ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

CREDIT CARD FRAUD DETECTION SYSTEM

PAPPA KANI.P
IT-Final year
Sri vidya engg &tech,
Virudhunagar.

MAHALAKSHMI.T
IT-Final year
Sri vidya engg &tech,
Virudhunagar .

Mrs.KAVI PRIYA.M
Assistant Professor / CSE
Sri vidya engg &tech,
Virudhunagar.

ABSTRACT- Credit card frauds are increasing day by day regardless of the various techniques developed for its detection. This project is developing used to detect and block from fraud transactions using a credit card. Credit-card-based purchases can be categorized into two types: 1) physical card and 2) virtual card. In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company. In the second kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information.

KEYWORDS: fraud detection, credit card fraud, various techniques for credit card frauds, OTP.

1. INTRODUCTION

In day to day life, online transactions are increased to purchase goods and services. According to Nielsen study conducted in 2007-2008, 28 of the world's total population has been using internet.85 of these people has used internet to make online shopping and the rate of making online purchasing has increased by 40 from 2005 to 2008.The most common method of payment for online purchase is credit card .In developed countries and also in developing countries to some extent ,credit card is most acceptable payment mode for online and offline transaction. It can give financial loses to issuing authorities .In the second method purchasing i.e. Online, these transactions generally happen on telephone or internet and to make this kind of transaction, The user will need some important information about a credit card (such as credit card number ,validity ,CVV number, name of card holder).

2. EXISTING SYSTEM:

In case of the existing system the fraud is detected after the fraud is done that is, the fraud is detected after the complaint of the card holder. And so the card holder faced a lot of trouble before the investigation finish. And also as all the transaction is maintained in a log, we need to maintain a huge data. And also now a day's lot of online purchase are made so we don't know the person how is using the card online, we just capture the IP address for verification purpose. So there need a help from the cyber crime to investigate the fraud. To avoid the entire above disadvantage we propose the system to detect the fraud in a best and easy way.

3. PROPOSED SYSTEM:

In proposed system, we present a new system FDS Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit. The details of items purchased in Individual transactions are usually not known to any Fraud Detection System(FDS) running

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

at the bank that issues credit cards to the cardholders. Hence, we feel that FDS is an ideal choice for addressing this problem. Another important advantage 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. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify, whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the FDS. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. If the FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

MODULES:

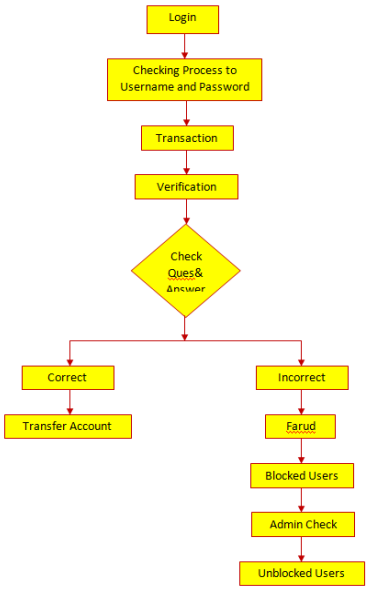
1. Accounts module

2. Registration
3. Security information

4. Transaction

5. Verification

DATA FLOW DIAGRAM



ACCOUNTS MODULE:

In this module, the customer gives there information to enroll a new card. The information is all about their contact details. They can create their own login and password for their future use of the card.

REGISTRATION:

In Login Form module presents site visitors with a form with username and password fields. If the user enters a valid username/password combination they will be granted access to additional resources on website. Which additional resources they will have access to can be configured separately.

SECURITY INFORMATION:

In Security information module it will get the information detail and its store's in database. If the card lost then the Security information module form arise. It has a set of question where the user has to answer the correctly to move to the transaction section. It contain informational privacy and informational self-determination are addressed squarely by the invention affording persons and entities a trusted means to user, secure, search,

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

process, and exchange personal and/or confidential information.

TRANSACTION:

The method and apparatus for pre-authorizing transactions includes providing a communications device to a vendor and a credit card owner. The credit card owner initiates a credit card transaction by communicating to a credit card number, and storing therein, a distinguishing piece of information that characterizes a specific transaction to be made by an authorized user of the credit card at a later time. The information is accepted as "network data" in the data base only if a correct personal identification code (PIC) is used with the communication. The "network data" will serve to later authorize that specific transaction. The credit card owner or other authorized user can then only make that specific transaction with the credit card. Because the transaction is pre-authorized, the vendor does not need to see or transmit a PIC.

VERIFICATION:

Verification information is provided with respect to a transaction between an initiating party and a verification-seeking party, the verification information being given by a third, verifying party, based on confidential information in the possession of the initiating party. In verification the process will seeks card number and if the card number is correct the relevant process will be executed. If the number is wrong, mail will be sent to the user saying the card no has been block and he can't do the further transaction.

4.CONCLUSION AND FUTURE WORK:

Since humans tend to exhibit specific behaviorist profiles, every cardholder can be represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system to detect and block from fraud transactions using a credit card. Here, I kindly convey that special feature of this software is the geniality and it can be worded on the personal computer, since the web page gives a variety option and the message gives clear understanding of the next page it is easy to follow and use .We are sure that this software will be useful for all company. this software, there is no need of knowledge of the computer operating method because, to enter into the menu just enter into windows and type the particular directory, in which the project is stored. In future this project will be using the following methods; With PCI [Payment Card Industry] compliance, vendors are required to harden their code and make access to personal information more secure. For instance, in order for our ecommerce engine to maintain its PCI certification, we are scanned by a third-party every night, and then we are tested to ensure we're not exposed. If we are, we're notified and we have between 24 and 72 hours to seal the leak, so-to-speak. If we miss the deadline, we lose our certification until we've completely sealed off the vulnerability.

5.REFERENCES:

1. "Microsoft ASP.NET" by MirdulPariha, Jeff Webb, Tata Mac Graw Hill.
2. Microsoft SQL SERVER2000 by Ray Rankings, Paul Bertucci, Paul Jensen

3. Gerry O'Brien," Microsoft IIS 5.0 Administration"
4. Sql Server - The complete Reference-Gayle Coffman
5. Teach yourself Sql Server-Richard Way Mire
6. Asp.Net-Stephen Walther (Second Edition)
7. Asp.Net-Daniel Maharry

ONLINE REFERENCE:

ASP.NET:

1. www.asp.net/(S(pdfrohu0ajmwt445fanvj2r3))/learn/data-access/
2. www.w3schools.com/aspnet/default.asp
3. www.411asp.net/home/sites
4. www.cristiandarie.ro/asp-net-tutorial/
5. www.asp.net-tutorials.com/basics/first-website/

SQL SERVER:

1. www.functionx.com/sqlserver/
2. www.technet.microsoft.com/en-us/library/ms169620.aspx
3. www.msdn.microsoft.com/en-us/library/ms169620(SQL.90).aspx
4. www.softwaretrainingtutorials.com/ms-sql-server-2005.php