www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume2 Issue 8 August, 2013 Page No. 2549-2554

Prevention of Credit Card Fraudulence in Point-of-Sale Terminus

Manoj Prabhakar
[#]Anna University, India
manojkrishs@gmail.com

Abstract— *The credit card fraudulence has become more vulnerable threat in recent days. The period between the credit card theft and blocking of it is sufficient for intruder to get away with all amount in it by swiping in POS (Point-Of-Sale) Terminus and stealing the entire amount in it. It can be prevented by taking the cumulative average of first 'n'(eg 10) transactions that has done by the user in that credit card through POS and when the next transaction has been done, if the Standard Deviation of amount usage is more than average of first 'n' transactions, then the banks should enable PIN(Personal Identification Number) for that particular transaction and if the PIN entered is wrong, the card will be blocked and the user should go to bank in person and reveal his identity and activate the card again*
.

***Keywords*— Personal Identification Number, Point-Of-Sale, credit card fraudulence, Standard Deviation, cumulative average**

Introduction

Credit card has become the most important part in man's life. These Cards are issued by the financial institutions like banks to help cardholders in making payments for services instead of providing ready cash. Generally these cards will be of size 8.5 cm by 5.5 cm. There are many fraudulence activities done by the mischievous people by stealing others credit cards. This can be eliminated by having the cumulative average of one person's consumptions over a particular period of time.

A card which indicates that, the card holder has granted a line of credit, which can be used by cardholder to withdraw cash, service or product up to a specific and set credit limit. Payments are usually made monthly or specific predefined period and interest is charged upon unpaid amount. It is generally termed as "Buy Now & Pay Later".

Credit card fraudulence has been the wide ranging theme in recent days with 4 out of every 10,000 transactions made in credit cards were found to be fraud.

I. *Credit Card*

Generally a credit card transaction consists of many stages in it. The Purchase transactions that are made with bank cards operate on four party payment systems, with every party playing a critical role in transactions.

a. Card Holder: Customer of a financial institution who have been issued card against the money he or she hold with the financial institute like banks.
b. Merchant: The merchant is a seller of goods or services to the cardholder. He will get the cash payment in his account which he holds with acquiring bank after the transaction with the card holder is over.
c. Card Issuer: It is the card issuing bank to the customer.
d. Merchant acquirer: The financial institution which charges MSC [Merchant Service Commission] to the merchant is known as acquirer. This same institution makes payment to the merchant. Usually merchant hold an account with acquiring bank.

The Following figure explains the general purchase transaction process. Here, there are two financial institutions, card issuer (card holder's bank) and merchant acquirer (Merchant's bank). They act as the providers of purchase transaction services to the 'consumers' of payment transaction services.

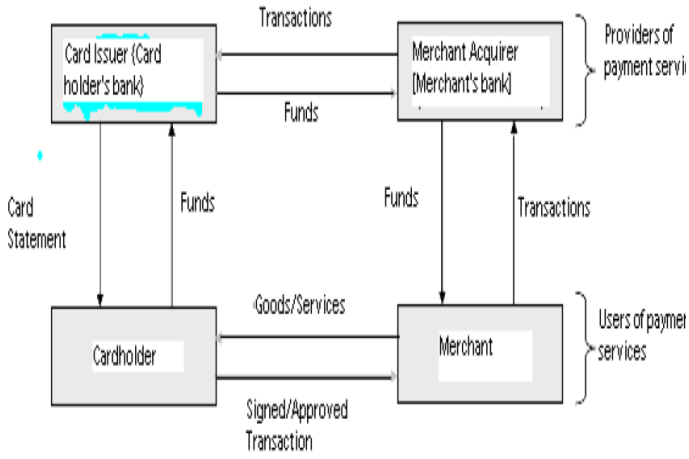

Fig 1: Four party purchase transaction process

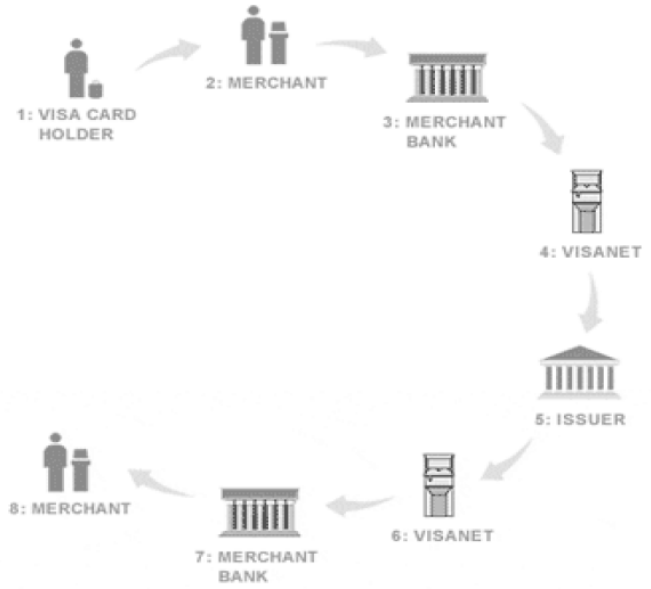

Fig 2: Authorization process

Depending on the payment market, there is fifth party also involved in bankcard transaction such as Visa or MasterCard, which directly or indirectly faclitates the transaction. The interaction between the four parties (issuer, acquirer, cardholder and merchant) is done through a system which is maintained and supported by this fifth party like visa or mastercard.

Authorization:

Authorization is the process of checking the availabliliy of sufficient funds available to cover the amount of transaction and to verify that the card is authentic and not reported stolen. An authorization number, which os of five digits, will be generated for every transactions.

The following figure explains the authorization process.

The cardholer/ customer presents the card to the merchant. The merchant forward this request to merchant bank via POS (Point-of-Sale) equipment. Merchant bank forwards this request electronically to issuer bank using card association networks like VISA in this case. Issuer banks chekcs the validity of the card and for the authorized customer. For payment, it is again routed to merchant bank through card association network.

Point-of-Sale Terminus:

Point-of-Sale equipment helps the customer to do merchandising or pay bills using his or card. It helps in cash less merchandizing. Standalone Point-of-Sale (POS) equipments, available with merchants, restaurants and hotels use a dial-up device to connect with card associations networkslike VISA. POS equipments are available with printing facilities for receipts, and PIN pads.

Fig 3: POS Machine

Simple POS Transaction Network:

A simple POS transaction can be explained woth the following figure,

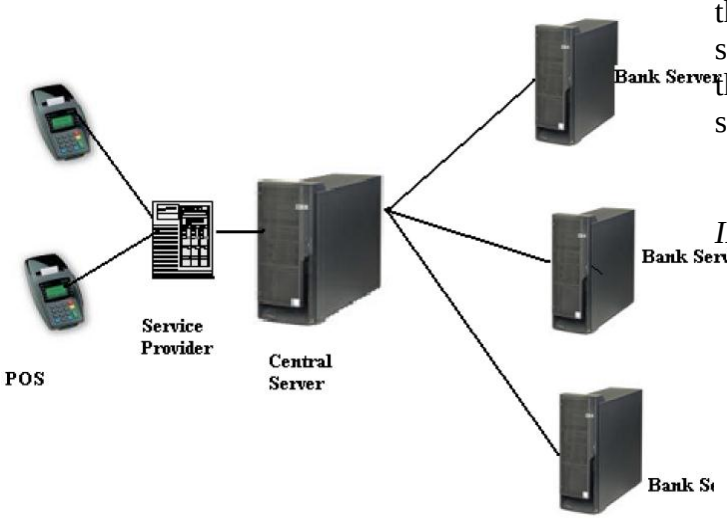

Fig 4: POS Transaction

The POS equipment is attahced to the central server via service provider. The service provider can be a telephone company for dial up or a leased line company. This centralized server is connected to the bank servers for authorization process.

II.Credit Card Fraud

Credit card fraud generally begins with the theft of the physical card from the owner or with the compromise of data that has been associated with that account, including the card account number or the other information that are needed by the merchants routinely during the appropriate transaction. The compromise can occur by many ways which are not known by the cardholder, merchant and the issuer, at least until the fraud transaction got over. Stolen cards can be reported quickly by the card holders as soon as he got to know that his card has been stolen. But when it has been compromised, then it is known to card holders only when the transaction has been done in it.

When a credit card is lost or stolen, it can be used by the person, with whom that card is present, illegally until the original card holder notifies the issuing bank about the lost card. Almost all the banks are nowadays having the 24 hours telephone banking to safe guard their customers from fraudulency. He or she can call the respective bank and can cancel the card before it has been used for any unauthorized transaction. Usually, the security PIN (Personal Identification Number) will be used by the card holders during transactions. The only common security measure that is present on all cards is a signature panel. But, depending on its design, these signatures can be easy to forge. There are some scenarios, where the merchants will have look of their picture ID like driving licence, to verify he or she is the original card holder.

III.Connectivity of the National Financial Switch [NFS]

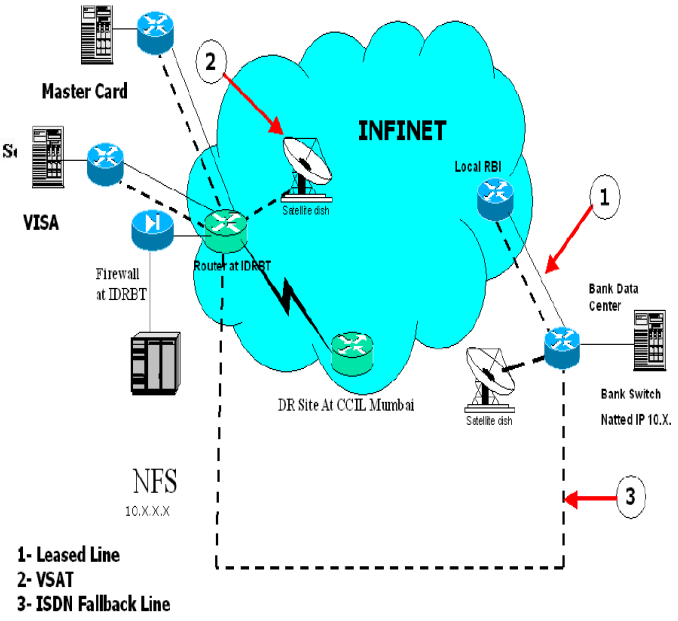

Fig 5: National and International Connectivity of NFS

The above figure explains the connectivity of national financial switch [NFS]. NFS use the INdian FInancial NETwork [INFINET], It is the satellite based communication network that generally works during the transaction in POS terminus present with the merchant. It happens between the closed user group of banking and financial sectors to connect the banks' financial switch to the RBI (IDRBT) main switch. The bank data centre is also connected to Clearing Corporation of India for financial clearing and settlement. System also provides ISDN fall back line in case of failure to keep network up. For international clearance and settlement, NFS is also connected to MasterCard and Visa networks.

IV.Fraudulence Detection

In order to overcome the credit card fraudulence in Point-of-Sale terminus, we can have a cumulative average of certain number of transactions that has been done in that card over a certain span of time. Generally, the cards will be given only PIN (Personal Identification Number) to enter during any

of the transactions that has been done by using the card. If the card has been manhandled, then it will be easily prone to attack. So, another extra pin will be given by the banks to that particular card in order to eliminate the case of theft. When the card pin is given to card holder, another set of custom pin should be set by the card holder, which in turn will be used only on the unusual circumstances.

In this case, when the card has been used by the card holder after his purchase of card, his account activities will be monitored and the amount he or spends in n number of transactions has been monitored closely. The cumulative averaging of all the records of transactions has been recorded and once the number of transactions is complete, the average of all the transactions will be considered. From the very next transaction, the amount spent by the consumer in Point-of-Sale terminus will be compared with the cumulative average of the previous n transactions. If the deviation from the current transaction with the recorded transaction is less, then normal PIN will be taken into consideration. If the deviation of amount from the cumulative transaction is more than the actual transaction, then the extra custom PIN that has been set by the consumer should be asked along with the normal PIN. If the consumer is real and if it has been used by original consumer, then he knows the second PIN, so that the transaction will be smoothly carried out. If the PIN is given false, then the card will be blocked instantly and it can be used only after releasing the card by proper guidelines.

This method will be very much useful because, usually if the card has been stolen, then the thief will have the mentality of using the card maximum amount in one swipe, which eventually will force him to buy everything in single purchase. In case, the original consumer took little extra time to block the card and before that when the thief tries to use that card in POS, he does not know about this sort of mechanism. When the second PIN is given wrong, the card will be blocked in the very first time, so that he will not have enough time to recover from it.

Here, in order to determine the cumulative averaging and for comparison of average and the next transaction, we will be using cumulative averaging algorithm and recursion algorithm.

A.Cumulative averaging algorithm

The cumulative averaging is the analysis of frequency of occurrence of values of a phenomenon less than that of a reference value. This phenomenon can be space or time dependent. This sort of cumulative frequency is also called as *frequency of non-exceedance.*

This algorithm is one where you incrementally accumulate a larger value by repeatedly adding, multiplying, etcetera, and storing the result into a variable over and over. One of the key aspects of this algorithm is that in a loop, a variable declared outside the loop whose values can be modified inside the loop.

```
        def factorial(n):
        if n < N: return 1
    return reduce(lambda x, y: x*y, xrange(2, int(n)+1))

  def prob(s, p, n):
    x = 1.0 - p

    a = n - s
    b = s + 1.0

    c = a + b - 1.0

    prob = 0

    for j in xrange(a, c + 1):
      prob += factorial(c) / (factorial(j)*factorial(c-j)) \
            * x**j * (1 - x)**(c-j)

    return prob

  def erf(z):
      t = 1.0 / (1.0 + 0.5 * abs(z))
      # use Horner's method
      ans = 1 - t * math.exp( -z*z -  N1 +
                                  t * ( N2 +
                                  t * ( N3 +
                                  t * ( N4 +
                                  t * ( N5 +
                                  t * ( N6 +
                                  t * ( N7 +
                                  t * ( N8 +
                                  t * ( N9 +
                                  t * ( N10))))))))))
      if z >= AV(N):
          return ans
      else:
          return -ans

  def normal_estimate(s, p, n):
    u = n * p
```

```
o = (u * (1-p)) ** 0.5

return 0.5 * (1 + erf((s-u)/(o*2**0.5)))
```

Cumulative frequency is the record of observed data x1,x2,,,,xN on a variable phenomenon X.

The Cumulative frequency Mx, of a reference value X is the frequency in which the observed values are less than or equal to X

$$M_{X_r} = \text{number}\{k|x_k \leq X_r\} = \sum_{k=1}^{N} I(x_k \leq X_r).$$

In this, the formula is the indicator function. The relative cumulative frequency, written as Fc(X), can be calculated from

$$F_C(X_r) = \frac{M_{X_r}}{N}.$$

This expression can be noted as

$$F_C = \frac{M}{N},$$

Where M = Mxr

When Xr = Xmin, where Xmin is the unique minimum value observed, it is found that Fc = 1/N, because M = 1. On the other hand, when Xr=Xmax, where Xmax is the unique maximum value observed, it is found that Fc = 1, because M = N.

In percentage the equation reads:

Fc(%) = 100M / N

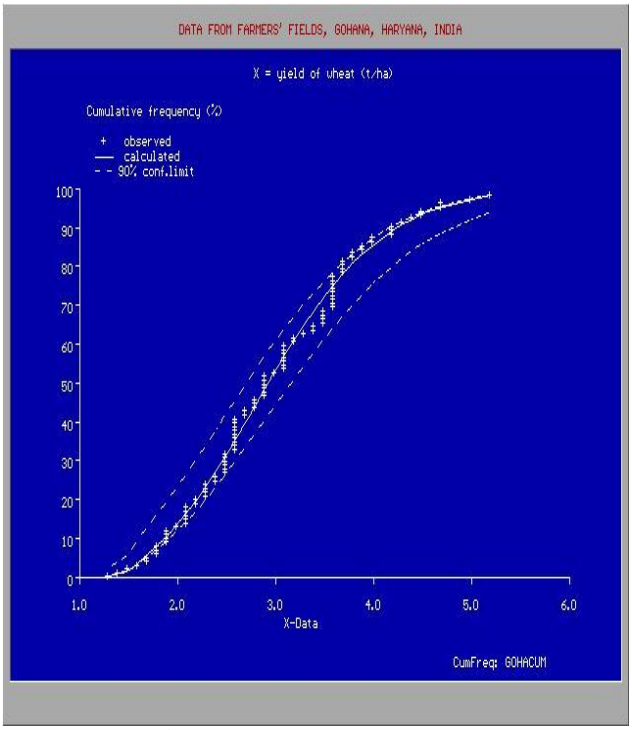

Fig 5: Cumulative frequency distribution, adapted cumulative probability distribution, and confidence intervals

The cumulative frequency can be encoded as the following code

```
using namespace std;

unsigned sumDigits(unsigned);
unsigned numDigits(unsigned);
unsigned cumSumDigits(unsigned);

int main(int argc, char *argv[]) {
  unsigned n;
  stringstream ss;
  string line;

  while (true) {
    cout << "> ";
    getline(cin,line);
    ss.str(line);
    if (ss >> n) {
      cout << cumSumDigits(n) << endl;
    }
    ss.clear();
  }
  return 0;
}

unsigned numDigits(unsigned n) {
  if (n < 10) return 1;
  return 1 + sumDigits(n / 10);
}
```

```
unsigned sumDigits(unsigned n) {
  if (n < 10) return n;
  return (n % 10) + sumDigits(n / 10);
}

unsigned cumSumDigits(unsigned n) {
  if (numDigits(n) == 1) return n;
  return cumSumDigits(sumDigits(n));
}

#if 0
```

B. Recursive Algorithm

A recursive algorithm is an algorithm which calls itself with "smaller (or simpler)" input values, and which obtains the result for the current input by applying simple operations to the returned value for the smaller (or simpler) input. More generally if a problem can be solved utilizing solutions to smaller versions of the same problem, and the smaller versions reduce to easily solvable cases, then one can use a recursive algorithm to solve that problem. For example, the elements of a recursively defined set, or the value of a recursively defined function can be obtained by a recursive algorithm. If a set or a function is defined recursively, then a recursive algorithm to compute its members or values mirrors the definition. Initial steps of the recursive algorithm correspond to the basic clause of the recursive definition and they identify the basic elements. They are then followed by steps corresponding to the inductive clause, which reduce the computation for an element of one generation to that of elements of the immediately preceding generation. In general, recursive computer programs require more memory and computation compared with iterative algorithms, but they are simpler and for many case a natural way of thinking about the problem.

The algorithm can be given as

```
def rec_cumsum(numbers):
    if len(numbers) == 0 : return temp

    # You need to check, if `temp` is empty, that means method is called first time.
    if not temp:
        temp.extend([numbers[0]])     // Just add the first element to it.

    else:
        # Else, get the last element from `temp`,
        # add it to `first elemt` in `numbers` and add it to `temp`.
        temp.extend([temp[-1] + numbers[0]])

    return rec_cumsum(numbers[1:])

my_list = [N1,N2,....N10]
temp = []
print rec_cumsum(my_list)
```

The recursive function can be sorted so that all the amount of transactions will be compared and done recursively. The algorithm has been shown for the sample size of 5

```
(define small-sort (a)
  "Sort a vector A of length 5"
  (if (> (aref a 0) (aref a 1))
     (rotatef (aref a 0) (aref a 1)))
  (if (> (aref a 2) (aref a 3))
     (rotatef (aref a 2) (aref a 3)))
  (if (> (aref a 0) (aref a 2))
     (progn
       (rotatef (aref a 0) (aref a 2))
       (rotatef (aref a 1) (aref a 3))))
  (if (> (aref a 4) (aref a 2))
     (if (> (aref a 4) (aref a 3))
        (progn)
        (rotatef (aref a 3) (aref a 4)))
     (if (> (aref a 4) (aref a 0))
        (rotatef (aref a 2) (aref a 4) (aref a 3))
        (rotatef (aref a 0) (aref a 4) (aref a 3) (aref a 2))))
  (if (> (aref a 1) (aref a 3))
     (if (> (aref a 1) (aref a 4))
        (rotatef (aref a 1) (aref a 2) (aref a 3) (aref a 4))
        (rotatef (aref a 1) (aref a 2) (aref a 3)))
     (if (> (aref a 1) (aref a 2))
        (rotatef (aref a 1) (aref a 2))
        (progn)))
  a)

(define check-sorted (a)
  (do ((i 0 (1+ i)))
     ((>= i (1- (array-dimension a 0))))
    ;;(format t "~S ~S~%" (aref a i) (aref a (+ 1 i)))
    (assert (<= (aref a i) (aref a (+ 1 i))))))
(define rr ()
  (dotimes (i 100000)
    (let ((a (make-array 5 :initial-contents (list (random 1.0) (random 1.0) (random 1.0) (random 1.0) (random 1.0) ))))
```

```
;;(format t "A=~S~%" a)
(let ((res (small-sort a)))
  (check-sorted res)
  ;;(format t "Res=~S~%" res)
  ))))
```

IMPACTS

Current Scenario:

Now-a-days, there are more fraudulence happening all over the world. Usage of credit card is on rise, which eventually will be very much advantageous for people when used properly and efficiently. It is the duty of every human being to safe guard his properties and banks to secure our money, so that it can be used by the rightful owner of that product. Technology advances have prepped credit cards for easier use and tighter security. It's now up to consumers to make the changes widespread. It's now possible to make a credit card purchase without ever taking the card out of your wallet. According to the recent survey conducted by Nilson report, there are about 181 million credit cards are used in USA and it is rapidly growing in all the emerging countries. So, it is wise to secure the credit cards from intruders.

After This Work:

After the implementation of this concept, the usage of credit cards will be much more secure and there will be more awareness among people regarding the usage of the credit cards in all merchant stalls. Apart from that, we can prevent most of the people from the hands of thieves, and can safeguard their earned money. The importance of protecting your credit card information is even more essential now, with the introduction of online shopping. As such, it's wise to be proactive in preventing such thing from happening to you. Furthermore, the responsibility always lies with credit card holders to safeguard their credit cards.

CONCLUSION

Thus this is the concept of implementing added security to our normally secured credit cards, thereby making the work of intruders as a nightmare and saving the money of people to the maximum extent. With further improvements in the technology the process can be made even better.

REFERENCES

[1] http://www.buildingjavaprograms.com/labs/3ed/ch04-cumulative-algorithms.shtml#slide2

[2] http://stackoverflow.com/questions/1095650/how-can-i-efficiently-calculate-the-binomial-cumulative-distribution-function

[3] http://en.wikipedia.org/wiki/Cumulative_frequency_analysis

[4] http://en.wikipedia.org/wiki/Credit_card_fraud

[5] http://money.howstuffworks.com/personal-finance/debt-management/credit-card2.htm

[6] http://stackoverflow.com/questions/1935194/sorting-an-array-with-minimal-number-of-comparisons

[7]http://www.cs.odu.edu/~toida/nerzic/content/recursive_alg/rec_alg.html

[8] http://stackoverflow.com/questions/13347515/recursive-cumulative-sums