Credit card fraud detection using machine learning techniques

Agrawal Tina N  
UG Student  
Department of Computer engg  
NES’s Gangamai College of Engineering  
Dhule, India  
rtsagrawal1997@gmail.com

Ahire Swati K  
UG Student  
Department of Computer engg  
NES’s Gangamai College of Engineering  
Dhule, India  
swati121ahire@gmail.com

Patil Swati G  
UG Student  
Department of Computer engg  
NES's Gangamai College of Engineering  
Dhule, India  
spswatipatil19@gmail.com

Prof. N. A. Suryawanshi  
Asst. Professor  
Department of Computer engg  
NES’s Gangamai College of Engineering  
Dhule, India  
nileshsuryawanshiapatil088@gmail.com

ABSTRACT
The enhancement in technology e-banking like credit Card, Debit Card, Mobile Banking and Internet Banking is the popular medium to transfer the money from one account to another. E-Banking is gaining popularity day by day, which increases the online transaction with the increase in online shopping, online bill payment like electricity, Insurance Premium and other charges, online recharges and online reservation of railways, bus etc., so the fraud cases related to this are also increasing and it puts a great burden on the economy, affecting both customers and financial bodies. It not only costs money, but also a great amount of time to restore the harm done. The purpose is to prevent the customer from online transaction by using specific technique i.e. based on Data Mining and Artificial Intelligence technique. The risk score is calculated by Bayesian Learning Approach to analyse whether the transaction is genuine or fraudulent based on the two parameters: Customer Spending Behaviour and Geographical Locations. The customer than spending behaviour that can be identified by KMEAN clustering algorithm and in geographical location the current geographical location is compared with the previous location. If risk score is greater 0.5 then transaction is considered to be fraudulent transactions and then the security mechanism authenticates the user by entering the 4 digit random number that appears on the screen and the genuine user enters the code in a correct manner.

Keywords
Data security, cloud computing environment, SLA, user/group policies

1. INTRODUCTION
Financial fraud is an ever growing menace with far reaching consequences in the finance industry, corporate Organizations, and government. Fraud can be defined as criminal deception with intent of acquiring financial gain. High dependence on internet technology has enjoyed increased credit card transactions. As credit card transactions become the most prevailing mode of payment for both online and offline transaction, credit card fraud rate also accelerates. Credit card fraud can come in either insider card fraud or external card fraud. Inner card fraud occurs as a result of consent between cardholders and bank by using false identity to commit fraud while the external card fraud involves the use of stolen credit card to get cash through dubious means. A lot of researches have been devoted to detection of external card fraud which accounts for majority of credit card frauds. Detecting fraudulent transactions using traditional methods of manual detection is time consuming and inefficient, thus the advent of big data has made manual methods more impractical. However, financial institutions have focused attention to recent computational methodologies to handle credit card fraud problem. Data mining technique is one notable methods used in solving credit fraud detection problem. Credit card fraud detection is the process of identifying those transactions that are fraudulent into two classes of legitimate (genuine) and fraudulent transactions. A number of challenges are associated with credit card detection, namely fraudulent behaviour profile are dynamic, that is fraudulent transactions tend to look like legitimate ones; credit card transaction datasets are rarely available and highly imbalanced (or skewed); optimal feature (variables) selection for the models; suitable metric to evaluate performance of techniques on skewed credit card fraud data. Credit card fraud detection performance is greatly affected by type of sampling approach used, selection of variables.

2. MOTIVATION
In our daily life financial fraud is ever growing with consequence in fanatical industry data mining had played imperative role in detection of credit card fraud in online transaction the performance of fraud detection is great affected by sampling approaches of dataset, selection of variable detection techniques.

3. PROBLEM DEFINITION
To design and develop a system which will provide user with and android application from where the user can view and products to similar ecommerce environment and system must detect credit card fraud at a time of payment which will be done using data mining algorithm.

4. OBJECTIVES AND SCOPE
The objective of credit card fraud detection are reduce losses due to payment fraud for both merchants and issuing a bank and increase revenue opportunities for merchants. Fraud represent significant financial risk to the merchant and issuing the bank to reduce fraud chip and pin technology.
• Creating an application to detect fraud Credit Cards.
• Implementing firewall to restrict entry outside the Network.
• Implementing naïve byes algorithm.
• Creating database containing all relevant information of Customer.
• Providing security to the customers at the time of transaction.

The system prevents fraudulent users from misusing the details of the credit-card of the genuine users for their personal gain. The spending habits of the credit-card owner is detect the fraud. As the fake user might not be aware of the spending habits of the owner, there will be an irregularity in the spending pattern, which the system will detect. The owner is immediately alerted about the attempted fraud and the transaction is blocked. Thus, the system protects legitimate users from financial loss. The system helps in making electronic payment safer and more reliable. The principles in the proposed system can also be adopted and implemented in other electronic payment services such as online banking facility and payment gateways.

5. PROPOSED SYSTEM

The aim of the proposed system is to develop a website which has capability to restrict and block the transaction performing by attacker from genuine user’s credit card details. The system here is developed for the transactions higher than the customers current transaction limit. As we seen the existing system detects the fraud after fraud has been occurred i.e. based on customers complained. The proposed system tries to detect fraudulent transaction before transaction succeed

1) In proposed system, while registration we take required information which is efficient to detect fraudulent user activity.
2) In proposed system we are using naïve byes algorithm which works on transaction behavior of user. By Using naïve byes algorithm , after certain transactions we find one threshold value by using this threshold value we can compare current transaction with threshold value if transaction is quite different from user behavior then check whether it is genuine or fraud OTP (full form) and security questions are used.

6. SYSTEM REQUIREMENTS SPECIFIC

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Pentium 4 Onwards</td>
</tr>
<tr>
<td>Hard Disk</td>
<td>As per OS500MB of free Hard-disk space</td>
</tr>
<tr>
<td>RAM</td>
<td>512 MB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>Windows 7 etc.</td>
</tr>
</tbody>
</table>

7. SYSTEM DESIGNE

The proposed system is a cloud based architecture where all the clients will communicate with one server via internet/Wi-Fi medium. The system will consist of relational MSQYL database which will be managed by the server. System will work in client server and consist of following modules:

1) User Android Application
2) Admin Desktop Software
3) Web Server

User Android Application:
The mobile application will be android application which user can install on their android smart phones. The front end of this application will be developed using android XML layouts. The backend code of the application will be in android java. This application will have following features:

1) User Registration
2) User Login
3) Search products
4) Add product to cart
5) Fill Delivery Information
6) Perform Payment

System Admin Desktop Software:
The admin software will be developed using java and will run on admin desktop. This software will be protected with user name and password. This software will have following features:

1) Admin Login
2) Add new Products
3) View Customer Orders
4) View reports

Web Server:
The web server will be developed in net beans editor. The web server will include java servlets for each and every operation that server will perform. The web server will access database using jdbc connection. Web server is responsible for
all the request and response handling mechanism. Web server will be driven by apache tomcat application server.

7. DFD DIAGRAM

**Figure.1** LEVEL 0 DFD

In level 0 DFD user can place order and perform in level 1 DFD Admin login to the system and that can manage item to the user registration for the place order. Transactions then system detect fraud.

**Figure .2 .LEVEL 1 DFD**

In level 1 DFD Admin has login to the system for managing the item and user login to the system for placed order to perform the transaction to the system and detect the fraud.

Android is a mobile operating system developed by Google, based on a modified version of the Linux kernel and other open source software and designed primarily for touch screen mobile devices such as smart phones and tablets. In addition, Google has further developed Android TV for televisions, Android Auto for cars and Wear OS for wrist watches, each with a specialized user interface. Variants of Android are also used on game consoles, digital OS for wrist watches, each with a specialized user interface. Variants of Android are also used on game consoles, digital cameras, PCs and other electronics. Android is also associated with a suite of proprietary software developed by Google, including core apps for services such as Gmail and Google Search, as well as the application store and digital distribution platform Google Play, and associated development platform. These apps are licensed by manufacturers of Android devices certified under standards imposed by Google, but AOSP has been used as the basis of competing Android ecosystems, such as Amazon.com's Fire OS, which utilize its own equivalents to these Google Mobile Services.

CONCLUSION
Online transaction has increased greatly and due to its simple and fast approach customer prefers it over cash payment. Companies and organization involve in ecommerce provide attractive discounts and offers for online payment. This has made customers to switch from the cash mode to online mode.

ACKNOWLEDGMENTS
With immense pleasure and satisfaction, I am presenting this project report as part of the curriculum of B.E. Computer Engineering. I wish to express my sincere gratitude towards all those who have extended their support during this work. I express my profound thanks to my guide Prof. Mr. N. A.SURYAVANSHI his continued support. Prof.G.M. Poddar (Hod, Computer Department) for their guidance and timely review. I am also thankful to Dr. A.M. Vaidya (Principal, Gcoe) for providing this opportunity. I would also like to express my thanks to all those who have directly or indirectly guided and helped me in preparation of this work.

REFERENCES