International Journal of Humanities and Social Science Invention (IJHSSI)
ISSN (Online): 2319 – 7722, ISSN (Print): 2319 – 7714
www.ijhssi.org ||Volume 7 Issue 06 Ver. IV ||Jun. 2018 || PP.05-10

Fraud Detection on Event Log Of Credit Business Using Hidden Markov Model Algorithm

Shilpa.Mukthapuram[1] ,Dr. J. Narayan Singh[2] , Shivaraj Kumar T H[3]
1Impact College Of Engineering and Applied Science
2 Professor Department of CSE,Impact College Of Engineering and Applied Science , Bangalore.
3 Assistant Professor Department of CSE,C Byregowda Institute of Technology, Kolar.
Corresponding Author: Shilpa.Mukthapuram

ABSTRACT: *Illegal instances of banks have ascended by 55% of every 2016. One reason is the misrepresentation in business forms can't be distinguished early. Reacting to that issue, this exploration proposes a strategy for identifying extortion on business forms in the bank credit application. This technique utilizes Hidden Markov Models and action data recorded in the occasion log. Concealed Markov Model that utilized for ascertaining likelihood plausibility of extortion in view of the occasion log. The outcomes demonstrate that HMM strategy can identify extortion properly.*
Hidden Markov Model that used for calculating probability possibility of fraud based on the event log. The results show that HMM method can detect fraud appropriately. The experimental results also show that the accuracy of the results is 96%.

KEYWORDS—*bank; event logs; financial; fraud; Hidden markov model; extortion;misrepresentation*

Date of Submission: 11-06-2018 Date of acceptance: 26-06-2018

I. INTRODUCTION

A bank has several business processes happening on day to day basis. The business processes are used to manage the bank [1]. The bank has many types of business processes. One of the types is bank financial credit business process. Bank financial credit business processes can be changed dynamically. This change is due to increased demand and information, changing of market conditions, or policy changes on the bank's business processes [2].

In bank fraud often occurs that causes a loss to the bank.

Fraud can occur due to violations of business processes or standard operating procedures and manipulation of data. Fraud can be defined as a crime that using deception as the main mode and includes a variety of irregularities by individuals and organizations. Fraud, if not prevented and detected will cause a great loss to the bank. Therefore need to research to find techniques that can be used to detect fraud in business process.[3].

In this research, the data obtained from the event log on each event log data on bank credit application. The event log data then analyzed using an algorithm Hidden Markov Model (HMM) In order to rebuild process model (a model that produces activity traces) and detect fraud symptoms. The analysis process is particularly useful for detecting anomalies on business processes that occur during the process of the Bank Credit Application

Hidden Markov Model will be helpful to find out the fraudulent event log data by using registration details of user which include the event log data uploaded to be verified. It works on the user authentication of event log data uploaded by the user which can be divided into major four types such as 1) Weak; 2) Medium; and 3) Strong 4)Very Strong. For every credit Business, the event log data to be verified will be different, so HMM can figure out an inconsistency of user submitted event log data andtry to find fraudulent transaction.

II. HIDDEN MARKOV MODEL

A Hidden Markov Model is a finite set of states; each state is linked with a probability distribution. Transitions among these states are governed by a set of probabilities called transition probabilities. In a particular state a possible outcome or observation can be generated which is associated symbol of observation of probability distribution. It is only the outcome, not the state that is visible to an external observer and therefore states are ``hidden" to the outside; hence the name Hidden Markov Model [5-7].

Hence, Hidden Markov Model is a perfect solution for addressing detection of fraud event log data through credit card. In this prediction process, HMM consider mainly three price value ranges such as [14-15]

1) Weak , 2) Medium and, 3) Strong 4)Very Strong. First, it will be required to find out event log datathat belongs to a particular category either it will be in Weak, medium, Strong and Very Strong.

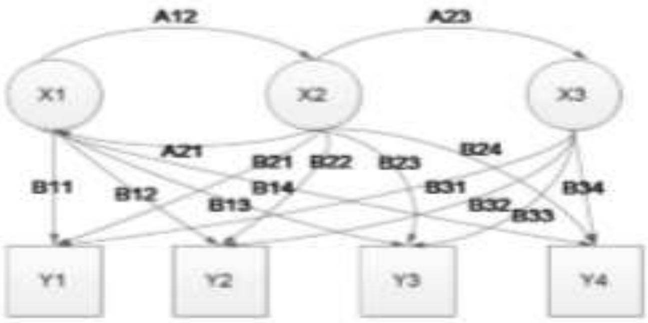


Fig. 2. Probabilistic parametric quantity Hidden Markov Model.

III. FRAUD:

The Association of Certified Fraud Examiners (ACFE) or the Association of Audit Fraud Certified) divides fraud into three types namely deviations on assets (asset Misappropriation), Statement of Counterfeit (Fraudulent Statement), and corruption (Corruption) [13].Here we focus on deviations on assets (asset Misappropriation).

IV. ASSET MISAPPROPRIATION FRAUD DETECTION USING HMM

Data Source:

The data obtained by the authors is the data of the financial system in the form of bank data division activities performed and data on bank employees in the form of data in .csv format. The data in .csv format consists of several columns containing:

1)Identity Documents
2)Account Documents
3)Credit Terms
4)Project information
5)Planned Business Location
6)Project Gross Value
7)Tax Documents
8)Business Loan Type
9) Assets and Liabilities Documents
10)Loan Reason
11)Loan Amount

Procedure Research

The procedures in this research starting from data collection event log .csv format. Then use the .csv formatted log event data to calculate the value probability matrix algorithms using hidden Markov models. After getting probability value matrix, checking the data which it contains elements of fraud or not. Fraud will be detected if the state probability of fraud is greater than the value of state probability of no fraud, and vice versa, if the value of state probability no fraud is higher than the probability of fraud, the state is not detected symptoms fraud case.

First the user approached bank for any transaction say request for loan amount need to first register with the bank. Then the same user on Login into application will be prompted with details mentioned above to enter.

After filling all these information, now the page will be directed to proposed fraud detection system which will be installed at bank’s server.

Fraud Detection System

All the information about user submitted event log data (Like Identity Documents, Account Documents, Credit Terms,Project information,Planned Business Location etc.) will be checked with corresponding database by the staff of bank where the user has requested for some transaction to happen. These each of these details are then authenticated by bank employee and rated as bad, very weak, weak, middle, strong or very strong.

Then the authentication and rating details done by bank staff will be submitted to bank superior employee say like bank manager for approval.

Based on these rating details of usersubmitted event log data probability possibility of fraud using HMM is calculated.

Design Workflow

Workflow design of bank credit application is as shown below.

By using this observation, determine users spending profile.The purchase amount will be checked with spending profile ofuser. By transition probabilistic calculation based on HMM, itconcludes whether the transaction is real or fraud. If transaction

may be concluded as fraudulent transaction then user must entersecurity information. This information is related with credit card

(like account number, security question and answer which areprovided at the time of registration). If transaction will not befraudulent then it will direct to give permission for transaction.

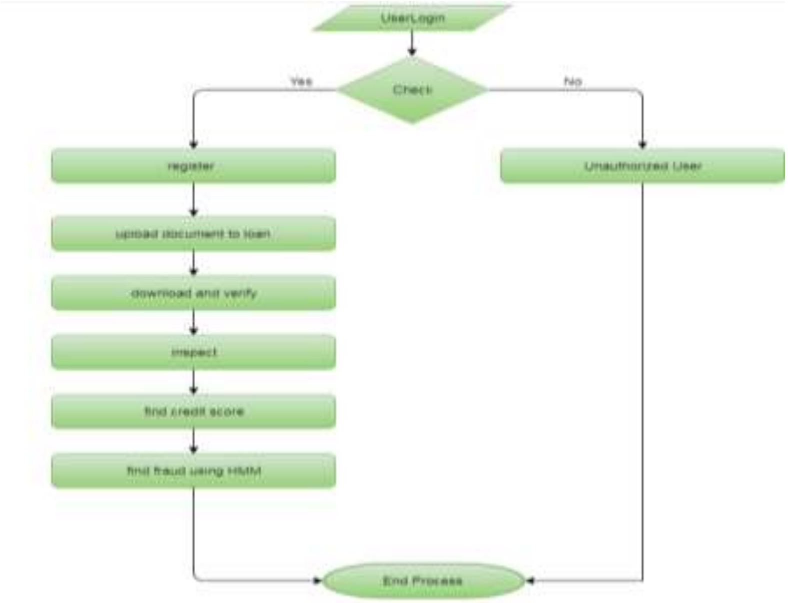


Fig. 1| Flow Chart of bank credit application

The implementation techniques of Hidden Markov Model in order to detect fraud transaction through credit cards, it create clusters of training set and identify the spending profile of card holder.

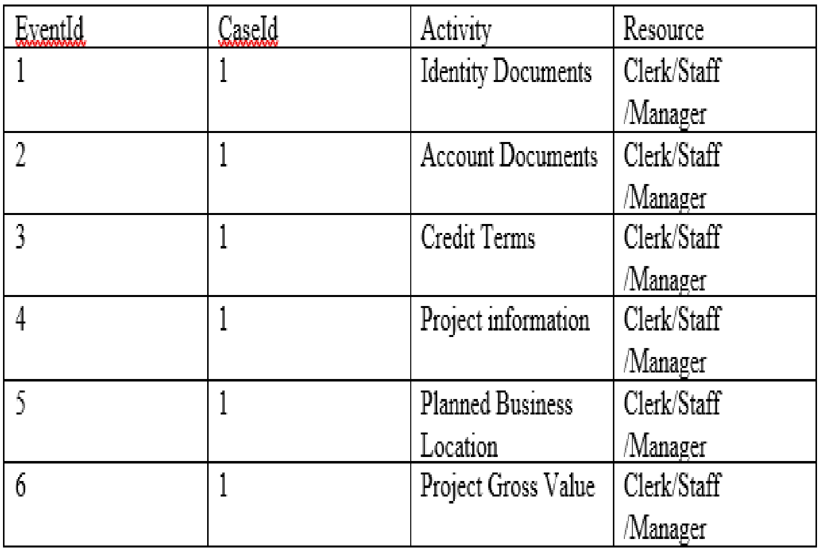
The number of items purchased, types of items that are bought in a particular transaction are not known to the Fraud Detection system, but it only concentrates on the amount of item purchased and use for further processing. It stores data of different amount of transactions in form of clusters depending on transaction amount which will be either in low, medium or high value ranges. It tries to find out any variance in the transaction based on the spending behavioral profile of the cardholder, shipping address, and billing address and so on.

The probabilities of initial set have chosen based on the spending behavioral profile of card holder and construct a sequence for further processing. If theFraud detection system makes sure that the transaction to be of fraudulent, it raises an alarm, and the issuing bank declines the transaction.

By using this observation, determine users spending profile.The purchase amount will be checked with spending profile ofuser. By transition probabilistic calculation based on HMM, itconcludes whether the transaction is real or fraud. If transactionmay be concluded as fraudulent transaction then user must entersecurity information. This information is related with credit card

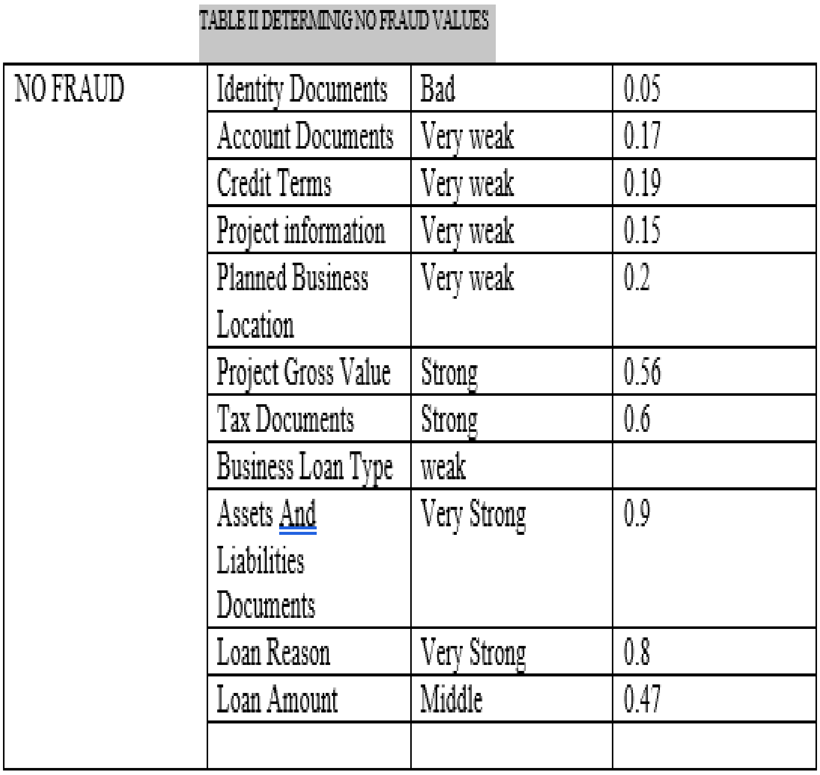
(like account number, security question and answer which areprovided at the time of registration). If transaction will not befraudulent then it will direct to give permission for transaction.

TABLE I. TABLE EVENT LOG BANK FINANCIAL CREDIT BUSINESS PROCESS



EventId	CaseId	Activity	Resource
1	1	Identity Documents	Clerk/Staff /Manager
2	1	Account Documents	Clerk/Staff /Manager
3	1	Credit Terms	Clerk/Staff /Manager
4	1	Project information	Clerk/Staff /Manager
5	1	Planned Business Location	Clerk/Staff /Manager
6	1	Project Gross Value	Clerk/Staff /Manager

TABLE II DETERMINIG NO FRAUD VALUES



NO FRAUD	Identity Documents	Bad	0.05
	Account Documents	Very weak	0.17
	Credit Terms	Very weak	0.19
	Project information	Very weak	0.15
	Planned Business Location	Very weak	0.2
	Project Gross Value	Strong	0.56
	Tax Documents	Strong	0.6
	Business Loan Type	weak	
	Assets And Liabilities Documents	Very Strong	0.9
	Loan Reason	Very Strong	0.8
	Loan Amount	Middle	0.47

TABLE III DETERMINIG FRAUD VALUES

[illegible]		[illegible]	[illegible]
[illegible]		[illegible]	[illegible]
[illegible]		[illegible]	[illegible]
[illegible]		[illegible]	[illegible]
[illegible]		[illegible]	[illegible]
[illegible]		[illegible]	[illegible]
		[illegible] Loan Type	Strong
[illegible]		Assess And Liabilities Statements	Very Strong
[illegible]		[illegible]	Very Strong
[illegible]		[illegible] Amount	Middle

V. RESULT AND ANALYSIS

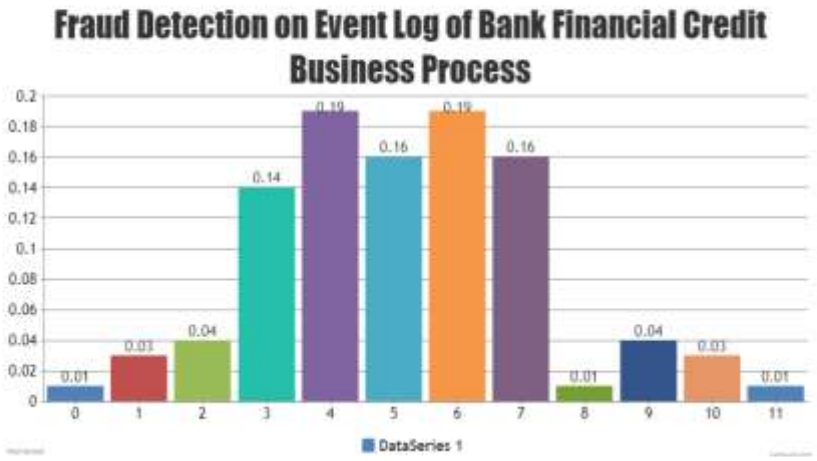
The experiments for this research is a bank loan application process. This research using event log to determine the activities are influenced by fraud.

Fraud will be detected if the state probability of fraud is greater than the value of state probability of no fraud, and vice versa, if the value of state probability no fraud is higher than the probability of fraud, the state is not detected symptoms fraud case.

Probability Initial State	*Fraud*	*0.5*
	No Fraud	*0.5*

VI. CONCLUSION

This experiment identifies 90 cases of bank loan applications event logs. The cases contain 5 cases of fraud and 85 cases of no fraud. This paper concludes that the accuracy of the experiment by using Hidden Markov Modell is 96%. The experiment results also showed that algorithm utilized Hidden Markov Model can obtain cases which detected symptoms of fraud in the testing data.



REFERENCES

[1]. K.-D. Gronwald, “ERP: Enterprise Resource Planning,” Integrated Business Information Systems, pp. 59–86, 2017

[2]. S.N. Chary, Production and Operations Management, New Delhi: Tata McGraw-HillEducation, 2009.

[3]. O.Monisola, "Effect of Internal Audit On Prevention of Frauds, Errors And Irregularities In Corporate Organisation," in IISTE, Nigeria, 2013.

[4]. W.V.D. Aalst, Process Mining: Discovery, Conformance and Enhancement of Business Processes, Netherlands: Springer, 2011.

[5]. A.Rozinat, and W. DerAalst, Conformance Checking of Processes Based on Monitoring Real Behavior, Netherlands: Eindhoven University of Technology, 2007.

[6]. I. Merriam-Webster, "Merriam Webster," Merriam WebsterIncorporated, 5 March 2015. [Online]. Available: http://www.merriamwebster.com/dictionary/credit. [Accessed 25 December 2016].

[7]. A.Kassahun, and B. Tekinerdogan, “Architecture Viewpoint for Modeling Business Collaboration Concerns using Workflow Patterns,” Proceedings of the 11th International Joint Conference on Software Technologies, 2016.

[8]. S. Huda, R. Sarno, and T. Ahmad, " Increasing Accuracy of Processbased Fraud Detection Using a Behavior Model," International Journal of Software Engineering and Its Applications (IJSE), pp. 175-188, 2016.

[9]. R. Sarno, H. Ginardi, E.W. Pamungkas, and D. Sunaryono, "Clustering of ERP business process fragments," International Conference on Computer, Control, Informatics and Its Applications (IC3INA), . 319 – 324, 2013.

[10]. R. Sarno, Kartini, W.A. Wibowo, and A.S.A, "Time Based Discovery of Parallel Business Processes," in The 2015 International Conference on Computer, Control, Informatics and its Applications (IC3INA), 2015.

Shilpa.Mukthapuram." Fraud Detection on Event Log Of Credit Business Using Hidden Markov Model Algorithm."International Journal of Humanities and Social Science Invention (IJHSSI) 7.06 (2018): 05-10.