ISSN No:-2456-2165

Fraud Detection in Internet Banking Transactions using Sliding Window Strategy

Abhinandan[1],Abhijeet Chauhan[2], Divyendu Shekhar[3], Narendra Kumar[4]
[1]Computer Science & Engineering, National Institute of Engineering, Mysore
[2]Computer Science & Engineering, National Institute of Engineering, Mysore
[3]Information Science & Engineering, National Institute of Engineering
[4]Computer Science & Engineering, National Institute of Engineering, Mysore

Abstract:- Internet Banking(IB) frauds are relatively eaisier for hackers and attackers with malafide intentions and so the number of Internet banking frauds these days are overwhelming. E-commerce platforms and many other online shopping portals have included Internet Banking as a payment mode, increasing the risk for IB frauds. The primary intent of this research work is to improvise and develop a unique and new fraud identification technique for Internet Banking Transactions by analysing the past transaction and banking details of the customer and deduce the patterns in the nature of transactions done so as to be able to detect an anomalous transaction in future. Where IB account holders are grouped into different categories based on their transaction and internet banking activites. Then we make use of the sliding window protocol or strategy, to assimilate the transactions and activities done by the customers from different internet banking channels so that the patterns and similarities in the nature and type of the transactions belonging to different categories or groups can be inferred and extracted respectively.

Keywords:- *Internet Banking Transactions, Sliding Window Strategy, Concdept Drift;*

I. INTRODUCTION

Internet Banking(IB) transactions being the cornerstone of cashless economy, there is a spike in the volume of such transactions. The statistics available with National Crime Records Bureau says that in excess of three thousand incidences of internet banking frauds were recorded in 2018. Internet banking data is highly disproportionate because there will often be more number of legitimate transactions when compared with fraudulent transactions. However, despite all adversaries, there are umpteen strategies and techniques to overcome this problem.

II. PROPOSED METHOD

Internet Banking (IB) activities including financial and non financial transactions are mostly unfamiliar when studied and compared to past records of the customer. The main aim of our research work is to device a method or algorithm to predict the legitimacy of the new IB transactions done by an accountholder and to simultaneously overcome the problem of concept drift. Table 1, shows basic attributes that are captured when any financial or non financial transaction is done.

Table 1: Raw attributes of Internet Banking activities

FEATURE NAME	BRIEF DESCRIPTION
UTR number	Unique Identification Number of a transaction
Account Number	Identifier of a user account
Total Amount	The total Amount transferred
Time	Time of the transaction
IP	IP address of the device from which transaction is done
Marker or Label	To specify whether the transaction is legitimate or fraudulent

2.1. Algorithm

- Firstly, we use a grouping mechanism to categorise the account holders into different categories or baskets based on their transaction volume, i.e., high, medium, and low using range partitioning technique.
- Using Sliding-Window protocol and strategy, we classify the Internet Banking activities into respective categories, i.e., extract features from the sliding window to find the user's behavioural patterns. Features like Geo-location (IP range), max amount, min amount of transaction, in the window and even the time taken in the process.

Algorithm 1: Algorithm to classify and group transaction details and to deducecustomerbehaviors using sliding window technique.

Input: account details of the customer, a sequence of transactions s and window size z.
Output: Classified transaction details and behaviors of account holder legitimate or fraudulent.

ISSN No:-2456-2165

```
d: length of S
Legitimate= [];
Fraudulent= [];
For g in range 0 to d-z+1:
        S: [];
        /* sliding window attributes*/
        For j in range g+z-1:
        /*Add the transaction to window */
        S=S+sj (id);
End
/* behavior extraction related to amount of
the transaction*/
bi1=MAX_AMT(Sg);
bi2=MIN_AMT(Sg);
bi3=AVG_AMT(Sg);
bi4=AMT(Sg);
For j in range i+z-1:
        /* Time taken for the transaction*/
        xi= Time(sj)-Time(sj-1)
End
Pi= (bg1, bg2,bg3,bg4,bg5,);
Q= LABEL(Sg);
/* grouping a transaction into fraudulent
or legitimate */
 if Qg=0 then
        Legitimate =
        (Legitimate)Union(Pg);
Else
        Fraudulent
        =(Fraudulent)Union(Pg);
 End
```

- Anytime a new activity or transaction is fed into the sliding window, the previous ones are removed and step-2 is re-executed for each category and group of transactions.
- After generating the score, we turn on an assessment system, wherein the current activities and updated scores are fed back to the system for subsequent study and comparisions.

III. CONCLUSION

In this research work we deviced a new approach and strategy for fraud identification and prevention in Internet banking transactions, where customers' data is grouped on the basis of their financial and non financial activities in internet banking channels and we extract behavioural patterns to dynamically build and incrementally develop a user profile for each and every accountholder or user. These runtime updations and changes in parameters and features lead the system or our algorithm to adapt to new accountholder's behavioural patterns punctualy and timely.

Going forward, whenever a new transaction is being done from the account of a particular accountholder, we can see if the behavior of the transaction matches the behavior of the accountholder. If the behavior is new or doubtful, we may use multifactor authentication to validate the legitimacy of the transaction before its execution and hense prevent potential frauds.

REFERENCES

[1]. http://www.rbi.org.in/Circular/CreditCard
[2]. https://www.kaggle.com/mlg-ulb/creditcardfraud
[3]. https://www.kaggle.com/uciml/default-of-credit-card-clients-dataset
[4]. https://www.npci.org.in
[5]. http://www.niti.gov.in
[6]. https://finmin.nic.in