in financial or personal benefit. It is a deliberate act that is against the law, rule or policy with a aim to attain unauthorized financial benefit. Lokesh Sharma and RaghavendraPatidar works on emerging technology Neural Network that can be used in banking or financial areas to detect fraud. They have been successfully applied to detect legitimate or fraudulent transactions.Association Rules can be applied to detect fraud.LindaDelamaire and Pointon et.al use the association rules to extract knowledge so that normal behavior pattern may be obtained in unlawful transactions.This proposed Methodology has been applied on data about credit card fraud of the most important retail companies in Chile. In the area of fraud detection, neural network like feed forward neural network with back propagation have found immense application. Usually such applications need to know previous data and on the behalf of this previous data they detect the fraud.
On super-resolution most of the papers are presented.We have taken the reference of different papers and some of papers are explained here. In the paper written by Swati.D.Shirke and Dr. C. Rajabhushnam [6] the technique which is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 12, December 2019

used to get the information from poor quality iris images is nothing but the superb-resolution technique.We can achieve the feature domain and pixel domain by using super-resolution algorithm.

Another statistically approach is feed forward network in which there is certain kind of relationship is found between user data and other parameters to get. The result. By the help of this approach or by using SOM, data can be filter out to analyze customer behavior (John T.S Kuah, M.Sriganesh)[11]. Another new emerging technology of Credit card fraud detection is based on the genetic algorithm and scatter search.

EkremDuMan,MHamdiOzclik[12] has publish an approach that was based on genetic algorithm and scattering search. In this approach, each transaction is scored and based on these score transactions are divided into fraudulent or legitimate transactions. They focused on a solution to minimize the wrongly classified transactions. They merge the Meta heuristic approaches scatter search and genetic algorithm.

Peer group analysis made by David Weston and Whitrow is a good solution regarding credit card fraud detection. Peer group analysis is a good approach that is based on unsupervised learning and it monitors the behavior over time as well. This peer group technique can be used to find anomalous transaction and help to detect the fraud in time.

In proposed system, We present a behaviour and Location Analysis (BLA).Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit. Card transaction processing sequence by the stochastic process various steps. The details of items purchased in Individual transactions are usually not known to any Fraud Detection System (FDS) running at the bank that issues credit cards to the cardholders. Hence, I feel that this is an ideal choice for addressing this problem. Another important advantage of the credit card fraud detectionis to avoid the all money loss transaction done by fraud users. An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the Fraud detection for check. FDS receives the card details and the value of acquisition to verify, whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the Fraud detection. It tries to find any abnormality in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. If the Fraud detectionsupport the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

The credit card fraud detection features uses user activity and location scanning to check for different patterns. These patterns include user characteristics such as user spending patterns as well as usual user geographic locations, face data, pin identification, unusual pattern is detected, the system requires reverification.

The system analyses user credit card data for various characteristics. These characteristics include user country, live location. Based upon previous data of that user the system recognisespecular patterns in the payment procedure. So now the system may require the user to login again or even block the user for more than 3 invalid attempts. The Advance technique of face recognition is added to this system so the exact authentication will be happened while doing every transaction. If the fraud transaction is happened then the live tracking system is used to track the location of fraud tracker when he is try to do next fraud transaction.

Swati D.Shirke and Suvarna Pansambal (shirke)[5] has discussed regarding authentication system by using iris recognition at a distance which can identity the person with the help of iris pattern automatically.

Wen-Fang Yu and Na Wang [9] has proposed methodology Outlier data-mining approach to identify fraudulent type of data-points from the dataset. In this concept, fraud is displayed as an isolated point in the vector space and it could appear independently or somewhat included in a small group of collected data-points.

Swati Swati D.Shirke and C.Rajabhushnam [11] has discussed the techniques about the human identification with how to enhance the performance of the system by using iris recognition system With Pre-processing system.

By using the IRIS recognition is a biometric technique we can recognize a single person. Physical biometric Frameworks such as use of eye, finger, hand, voice and Iris for Identification as ID.[6].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 12, December 2019

III. PROPOSED SYSTEM

Following diagram is our system's architecture diagram:

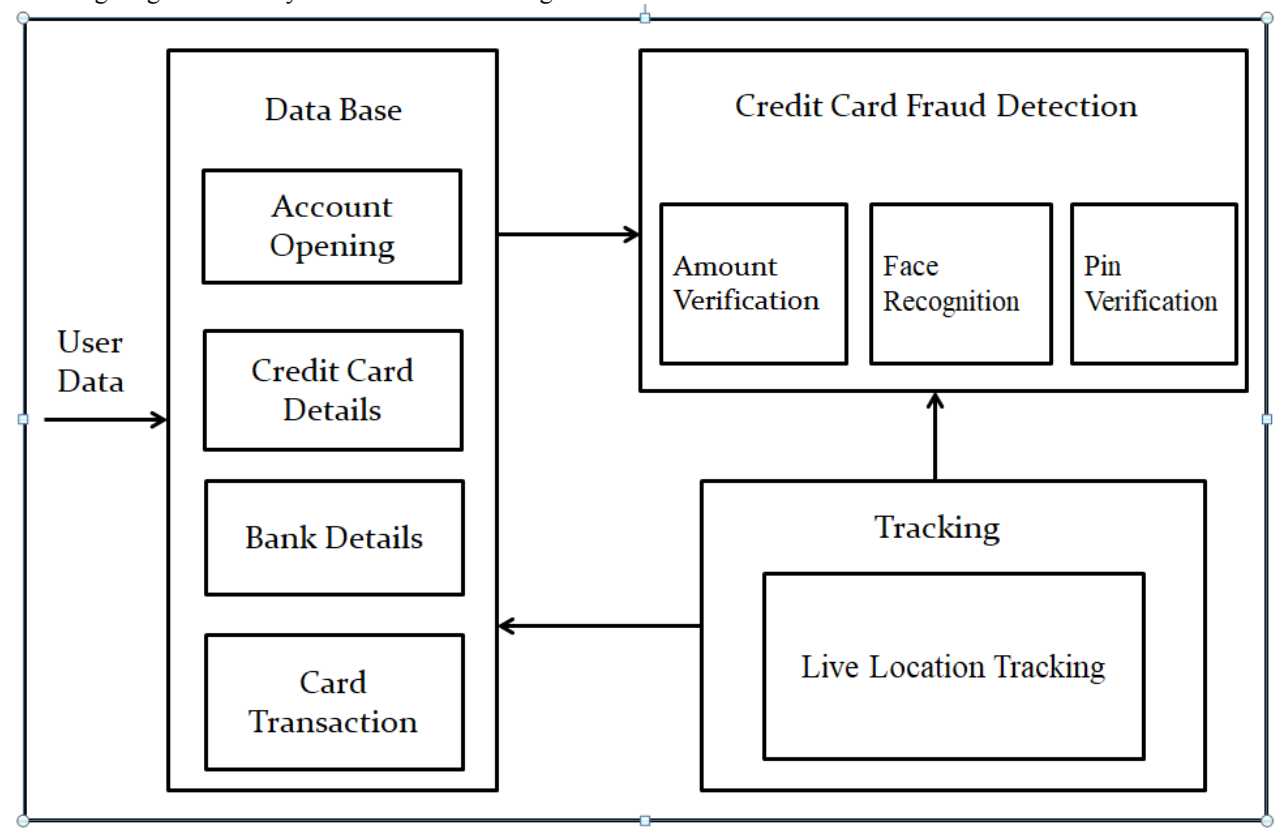

Figure 1: system architecture

Describing the overall features of the software is concerned with defining the requirements and establishing the high level of the system. During architectural design, the various pages and their interconnections are identified and designed. The major software components are identified and decomposed into processing modules and conceptual data structures and the interconnections among the modules are identified. The following modules are identified in the proposed system .The above architecture describes the work structure of the system

IV. CONCLUSION

This project purpose is to find out the fraud transections done by fraud users with high accuracy security system. By using the user behaviour methodology its easy to detect the pattern of transaction to detect the transaction purpose. Make every online transaction more and more secure with multiple authentication system. This System track the fraud used using location tracking system with google map API. Account blocking facility is added in application to avoid fraud transactions. In particular, since there is no limit on the number of features that can be calculated, a system may take too long to make a decision based on the time spent recalculating the features with each new transaction.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 12, December 2019

REFERENCES

[1] The Nelson Report (2015, May 30). Charts & Graphs Archive (2013). Available: https://www.nilsonreport.com/publication_chart_and_graphs_archive.ph p?1=1&year=2015
[2] BangkoSentralngPilipinas (2014, November 21). Media Releases: MB Approves the Implementation Guidelines for Shifting to More Secure EMV Chip-Enabled Cards. Available: http://www.bsp.gov.ph/publications/media.asp?id=3593
[3] About EMV (2015, October 25).EMVCo (2015). Available: https://www.emvco.com/about_emv.aspx K. Elissa, "Title of paper if known," unpublished.
[4] IEEE Spectrum (2014, August 7). Black Hat 2014: A New Smartcard Hack. Available: http://spectrum.ieee.org/riskfactor/telecom/security/black-hat-2014-howto-hack-smartcards-and-termsofservice
[5] Swati.D. Shirke and Dr. C. Rajabhushnam : Iris Recognition Using Visible Wavelength Light
Source and Near Infrared Light Source Image Database: A Short Survey. Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019)
IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8
[6] Swati.D. Shirke and Dr. C. Rajabhushnam:"Biometric Personal Iris Recognition from an Image at
Long Distance", Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8
[7] Statistic Brain Research Institute (2014, July 12). Credit Card Fraud Statistics (2014). Available: http://www.statisticbrain.com/credit-cardfraud-statistics/
[8] Haiying Ma &Xin Li, "Application of Data Mining in Preventing Credit Card Fraud" in International Conference on Management and Service Science, 2009 ©, DOI: 10.1109/ICMSS.2009.5304330, pp 1 – 6
[9] Wen-Fang Yu & Na Wang, "Research on Credit Card Fraud Detection Model Based on Distance Sum" in International Joint Conference on Artificial Intelligence, 2009 ©, DOI: 10.1109/JCAI.2009.146, pp 353 – 356
[10]Swati.D. Shirke and Suvarna Pansambal (shirke): **"**Enhancement of IRIS Recognition Using Gabor Over FFBPANN".*2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*
[11] John T.S Kuah, M.Sriganesh :"Survey Paper on Credit Card Fraud Detection", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 3, March 2014
[12] Ekrem DuMan,MHamdi Ozclik:"Detecting credit card fraud by genetic algorithm and scatter search". Expert Systems with Applications 38 (2011) 13057–13063.