International Journal of Advanced Research in

Business Management and Administration

Volume: 1 Issue: 1 13-Apr-2015,ISSN_NO: 2348 -2354

SECURING FINANCIAL TRASACTIONS USING HMM AND LOCATION BASED SERVICE.

Purval kharat , Ankush bhat , Rohitwattal,Yogesh kamble.

Abstract: *ATMs have brought so much relief to the financial world. Various problems were solved with the advent of these machines ranging from keeping the banking hall free of traffic with its attendant issues. Gone are the days of maintaining long queues in the banking hall which made the work of bankers more difficult thus leading to all forms of errors. Even to customers, having to leave the comfort of their homes for financial transactions before bankers close for the day's business is a major problem solved by Automated Teller Machines. However, as man begins to realize the gains of technology brought about by this machine to supplement human tellers, little did one know that the joy shall be short lived by the various sharp practices leading to financial losses. As banks are losing, so are the customers. News Media are filled with various forms of complaints on how users are losing money to fraudsters. Some have vowed never to come near usage of various cards – debit, credit or prepaid – local or international. The problem may even go as deep as engaging in legal battle between banks and their customers. The need to find a lasting solution is the main focus of this project.*

Keyword-Hidden Markov Model ,online transaction, Ecommerce, Clustering ,location based services.

1, Introduction:

Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years. A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it

are also rising. In this paper, we model the sequence of operations in credit card transaction processing using a hidden Markov model (HMM) and show how it can be used for the detection of frauds. Along with HMM we are providing location based service that is user is allowed to do transactions from specified locations only.If he does transactions from unspecified locations the system will detect that some fraud activity is taking place and he or she is denied acess.

1.1, Introduction of HMM:

A Hidden Markov Model is a finite set of states; each state is associated with a probability distribution. Transitions among these states are administered by a set of probabilities called transition probability. In a specific state a conceivable outcome or observation can be created which is associated symbol of observation of probability distribution. It is only the result, not the state that is evident to an external viewer and therefore states are ``hidden" to the outside; resulting the name Hidden Markov Model. Hence, Hidden Markov Model is a perfect way out for dealing with detection of fraud transaction using credit card.

HMM consider mainly three price value ranges such as

1) Low (l)

2) Medium (m) and

3) High (h).

First, it will be required to find out transaction amount belongs to a particular group either it will be in low, medium, or high ranges.

TABLE 1
Example Transactions with the Dollar Amount Spent in Each Transaction

Transaction No.	1	2	3	4	5	6	7	8	9	10
Amount (in $)	40	25	15	5	10	25	15	20	10	80

Volume: 1 Issue: 1 13-Apr-2015,ISSN_NO: 2348 -2354

The implementation technique used in HMM is creating clusters of training sets so as to identify spending profile of card holder. The type of items purchased works as states for the model. The transition from one state to another is determined by probability distribution. It requires minimum 10 previous transactions, on the basis of which the fore coming transaction is chosen as fraud or genuine.

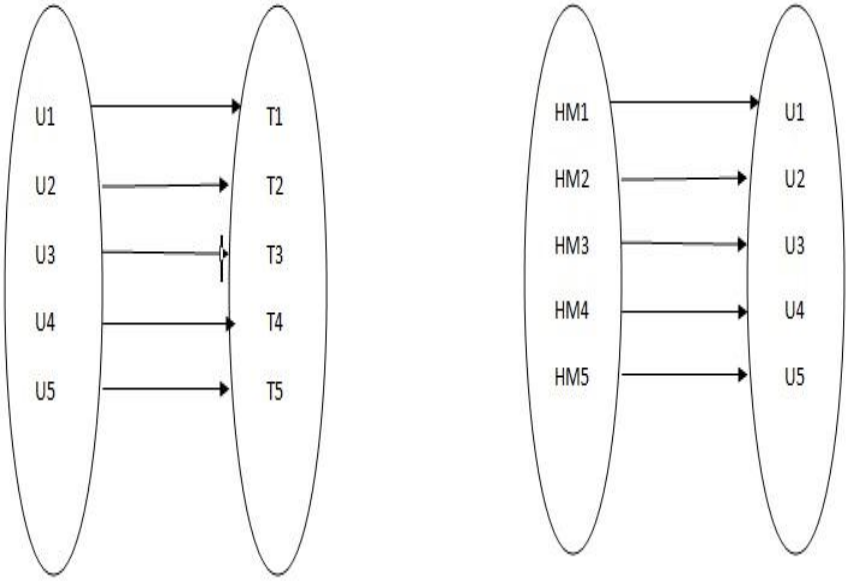
The model goes through two stages. In the first stage training of the system is done. Second stage works for the detection of the fraud, based on the expected range of amount the transaction. The expected amount and the actual amount for the next transaction are compared on the basis of probability distribution during training phase. If the deviation is above a threshold value then it is treated as fraud else legal. In case of fraud alarm is generated and transaction is terminated or else it is routinely accomplished.

2, Mathematical model:

S={U; T; A; P; F;G}

Login = {U;A}
U := No of usersU1;U2;Un::::::
A := Authentication
T := Transaction 1; T2; Tn::::::
P := Pass
F := Fraud detection
G := {HM;HS; SMS}
HM := Flash code generation:
HS := History of Sequence and Amount
O=P := SMS

Volume: 1 Issue: 1 13-Apr-2015,ISSN_NO: 2348 -2354



a) One user at one place b) unique flash code generation for one user

3, Algorithm:

1.User will login In the system for mobile banking.

2. If login is from the preferred location specified then go to step 4.

3. If login is not from preferred location then process will be halted to get the preferred location.

4. Perform transaction.

5. Check HMM.

- The sequence of previous transactions is checked
- The transaction amount history will be checked.
- On the basis of the new transaction future transactions are predicted.

6. If valid transaction then go to step 12.

7. If transaction is new to the behaviour or invalid then generate ash code to validate authentication of the user

8. The unique ash code will be generated every time.

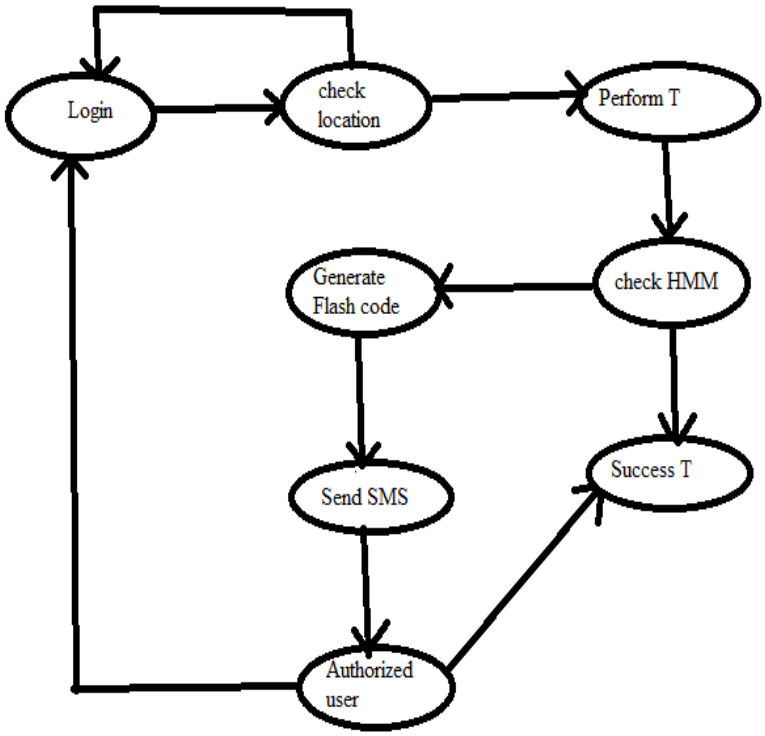
Volume: 1 Issue: 1 13-Apr-2015,ISSN_NO: 2348 -2354

9. Flash code will be sent to authorized user via sms.

10. User will enter the ash code for authentication

11. If false code is entered or no entry then transaction process is halted go to step 1.

12. For authorized user the transaction is allowed and transaction is success.



State transition diagram

4, Experimrntal Results and analysis:

Consider a student is making transaction of Rs 1000 from his account after every three days so his probability of making transaction of Rs 1000 after three days will be higher.

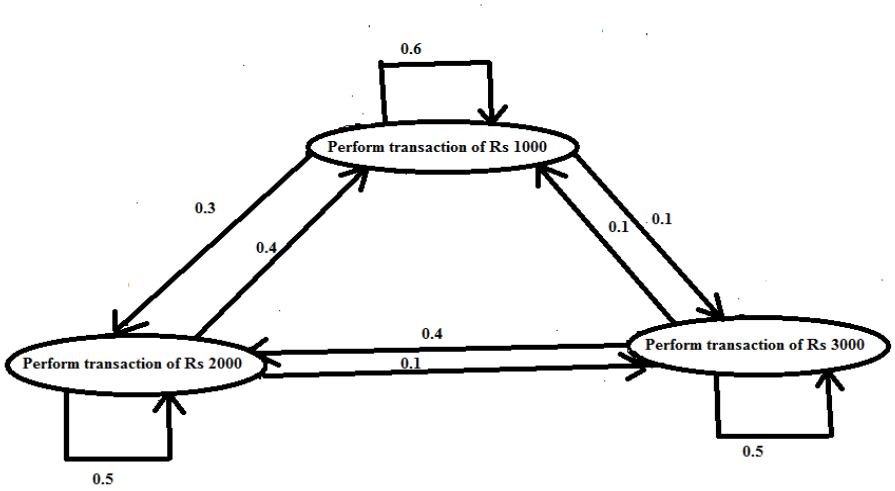
But there may be case where student makes transaction of Rs 2000 or 3000 but there probility will be lesser than making transaction of Rs 1000 .

Similarly if a student is making transaction of Rs 2000 after every three days his probability of making transaction of Rs 2000 after three days will be higher than making transaction of Rs 1000 or Rs 2000.

Volume: 1 Issue: 1 13-Apr-2015,ISSN_NO: 2348 -2354

But there may be case that student requires only Rs 1000 .so probability of making transaction of Rs 1000 will be higher than Rs 3000 but lesser than Rs 2000.

Similary there may be case when student makes transaction of Rs 3000 after every three days.In such probability of making transaction will be more favourite than making transaction of Rs 2000 or 1000.



5, Conclusion :

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised, but ones' biometric is undeniably connected to its owner. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Secure authentication technology using Flash Code identifier may solve this problem since a person's registered mobile receive the Flash Code and is unique for every individual. The

system has a securing transaction based on the user ATM behavior. This is achieved using HMM technique. So the system is helpful both in Authentication and Transaction.

References:

[1] Implement Credit Card Fraudulent Detection Hidden Markov Model Ashphak Khan, Tejpal Singh, Amit Sinhal

[2]International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-3, February 2012 49 A Survey on Hidden Markov Model for Credit Card Fraud Detection

[3]International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-3, February 2012 49

[4]A Survey on Hidden Markov Model for Credit Card Fraud Detection

[5]Credit card fraud detection using Hidden Markov Model Information and Communication Technologies (WICT), IEEE 2011 World Congress on Date of Conference: 11-14 Dec. 2011

[6]Adeoti, J. (2011). Automated Teller Machine (ATM) frauds in Nigeria: the way out.