A parameter optimized approach for improving credit card fraud detection

A.Prakash [1], Dr.C.Chandrasekar [2]

[1] Manonmaniam Sundaranar University, Tirunelveli,
Tamil Nadu, India
prakashankar75@gmail.com

[2] Department of Computer Science, Periyar University,
Salem, Tamil Nadu, India
ccsekar@gmail.com

Abstract

The usage of credit cards has highly increased due to high-speed innovation in the electronic commerce technology. Since credit card turns out to be the majority well-liked manner of payment for mutually online as well as habitual purchase, cases of fraud correlated through it are as well increasing. In normal Hidden Markov Model the problem of cannot find an optimal state sequence for the underlying Markov process also this observed sequence cannot be viewed as training a model to best fit the observed data. In this research, the main aim is to model the sequence of observations in credit card transaction processing using an Advanced Hidden Markov Model (AHMM) and show how it can be utilized for the exposure of frauds. In this process an AHMM is initially trained with the regular manners of a cardholder. If an incoming credit card transaction is not recognized by the trained AHMM with adequately high probability, it is believed to be fraudulent. This proposed work desire to regulate the model parameters to best fit the observations. The ranges of the matrices (N and M) are fixed but the elements of A, B and π are to be decided, focus to the rank stochastic condition. The information that can efficiently re-estimate the model itself is one of the more incredible features of HMMs this referred here as AHMM.

Key Words: *Hidden Markov Model (HMM), Advanced Hidden Markov Model (AHMM), Hill Climb, and credit card fraud detection*

1. Introduction

An unauthorized account movement by a person for whom the account was not be set to can be referred as credit card fraud. Preparedly, this is an event for which action can be taken to discontinue the misuse in steps forward and integrate risk executive applies to defend alongside comparable acts in the future. In straightforward expressions, Credit Card Fraud is described as when an individual exploits another individual's credit card on behalf of personal causes though the proprietor of the card and the card issuer are not conscious of the information that the card is being used. In addition to the persons using the card has not at all having the association with the cardholder or the issuer and has no purpose of making the repayments for the acquire they done. The anticipate user behavior in economic systems can be utilized in many situations. Forecasting client relocation, public associations can accumulate a lot of wealth and other assets. One of the most motivating pastures of forecast is the fraud of credit stripes, especially credit card expenditure. Positively, all transactions deals with financial records of known abuse are not authoritative. However, there are transactions which are officially suitable, but knowledgeable people can advise that these transactions are probably misused, caused by stolen cards or fake merchants. So, the assignment is to avoid a fraud by a credit card transaction previous to it is known as "illegitimate". By means of growing number of transactions people can no longer manage all of them. As a solution, one might hold the experience of the experts and put it interested in an expert system. This habitual approach has the disadvantage that the expert's knowledge, yet as it can be mined unambiguously, alters quickly with novel manners of prepared attacks and models of credit card fraud. So as to keep track with this, no predefined fraud models but routine learning algorithms are needed.

HMM-based applications are ordinary in an assortment of areas such as speech recognition, bioinformatics, and genomics. Ourston et al have projected the application of HMM in identifying multistage credit card attacks. Hoang et al projected a new method for abnormality exposure using HMM. The main idea is to construct a multilayer model of transaction behaviors based on HMMs and specifying methods for anomaly detection. In recent days, Joshi and Phoba have examined the capabilities of HMM in credit card fraud detection. Cho and Park recommended an HMM-based credit card fraud detection system that advances the time to model and routine by allowing for only the right transition streams based on the province knowledge of assaults. Lane has examined HMM to model human behavior. On one occasion human behavior is properly formed, any sensed departure is a reason for concern because an attacker is not predictable to have a behavior similar to the genuine user. For this reason, in this research work the Advanced Hidden Markov Model is formed to find the credit card fraud detection. In HMM one more drawback is that for the dynamic programming approach the optimal observation sequence would not be found. With this the best fit point should modeled. In AHMM the drawbacks will be resolved with α and β value. The contribution of the works as follows:

1. In training phase obtain the card holder profile and calculate the probability for each transaction.

2. Using the AHMM creates the observation model with best fit observation states and regulates the model parameters (α and β) to best fit the observations.

3. In testing phase the detection of fraud is obtained If both probability value from multiple observation are same it will be a normal customer else there will be fraud signal will be provided.

The remainder of this paper is as follows: The related work is discussed in section2. The hidden markov model is explained in section 3. In section 4 the Advanced Hidden Markov Model is explained. The section 5 is deal with experimental results and discussion. In section 6 the conclusion of the paper is described.

2. Related Work

A lot of research notice and a number of techniques have developed to the Credit card fraud detection, with unique prominence on data mining and neural networks, have been proposed. Recently, Syeda et al [4] have employed parallel granular neural networks (PGNNs) for civilizing the rapidity of data mining and knowledge discovery process in credit card fraud detection. Aleskerov et al [7] developed CARDWATCH, a database mining system employed for credit card fraud detection which is based on a neural learning module, offers a crossing point to the variety of commercial databases. Ghosh and Reilly [2] have proposed credit card fraud detection with a neural network which is trained on a large illustration of labeled credit card account transactions. These transactions enclose instance fraud cases due to gone cards, stolen cards, purpose fraud, forged fraud, mail-order fraud and non-received issue fraud. Where a drawback is that a complete system has been implemented for this purpose which is time consuming. Stolfo et al [5] recommend a credit card fraud detection system (FDS) by means of meta-learning techniques to discover models of fraudulent credit card transactions.

A general strategy that provides a means for combining and integrating a number of separately built classifiers or models is called as Metalearning. This will be trained correlation of the predictions of the base classifier. The equivalent collection has also labored for fraud and intrusion detection on a cost-based model [6]. Kim and Kim [8] have recognized twisted distribution of data and mix of legal and fraudulent transactions as the two main motivations for the complexity of credit card fraud detection. Supported on this observation, they utilize fraud density of real transaction data as a confidence value and produce the weighted fraud score to diminish the number of misdetections. Fan et al [9] suggested the application of distributed data mining in credit card fraud detection. Brause et al [10] have extended an approach that entails advanced data mining techniques and neural network algorithms to attain high fraud coverage. Chiu and Tsai [11] have proposed web services and data mining techniques to initiate a collaborative scheme for fraud detection in the banking industry.

By means of this system, participating banks partition knowledge about the fraud patterns in a heterogeneous and distributed environment. Phua et al [12] have done a research based a widespread survey of existing data mining supported fraud detection systems and published an inclusive information. Prodromidis and Stolfo [13] exploited an agent based move toward with distributed learning for detecting frauds in credit card transactions. For achieving higher accuracy it is supported on artificial intelligence and inductive learning algorithms and Meta learning methods is combined. Phua et al [16] proposed the use of Meta classifier similar to [5] in fraud detection troubles. They believe naïve Bayesian, C4.5 and Back Propagation neural networks as the base classifiers. Vatsa et al [17] have recently planned a game theoretic approach to credit card fraud detection. They model the communication among an attacker and a fraud detection system as a multi-stage game between two players, each trying to take full advantage of his bribe. The difficulty with most of the above-mentioned approaches is that they want labeled data for both authentic as well as fraudulent transactions to train the classifiers. Receiving real world fraud statistics is one of the major harms connected with credit card fraud detection. In addition, these approaches cannot discover new categories of frauds for which branded data is not accessible.

3. Credit Card Fraud Detection Using Hmm

The credit card fraud detection system is based on Hidden Markov Model, which does not require fraud signatures and still it is capable to perceive frauds just by bearing in mind a cardholder's spending habit. The specifics of purchased items in single transactions are generally unidentified to any Credit card Fraud Detection System organization either at the bank that issues credit cards to the cardholders or at the commercial site where goods is going to be obtained. As business processing of credit card fraud detection system runs on a credit card issuing bank site or merchant site. Every arriving transaction is submitted to the fraud detection system for verification intention. The fraud detection system recognize the card details such as credit card number, cvv number, card type, expiry date and the amount of items acquire to validate, whether the transaction is genuine or not.

The accomplishment techniques of Hidden Markov Model in order to notice fraud transaction through credit cards, it generate clusters of training set and identify the spending profile of cardholder. In that process the number of items purchased by customers, types of items that are bought in a particular transaction deliberates on the amount of item acquired and use for further processing that are not known to the Fraud Detection system completely. It supplies higher amount of dissimilar data transactions in form of clusters depending on transaction amount which will be moreover in low, medium or high value assortments. It tries to discover out any discrepancy in the transaction

based on the spending behavioral profile of the cardholder, shipping address, and billing address and so on. Based on the expenditure behavioral profile of card holder the probabilities of initial set have been selected and bring together a series for additional processing. If the fraud detection system generates sure that the transaction to be of fake, it raises an alarm and the issuing bank refuses the transaction.

For the protection purpose, the refuge information module will get the information features and its store's in database. To identify the safety measures information if the card missing then the security information module structure arises. The security form has a number of safety questions like account number, date of birth, mother name, other personal question and their answer, etc. where the abuser has to respond it correctly to move to the transaction division in which all those information must be known by the card holder only and can continue only by the card holder. It has informational confidentiality and informational self strength of mind that are tackled consistently by the novelty giving people and entities a trusted means to user, protected, search, process, and exchange personal and/or secret information.

The system and tools for pre-authorizing commerce offered that a relations tool to a trader and a credit card proprietor. By communicating to a credit card number, card type with expiry date and storing it into database, a unique portion of information that describes a fastidious transaction to be complete by a trustworthy user of the credit card at a later occasion the cardholder will be initiating a credit card transaction procedure. The particulars are conventional in the type of system data in the database only when if a correct individual recognition code is used with the statement the cardholder can precede with further steps with the credit card. Because the transaction is pre-authorized, the merchant does not require observing or transmitting an accurate individual recognition code.

1. The number of states in the model is N. The set of states is $S = \{S_1, S_2, \ldots S_N\}$, where S_i, $i = 1, 2, \ldots, N$ is an individual state. The state at time instant t is denoted by q_t.

2. The number of distinct observation symbols per state is M. The set of symbols is $V = \{V_1, V_2, \ldots V_3\}$, where V_i, *i = 1; 2; . . .; M* is an individual symbol.

3. The state transition probability matrix $A = [a_{ij}]$ where $a_{ij} = P(q_t + 1 = S_j \mid q_t = S_i)$; $1 \le i \le N$; $1 \le j \le N$; $t = 1$; 2; …: where $a_{ij} > 0$ for all i, j. Also, $\sum_{j=1}^{N} a_{ij} = 1, 1 \le i \le N$.

4. The observation symbol probability matrix $B = [b_j(k)]$, where $b_j(k) = P(V_k \mid S_j), 1 \mid \le j \le N, 1 \le k \le M$ and $\sum_{k=1}^{M} b_j(k) = 1, 1 \le j \le N$

5. The initial state probability vector $\pi = [(\pi_i)]$, where $\pi_i = P(q_1 = S_i), 1 \le j \le N$, such that $\sum_{k=1}^{M} \pi_i = 1$

6. The observation sequence $O = O_1, O_2, O_3 \ldots O_R$, where each observation O_t is one of the symbols from V, and R is the number of observations in the sequence.

3.1 HMM Model for Credit Card Transaction Processing

First begin through deciding the observation symbols in our model which is to record the credit card transaction processing function in terms of an HMM. Then quantize the acquisition values x into M worth ranges V_1, $V_2 \ldots V_M$ structuring the observation symbols at the issuing depository. The concrete outlay range for every symbol is configurable based on the expenditure routine of individual credit card holders. These worth ranges can be found dynamically through applying a clustering method on the values of each cardholder's transactions. Let assume V_k, $k = 1, 2, \ldots M$ to stand for both the observation symbol as well as the equivalent charge assortment. A credit cardholder constructs diverse types of purchases of unlike amounts more than a period of time. Single prospect is to believe the sequence of transaction amounts and look for divergences in them.

On the other hand, the sequence of kinds of purchase is additional constant contrasted to the series of transaction quantities. The motive here is that, a cardholder precedes purchases depending on his require for procuring diverse types of items greater than a period of time. Consecutively, produces a series of transaction quantities. The kinds of each acquire are linked to the row of business of the equivalent trade. The kind of purchase of the cardholder is hidden from the FDS. The position of all probable categories of purchase and consistently, the position of every one potential lines of commerce of merchants structures the position of concealed states of the HMM. The line of business of the commercial is identified to the acquiring bank which should be noted at this stage that, since this information is furnished at the time of registration of a merchant. As well, a number of merchants might be trade in various types of merchandise. Such kinds of line of business are judged as Miscellaneous and there is no need to determine the authentic types of items purchased in these transactions.

A few assumptions as regards accessibility of this information with the issuing depository and therefore with the FDS are not matter-of-fact hence, would not have been suitable. In the consequences part shows the cause of choice of the number of states on the method performance. Subsequent to deciding the state and symbol illustrations, after that have to find out the probability matrices *A*, *B* and π thus the representation of the HMM is inclusive. These three model parameters are found in a training phase. Hence, they should be chosen carefully through preliminary selection of parameters influences the performance of the algorithm. A method based on Hidden Markov Models (HMMs) is a stochastic method, which

can be very useful for some applications involves the making of auditory models of program that build use of temporal information. The HMMs can model a lesser unit of the statement. The HMMs can be analysed as fixed state machines, wherever every unit of time, a state transition happens, and all state produces an auditory vector with a connected likelihood density function. So as to is, in every state, a GMM (Gaussian mixture model) is second-hand to exemplify an auditory vector experiential.

4. AHMM For Credit Card Fraud Detection

Here to alter the model parameters to best fit the observations. The ranges of the matrices (N and M) are fixed however the elements of A, B and π are to be determined, focus to the strip stochastic condition. The actuality that can professionally re-estimate the model itself is one of the more astonishing aspects of HMMs. Let assume $\lambda = (A, B, \pi)$ be a given model and series of observations $O = (O_0, O_1, \dots O_{T-1})$. For $t = 0,1, \dots . T-2$ and $i, j \in \{0,1, \dots, N-1\}$, define "$di - gamma$" as

$$\gamma_t(i,j) = P(x_t = q_i, x_{t+1} = q_j | O, \lambda)$$

$$\gamma_t(i) = \frac{\alpha_t(i)\beta_t(i)}{P(O|\lambda)}$$

Table 1: Notations

SYMBOL	REPRESENTATION
T	Observation sequence length
N	Number of states in the model
M	Number f observation symbols
O	Observation sequence $(O_0, O_1, \dots O_{T-1})$
Q	Markov process fo distinct states $\{q_o, q_1 \dots q_{N-1}\}$
V	Set of possible observations $\{0,1 \dots . M-1\}$
A	Probability for each state transition
π	Probability matrix of observation sequence

Then $\gamma_t(i,j)$ is the probability of being in state q_i at time t and transiting to state q_j at time $t+1$. The di-gamma will be formed with the terms taken as α , β, A and B as:

$$\gamma_t(i,j) = \frac{\alpha_t(i)a_{ij}b_j(O_{t+1})\beta_{t+1}(j)}{P(O|\lambda)}$$

In this we should re-estimate this with the parameter $\beta_t(i)$ which measures the relevant probability after time t

$\beta_t(i) = \frac{\gamma_t(i)P(O|\lambda)}{\alpha_t(i)}$ which is represented also as:

$$\beta_t(i) = \sum_{j=0}^{N-1} a_{ij} b_j(O_{t+1})\, \beta_{t+1}(j)$$

Where $\beta_t(i) = P(O_{t+1}, O_{t+2} \dots O_{T-1} | x_t = q_i, \lambda)$

Denote the $\beta_t(i,j) = P(x_t = q_i, x_{t+1} = q_j | O_{t+1}, \lambda)$,define the $di - Betas$ as

$$\beta_t(i,j) = \frac{\alpha_t(i)a_{ij}b_j(O_{t+1})\gamma_{t+1}(j)}{P(O_{t+1}|\lambda)}$$

Where $\beta_{t+1}(j) = \frac{\gamma_t(i,j)P(O|\lambda)}{\alpha_t(i)a_{ij}b_j(O_{t+1})}$. The $P(O|\lambda)$ is obtained by summing $\alpha_{T-1}(i)$ over i. From the defenition of $\beta_t(i)$it follows the most likely state at time t is the state q_i for which $\beta_t(i)$ is maximum,where the maximum is taken over the index i.

$\beta_t(i)$ and $\beta_t(i,j)$ are related by

$$\beta_t(i) = \sum_{j=0}^{N-1} \beta_t(i,j)$$

Given with the β and di- Betas verify the model $\lambda = (A, B, \pi)$ can be re-estimated as follows:

1. For $i = 0,1, \dots . N-1$
2. For $i = 0,1, \dots . N-1$ and $j = 0,1, \dots . N-1$ compute

$$a_{ij} = \frac{\sum_{t=0}^{T-2} \beta_t(i,j)}{\sum_{t=0}^{T-2} \beta_t(i)}$$

The numerator of re-estimated a_{ij} can be observed to give the supposed number of transitions from state q_i to state q_j and the denominator denotes the expected number of transition from the state q_i to any state. Then the ratio is the probability of transiting as of state to q_i state q_j, which is the desired value of a_{ij}.

3. For $j = 0,1, \dots . N-1$ and $k = 0,1, \dots . M-1$ compute

$$b_j(k) = \frac{\sum_{t \in \{0,1 \dots T-2\} O_t = k} \beta_t(i)}{\sum_{t=0}^{T-2} \beta_t(i)}$$

The numerator of the re-estimated $b_j(k)$ is the anticipated number of times the model is in state q_j with observation k, at the same time as the denominator is the estimated number of times the model is in state q_j. The ratio is the probability of observing symbol k, given that the model is in state q_j, which is the desired value of $b_j(k)$.

Re-estimation is an iterative process. Foremost, we initialize $\lambda = (A, B, \pi)$ through a best guess or, if no logical guess is obtainable, choose with arbitrary values such that $\pi_i \approx 1/N$and $a_{ij} \approx 1/N$ and $b_j(k) \approx 1/M$. It's vital that A, B and π be randomized, because precisely consistent ideals will consequence in a confined maximum from which the model cannot Hill climb. As constantly, π, A and B must be row stochastic. The AHMM process can be summarized as follows.

1. Initialize the model, $\lambda = (A, B, \pi)$

2. Evaluate $\alpha_t(i), \gamma_t(i), \beta_t(i)$and $\beta_t(i, j)$

3. Re-estimate the model$\lambda = (A, B, \pi)$.

4. If $P(O|\lambda)$increases, goto 2.

Certainly, it may be enviable to end if $P(O|\lambda)$does not increase by at any rate various predestined threshold and/or to locate a maximum amount of iterations.

6. Experimental Results And Discussion

5.1 Precision accuracy

This graph shows the precision rate of existing and proposed system based on two parameters of precision and the number of Dataset. From the graph we can see that, when the number of number of Dataset is advanced the precision also developed in proposed system but when the number of number of Dataset is improved the precision is reduced somewhat in existing system than the proposed system. From this graph we can say that the precision of proposed system is increased which will be the best one. The values are given in Table 1:

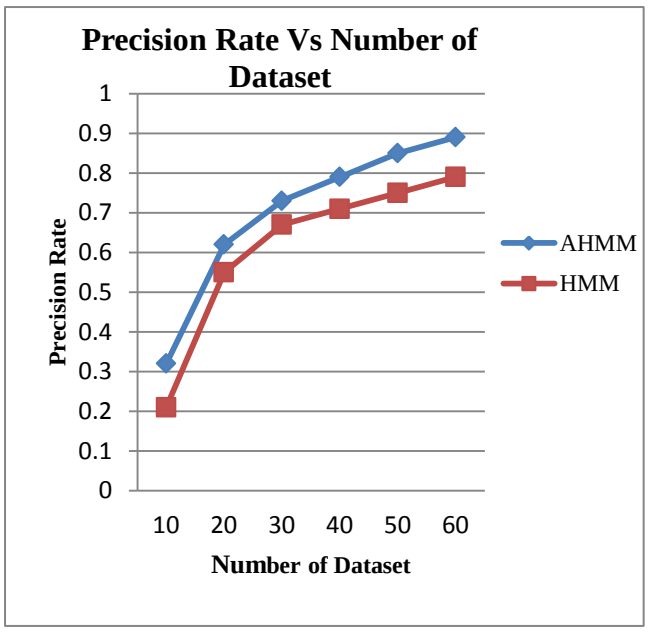

Fig 1: Precision vs. Number of Dataset

Table 2: Precision vs. Number of Dataset

SNO	Number of Dataset	AHMM	HMM
1	10	0.32	0.21
2	20	0.62	0.55
3	30	0.73	0.67
4	40	0.79	0.71
5	50	0.85	0.75
6	60	0.89	0.79

In this graph we have chosen two parameters called number of Dataset and precision which is help to analyze the existing system and proposed systems. The precision parameter will be the Y axis and the number of dataset parameter will be the X axis. The blue line represents the existing system and the red line represents the proposed system. From this graph we see the precision of the proposed system is higher than the existing system. Through this we can conclude that the proposed system has the effective precision rate.

5.2 Recall vs. Number of Dataset

This graph shows the recall rate of existing and proposed system based on two parameters of recall and number of Dataset. From the graph we can see that, when the number of number of Dataset is improved the recall rate also improved in proposed system but when number of number of Dataset is improved the recall rate is reduced in existing system than the proposed system. From this graph we can say that the recall rate of proposed system is increased which will be the best one. The values of this recall rate are given below:

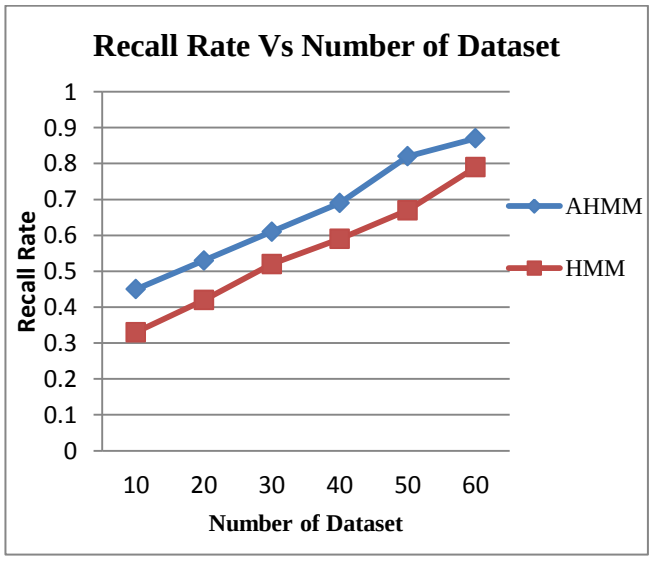

Fig 2: Recall vs. Number of Dataset

Table 3: Recall vs. Number of Dataset

SNO	Number of Dataset	AHMM	HMM
1	10	0.87	0.78
2	20	0.82	0.72
3	30	0.76	0.63
4	40	0.64	0.54
5	50	0.56	0.45
6	60	0.46	0.34

In this graph we have chosen two parameters called number of Dataset and recall which is help to analyze the existing system and proposed systems on the basis of recall. In X axis the Number of dataset parameter has been taken and in Y axis recall parameter has been taken. From this graph we see the recal rate of the proposed system is in peak than the existing system. Through this we can conclude that the proposed system has the effective recall.

5.3 Fmeasure vs. Number of Dataset

This graph shows the Fmeasure rate of existing and proposed system based on two parameters of Fmeasure and number of Dataset. From the graph we can see that, when the number of number of Dataset is improved the Fmeasure rate also improved in proposed system but when the number of number of Dataset is improved the Fmeasure rate is reduced in existing system than the proposed system. From this graph we can say that the Fmeasure rate of proposed system is increased which will be the best one. The values of this Fmeasure rate are given below:

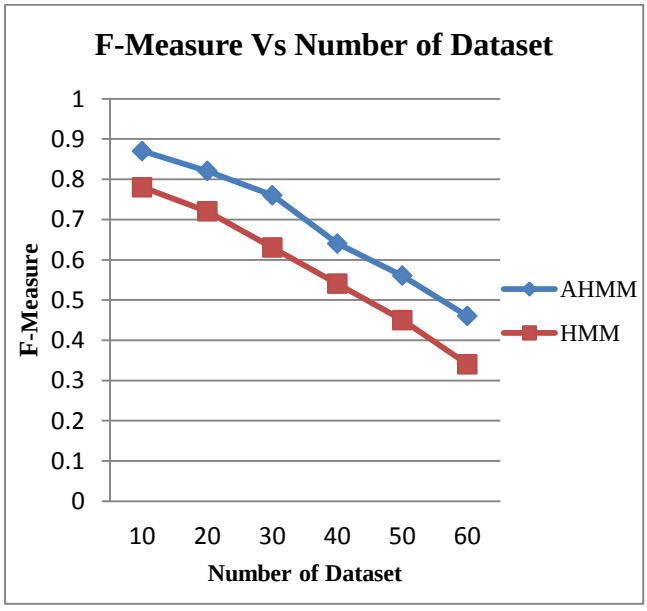

Fig 6: Fmeasure vs. Number of Dataset

Table 3: Fmeasure vs. Number of Dataset

SNO	Number of Dataset	AHMM	HMM
1	10	0.87	0.78
2	20	0.82	0.72
3	30	0.76	0.63
4	40	0.64	0.54
5	50	0.56	0.45
6	60	0.46	0.34

In this graph we have chosen two parameters called number of Dataset and recal which is help to analyze the existing system and proposed systems on the basis of Fmeasure. In X axis the Number of dataset parameter has been taken and in Y axis Fmeasure parameter has been taken. From this graph we see the Fmeasure of the proposed system is in peak than the existing system. Through this we can conclude that the proposed system has the effective Fmeasure.

6. Conclusion

The credit card transaction method is examined as the basic stochastic process of an (Advanced Hidden Markov Model) AHMM. The variety of transaction quantity considered as the observation symbols, while the kinds of item have been deemed to be states of the AHMM. In addition to comprise recommended a technique for decision the spending profile of cardholders is authorized or not. As well as purpose of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters with the best fit observation is that providing an effective credit card fraud detection system. It has also been enlightened how the HMM vary with the AHMM can detect whether an arriving transaction is fake or not. Experimental results show the performance and effectiveness of AHMM system and show the efficiency of knowledge the spending profile of the cardholder in AHMM system.

REFERENCES

[1]. L.R. Rabiner, “A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition,” Proceedings of the IEEE, vol. 77, no. 2, pp. 257-286, 1989.

[2]. S. Ghosh and D.L. Reilly, “Credit Card Fraud Detection with a Neural-Network,” Proc. 27th Hawaii International Conference on System Sciences: Information Systems: Decision Support and Knowledge-Based Systems, vol. 3, pp. 621-630, 1994.

[3]. S. Axelsson, “The Base-Rate Fallacy and the Difficulty of Intrusion Detection,” ACM Transactions on Information and System Security, vol. 3, no. 3, pp. 186-205, 2000.

[4]. M. Syeda, Y. Q. Zhang, and Y. Pan, "Parallel Granular Networks for Fast Credit Card Fraud Detection," Proc. IEEE International Conference on Fuzzy Systems, pp. 572-577, 2002.

[5]. S.J. Stolfo, D.W. Fan, W. Lee, A.L. Prodromidis, and P.K. Chan, "Credit Card Fraud Detection using Meta-Learning: Issues and Initial Results," Proc. AAAI Workshop on AI Methods in Fraud and Risk Management, pp. 83-90, 1997.

[6]. S.J. Stolfo, D.W. Fan, W. Lee, A. Prodromidis, and P.K. Chan, "Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAM Project," Proc. DARPA Information Survivability Conference and Exposition, vol. 2, pp. 130-144, 2000.

[7]. 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 Engineering, pp. 220-226, 1997.

[8]. M.J. Kim and T.S. Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," Proc. International Conference on Intelligent Data Engineering and Automated Learning, Lecture Notes in Computer Science, Springer Verlag, no. 2412, pp. 378-383, 2002.

[9]. 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.

[10]. R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for Credit Card Fraud Detection," Proc. IEEE International Conference on Tools with Artificial Intelligence, pp. 103-106, 1999.

[11]. C. Chiu and C. Tsai, "A Web Services-based Collaborative Scheme for Credit Card Fraud Detection," Proc. IEEE International Conference on e-Technology, e-Commerce and e-Service, pp. 177-181, 2004.

[12]. C. Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-based Fraud Detection Research," available on-line at http://www.bsys.monash.edu.au/people/cphua/, 07 March 2007.

[13]. S. Stolfo and A.L. Prodromidis, "Agent-based Distributed Learning applied to Fraud Detection," Technical Report, CUCS-014-99, Columbia University, USA, 1999.

[14]. D.J. Hand, G. Blunt, M.G. Kelly, and N.M. Adams, "Data Mining for Fun and Profit," Statistical Science, vol. 15, no. 2, pp. 111–131, 2000.

[15]. Sushmito Ghosh and Douglas L. Reilly, "Credit Card Fraud Detection with a Neural-Network." Nestor, Inc. IEEE (1994).

[16]. C. Phua D. Alahakoon, and V. Lee, "Minority Report in Fraud Detection: Classification of Skewed Data," ACM SIGKDD Explorations Newsletter, vol. 6, no. 1, pp. 50-59, 2004.

[17]. V. Vatsa, S. Sural, and A.K. Majumdar, "A Game-theoretic Approach to Credit Card Fraud Detection," Proc. 1st International Conference on Information Systems Security, Lecture Notes in Computer Science, Springer Verlag, pp. 263-276, 2005.

A.Prakash done M.Sc (CT), from Periyar University Salem in 2001, completed M.Phil.(CS), from Manonmaniam Sundaranar University,Tirunelveli in 2003. Received MCA, from Periyar University Salem in 2011. Currently working as a Asst. Professor in Dept. of Computer Applications, Hindusthan College of arts and science, Coimbatore. His research area is data mining.

Dr. C. Chandrasekar received his Ph.D. degree from Periyar University, Salem, TN, India. He has been working as Associate Professor at Dept. of Computer Science, Periyar University, Salem – 636 011, Tamil Nadu, India. His research interest includes Wireless networking, Mobile computing, Computer Communication and Networks. He was a Research guide at various universities in India. He has been published more than 50 research papers at various National / International Journals.