Virtual Card Creation for Secured Transaction

Manikandan P[1] and Latha R[2],
[1]PG Scholar and [2]Assistant Professor,
[1,2]Department of MCA,
Vel Tech High Tech Engineering College, Chennai, India.

Abstract: Virtual card may be a limit virtual Debit (VDB), which might be created mistreatment any net banking facility fir ecommerce (online) transactions. The VDB is accustomed look on-line at any merchandiser web that accepts visa cards, with none distinction from a daily plastic card, the cardboard are going to be issued by marking a lien on the chosen account and actual debit to the account an happen only the cardboard is employed. You able to use your virtual card in the slightest degree merchandiser websites in Asian nation that settle for virtual visa card virtual master card debit card as a payment choice (payment in Indian Rupee). However, sites like the adult entertainment-sites, gambling are prohibited. Virtual Card cannot be used POS machines or ATM for money withdrawal or for continual/installments payments or for the other dealings that needs physical card.

Keywords: Component; Secret key generation; multiple transaction; online transaction; security

I. INTRODUCTION

A transaction system which will replace physical wallets with card-based virtual wallets and allow wallet to transactions, thereby passing the master card or visa network. In order to appreciate the concept it is important to understand the typical process flow for credit and debit card based transaction at a merchant outlet and the commission or charges involved therein. The larger number of credit and transactions including online and regular purchases. As the number of credit card user riskworldwidethe opportunities for attackers to steal credit card details and subsequently, commit fraud are also increasing Credit card based purchases can be categorized into two types: 1) physical card and 2) virtual card In a p 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 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 know the card details.

II. RELATED WORK

Credit card fraud detection has drawn a lot of research interest and a number of techniques with special emphasis on data mining and neural networks have been suggested. [1]Ghosh and Reilly have proposed credit card fraud detection with a neural network they have built a detection system which is trained on a large sample of labeled credit card account transactions.

Mata learning is a general strategy that provides a means for combining and integrating a number of separately built classifiers or models[2]Chiu and Tsai have proposed web services and data mining techniques to establish a collaborative scheme for fraud detection in banking industry With this scheme participating banks share knowledge about the fraud patterns in a heterogeneous and distributed environment The problem with most of the above mentioned approaches is that they require labeled data for both genuine as well as fraudulent transactions to train the classifiers E-commerce is booming increasingly these years however both merchant organization and consumer still remain concerns about security issue in online payment applications.

We present a Hidden Markov Model (HMM) based credit card FDS which does not require fraud signatures and yet is able to detect frauds by

considering a cardholders spending habit. The model a credit card transaction processing sequence by the stochastic process of an HMM the details of items purchased in individual transactions are usually not known to and FDS running at the bank that issues credit cards to the card holders. This can be represented as the underlying finite Markov chain which is not observable.

III. METHODOLOGY

Virtual Card is really not a card but a set of numbers that is generated by a financial service provider to enable a consumer to make online purchases. A Virtual Card comes with a credit limit and is usually accompanied by an expiration date Depending on choices offered by the financial entity and options taken by the usera Virtual Card may work for multiple transactions or may expire with only one single use. Most of the time a Virtual Card is generated to be used with one merchant and for one specific purchase only.

A Virtual Card is seen by many as an excellent method to reduce the potential of credit card fraud for many reasons A Virtual Card is usually created to be used for a specific purchase of a specific value with a specific merchant Technically it is highly unlikely that a Virtual Card can be used to make any other form of purchases even if the details are stolen For all practical purposes virtual credit cards can only be used online and are the perfect solution for online shopping.

The instances where transactions can be carried out over the mail in such cases the virtual credit card is only useful if the sales executive undertaking the transaction is using the online payment channel on behalf of the customer.

In this case the amount is topped up into the virtual card is debited from the person's savings bank account Another good option is the e-wallet which is generated and set up against the customer's savings bank account These options also come with the same provisions and limitations as that of a virtual credit card The only difference is that in this case the balance amount on the card is transferred back to the user's savings bank account and the amount is deducted immediately from the customer's bank account and not billed against their card.

An HMMis a double embedded stochastic process with two hierarchy levels It can be used to model much more complicated stochastic processes as compared to a traditionalMarkov model AnHMMhas a finite set of states governed bye set of transition probabilities In a particular state an outcome or observation can be generated according to an associated probability distribution It is only the outcome and not the state that is visible to an external observer [3] HMM-based applications are common in various areas such as speech recognition bioinformatics and genomics Inrecent years Joshi and Phobia [4] have investigated the capabilities ofHMMin anomaly detection They classify TCPnetwork traffic as an attack or normal using HMM. Cho and Park [5] suggest an HMM-based intrusion detection system that improves the modeling time and performance byconsidering only the privilege transition flows based on the main knowledge of attacks. Ours ton et al [6] have proposed the application of HMM in detecting multistage network attacks Hoang et al [7] present a new method to process sequences of system calls for anomaly detection usingHMMthe key idea is to build a multilayer model of program behaviors based on both HMMs and enumerating methods foranomaly detection.We implement the idea of virtual card transaction into an organization here we describe the virtual card transaction provide alert message to organization manager Once the user make transaction then the one time password expired Then the alert message is send to the manager to check the transaction detail via (mail) The alert message contains the transaction amount and purchased date Time and the name of the product that purchased The manager has authority to cancel the transaction within one hour after the transaction successful If virtual card manager check transaction detail via mail and then check the transaction are belongs to the organization if transaction are not belong to organization or not authorized then the transaction are canceled by the virtual card manager Hence the virtual cannot be misused in any time.

Organization manager: With every transaction the organization manager get request of the transaction and then the manager need to make conform click to make the successful transaction before the conformation the manger check the detail of the transaction in the transaction request.

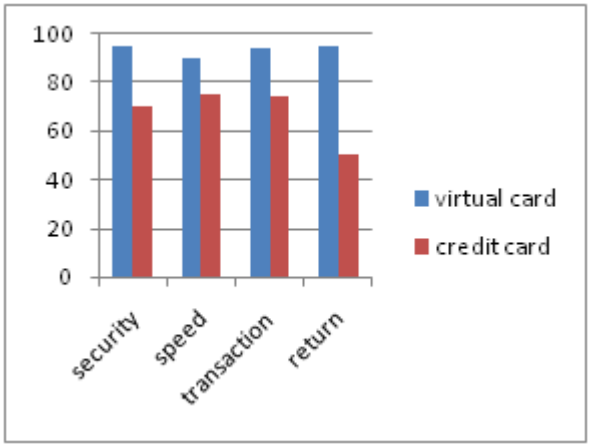

Fig-1: Transaction Comparison between Virtual Card and Credit Card

Virtual card created by organization manager, he has given virtual card to his client members. It is valid only particular period of time, so it makes the transaction as more security and effective manner. Time limit of transaction is fixed, hence the speed and number of transaction will be increases, if transaction goes fails then money of virtual card will be return to organization account. In credit card has no return policy.

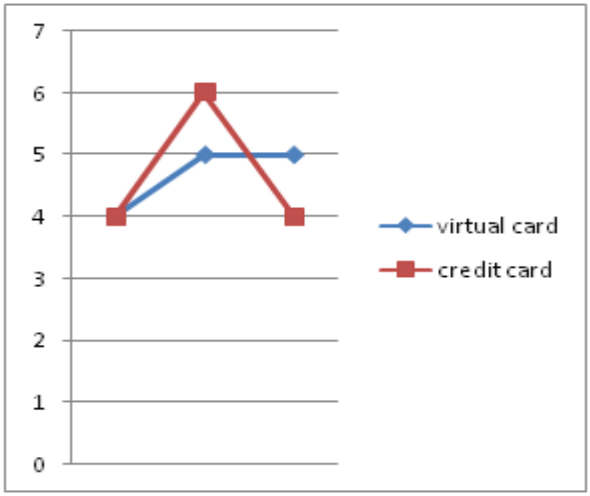

Fig. 2 Time Efficiency of Virtual Card

CONCLUSION

In our proposed system we are implement the virtual card system and its transaction.Virtual card having unique no and time limit. Each transaction must be completes within its time exist else the transaction will be canceled and amount will return to their account.Once the transaction is completed then we can reuse the same virtual card for another transaction.Transaction will be increased as secure manner and fraud usage was avoid successfully.

REFERENCES

[1] S. Ghosh and D.L. Reilly, "Credit Card Fraud Detection with neural-Network," Proc. 27th Hawaii Int'l Conf. System Sciences: Information Systems: Decision Support and Knowledge-Based Systems, vol. 3, pp. 621-630, 1994.

[2] C. Chiu and C. Tsai, "A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. e-Technology, e-Commerce and e-Service, pp. 177-181, 2004

[3] "A gentle tutorial of the EM algorithm and its application to Parameter Estimation for Gaussian mixture and Hidden Markov Models", J. A.

[4] S.S. Joshi and V.V. Pahoa, "Investigating Hidden Markov Models Capabilities in Anomaly Detection," Proc. 43rd ACM Ann. Southeast Regional Conf., vol. 1, pp. 98-103, 2005.

[5] Credit card fraud detection using Hidden Markov Model", Albina Srivastava, MalanKudu, Shamik Sural, Senior Member, IEEE, and Arum K. Maunder, Senior Member, IEEE

Credit card fraud detection using Hidden Markov Model", Albina Srivastava, Amlan Kudu, Shamik Sural, Senior Member, IEEE, and Arum K. Maunder, Senior Member, IEEE

[6] E. Aleskerov, B. Freisleben, and B. Rao, "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection," Proc. IEEE/IAFE: Computational Intelligence for Financial Eng., pp. 220-226, 1997.

[7] M.J. Kim and T.S. Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," Proc. Int'l Conf. Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002.

[8] W. Fan, A.L. Prodromidis, and S.J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," IEEE Intelligent Systems, vol. 14, no. 6, pp. 67-74, 1999.

[9] R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. Tools with Artificial Intelligence, pp. 103-106, and 1999.

[10] C. Chiu and C. Tsai, "A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. e-Technology, e-Commerce and e-Service, pp. 177-181, 2004.