JIBC

Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, August 2017, vol. 22, no. 2

SECURED CREDIT CARD TRANSACTION USING MCOP

SARAVANAN SK

Department of Computer Applications, Valliammai Engineering College, Chennai, Tamil Nadu, India

Tel: 9500967016;

Email: **saravanan4phd@gmail.com**

SURESH BABU GNK

Department of MCA, Acharya Insititute of Technology, Bengaluru, Karnataka, India

Abstract

With the improvement of changed correspondence systems, online payment exchanges and in addition web based business is spreading step by step. Additionally, the money related cheats related with these exchanges are likewise expanding which in this manner brings about significant budgetary misfortunes consistently comprehensively. Credit card extortion is drilled most every now and again among the changed money related cheats because of its acknowledgment and across the board use as it offers more accommodation to its clients. Monetary foundations, for example, banks require more advanced methods for recognizing misrepresentation. Budgetary fakes are frequently difficult to distinguish and break down as the deceitful conduct is changing, scattered in unmistakable client profiles, and spread crosswise over gigantic imbalanced genuine datasets (e.g. client spending profiles, web logs, exchange logs). Moreover, clients once in a while audit

their web based keeping money history and thus are not ready to uncover the false exchanges at the ideal time. Likewise, because of the wide use of credit cards as a method of payment for acquiring merchandise and enterprises, there comes a need to decide if the exchanges made using a credit card is a substantial exchange done via card holder or it is a deceitful exchange done by the fraudster. To stay away from or control the online extortion this review presents another method Multi Combination of Password Technique (MCOP).

Keywords: **MCOP; Data mining; Credit card; Fraud**

INTRODUCTION

In customary methodologies, it can be made sense of whether the exchange done is a legitimate exchange or a fake exchange once the charging has been finished. This prompts generous budgetary misfortunes. Along these lines, it is important to decide the fake exchanges before playing out the charging activities. In spite of the fact that fraud detection has a long history, very little research has occurred around there. The cause is that this present reality information is difficult to acquire since the monetary establishments are not prepared to unveil their touchy client transaction information because of the protection limitations inferred by the greater part of the money related organizations which additionally confines the researchers to play out the analyses and get the results. Besides, the specialists of the financial institutions change the field names so that the analysts don't become acquainted with about the real fields. Because of these secret parts of this present reality dataset, fraud detection models have not been created and portrayed in the scholarly writing and extremely less models are executed in the genuine identification systems. Still there exist a portion of the fruitful applications that utilization distinctive information mining procedures including self-composed maps, neural systems, manufactured insusceptible framework, shrouded markov models, fluffy rationale frameworks, restrictive weighted exchange accumulation, frequent set mining, cryptographic calculations, and exception identification methods in fraud detection.

Data Mining Techniques

John Akhilomen presents an application in view of information mining that has been planned as a subsystem and can be pertinent to the vast majority of the money related organizations to identify credit card fraud. This application acknowledges input designed on a specific example and testicles it with the credit card holder's example and afterward it characterizes a constant exchange as either being a honest to goodness, suspicious or an ill-conceived exchange. This approach makes utilization of an "oddity recognition algorithm" in view of "neural systems" to find misrepresentation in the exchanges occurring progressively and it doesn't acquaints

any imperfections due with its prepared classifier which allocates every continuous exchange as either being a true blue, suspicious or a deceitful exchange [1]. Fraud manages cases that occur because of criminal reason which are hard to distinguish. Misrepresentation can be for the most part separated into two sorts:

Offline Fraud: Most of the offline extortion occurrences happen because of the take of wallet that contains essential archives. Records, for example, Driving License, ID card and so on contains significant data, for example, name, date of birth, exchange slips and so on [2].

Online Fraud: Online misrepresentation happens when impostor display their site as a certifiable site with a specific end goal to acquire essential individual information of a client and perform illicit exchanges on such client account [2]. Credit card is additionally a standout amongst the most illicit sorts of misrepresentation. Credit Card is a plastic card issued to clients of a bank as one of the method of payment. It enables cardholders to buy products and ventures from the shopping sites or from the market. Credit card Fraud is characterized as, when an individual uses another individual Credit card for individual utilize while the proprietor of the card and additionally the card guarantor don't know about the thing that the card is being utilized [3].

Figure 1 in the event that credential data of a client has stolen and utilizes for internet shopping, the card holder recognizes exchange subtle elements after the extortion has been submitted and after that client asks the bank for exchange. There is no such procedure that can forestall false exchange at the season of happening. So there is a need of such interface that keeps from online exchanges (Figure 2).

Figure 1: Sample structure for Credit card fraud.

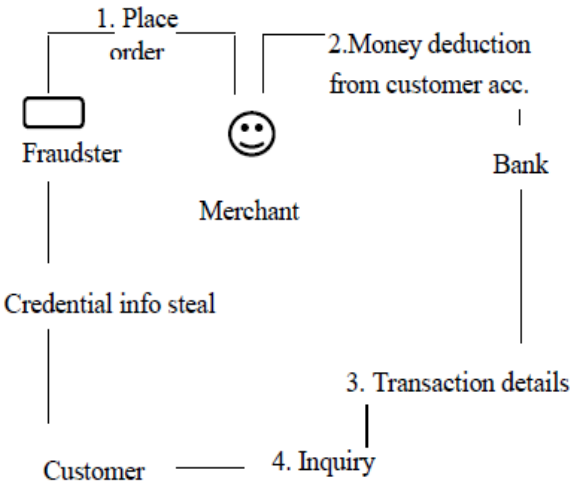
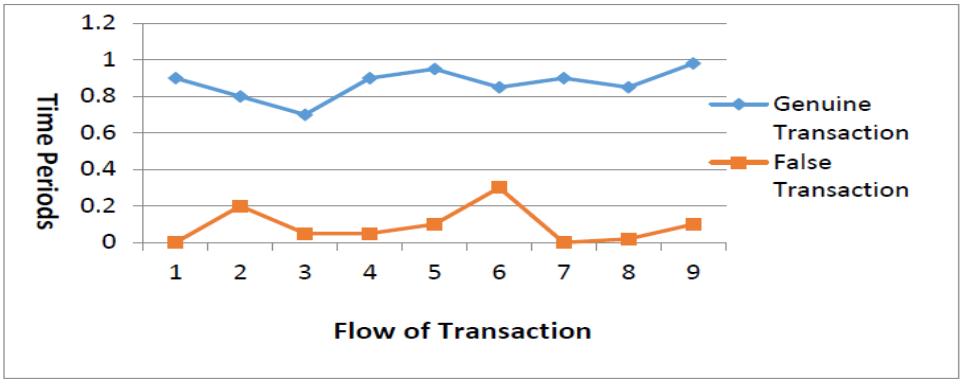


Figure 2: Mean distribution of Fraud.



Transaction X – Mean, Y – Number of transaction.

Security Mechanism to Prevent from Fraud

Address Verification Service (AVS): In this procedure it coordinates the cardholder charging location and transportation address and recognizes whether the cardholder has obtained item on this address. Be that as it may, this strategy contains a few shortcomings i.e. the address data is accessible on the web; the investor feels exhausting to check record of each client to keep from deceitful exchange; it can't check the whole informational card [4].

Fraud Rates: This method checks for perceived examples i.e. utilized by the fraudster to submit the extortion. The favorable position that it is anything but difficult to design and see, yet the weakness fraudster changes their example changes at general interim [4].

Relocation: This method recognizes the client geographic area by distinguishing its IP addresses.

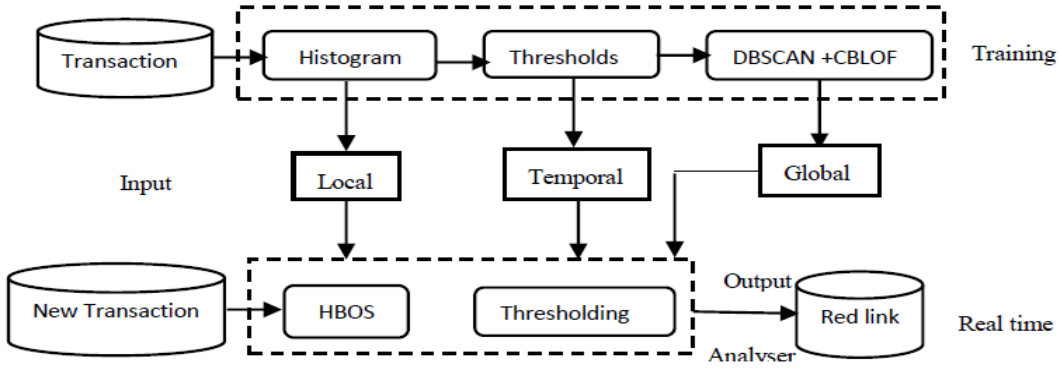
Chip & Pin: A PIN is a 4 digit one of a kind and mystery number that client needs to enter before doing exchange by ATM/Debit Card/Credit Card. The 4 digit stick is utilized to distinguish whether the client is real or not [5].

3D-Secure: This method chips away at the rule of verifying the client secret word with the watchword that is put away in the database. The primary preferred standpoint of this framework is that fraudster needs a user's secret key to play out the exchange [5].

Biotechnology: The unique characteristic for every client, for example, fingerprints, voice, mark, iris and other comparable organic parts is put away in a PC so that a PC can read it. At that point the PC looks at the put away examples to the individual who is playing out the exchange to distinguish whether the client is bona fide. The primary burden of this innovation is that will be that it requires extra equipment cost.

One Time Password: The random number is created at server side and is send to the customer's cell phone through the assistance of the web administrations to guarantee that the right client is playing out the exchange right then and there of time. The client needs to enter a similar secret key for getting the approval from the bank side (Figure 3).

Figure 3: Architecture of Bank Sealer.



How does a credit or debit card transaction actually work behind the scenes?

1. Credit Card or Debit Card is swiped or scratched at shipper.
2. Merchant sends information to their processor, which is typically a getting bank.
3. Procuring bank courses exchange through proper card arrange (like Visa Net).
4. Exchange achieves card holder's issuing bank.
5. Issuing bank endorses or decays exchange.
6. Endorse/decay sent back through system to trader to finish buy.
7. Procuring bank settles with issuing bank.
8. Procuring bank settles with vendor.

Next-Gen Payment Processing Technologies

The numerous threats that have preyed on the traditional credit card payment system, coupled with new technology, has led to the development of different payment processing technologies that not only allow for more convenient transactions, but also ones that are more secured. Click on the links below to read about the new technologies, how they work, and their advantages and disadvantages [6]. The various dangers that have gone after the conventional credit card payment framework, combined with new innovation, has prompted the improvement of various payment handling advances that take into account more advantageous exchanges, as well as ones that are more secured. Tap on the connections beneath to peruse about the new innovations, how they work, and their focal points and weaknesses.

EMV Credit Cards: Also called Chip-and-PIN cards, these cards include a chip that stores a cryptogram that distinguishes changed exchanges. It additionally requires a PIN for additional verification.

Contactless RFID Credit Cards: This payment innovation utilizes detached Radio Frequency Identification that enables cardholders to wave the cards before RF terminals to finish exchanges.

Mobile Wallets: First propelled in Japan in 2004, this innovation deals with NFC empowered cell phones, and has since been actualized by Google and Apple through their versatile stages.

Apple Pay: First presented in 2014, Apple Pay is an payment application elite to specific emphases of Apple's cell phone biological system, in particular the iPhone 6 (and later), iPad 2 (and later), iPad Mini 3 (and later) and the Apple Watch. It includes the utilization of a different Secure Element (a chip much the same as chip-and-stick Visas) to store the client's credit card data in the gadget which is separate from the principle processor where applications execute. It likewise works with the inherent Touch ID Fingerprint Reader include, at the time one of the most recent components to be planned into that specific era of Apple gadgets [7].

Apple Pay utilizes two techniques: a cryptogram, like EMV exchanges, and tokenization. At the point when the client initially inputs their Credit Card into the Apple Pay application, the Credit Card brands (Visa, MasterCard, or American Express) will send a token and a cryptogram to the Apple gadget. The token is a 16-digit number that replaces the real Credit Card number. The token and the cryptogram is then put away in the Secure Element chip, and is sent to the card brand's system for check each time the client approves an exchange (by method for the unique finger impression scanner, the main approving component expected to do as such).

The card mark organize gets both components, decodes the cryptogram and after that checks it for validness. On the off chance that the cryptogram is observed to be valid, the system then passes the token to the backer bank of the Credit Card. The backer decodes the token, and after a last check for credibility, finishes the exchange. A few exchanges in this line additionally require the client to include their postal code, for included security and check

Google Wallet, which was prevailing by Android Pay in September 2015, is the versatile payment application for Android clients. Bolstered by Android KitKat and more up to date, Android Pay underpins tap-and-pay exchanges utilizing the gadget's close field interchanges (NFC) highlight. To make it work, clients need to introduce the application and info the card number and different points of interest essential for payment confirmation, for example, name and address. Clients who

have accounts with significant credit or check cards in the US can simply take a depiction of the card utilizing their cell phones camera and it consequently inputs the date of lapse.

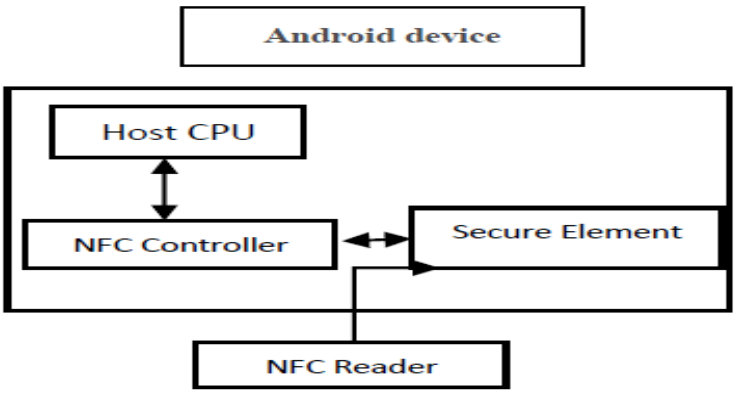
Google Wallet/Android Pay works in two ways card imitating with secure element (SE) and host-based card copying. In card imitating with secure component, the gadget is put on the NFC terminal and every one of the information read will be directed in SE, which is in charge of the correspondences with the NFC terminal. Once the exchange is done, the application can question the SE with respect to the status and tell the client [8].

With host-based card copying, the Android OS and the application is specifically required in the handling of payment exchange. Once the client conveys the gadget up to the NFC (fig.4 & fig.5) terminal, the application plays out the card imitating and handles correspondence with the terminal. All information is facilitated in a cloud situation, which does the real exchange preparing before it conveys back the status to the application [9].

Advantages: Aside from the convenience it offers, given that it cooperates with real credit and debit organizations and is bolstered by a ton of US retailers, Google Wallet/Android Pay has the information transmitted amid exchanges in a safe cloud condition. It doesn't store any of the client information on the gadget itself, which implies that if the Android gadget is contaminated with data taking malware, the client data and qualifications utilized by this application won't really be stolen by the cyber criminals.

Disadvantages: It’s a well-known fact that the open source Android stage has experienced a not insignificant rundown of vulnerabilities and endeavours. And keeping in mind that Google pushes refreshes for these vulnerabilities, not all gadgets of various makers can get those patches because of portable fracture. This can make those gadgets powerless against assaults (Figure 4).

Figure 4: Card Emulation with a secure element.



There are additionally reports in regards to Google Wallet Relay assault that requires the objective card to be in closeness with a per user gadget, other than expecting to introduce hand-off programming to work. In actuality, it can possibly convey the information transmitted over the system or have benefit access to it (Figure 5) and (Figure 6).

Figure 5: Host-based card emulation (Source: developer.android.com).

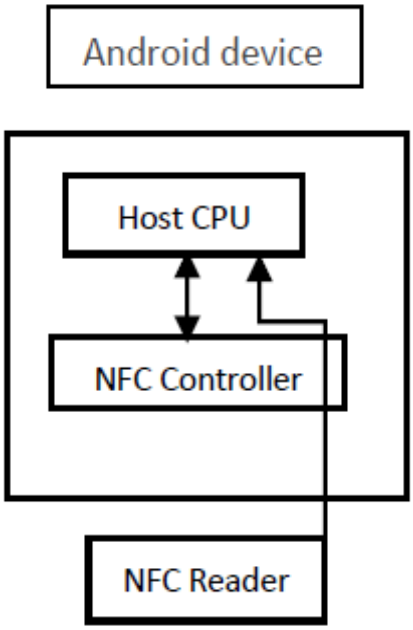
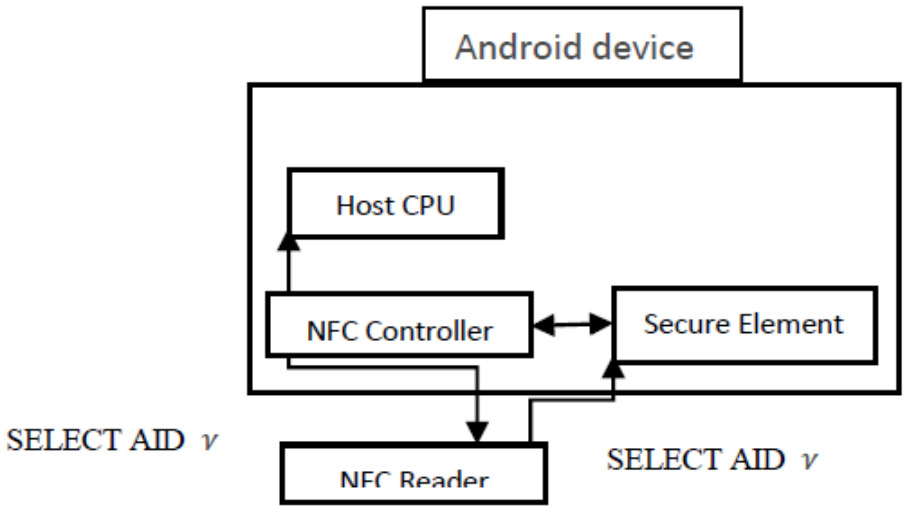


Figure 6: Device operating both SE and HCE (Source: developer.android.com).



New Payment Processing Architectures three next generation structures intended to enhance secure portable payment.

- Encryption and tokenization
- Cloud-based PoS frameworks
- Secure Element frameworks

A quickly expanding number of people make payments through cell phones, for example, cell phones and tablets. They buy applications, music, customer merchandise, and a wide cluster of different items and administrations. Utilizing conventional credit cards or even contactless cards, these payments are regularly at danger of assault [2]. For instance, actually credit cards can't counteract Point-of-Sale (PoS) terminal assaults. The chip-on-card makes it to a great degree troublesome for culprits to produce fake charge cards utilizing stolen information in this way lessening fake and lost or stolen card extortion. In any case, that doesn't shield these cards from different sorts of assaults, especially those that hope to take information amid a transaction [9]. One basic contactless assault is the transfer assault. The assault chain comprises of:

- A transfer per user gadget called a mole, which is set in closeness to the card being assaulted.
- A card emulator gadget called an intermediary, which is utilized to speak with the PoS terminal.
- A quick correspondence channel between the transfer and the intermediary.

The mole produces radio recurrence vitality and forces the RFID chip on the card being attacked. The intermediary associates with the PoS terminal and advances charges to the card through the mole. The mole catches the card's reactions and sends them back to the intermediary, which then advances it to the PoS terminal. Encryption does not ensure against this kind of attacks since this is catching a current information exchange, with the mole and the intermediary transferring information [2]. There are at present three essentially models that advance a cutting edge answer for secure versatile payment. These are encryption in addition to tokenization, cloud-based PoS frameworks, and secure component frameworks.

Encryption plus Tokenization: This payment design scrambles and tokenizes the credit card information, accordingly making Visa information robbery for all intents and purposes outlandish for the cybercriminals [2].

The handling work process is as per the following:

- The client swipes their Visa at the dealer's PoS terminal to finish their buy.
- The PoS terminal peruses and encodes the Credit Card information and transmits it for preparing.

- The processor advances the credit card information to the banks for approval.
- The processor utilizes a tokenization calculation to supplant the genuine credit card information with a token.
- The produced token and bank approval status is send back to the dealer's PoS framework.
- The dealer's PoS framework stores the token rather than the genuine charge card information in all spots.

This system guarantees that the real credit card information is never present in gadget memory or in some other framework on the vendor's end. Stolen tokens can't be utilized to make fake Visas and can't be utilized as a part of card-not-present exchanges [10].

Cloud PoS Systems

With Software-as-a-Service (SaaS) getting to be noticeably famous, there is an expanding shift towards cloud based PoS frameworks. Cloud PoS frameworks furnish shippers with a minimal effort, include rich, adaptable, and secure payment exchange system.

- There is no costly setup costs included. Vendors can introduce the payment applications all alone tablets, cell phones, PCs and so forth and begin getting payment.
- Most cloud PoS frameworks offers simple joining with existing online business sites.
- Cloud PoS frameworks do secure transmission and capacity of touchy charge card information.
- Cloud PoS merchants ensure framework uptime and administration accessibility.
- Data from various gadgets and areas are midway put away and prepared in the cloud. This improves information administration and gives secure access to that information from any gadget, wherever.
- Cloud PoS frameworks have a disconnected mode in case of a system disappointment. The payment application will group exchanges and send them once the system association is re-built up.

While cloud-based PoS gives minimal effort, highlight rich, adaptable, and secure payment exchange systems, there are some natural dangers exhibits. Payment applications that keep running on tablets, cell phones, PCs still procedures the card information in memory before safely transmitting it to the Cloud PoS. This opens the gadgets to potential RAM scrubber attacks. With the expanding adoption of Cloud PoS, merchants are information break focuses for digital crooks [10].

Secure Element: This structural arrangement utilizes a safe component to process credit card exchanges. In this method, the credit card data is perused by the PoS

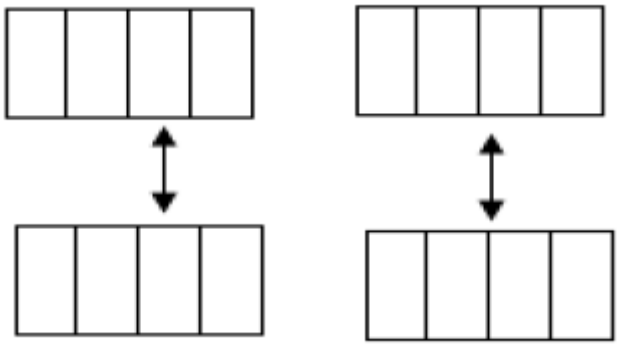
terminal and sent straightforwardly to a safe component, which Intel calls Protected Applet (PA), bypassing the PoS programming. The PA deals with all exchange preparing demands with the banks and can be arranged to impart certain information to the PoS programming. Moving credit card processing activities to the protected component and totally bypassing the RAM guarantees the delicate information can't be stolen by RAM Scraper malware. The safe component is intended to be altering safe and can't be tainted by malware [11]. These solutions speak to the best prospects for secure payment exchanges sooner rather than later.

While they are more secure than existing versatile payment techniques, they have certain components that still have the potential for attacks [12-14].

Single point crossover in Genetic algorithm

It is a hybrid procedure which includes choosing one cross point arbitrarily from the populace (fig.7). That is the hybrid point is picked in both of the parent arrangements. The parent arrangements are being acquired from the choice. Utilizing the arbitrarily chose cross point and the parent arrangements the hybrid system is connected. The information past that hybrid point is intermixed which yields a solitary child [15,16] (Figure 7).

Figure 7: Crossover.



The psuedocode of the crossover technique is as shown below

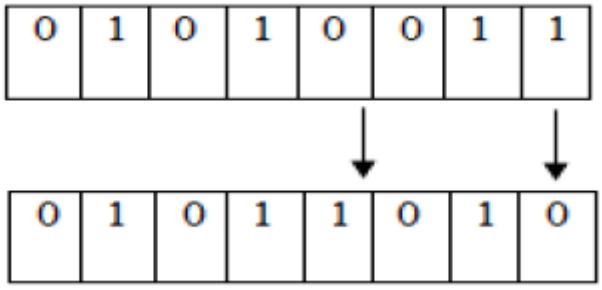
Crossover ()

```
For each intermediate transactions
  For Cross point from 0 to father.length do
    for I from 0 to father. Length do
      if i< Cross point
       Child [i] = father [i]
     else
Child [i] = mother [i]
```

Mutation: It is likewise a genetic administrator in the genetic calculation. The change

is primarily used to keep up heterogeneity in the populace. It modifies a portion of the qualities in view of which the whole solution. Subsequently forward utilizing mutation in genetic calculation we can acquire the better solutions from the chose dataset (Figure 8).

Figure 8: Mutation.



The psuedecode of the cross over technique is as shown below Mutation ()
For each intermediate transaction data do
i <- random (0, 1)
j <- random (0, N)
k <- random (0, 3)
if k <- 1 then
pop [I][j] <- pop[I][j] + I
else
pop [I][j] <- pop[I][j] -I

Multi Combination of Password Technique (MCOP)

Usually when performing a Credit Card transaction user needs to enter with the Credit Card Number, Card Holder Name, CVV, Card Type and OTP\3D Number. While analysing the above information except OTP or 3D number all other credentials can be easily stolen. Fraudster usually calls the user and identified him as he is from bank and asking for OTP. Once he got the OTP he can easily probe the money of the card holder. The below diagram shows the high percentage of misuse of OTP. To avoid this new technique called MCOP can be used. An MCOP contains below information.

- Four favourites letters of user (x1)
- Online Transaction Code (x2)
- OTP (x3)
- A Numeric Symbol (x4)

Four favourite letters of user (x1): This letter can be the user's choice when

customizing the MCOP. For example when a user customizing the MCOP he can choose letters like Good, Hura, Made, Cate and so on.

Online Transaction Code (x2): It is like PIN number. User can choose his own OTC like 5568, 8754, 6336, etc.

OTP (x3): Sent by banker.

A Numeric Symbol (x4): This is also user's choice, example &, *, #, etc.

Now a user can choose which comes first, second, third and fourth. For example a user can choose like below MCOP format. Online Transaction Code (x2) + four favourite letters of user (x1) + OTP (x3) + A Numeric Symbol (x4).

A sample MCOP will be like: 4586Good1789&

By giving multiple choices to the user for customization of MCOP anytime an online transaction can be highly secured.

The Algorithmic approach

Let universe of discourse X={x1, x2,…., xn}be the object to detect. Every object has m indexes, namely xi ={ xi1, xi2, ….xim} , i= (1,2, … n) .The following data matrix shows it in the following way:

$$X = \begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1m} \\ X_{21} & X_{22} & \cdots & X_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ X_{n1} & X_{n2} & \cdots & X_{nm} \end{bmatrix} \quad (1)$$

Now required to figure out the outlier sets of n objects. To judge the diffusion degree of every object in X, We comprises the dij which denotes the distance between any two objects and composes distance matrix R, described as follows,

$$R = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1m} \\ d_{21} & d_{22} & \cdots & d_{2m} \\ \vdots\vdots & \vdots & \ddots & \vdots \\ d_{n1} & d_{n2} & \cdots & d_{nm} \end{bmatrix} \quad (2)$$

It is very important to select any distance function. This paper selects the Euclidean distance.

$$DIS(U,F)=\sqrt{\sum_{i=1}^{n}(O_i-f_i)^2} \tag{3}$$

$$p_i=\sum_{j=1}^{n}d_{ij} \tag{4}$$

Where Pi is the sum of i^{th} row in matrix R. The bigger Pi is, the longer the distance between i object and other object is. Then Pi is said to be the candidate item of outlier set.

$$\lambda_i=\frac{P_i-P_{min}}{P_{min}}\times 100\% \tag{5}$$

where, λ denotes threshold and the objects with λi ≥ λ are taken to be the outlier set (Figure 9) and (Table 1).

Advantages of MCOP Model

- It manages nonlinear information for extortion recognition.
- It is competent to distinguish the extortion when fake exchange is in
- It can deal with nonlinear and intuitive impacts of information factors.
- It has complex calculation. Indeed, even a little change in watched information may change the structure of a tree.
- It does not require building up any prescient model before grouping.

Figure 9: Proposed model of credit card fraud detection after training during detection.

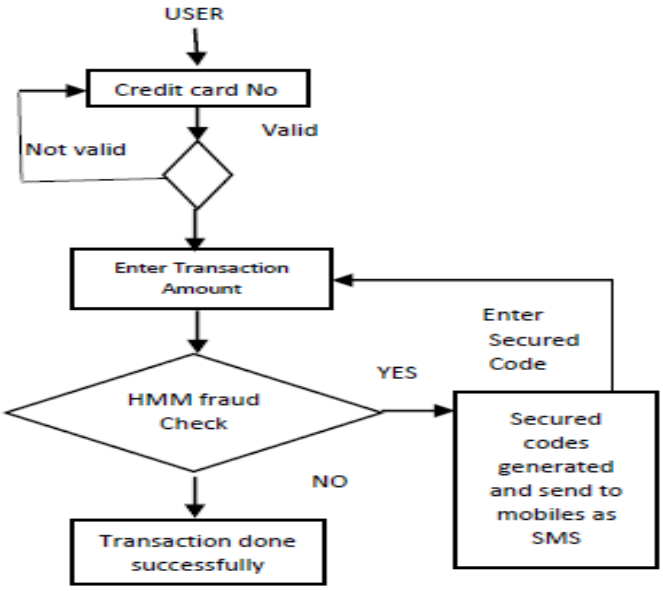
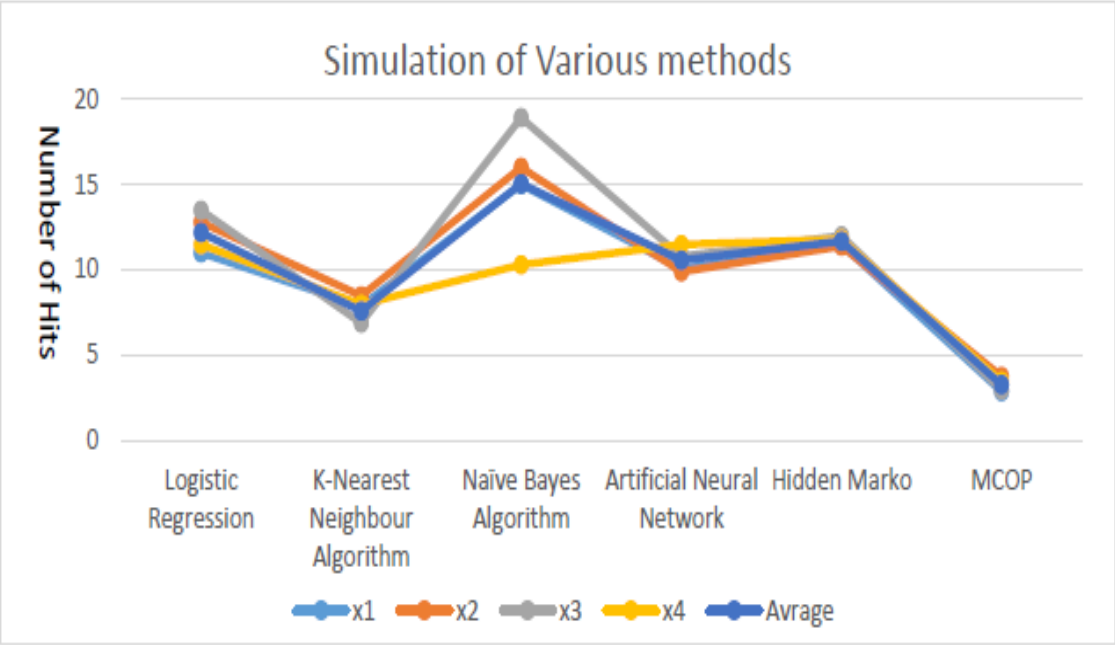


Table 1: Comparison of FDT.

Fraud Detection Technique (FDT)	**Pros**	**Cons**
Logistic Regression	It produces a Simple probability formula classification. It works well with linear data for credit card fraud detection.	It does not deal with nonlinear data for credit card fraud detection. It is not capable to detect the fraud at a time when fraudulent transaction is in.
Decision Tree	It can handle nonlinear and interactive variables.	It has complex algorithm. Even a small change in observed data might change the structure of a tree. Choosing splitting criteria is also difficult. It is not capable to detect the fraud at a time when fraudulent transaction is in progress.
K-Nearest Neighbour Algorithm	It does not require establishing any predictive model before classification.	1) Accuracy is highly dependent on the measure of distance. 2) It is not capable to detect the fraud at a time when fraudulent transaction is in progress.
Naïve Bayes Algorithm	It only provides a theoretical justification to the fact but does not use Bayes theorem.	1) In real practice the dependences exists between the variable. 2) It is not capable to detect the fraud at a time when fraudulent transaction is in progress.
Artificial Neural Network	It detects the fraudulent transaction at the time when transaction is in progress.	Number of parameters to be set before training begins. There are no clear rules to set these parameters. Network differs in the way their neurons are interconnected and so far there is no method that determine optimal topology for a given

		problem.
Hidden Marko	It is capable to detect the fraudulent transaction is in progress. The main feature of the HMM-based model is reducing in False Positive (FP) transactions predict as fraud by a fraud detection system even though they are really genuine customer.	It detects the fraud only after some transactions so it is not secured for initial some transactions.
MCOP	It deals with nonlinear data for fraud detection. It can handle nonlinear and interactive effects of input variables. It has complex algorithm. Even a small change in observed data might change the structure of a tree. Cannot easily hack the password.	User needs to remember the combination and should capable to customize the MCOP.

Figure 10: Simulation result of various algorithmic approaches.



The major threads when analyzing the data set, the Stealing OTP is normally happening by call the user over phone and claimed he is from bank authority and asking the OTP for security purpose. Interfering the mobile network or hacking the mobile is happening in a very lower percentage. Stealing Credit Card information normally takes place when we use card in public places. Mainly a chip will be attached in the swipe machine and it observes the card information (Figure 10).

Stealing PIN: Camera in the ATM centers or in the malls is a main loop hole to steal the PIN number. Moreover hacking the user network also leads to stealing the PIN.

Stealing 3-D secure number: This is also happens by calling the user and asks for 3-D secure number as he claims from bank or authority. Moreover hacking the user network also leads to stealing the 3-D secure number.

Cloning Card: Crooks are using tiny camera recording PIN which is attached in the ATM are reading the card and skim the information save it to a memory and also have an overlay of the keypad and when enter the card , they can download all the information and clone it a bank card.

A sample data set has been taken and did some transaction by using OLTP tool to find out how MCOP is effective than any other existed method in the industry. The results shows in Table 2 surprised results listed below table shows the results of probability percentage of hacking online transactions (Table 2) and (Table 3).

Table 2: Results of probability of hacking online transactions.

Methods	**OTP**	**Cloning**	**3-D secure**	**PIN**	**Overall**
AES (Advanced Encryption Standard)	12	5	3.75	16.8	9.39
Triple DES (Data Encryption Standard)	11.2	3	2.25	15.68	8.03
HMM	15	7.1	5.325	21	12.11
Blow fish	10	4	3	14	7.75
Two fish	12.6	6.1	4.575	17.64	10.23
Advanced RSA	9.8	3.4	2.55	13.72	7.37
Hidden Marko	14.1	8.6	6.45	19.74	12.22
MCOP	7.2	1.8	1.35	10.08	5.11

Table 3: The effectively use of TOOL.

Actions	**OLTP System Tool**
Source of data	Operational data; OLTPs are the original source of the data.
Purpose of data	To control and run fundamental business tasks
What the data	Reveals a snapshot of ongoing business processes
Inserts and Updates	Short and fast inserts and updates initiated by end users
Queries	Relatively standardized and simple queries Returning relatively few records
Processing Speed	Typically very fast
Space Requirements	Can be relatively small if historical data is archived
Database Design	Highly normalized with many tables
Backup and Recovery	Backup religiously; operational data is critical to run the business, data loss is likely to entail significant monetary loss and

CONCLUSION

OLTP system tool is used to derive the result. This tool is characterized by a large number of short on-line transactions (INSERT, UPDATE and DELETE). The main emphasis for OLTP systems is put on very fast query processing, maintaining data integrity in multi-access environments and an effectiveness measured by number of transactions per second. In OLTP database there is detailed and current data, and schema used to store transactional databases is the entity model (usually 3NF). In this paper we have brief discussion on credit card fraud detection using MCOP Model. Here we have shown how the MCOP can detect whether an incoming transaction is fraud or genuine also we have given a new approach to customize passwords with the combination using MCOP algorithm. MCOP used to generate 9 digit unique security codes. In MCOP model we have proved that it gives more security and to reduce the fraud. The results using OLTP tool shows that the MCOP has very less probability of hacking and adds more security to online transactions.

REFERENCES

1. Patel T, Kale O (2014) A secured approach to credit card fraud detection using hidden Markov model. International Journal of

Advanced Research in Computer Engineering and Technology.

2. Pawar D, Rabse S, Paradkar S, Kaushik N (2016) Detection of fraud in online credit card transactions. International Journal of Technical Research and Applications 4: 321-323.
3. Adiga P, Bhat SV, Javagal SR, Lavanya BS, Chandrika J (2017) Credit card fraud detection-a hybrid approach using simple genetic and apriori algorithms. International Journal of Recent Scientific Research Research 8: 16308-16313.
4. Singh P (2015) Fraud detection by monitoring customer behavior and activities. International Journal of Computer Applications.
5. Patidar R, Sharma L (2011) Credit card fraud detection using neural network. International Journal of Soft Computing and Engineering.
6. Sethi N, Gera A (2014) A revived survey of various credit card fraud detection techniques. International Journal of Computer Science and Mobile Computing 3: 780-791.
7. Ali MA, Arief B, Emms M, Van Moorsel A (2017) Does the Online Card Payment Landscape Unwittingly Facilitate Fraud? IEEE Security and Privacy.
8. Rathore S, Jain M (2016) A hybrid technique for credit card fraud detection Communications on Applied Electronics. Foundation of Computer Science FCS, New York, USA.
9. Sonawne VD, Gupta P, Raut A, Saudagar F (2016) ATM card fraud detection using hidden Markov model. International Journal of Innovative Research in Computer and Communication Engineering.
10. Carminati M, Caron R, Maggi F, Epifani I, Zanero S (2015) Bank Sealer: A decision support system for online banking fraud analysis and investigation. Elseiver.
11. Patel S, Gond S (2014) Supervised Machine (SVM) learning for credit card fraud detection. International Journal of Engineering Trends and Technology.
12. Avanti H, Vaidya SW (2014) Mohod Internet Banking fraud detection using HMM and BLAST-SSAHA Hybridization. International Journal of Science and Research.
13. Abu-Shanab E (2015) Security and fraud issues of E-banking. International Journal of Computer Networks and Applications.
14. Sivakumar N, Balasubramanian R (2015) Fraud detection in credit card transactions: classification, risks and prevention techniques. International Journal of Computer Science and Information

Technologies.

15. Jain R (2016) A hybrid approach for credit card fraud detection using rough set and decision tree technique. International Journal of Computer Applications.
16. Agaskar V, Babariya M, Chandran S, Giri N (Year) Unsupervised learning for credit card fraud detection. International Research Journal of Engineering and Technology.