International Conference on Innovative Research in Engineering, Management and Sciences
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 9 | ISSN : 2456-3307

# Timestamp and IP Address based Fraud Detection in Credit Cards using Hidden Markov Model

**Deepti Rai**[*1]

[*1]Department of Computer Science & Engineering, New Horizon College of Engineering, Bangalore, Karnataka, India.
deeptiraj@newhorizonindia.edu[1]

## ABSTRACT

Online activities mainly involve purchasing products, electronic devices and other similar things in a regular basis. There are many online transaction methods particularly made for such activities, which ensures the security by authorizing the transfer of funds. The online transactions are achieved by different bank cards that, makes the process simple. Although they are having notable advantages, they confront some of their drawbacks regarding the security. The credit card frauds can happen for many reasons, mainly to get access to non-accredited funds from the account. It is a responsibility for the bank to screen and protect the card details of the user while doing online transactions. Our approach is based on the Hidden Markov Model. HMM detects the fraud in the transactions and blocks it. It also stores the details about the timestamp and IP address of the fraudster' s machine. Whenever a new transaction is made, the system will make a note of it by recording the transaction. The spending profile of the card holder is created based on his previous transaction history using HMM. Now if any intruder tries to make transactions with any registered credit card, the system notices the difference in the spending pattern of the card holder and thus the intruder gets easily trapped.

**Keywords :** E-Transactions, Fraud Detection, Hidden Markov Model, Credit Card

## I. INTRODUCTION

The procedure of examining certain hidden patterns of data based on different outlooks in order to categorize it into useful information, which is collected from

common areas for efficient analysis of data mining algorithms in order to facilitate decision making for business and other data requirements to basically decrease costs and increase the revenue is called data mining. It is the method of discovering patterns from huge collection of data involving techniques at the junction of statistics, database systems, and machine learning. Its aim is to withdraw data from a data set and to modify the data into a thorough structure for future use. Network security includes the policies and practices acquired for prevention and monitoring misuse, unauthorized access, alteration or refusal of a network. It includes the permission to retrieve the data which is present in a network that is controlled by an administrator Hidden Markov Model is composed of definite set of states, were each state is affiliated with a probability distribution. It is called so because only the outcome is exposed to the observer and not the states. Based on the affiliated probability distribution, a result will be generated for a particular state. Online activities mainly include purchasing goods, electronic devices and other such things. The online transaction made for the above online activities are secure payment methods that authorize the transfer of funds. These transactions are supported by different bank cards which makes the operation easy. Apart from its impressive advantages they also have a few pitfalls regarding the security. The corrupt use of credit card is mainly done to get unauthorized funds from the account. It is thus the responsibility of the bank to safeguard the amount transferred online on the internet of the card holder. Among the various fraud detection techniques available, our approach focuses on HMM which detects the unauthorized transactions and simultaneously reports the timestamp and IP address of

the intruder's machine. Every time a new transaction made is recorded in the system. The HMM then automatically generates the spending pattern of the user. Now if any intruder tries making a transaction with any registered credit card, then its spending pattern will vary from the spending pattern of the authenticated user and can be recorded easily. The system also records the IP address and timestamp of the intruders machine so that we can easily trace his geographical location.

## II. RELATED WORK

In [1], Yonghui Xiao et al. proposed a location cloaking system using the Hidden Markov Model. It is used to secure the positions of a user with distinctive confidentiality. There are two features in LocLok: it safeguards positions under sequential associations defined through hidden Markov model and it reliefs the optimum noisy position with the proportional isotropic appliance, This approach is Faster and more accurate compared to other methodologies. The standard differential confidentiality merely guards user-level confidentiality; Here the defense system needs to be imposed for a particular user. Thus the user cannot leave the system ,else there is no statistics to safeguard. In this system the protection is enforced only for the single user.

In [2], Lutao Zheng et al. proposed a transaction fraud detection system based on the total order relation and behavior diversity, which has used behavior profile based fraud detection to detect the fraudulent transactions. It characterizes the diversity of users behavior. But it is slow detection as it has to go through a lot of user behaviours. In this paper, they proposed a method to extract users BPs based on their transaction records, which has been used to detect transaction fraud in the online shopping scenario. OM overcomes the shortcoming of Markov chain models since it characterizes the diversity of user behaviors. Experiments also illustrate the advantage of OM. The future work focuses on some machine-learning methods to automatically classify the values of transaction attributes so that the model can characterize the user's personalized behavior more precisely. In addition, they have planned to extend BP by considering other data such as user's comments.

In [3], Ishan Sohony et al. proposed a fraud detection system for credit cards using Ensemble Learning. It minimizes the misclassification that usually happens, but it is limited to only the datasets which are having numerical values. In this paper, they look at the serious and difficult task of discovering credit card fraud in a extremely twisted set. They propose an collaborative model that combines best of Random Forest and Feed Forward Networks to accurately detect fraud. An open direction of their work is improvement of accuracy parameters of the classifier. Although, the scope of their work is limited to the datasets having numerical values, yet in a more general case, for e.g., the datasets having text values it would be interesting to extend their work by including some more sophisticated techniques.

In [4], Phuong Hanh Tran et al. proposed a fraud detection system for credit cards using the approach that drives the real time data. The advantage is, it gives high-level of revealing accurateness and a decreased negative alarm. However, it’s not applicable for large stream datasets. In this paper they have proposed two approaches towards fraud detection without anomalies in the training set using maintenance vector machine with the optimal core limit selection and controller plan. Numerical results shown that it has achieved a optimal discovery exactness and a low negative alarm degree. In the future, they would like to address the fraud detection problem using auto encoder and control charts, targeting on time series data with uncertainties. They also focus on the detection ability of their proposed approach for large stream data.

In [5], Roger A. Leite et al. proposed a Visual Analytics and Event Detection system for detecting frauds related to credit cards. It performs more accurate detection compared to other existing systems at that time. But the factors like Network Analysis, New Customer Classification and different kinds of frauds have not achieved. Event detection is an im- portant in many domains like finding interesting changes that happens in stock markets, spot- ting glitches in health constraints, or spotting financial fraud. Considering these actions in a sequential setting allows the identification of perceptions such as rate, inclinations, and changes. Moreover, the investigation permits the expert to spot risks, sudden changes, or occasional occurrences. In this work they focus on the identification of irregular happenings in the financial sector.

In [6], Andrea Dal Pozzolo et al. proposed a system for detecting frauds related to credit cards using Novel Learning Strategy and Realistic Modeling . The precision of the reported alerts is more accurate. However, the process can be long and tedious. Future work concerns the study of adaptive and possibly nonlinear aggregation methods for the classifiers trained on feedback and deferred administered models. They also expect to further increase the alert precision by implementing an approach where it learns to rank that would be specifically designed to replace the linear aggregation of the posterior probabilities. In their experiments, they exhibit the impression of class disturbance and theory implication in a information stream containing millions of transactions over a time of three years.

In [7], Alexander Artikis et al. proposed a prototype for a system which manages credit card frauds. The system uses Online learning settings, Logic programming and answer set programming. Advantage of this system is that it efficiently adapts to the continuously changing fraud types. But the consumption of time is high and has to be performed on huge datasets for it to be effective. They recommended a approach, and established a model for preemptive event-driven planning. The machine learning section maintenance the online production of fraud configurations, permitting it to capably familiarize to the continuously growing fraud types. Also, the user interface of the model allows fraud specialists to make the most of the outcomes of computerization (complex event processing) and thus grasp informed decisions. The valuation of the modules is based on characteristic operation datasets, permitting for a accurate evaluation.

In [8], Jan Henrik Ziegeldorf et al. proposed a system for preserving privarcy using HMM Forward Computation. The system uses Privacy-Preserving HMM Forward Computation. Areas like bioinformatics, recognition of patterns, and signal processing, Hidden Markov Models have grown into an essential algebraic tool. A fundamental construction for this framework is the advancing algorithm which calculates the Likely hood to notice a specified arrangement of productions for a given HMM. The classical Forward procedure needs that one party holds both the model and remarkable arrangements. They observe for many emerging applications and services that the models and observation sequences are held by different parties who are not able to share their information due to applicable data protection legislation or due to concerns over intellectual property and privacy. In this paper, they show how to resolve the evident conflicts using protected two-party calculation. Concretely, they suggest Priward which enables two equally untrusting events to calculate the Forward algorithm steadily, i.e., without demanding either events to share their sensitive ideas with the other or any third event. It is less expensive. Although It's less expensive, it drains the battery of a mobile user.

In [9], Zheng-Guang Wu et al. proposed passivity asynchronous control model based on passivity for the Markov Jump Systems. The desired asynchronous controller can be resolved easily by available LMI Toolbox here. However, the mode of information is not fully available to the controller/ filter at every instant. Here they learn the difficult of inactive asynchronous mechanism Markov jump systems for distinct time. Therefore, the resulting loop system that is secure is named as the hidden Markov jump system. By using the matrix variance method, three equal sufficient circumstances are projected to confirm the stochastic indifference of the hidden Markov jump systems. In reference to the recognized circumstances, the structure of asynchronous controller which shields synchronous controller and mode-free controller as distinct circumstances is addressed. A statistical example is specified to prove the effectiveness of the resulting outcomes.

In [10], Kang Fu et al. proposed the Convolutional Neural Networks method for detection of credit card frauds. The most relevant attributes would reduce the processing time and hence such attributes need to be considered . But the accuracy of fraud detection is low. In this section, they firstly provide a description of fraud detection framework based on CNN. Secondly, they have proposed a feature of novel trading. Thirdly, there is an elaboration of sampling method that is cost based. At the end, the problem of frauds related to credit cards is solved by employing the CNN model. This method has found its base from the many different types of methods taken into account before.

In [11], Nader Mahmoudi and Ekrem Duman proposed a system for detecting credit card frauds using the Modified Fisher Discriminant Analysis. Its performance is best in terms of maximizing the total profit. The number of fraudulent transactions that can be captured by this system can be increased.In this paper, details of investigation using the Fisher Discriminant Analysis technique. Evaluation of the model is done by calculating the total saving amount. This amount is calculated for every case in question. To obtain a thorough view of the execution of the lodged methods, three other methods such as FDA and the Modified FDA technique (MFDA) on datasets including ANN, DT and NB are applied.

In [12], Ivo Correiaet et al. proposed proposed a system for detecting credit card frauds. It uses Event Processing Network in its implementation. It detects the potential fraud incidents that take place in real-time, so that the corrective actions can be taken. The inclusion of uncertainty aspects affects all levels of the architecture and logic of an event processing engine. Proactive Technology Online implements the extensions that include operands of new types , in addition with new built-in functions and attributes, and support for event processing patterns to cope with all these. These new capabilities were enforced as building items and were used as basic primitives within the complicated programmatic language for event processing. Their preliminary results show potential benefits that come from including uncertainty features to the task of detecting credit card frauds.

In [13], Gabriel Preti Santiago et al. proposed an approach in modeling for detection of frauds done using credit cards during payments through electronic services. The system implements Modelling and Classification approach as its methodology. Detects most of the difficult frauds which were not detected by the existing procedures in the company. However, the seller entity of the model was not considered in the experiment as it had a peculiar behavior. There is a rise in the amount of electronic transactions being done over the internet in the recent years, which is mainly due to the significant growth in e-commerce. This scenario makes the frauds in electronic transactions a matter of high importance. They present a system to solve this problem, using the history of the transactions

and then extract the features to classify and predict if the transaction is a fraudulent transaction or not.

In [14], Ashphak Khan et al. proposed a system to get the observation probabilities in HMM for detecting frauds related to credit cards. It also explains how the HMM detects whether a transaction being performed is fraud or not. The transaction amounts are divided into

3 groups i.e, high, medium and low. In HMM strategies are incredibly low compared to other techniques used for detecting frauds. It has been explained that the HMM can identify whether a transaction done is fraud or not. It is very robust, highly effective and scalable. Correctness and Effectiveness of the prediction to certain datasets can be expanded. In this paper, they have implemented HMM for detecting credit card frauds. The system is scalable large volumes of transactions can be dealt.

In [15], Nitin Rakesh and Ankit Mundra proposed an approach for online fraud detection and prevention which is done using the technique of Online Hybrid Model. OHM approach has been implemented in : theft of identity, fraud in online auction or fraud using card theft and non- delivery/merchandise fraud. OHM is also effective in detecting many other frauds like counterfeit card fraud, spam/spin fraud, etc. Thus, OHM is an extremely effective and robust outlook for online fraud detection and prevention. It is robust but it is slow and gives less accurate estimation compared to other systems.

## III. METHODOLOGY

In this phase the amount of each transaction is collected in a loop. For every new transaction, the difference in the amount with of the recent transaction and the previous 10 transaction of the particular user is computed. The difference observed is compared with the threshold value set. If the current value is higher than the threshold value, then it is considered to be fraudulent.

The basic architecture of the operations performed is shown in the Figure 1. The buyer visits the website, purchases the item and does the online payment. This payment is them checked to see if it is done by the valid user or a fraudster.

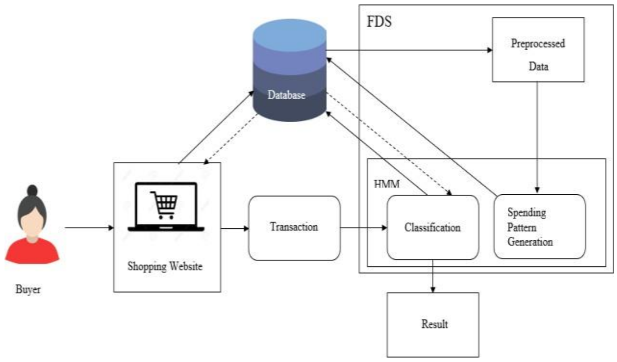

Figure 1: Architecture Diagram for Fraud Detection

For each transaction the user credentials such as username and password and card details such as card number, cvv, expiry year and month are also validated before the particular transaction is being processed. We have also considered the IP address of the system. It is recorded for each transaction. Once a system's IP Address is considered as fraud then it blocks the transactions from that particular IP Address. The number of daily transactions is also limited to 3 transactions.

If a genuine user does the transaction which is above the set threshold value, then the registered number receives a OTP using which the transaction can be processed. System logs out and gets itself blocked the moment any suspicious transaction is detected.

The algorithm takes the transaction of the user as input, undergoes various operations and based on the result of these computations it classifies the transaction into genuine and fraud. The genuine transactions are processes and fraudulent once are blocked as shown in Figure 2.

```
    ALGORITHM:
    Input: Transactions of the user.
    Output: Transaction classified into genuine
    and fraud.
1.  Start.
2.  Set the initial probability values
3.  For every new transaction
    3.1. Traverse through previous 10 transaction
         of the user
    3.2. Compute the difference in the amount
4.  Compare the difference value with
    the predefined value.
5.  Validate the user and the card details.
6.  Check for the IP Address in the Fraud List.
7.  Classify into Fraud and Genuine transactions.
    7.1. If amount is within the threshold value
         and all conditions are true then process
         the transaction as genuine.
    7.2. If amount is greater the threshold value
         and all conditions are true then send a
         otp for verification.
    7.3. If any of the conditions is not satisfied or
         a wrong otp is entered then then
         transaction is labelled as fraud.
8.  If the transaction is genuine process it and if it
    is detected as fraud then block it.
9.  Stop.
```

Figure 2: Algorithm for Fraud Detection System

## IV. EVALUATION

The experimental results revolve around the number of losses incurred. We propose the application of HMM in detecting the credit card frauds thereby recording the IP of the fraud system along with the timestamp. It is dependent on limit of the credit card which varies with the user.

In our system, we have proposed the use of Hidden Markov Model in detecting the frauds in credit cards thereby recording the IP of the fraud system along with the time stamp when malignant attempted to attack. The model generates a spending profile of the user for given sequence. The difference in the amounts of the previous and new transaction sequence is compared with the threshold value which is used to decide if the current transaction is a fraud or not. Initially the rate of financial loss due to frauds done using credit cards was high. After the implementation of the system for fraud detection using HMM, the rate of loss is decreased. The percentage of detection of frauds is increased to a great extent.

## V. CONCLUSION

In our system we have proposed the application of Hidden Markov Model for detecting the frauds done using credit cards and also record the IP address of the fraud system along with the timestamp when the fraud was done. It can be useful in tracing the geographic location of the attacker. The model also generates the spending profile of the user. The change in the amount of previous and new transaction sequence is compared with the threshold value which decides whether the upcoming transaction is fraudulent or not. In our simulation model we have taken a small set of data, but our proposed system can handle larger range of transactions that is quite certain in real life scenarios. The current system that is developed is a simulation model for detecting fraud during online credit card transaction. In future the system can be used to detect frauds in real time. Specific banks can be taken in confidence for detecting frauds for bank specific cards. The system can be expanded to detect other type fraud transaction such one done using debit cards.

## VI. REFERENCES

[1] Yonghui Xiao, Li Xiong, Si Zhang, Yang Cao, "Loclok: Location cloaking with diferential privacy via hidden markov model", Proceeding in VLDB Endowment 10(12) (ACM), pp.1901-1904, August 2017.

[2] Lutao Zheng, Guanjun Liu, Chungang Yan, and Changjun Jiang, "Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity", IEEE Transaction May 2018.

[3] Ishan Sohony, Rameshwar Pratap, Ullas Nambiar, "Ensemble Learning for Credit Card Fraud Detection", ACM ISBN 978-1-4503-6341-9/18/01'(ACM), January 2018.

[4] Phuong Hanh Tran, Kim Phuc Tran, Truong Thu Huong, Cedric Heuchenne, Phuong HienTran, Thi Minh Huong Le, "Real Time Data-Driven Approaches for Credit Card Fraud Detection", ACM ISBN 978-1- 4503-6368-6/18/02, Febraury 2018.

[5] Leite R. A., Gschwandtner T.,Miksch S., Kriglstein S., Pohl M., Gstrein E.,Kuntner J., "Eva: Visual analytics to identify fraudulent events", IEEE Transactions on visualization and computer graphics 24, 1 (2018), 330:339, March 2017.

[6] Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, G. Bontempi, " Credit card fraud detection: "A Realistic Modeling And A Novel Learning Strategy ", IEEETransactions on Neural Networks and Learning Systems D.O.I. 10.1109/TNNLS.2017.2736643, June 2017.

[7] Alexander Artikis, Nikos Katzouris, Ivo Correia, Chris Baber, Natan Morar, Inna Skarbovsky, Fabiana Fournier, Georgios Paliouras, "Industry Paper: A Prototype For Credit Card Fraud Management ", ISBN:978-1-4503-5065-5/17/06, Proceedings of the 7th ACM 2017.

[8] Ziegeldorf JH, Metzke J, Ruth J, Henze M, Wehrle K., "Privacy-Preserving HMM Forward Computation ", in proceedings of the 7th ACM Conference on Data and Application Security and Privacy. New York, ISBN 978-1-4503-4523-1/17/03, ACM 2017.

[9] Z. G. Wu, P. Shi, Z. Shu, H. Su, and R. Lu, "Passivity-based asynchronous control for Markov jump systems", IEEE Transaction Autom. Control, to be published, DOI:10.1109/TAC.2016.2593742, May 2017.

[10] F. Kang, Dawei Cheng, Yi Tu, and Liqing Zhang, "Credit Card Fraud Detection Using Convolutional Neural Networks", in Proceeding of the International Conference on Neural Information Processing, Springer Inter-national Publishing, 2016.

[11] N. Mahmoudi and E. Duman, "Detecting credit card fraud by modified Fisher discriminant analysis", Expert Syst. Appl. 42 (April (5))(2015) 2510 : 2516, Elsevier 2014.

[12] Ivo Correia, Fabiana Fournier, and Inna Skarbovsky, "The uncertain case of credit card fraud detection", in ACM DEBS. 181 : 192, ACM 978-1-4503-3286-6/15/06, ACM 2014.

[13] Santiago, G. P., Pereira, A. C. M. Hirata, R. (2015), "A modeling approach for credit card fraud detection in electronic payment services", 30th Annual ACM Symposium on Applied Computing, 978-1-4503-3196-8/15/04 ACM 2015.

[14] Ashphak Khan, Tejpal Singh and Amit Sinhal, "Observation Probability in Hidden Markov Model for Credit Card Fraudulent Detection System", Springer 2016.

[15] Ankit Mundra and Nitin Rakesh, "Online Hybrid Model for Online Fraud Prevention and Detection", Intelligent Computing, Networking, and Informatics, Springer India 2014.