Academic Research Journal of Science and Technology (ARJST) Volume: 01, Issue: 02, October 2024

Credit Card Fraud Detection and Prevention In Point of Sale Using Apriori Algorithm

1. M.Dhavapriya
Assistant Professor, Department of Computer Science, NGM College Pollachi – 642001. EMail: ngm@ngmc.org

2. Dr. V. Anuratha
Assistant Professor, PG Department of Computer Science Sree Saraswathi Thyagaraja College Pollachi - 642205

Abstract - Along with the great increase in credit card transactions, credit card fraud has become increasingly widespread in recent years. In Modern day the fraud is one of the major causes of great financial losses, not only for merchants, individual clients are also affected. Banks also use information provided by their own customers to help identify possible fraud. Credit card companies will record fraud attempts recognized by the customer rather than the credit card company *and* take steps to recognize similar charges on other customer's credit cards. If it's fraud for one person, it may also be fraud for another. Credit Card fraud begins either with the robbery of the physical card or with the concession of data associated with the account, including the card account number or other information that would routinely and necessarily be available to a merchant during a rightful transaction. The fraud is detected after the fraud is done i.e. the fraud is detected after the complaint of the card holder. So card holder faces a lot of trouble before the investigation finish. To avoid the above disadvantages the proposed system is used to detect the fraud in a best and easy way.

Keywords – Apriori Algorithm, Credit Card Fraud, Fraudulent types, Hidden Markov Model.

I. Introduction

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 gives the card physically to a merchant for making a payment. To bring out fraudulent transactions in this sort of purchase, an attacker has to steal the credit card. If the cardholder does not recognize the loss of card, it can direct 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. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to identify the details of card. Most of the time, the authentic cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the "usual" spending patterns. Fraud detection based on the analysis of presented purchase data of cardholder is a promising way to reduce the rate of booming credit card frauds. Every cardholder can be represented by a set of patterns containing information about the usual purchase category, the time since the last purchase, the amount of money spent, etc.

Ii. Credit Fraud

The main contribution of this work is related to credit card fraud. Credit card fraud is a term used to refer to the family of frauds which are perpetrated in usage of credit card in POS terminal. It is the most important and dangerous type of credit fraud.

- **The Use of Credit Card and its Stakeholders**

Credit card usage has enormously been increased during the last few years. According to [4], 120 million cards were created in India in 2004 which led to total credit card purchases of 375 billion at the same year [1], which led to increase of 4% on the overall credit card usage [1]. Delamaire et al. defined credit card as “a method of selling goods or services without the buyer having cash in hand” [1]. A credit card transaction involves four entities. The first entity is the consumer; that is the person who owns the card and who carries out the legitimate transactions. The second entity is the credit card issuer; that is usually the consumer’s bank - which provides the credit services to consumer. The credit card issuer sends the bill to the consumer in order to request a payment for their credit card transactions. The third entity is the merchant who sells goods or services to the consumer by charging consumer’s credit card. This charge is achieved through merchant’s bank – the forth entity – which sends the request for the transaction to the issuing bank. The issuing bank will check whether the amount of the transaction does not reach the credit card’s limit before authorizing that transaction. If the transaction is valid the issuing bank will block the requested amount from consumer’s credit card account and send an authorization response to merchant bank. As soon as the authorization response is received by the merchant’s bank, the merchant is notified; the transaction is marked as completed and the consumer can take the goods.

- **Credit Card Fraud Techniques**

Various types of fraud techniques are as follows:

- **Site Cloning**

In site cloning the fraudster clone an entire site or just the payment page of the site where customer make a payment. The customer give up a credit card detail to the fraudster and then fraudster sends the customer a transaction receipt via email as genuine site. Thus fraudsters have all details of customer’s credit card so they can commit fraud without customer’s awareness.

- **Stolen / Lost Credit Card**

When customer card is lost or stolen by fraudster he gets all the information of the cardholder in the easiest way without investing any modern technology. It is difficult form of credit card fraud to detect.

- Skimming

Skimming is one of the popular forms of credit card fraud. It is a process where the actual data on a card is electronically copied to another. It is very difficult for cardholder to identify this type of fraud.

- **Credit Card Generator**

In credit card generator the computer program generates the valid credit card number and expiry gate. This generator creates a valid credit card highly reliable that it looks as the valid credit card number only and are also available for free download off the internet.

- **Phishing**

In phishing the fraudster sends lots of false email to card holder. The e-mail looks like they came from the website where the customer trust for example customers bank. The e-mail asks the customer to provide personal information like credit card number. With the help of these details fraudster commits crime.

- **Internal Fraud**

The employee or owner access customers detail. They steal the customer's personal information to commit crime or pass on the information about cardholder to fraudster for money. Although the use of credit cards as a payment method can be really convenient for our daily transactions; people must be aware of the risks that they impose themselves while using their credit cards. More accurately, the incremental usage of credit cards gave the chance to fraudsters to make use of their vulnerabilities [3]. Credit card fraud refers to any unlawful and unauthorized activity on the use of credit cards which is undertaken by a fraudster. According to [5] credit card fraud has been increased between 2005 and 2007.

An interesting query arises as to who is responsible to pay for all those losses in case of a credit card fraud. Delamaire et al. claim that merchants are really vulnerable in case of a credit card fraud because they are required to pay for the losses due to the so-called charge-backs [6]. Charge-backs are requested by the consumer's bank as soon as the consumer reports a transaction as unauthorized. Quah et al. congregates with the above statement by adding that merchants not only have to pay for the amount of the illegal transactions but also for any additional charges that are imposed by the credit card issuer [8]. So far banks are required to pay the costs of investigating whether a transaction, which is reported as illegitimate by the consumer, is indeed illegitimate as well as the costs of having the appropriate equipments for detecting fraudulent transactions [8].

Although clients are the least helpless in case of a credit card fraud there are states which enforce consumers to pay for the losses under particular circumstances. This happens in many countries in case the consumers do not understand that their credit cards have physically been stolen and fail to report the lost to their banks [8]. In particular the consumers are not forced to pay the losses of an illegitimate credit card transaction if they report the physical lost of card in time or if the card is not physically lost at all. In the first case there shall be no unlawful transaction at all since the credit card will be locked before the fraudster directs to use it. In the second case where only the details of the credit card are stolen and not the physical card itself; the unlawful transaction can be take on in places where the physical card is not required to be present like phone or internet. With today's technological advances that last type of fraud is very difficult to prevent and therefore the consumer is no longer liable for any losses that may occur. Therefore those losses burden merchants and issuing banks.

- **Credit Card Fraud Detection**

It has already been brought up that the losses of a credit card fraud can affect all consumers, merchants and issuing banks. Therefore, it is significant to establish techniques for detecting and preventing credit card fraud. There are varieties of methods which can be used to build fraud detection systems. Understanding the distinctiveness of all those techniques can be a tedious task. A technique which promises a high predictive accuracy may be an tempting candidate to be used in the fraud detection system. However, there are various different parameters that need to be considered before deciding which technique best suits the needs of a particular situation. For instance, if the above mentioned technique which assures a high predictive accuracy can be applied to a large data set and is appropriate for our situation.

A. Data Mining and Detection Techniques

This section describes the concept of data mining and the techniques which are used for detecting credit fraud. The main reason why these techniques are examined is that they form the source of the credit fraud detection and they are reported as an implementation advice by the expert system.

*B.*Data Mining

Supervised Learning

This is the most common learning approach where the model is trained using pre-defined class labels [6]. In the context of credit card fraud detection the class labels may be the legitimate or fraudulent transactions. A supervisor provides a training data set whose

transactions are classified in advanced as belonging to the "legitimate" or the "fraudulent" class. The training set can be used to build the predicting model. Any new transaction can be compared against the model to predict its class. If the new transaction follows a similar pattern to the illegitimate behavior – as this is described by the trained model – it will be classified as a fraudulent transaction.

Detection Techniques

Various data mining techniques can be used to detect credit fraud. Existing System uses HMM (Hidden Markov Model) for finding fraudsters.

Hidden Markov Model (HMM)

HMM allows more than one observations to be emitted by each state [44]. This is done by declaring different probabilities for each observation of each state [44]. Figure 1 which is taken from [44] illustrates a HMM.

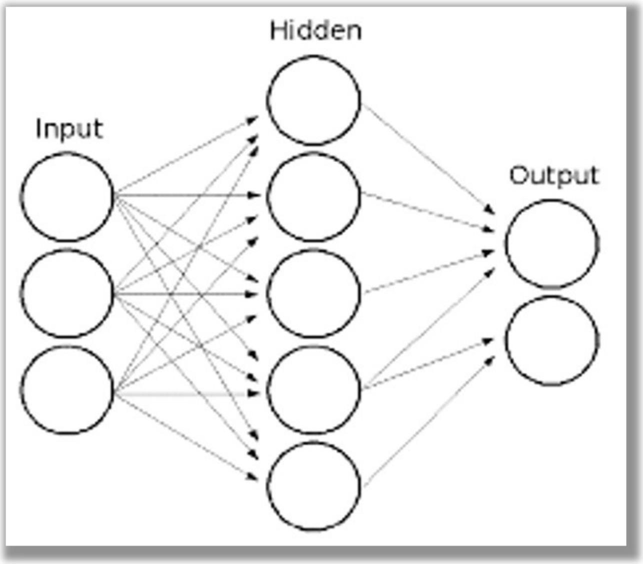


Fig 1. Hidden Markov Model

HMM consider mainly three price value ranges such as. a. Low (l), b. Medium (m) and, c. High (h). It finds out transaction amount belongs to a particular category either it is in low, medium, or high ranges based on threshold value. If the deviation is above a threshold value then it is treated as fraud else legal. But if the fraudulent transaction is less than threshold value it is not considered as fraud so no security questions are asked and the transaction will take in

progress. This is the main drawback of HMM model so Apriori algorithm used in proposed system to provide more security on POS card transaction.

- **Apriori Association Algorithm**

Apriori is an algorithm for frequent item set mining and association rule learning over transactional databases.

Frequent item set mining is used apriori and association rule learning technique for grouping legal and fraud transaction pattern efficiently from the database which contains large item set.

It proceeds by recognizing the frequent individual items in the database and widening them to larger and larger item sets as long as those item sets appear sufficiently often in the database. Card holders frequent purchase shops are easily identified from frequent item set. If new card swiping is done at any merchant shop, the details are compared with frequent item set and transaction proceeds only if new merchant is present in the data set else the cardholder has to give OTP for completing the process which will be sent as SMS to the registered mobile number. If card holder does not provide OTP then the transaction is considered and fraudulent transaction and it is blocked. This makes POS card transaction to be more secure and detect whether an incoming transaction is fraud or genuine in an effective way.

Advantages:

- avoid rescanning the database
- reduce the size of candidate itemsets
- accelerate both joining and the pruning process.

Case 1: Valid User Access

If a user carry outs an online transaction then his spending profile is matched into the database and if it matches then the transaction is carried out successfully and then user is notified that transaction is done successfully.

Case2: Invalid User Access

If an invalid user tries to perform an online transaction and if the spending profile doesn't matches into the database then access is blocked to that user and system failure occurs and it also sends notification on authorized user's mobile number and raises the alarm to Admin System. The accuracy for the proposed method is shown in the Fig 3.

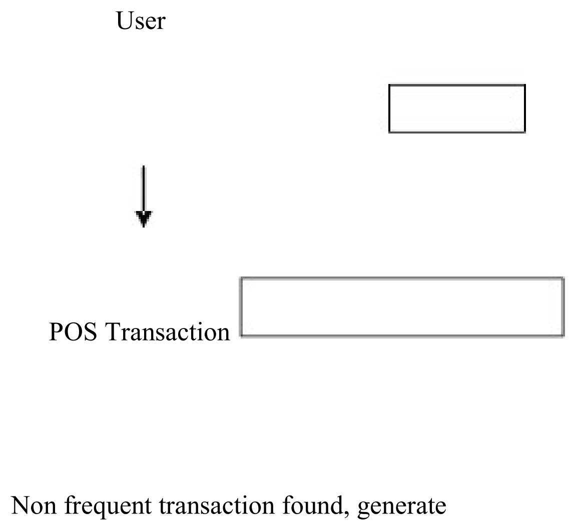
The benefit of the Aprori-based approach is large reduction in the number of False Positives transactions acknowledged as malicious by a fraud detection system even though they are categorically genuine.

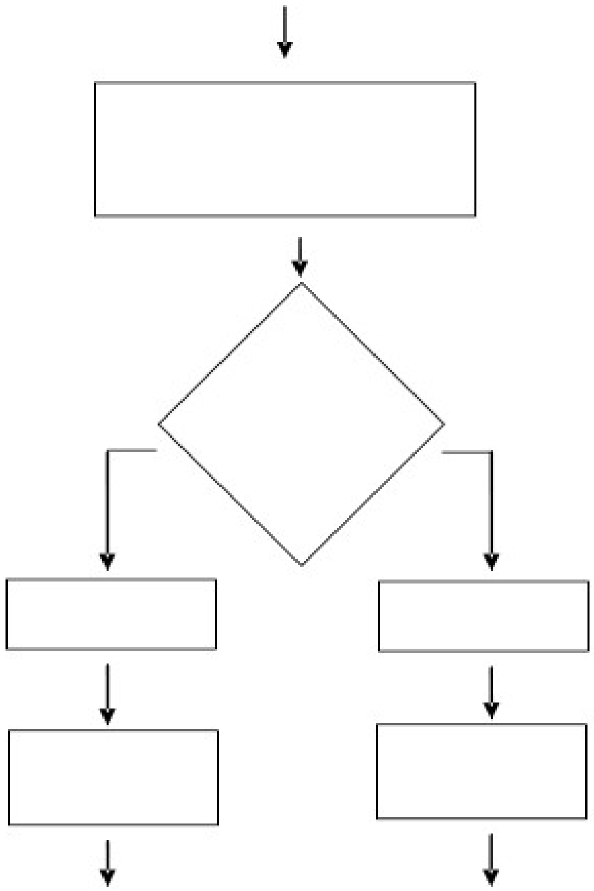
Conclusion

Apriori is used to detect fraud activities on credit card. The model maintains the database in which users transaction behaviors and pattern are saved and if any unusual transaction is carried out which is different from passed behavior of that user then system raise alarm and the transaction is blocked. This algorithm makes the processing of detection very easy and tries to remove the complex difficulty. Efficient credit card fraud detection system is an utmost required for card issuing bank to all type of online transaction that through using credit card. The very easily detect and remove the complexity of system by using Apriori model. It has also explained how to detect an incoming transaction is fraudulent or not. Comparative studies reveal that the accuracy to the system is also 87-90% over a wide variation in the input data. The system is also scalable for handling large volumes of transaction.

Working System Model

The working system has the two possibility case; it is represented in the Fig 2.





OTP and send as SMS to registered Mob. no.

Yes If No

User

Provides

OTP

Give Access Block Access

Transaction Transaction

Successful Failure

Send Notify the Notification to

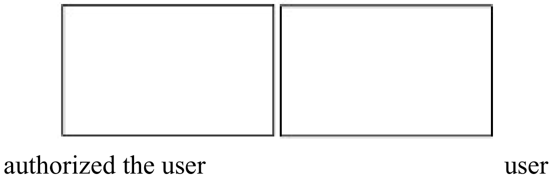


Fig 2. Flow of Apriori Algorithm

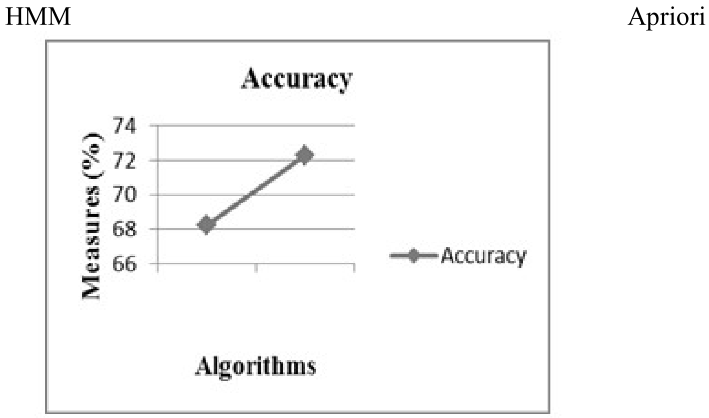


Fig 3. Comparison of Accuracy in line graph

References

- Linda Delamaire, Hussein Addou, John Pointon, "Credit card fraud and detection techniques: a review", Banks and Bank Systems, vol. 4, no. 2, pp. 57-68, 2009.
- J.T. Quah, M. Sriganesh, "Real - time credit card fraud detection using computational intelligence," Expert Systems with Applications, pp. 1721-1732, 2008.
- M. F. A. Gadi, X. Wang and A. Pereira do Lago, "Credit Card Fraud Detection with Artificial Immune System" , Springer - Verlag Berlin Heidelberg, pp. 119- 131, 2008.
- T. Kavipriya, N. Geetha, " An identification and detection of fraudulence in credit card fraud transaction system using data mining techniques", International Research Journal of

Engineering and Technology (IRJET), Volume: 05 Issue: 01, Jan-2018.

- Mhamane S. S, Lobo L. M. R. J., “Use of Hidden Markov Model as internet banking fraud detection”, International Journal of Computer application (0975- 8887), vol. – 45- No. 21, May 2012.
- Dr. D. Ourston, Ms. S. Matzner, Mr. W. Stump, Dr. B. Hopkins, “Applications of Hidden Markov Models to Detecting Multi -stage network attacks”, Proc. Of the 36th Hawaii International Conference On system sciences (HICSS’03), IEEE, 2002.
- Renu, Suman, “Analysis on Credit Card Fraud Detection Methods”, International Journal of Computer Trends and Technology (IJCTT) – Volume 8 number 1 – Feb 2014.
- C. Phua, V. Lee, K. Smith, and R. Gayler, “A Comprehensive Survey of Data Mining-Based Fraud Detection Research,” http://www.bsys.monash.edu.au/people/cphua/. Mar. 2007.
- Shailesh S. Dhok, Dr. G. R. Bamnote, “Credit Card Fraud Detection Using Hidden Markov Model”, International Journal of Advanced Research in Computer Science, Volume 3, No. 3, May 2012.
- N. Laleh and A. M. Azgomi, “A Taxonomy of Frauds and Fraud Detection Techniques,” ICISTM, vol. 31, pp. 256-267, 2009.
- I - Cheng Yeh and Che – hui Lien , et al. “The comparisons of data mining techniques for the predictive accuracy of probability of default of Credit Card Clients”, “Expert Systems with Applications” 2009.
- Mohamed Hegazy, Ahmed Madian,Mohamed Ragaie, “Enhanced Fraud Miner: Credit Card Fraud Detection using Clustering Data Mining Techniques”, Egyptian Computer Science Journal (ISSN: 1110 – 2586) Volume 40 – Issue 03, September 2016.