Hidden Markov Model Application for Credit Card Fraud Detection Systems

Agbakwuru A. O.
Department of Computer Science,
Faculty of Science
Imo State University,
Owerri, Imo State-Nigeria

Amaefule I. A
Department of Computer Science,
Faculty of Science
Imo State University,
Owerri, Imo State-Nigeria

Elei F.O
Department of Computer Science,
Faculty of Science
Imo State University,
Owerri, Imo State-Nigeria

Abstract:- Evidently, the use of electronic card based (Credit and Debit) for transaction has increased rapidly due its convenience and ease of use for payment of online transaction and regular purchases. However, the integration of electronic payment for goods and services has created the chances of incidence of fraudulent activities. This paper is aimed to authenticate the credit card transaction through a scalable security system which will promote trust in communication channels using Hidden Markov Model (HMM) which will accept or decline incoming transaction based on the cardholder spending pattern. Fraud Detection System (FDS) developed is an online tool which used the HMM to detect, control and Monitor fraud in electronic card transaction. Through this process the result demonstrates that HMM can decrease fraud loss.

Keywords:- *Fraud Detection, Spending Pattern, Credit Card, Electronic Commerce.*

I. INTRODUCTION

The coming of electronic banking has aided online transactions, especially in the era of cashless policy. The development of electronic payment channels and the fast advancement of electronic channel ecosystem have increased the rate of e-fraud.

Electronic shopping have gained rapid acceptance with the use of electronic cards; electronic transactions can be performed with virtual and physical card for internet and offline business. In online payment mode, the fraudster needs to know the credit card details to performed fraudulent transaction. In physical payment mode, the fraudster has to pilfer the card from its owners to commit fraud with the card which could lead to significant monetary loss if not noticed on time. Discovering credit card fraud is a very complex job when using usual procedure. Advancement of the credit card fraud detection models has become of great significance for researchers and financial institution.

There is no assurance among credit card users upon payment transaction system. Reliable and secure fraud detection method is crucial to maintain secure card handling for financial institutions and advancement of electronic commerce. Fraud detection based on evaluating current spending pattern records of cardholder is a potential approach for dropping the occurrence of credit card frauds. However, fraud is spreading all over the globe with consequences of huge amount of financial loss through the advancement in Technology and improvement in the communication channels.

A. Types of Credit Card Fraud

Credit card fraud is an illegitimate use of credit card or its details without the awareness or permission of the owner. Application and Behavioral fraud are two major forms of different credit card tricks. [1]. Application fraud: Applying for new cards from issuing banks with false information. Multiple applications may be tendered by a fraudster with one particular user details called duplication fraud or identity fraud (different user with identical details). Behavioral fraud has four principal types

- Counterfeit card
- Card holder not present
- Stolen/Lost card
- Mail theft

Counterfeit card and Card holder not present fraud; credit card details are obtained without the cardholder knowledge. Counterfeit cards are made based on card information whereas card holder not present fraud transactions are made using card information via phone, mail and the internet. [2]. Stolen/lost card fraud takes place when swindler steals a credit card or has access to a missing card. Mail theft fraud happens when a swindler gain access to a credit cardholder mail or private details from financial institution before getting the authentic cardholder. [1].

B. Different Types of Fraudster

[3], has classified fraudsters into one of these three groups below.

- ***Pre-Planned Fraudsters:*** those with intention to commit fraud right from the beginning. They can be temporary players like many who use false social security number or stolen credit cards; or longer term those who carry out intricate money laundering systems and bankruptcy.
- ***Intermediate Fraudsters*:** those with honest mind and intent but turn to fraud when life get tough or life trials such as not been promoted as when due or need to pay bills for family members, change the normal mode.
- ***Slippery-Slope Fraudster*:** this concerns a common trader or a key commerce group. Neutrally they are not

in any arrangement to pay their debts but simply carry on trading.

II. LITERATURE REVIEW

Today, fraud which is as old as human trade and transactions is considered a multi-million dollar business in the world and its financial volume is on the increased. In recent times, the advancement of latest technologies has opened many ways for fraudsters to commit fraud. With the wide use of credit card, fraud emerges as a main concern in credit card business.

[4]; presented a CARDWATCH: Built upon the neural network learning algorithm. This method is aimed towards business execution and therefore can handle huge records, and considerations of an investigation can be simply adjusted inside a graphical user interface (GUI). Card watch employs three major neural network learning methods: conjugate gradient, back propagation, and batch back propagation. This system is a useful product for large financial establishments due to its ease of execution with commercial databases. However, the algorithm suffered major set because the system needs to build a separate neural network for each customer, take a long time to proceed due to the complex analyses, cannot discover complex pattern and has extremely huge overall network that needs comparatively huge amounts of funds to sustain.

Another limitation of the system proposed by [5] is; the system finds it very complex in deciding a significant set of identification variables and it encounters difficulties in finding effectual datasets to train with. Neural Fraud Detection in Credit Card Transaction; called Minerva was proposed by [5]. The work major focal point is to imbed the fraud detection system (FDS) capable of detecting fraud in real time. It employs a fresh nonlinear categorized evaluation procedure that combines the multilayer acuity structural design of a neural network with Fisher's categorized evaluation procedure. Minerva does not need a huge set of past records because it acts exclusively on immediate preceding record, and can categorize operation in sixty minutes.

The main problem in the system proposed by [6]; is the customer records are not dynamically adjustable, continual updates are needed when customer habits and fraud behaviors' change and the techniques are based on anticipations, and illogical anticipations may lead to defects and blunders in the decision tree. [6], proposed to generate a customer record for every credit card account and check current transactions, matching it with corresponding customer's record. The features used to build these records are: credit card numbers, transaction dates, type of business, place, and amount spent, card limit and expiration date. [6], recommended a Similarity Tree algorithm, a change of Decision Trees, to get customer's behaviour. The analyses found that the technique has a very little prospect for false negative errors.

[7], proposed a Multiple Algorithms for Fraud Detection; a case-based reasoning method that consists of two parts, retrieval module and decision module, to reduce the amount of fraud investigations in the credit authorization process. The retrieval module employs a weighting matrix and nearest neighbor strategy to identify and extract suitable cases to be used in the concluding diagnosis for fraud, whereas the decision module utilizes a multi-algorithm strategy to evaluate the captured cases and attempts to reach a concluding diagnosis. Nearest-neighbor and Bayesian algorithms were used in the multi-algorithm strategy. Initial results of 80% non-fraud and 52% fraud Recognition. These suggest that their multi-algorithmic case-based reasoning method is proficient enough of high accuracy detections. However, its limitations are evidences of High computation difficulty; to detect the k nearest neighbor parameters, among other factors.

III. METHODOLOGY

A. Implementing Hidden Markov Model Techniques for Credit Card Fraud Detection System:

To detect and monitor credit card fraud using Hidden Markov Model (HMM). The study was conducted using two module called Admin (Bank) and User (Customer) module, and each of the module has sub menus that determine various functions and also three data engine which are customer databases, bank database and fraud database which has its specific function in fraud detection and monitoring system. The fraud detection system (FDS) will check the credit card information's (such as credit card number, CVV number, Type, expiry date etc.) with the credit card customer database. It will equally ask for personal identification number (PIN) and match it with the database and check the account balance; then fraud authentication will be activated. The HMM receive its input and check the geo-location, email address and phone number which the cardholder has frequently made genuine transactions which are presented at the time of card registration.

During incoming operation the FDS will check on the ten recent transaction of the cardholder based on the threshold value of (high, medium, low) using this observation, will determine the personal expenditure routine of the cardholder. If the credit card user has less than ten transactions it will build up to ten genuine transactions for authentication check to be fully activated. For further authentication check, the FDS will ask directly credit cardholder that has up to ten or less than ten transactions for dynamic password and personal security question to continue the transaction (like Confirmation code, mother maiden name vowels and consonant, favorites, friend name, etc.) the customer must response to them correctly for the transaction to take place.

After the checked, if incoming transaction is genuine the FDS gives its authorization for the transaction and store in bank database for future reference. If detected as suspicious the fraud alert will automatically send to the bank, customer and fraud database, the bank will terminate the transaction and block the account temporary.

B. Credit Card Fraud Detection Model:

There is a predetermined behaviour on how credit card holders make their purchases online. This predetermined behaviour can be drawn from past genuine records of transaction by the cardholder; the place where these genuine transactions were made, electronic mail addresses and phone number frequently used for notifications by the cardholder.

The HMM technique for fraud detection in credit card can be trained with predetermined behaviour and apply it as information in categorizing a real-time operation as illegitimate or genuine transaction. Immediately the record to be evaluated is chosen, the fraud detection model will be apply to execute by transition probabilistic calculation based on HMM procedure for matching the activities of the present transaction, if it varies in spending profile activities with the cardholder past records of transaction; it will maintain the check by subjecting it to further authentication checks to confirm that the transaction is genuine through dynamic password the system will send to the credit cardholder's phone number provided during card registration as well, the personal security question. If the current transaction is legitimate, the system will allow it and stores it in the Bank Database and consider it in subsequent fraud detection; if detected as suspicious, the fraud alert will automatically send to admin (Bank), User (Card owner) and fraud database for further investigation. The issuing bank regrets the transaction and blocks the account temporarily.

C. Behavioral Pattern Recognition to Train HMM:

➢ *Spending Records of the Cardholder:*

Credit card Fraud Detection System (FDS) based on Hidden Markov Model (HMM) was designed, the model does not require fraud signature and can effectively detect fraud just through credit card owner spending pattern. The vital advantage of the HMM based technique, it significantly reduces the number of genuine transaction (false positive) recognized as suspicious by fraud detection system. The HMM checks the spending behaviour of the card owner based on the threshold price value of high (h), medium (m) and low (l). It dynamically determines the threshold value using clustering algorithm of every cardholder personal expenditure routine. However, it is pertinent to note; every state of the model were fully connected with the Hidden Markov Model which can be reached just in a single step; this scalability forms the optimum consideration.

D. Architecture of Credit Card Monitoring and Detection Techniques based on Hidden Markov Model

This is new credit card monitoring and detection architecture as shown in fig. 1 below

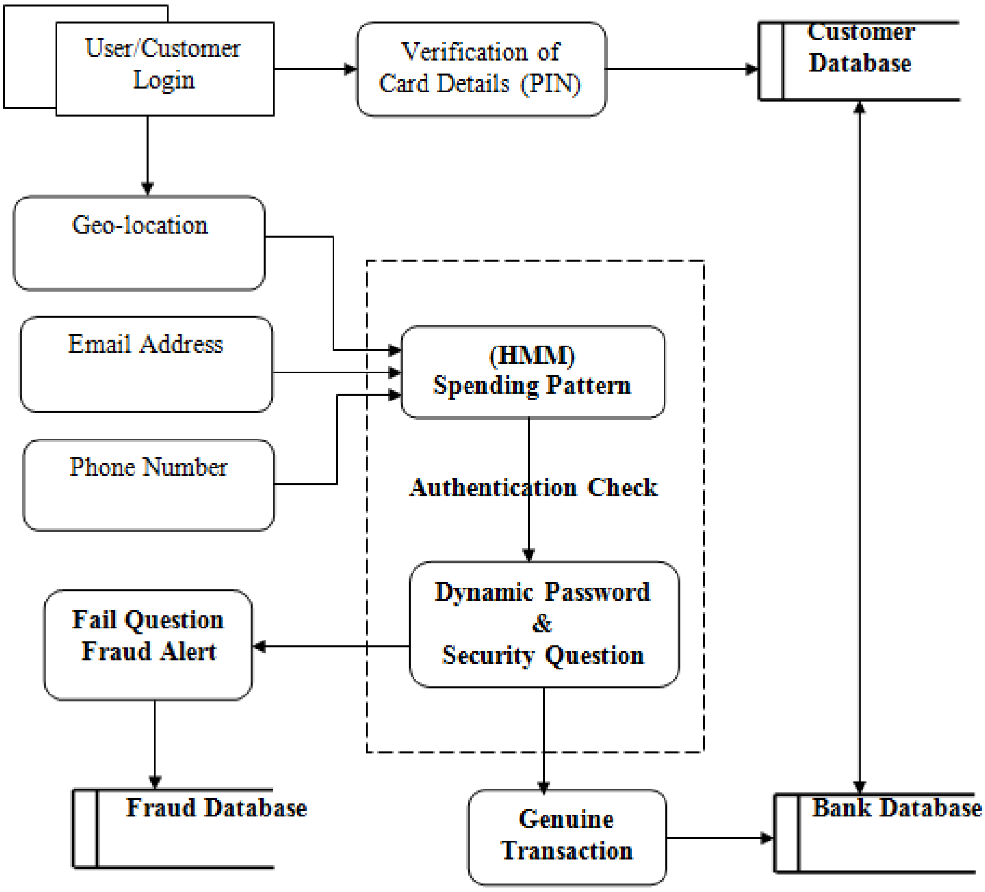

Fig 1:- Architecture of HMM Credit Card Monitoring and Detection Techniques

IV. IMPLICATION/CONCLUSION

Building precise and simple credit card fraud detection and monitoring system in an automatic, controlled and general acceptable way is a major task for financial institution. The Hidden Markov Model method is employed to discover different unnoticed (hidden) actions on credit cards. It keeps databases where previous records of transactions are saved. Card owner is informed through a method of communication if an abnormal transaction occurs, which deviates from the past activities of the card owner. This paper presented a Hidden Markov Model application which has been modeled as a subsystem and can be apply in software system and embedded application in financial institution to identify credit card fraud. The FDS is scalable for managing large volume of transactions; it is an enhanced algorithm of less complexity and does not take time to process fraud check. At the primary state HMM check the incoming transactions whether is genuine or fraudulent and to know whether to accept the next transaction or not based on the prospect outcome. The price value of low, medium and high were considered; geographical location, email address and phone number of the credit card owners were also considered. For further authentication the system send dynamic code to the user and personal security question before alert is being send to admin (Bank), User (Card owner) and fraud database for further investigation regarding the suspicious fraudulent transaction. The issuing bank regrets the transaction and blocked the account temporary. This decreases the categorization of genuine transactions as false, guaranteed precise and dependable result. This strengthens the reliability and capability of Hidden Markov Model as survey tool.

ACKNOWLEDGMENT

We are sincerely grateful to **TETFUND** for the sponsorship of this research, and also the Vice Chancellor of Imo State University, Owerri for encouraging collaborative research in the institution.

REFERENCES

[1]. Linda Delamaire, Hussein Abdou, John Pointon, (2009). Credit card fraud and detection techniques: a review, *Banks and Bank Systems*, Volume 4, Issue 2,

[2]. Samaneh Sorournejad, Zahra Zojaji, Reza Ebrahimi Atani and Amir Hassan Monadjemi (2016). A Survey of Credit Card Fraud Detection Techniques: *Data and Technique Oriented Perspective.*

[3]. Wells, J., (2013), Corporate fraud handbook: prevention and detection 2nd ed. Hoboken, NJ: John Wiley and Sons. http://www.fspro.net/sec/. Ultimate security solutions for home and office- from fspro labs

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

[5]. Dorronsoro J.R., Francisco G., Carmen S., and Carlos S.C., (1997). Neural Fraud Detection in Credit Card Operation. IEEE Transaction on Neural Network, vol.-08, no.-04, pp.: 827-834

[6]. Kokkinaki, A. (1997). On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling. Knowledge and Data Engineering Exchange Workshop. IEEE, pp.:107-113.

[7]. Wheeler R. and Aitken S. (2000). "Multiple algorithms for fraud detection", Knowledge-Based Systems, no. 13 pp.: 93-99,