IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

A Study on Credit Card Fraud Detection based on Behaviour and Location Analysis

Shaikh Sahil Anwar and Shaikh Sohail Shujauddin
Student, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *In this system we present Behavior and Location Analysis (BLA). Here the system analyzes the behavior pattern of the user while using his credit card and detects the location and physical address to identify the user. This pattern includes the characteristics such as the spending pattern, device information and the geographic location of the user to verify his identity. If any unusual pattern is detected, the system requires re-verification.*

Keywords: Credit Card, Behavior and Location Analysis (BLA), Fraud Detection System (FDS).

I. INTRODUCTION

Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction . The Main purpose of a fraudster is to obtain goods without paying for it or to obtain the funds from an account without authorization. Credit card fraud is the most common form of reported identity theft followed by government documents/benefits fraud . In existing system, System doesn't keep record of the spending pattern of the user or it doesn't bother about the location from where a transaction is done. If the user finds his credit card being lost or his card is used without his authorization, he registers a complaint and requests the bank or system to Block his Card.

So, here we propose a system where it will detect the credit card fraud activities based on the spending pattern, physical address of the device or machine used for a transaction and the geographical location of the user with the help of Behaviour and Location Analysis (BLA). This system will also detect the location of the user with the help of Behaviour and Location Analysis. Fraud Detection System (FDS) will be available in Bank who issues credit card for the user. BLA is a part of FDS which will be executed first, it will check for a pattern and if the Pattern is unusual the normal or the usual procedure will be skipped and BLA will take over till the end of the transaction.

II. EXISTING SYSTEM

Credit Card online payment is very much secured giving the best security, multiple options of paying and many more. While using a credit card at an ATM is not so secured as it doesn't involve so many steps, making it less secure in case of a Credit Card Theft. ATM machine will just check for the Card Details and the 4 digit pin.

BLA can also be adapted here just minimizing the pattern to the spending pattern of the user.

The steps involved in Online Payment are:

- Authorization
- Batching
- Clearing and Settlement
- Funding and
- Chargebacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

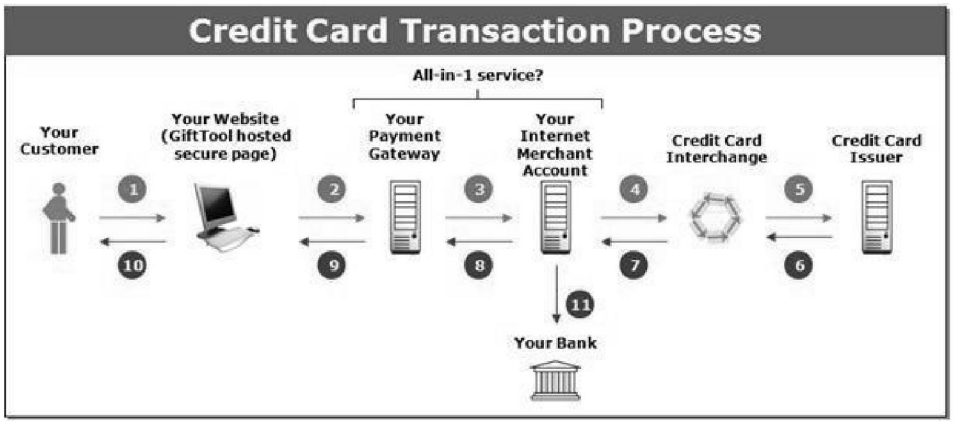

Figure 1. Credit Card Transaction Process [4]

III. PROPOSED SYSTEM

Several techniques have been developed to detect fraud transaction using credit card which are based on neural network, genetic algorithms, data mining, clustering techniques, decision tree, Bayesian networks etc. In proposed system, we present a behavior and Location Analysis (BLA), which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit and other sources. The details of the items are usually not known to any Fraud Detection System (FDS) running at the bank that issues the credit cards to the cardholders. Hence, we feel that BLA is an ideal choice for addressing this problem. Another important advantage of the BLA - based approach is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine.

False Positive Transaction means a user who is a genuine cardholder and is doing an online transaction but many a time the FDS claims or predicts it as a malicious transaction causing it to stop the transaction from committing. An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify whether the transaction is genuine or not. It tries to find any anomaly in the transaction based on credit card, the spending profile of the cardholder, address etc. If the FDS confirms the transaction to be a fraud, it raises an alarm, and the issuing bank declines the transaction.

BLA uses the behavior and location scanning to check for unusual patter of the user. These patterns include user characteristics such as user spending patterns, device information and the geographic location of the user to verify his identity. If any unusual pattern is detected, the system requires re-verification.

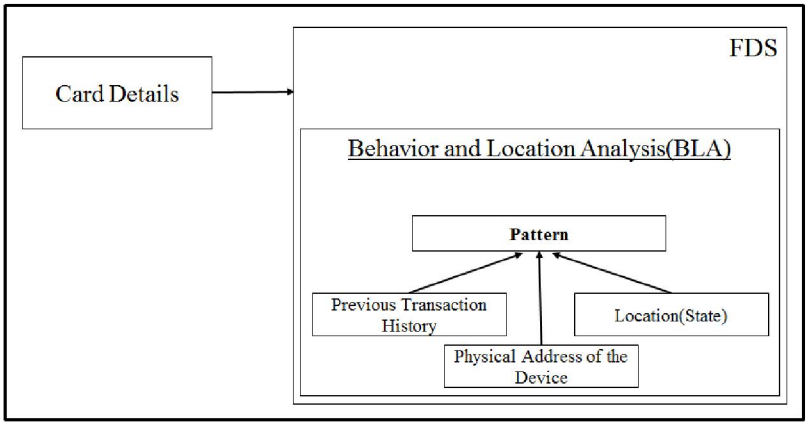

Figure 2. Overview of BLA"

Usually the user uses his machine or device to make payment maximum times, so at the time of first online transaction the Physical address is stored in the database and every time when the same user makes a payment the Physical address

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

is checked. In the same way the Geographical location is also taken as a pattern in BLA. So basically there are 3 factors used for making the pattern, and all together 3 factors act as individual pattern and used for the identification of the user.

3.1 Secure Code

Secure Code is similar to a 4 digit pin which is given at the time of Credit Card.

Secure Code is different to a pin number as pin number is always known by you or your family, friends etc. So it will not take much time for a thief or intruder to know it. If we talk in the case of Hackers, if hacker is continuously stalking into your PC etc, will at least get to know once about the Net banking or 3d secure code as it is the same and no one bothers to change it.

Secure code is rarely used and if u even forget to get the code the user has to contact the bank. In case of online payment the system will generate a OTP which will last for 5 to 10 minutes, not like the regular OTP which lasts for 4 hours.

3.2 Pattern

3.2.1 Spending Pattern:

The Spending pattern of whether it is online payment or cash withdrawals are considered, excluding the transfers. An average of all the credited transaction is calculated which is multiplied by 30% and an amount is calculated. This figure is added to the average and final amount is calculated.If the user demands or his shopping amount is more than the final amount then the system asks for the Secure Code.

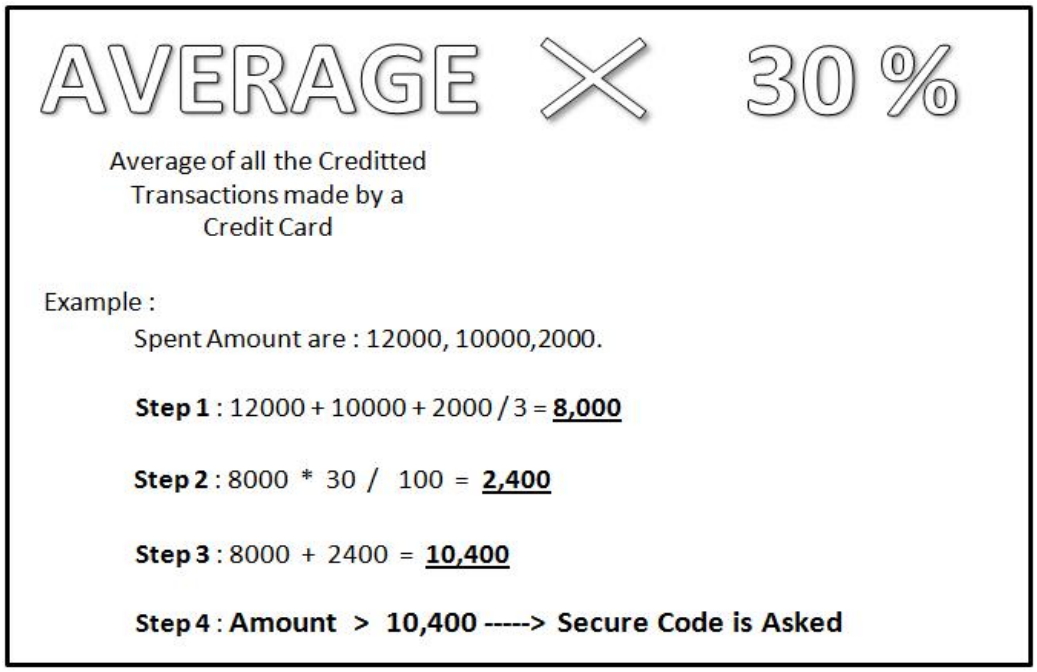

Figure 3. Spending Pattern

3.2.2 Physical Address

When the user makes his first online payment the Physical Address is stored in the database.Usually a user shops or does most of his online transaction on his same Machine. So every time a transaction is made the physical address is checked by the system and if it mismatches the secure code is asked and the new Physical Address is verified by sources and if it is genuine it is stored in the database.

For Example; I did my first transaction from my Office PC and second from my home PC, both are genuine but different, so it is verified and stored. Physical Address comes into picture only when an online payment in made, not for ATM transactions.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

3.2.3 Location

In BLA the Geographical location is taken and when the user makes a payment it checks whether the user has made the transaction in the same state, if you are out of your state, the Secure Code is asked by the system.

IV. WORKING OF BEHAVIOR AND LOCATION ANALYSIS (BLA)

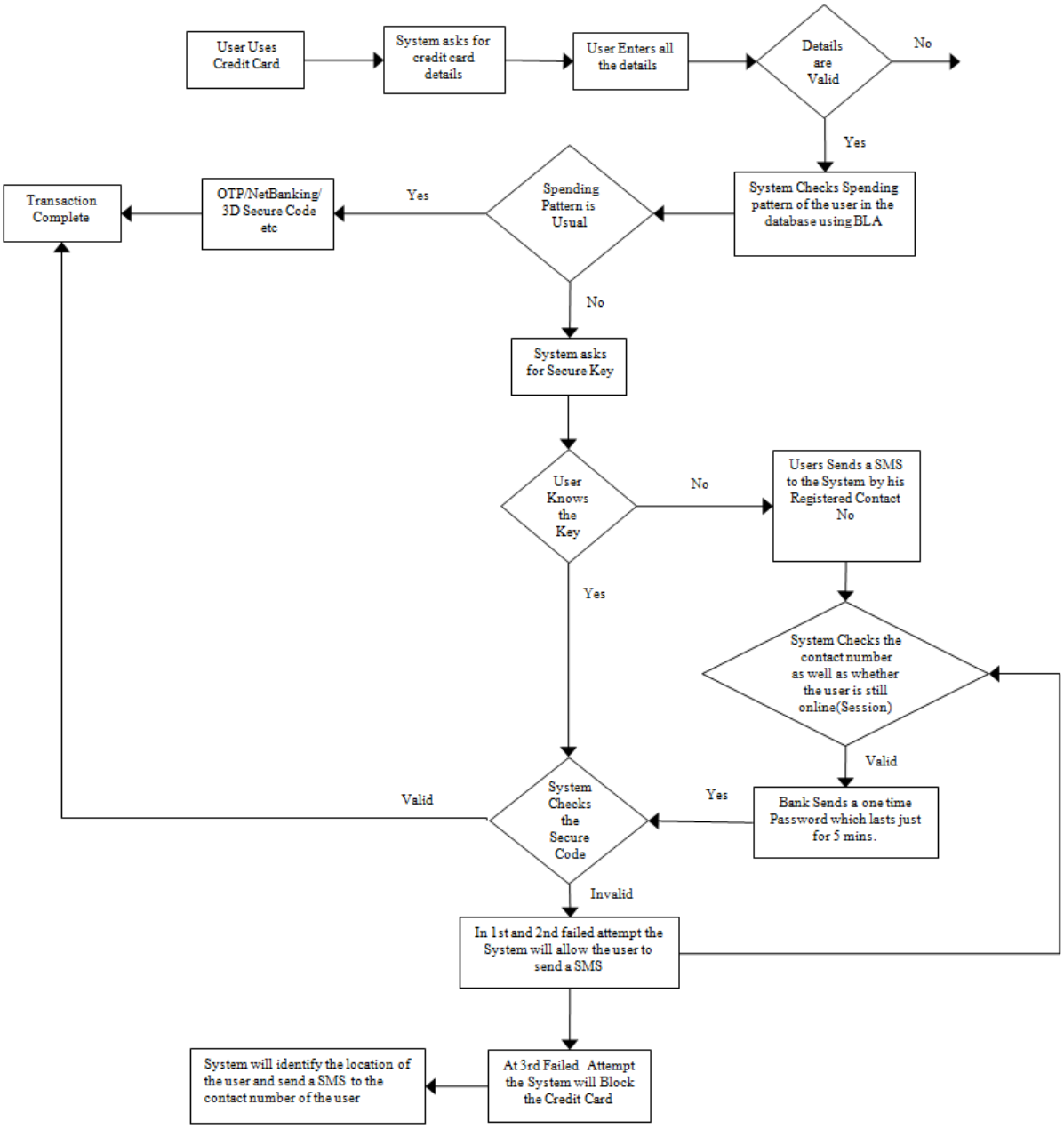

Figure 4. Flow of BLA

1. The user enters the card details in the case of online payment.
2. The System will check the card details and the amount whether the user has the amount in his account, if no it checks whether it comes under his overdraft limit.
3. Now FDS implements the BLA System, BLA starts analysing all the 3 factors.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

4. If the pattern is usual then the usual process is executed i.e. Net banking, 3D Secure code, OTP etc.
5. If the pattern is unusual the Secure Code is asked by the system.
6. If the user knows the code he enters and if it is valid the transaction is successful and in 3 failed attempts the credit card will be blocked and a message will be sent to the users registered contact number regarding the block and the location from where it was tried to access.
7. If the user doesn't remember the Secure Code, the system tells him to send a message.
8. The System will create a session for n minutes and wait for the user to send a message from his registered mobile number. If the system doesn't receives the message it will decline the transaction.
9. If the system receives the message within the session period, it sends an OTP which will last for 5 to 10 minutes.
10. The user has to enter the OTP and the transaction is committed.

V. COMPARISON OF EXISTING AND PROPOSED SYSTEM

- In case of ATM, the only security provided for current system is the pin number. But in proposed system, system will ask for pin number as well as it checks the spending pattern of the user. If the spending pattern is usual, system will allow the user to go further with his transaction. If the system detects that the amount is more than the calculated amount, System will ask the user to enter the secure code. If the code is right system will process the transaction otherwise system will block the credit card of the user and will identify the location of the intruder and will send an SMS to the registered contact number of the user.
- In existing system, System does not block the credit card immediately when the system detects the credit card is used by the intruder for malicious activities. In proposed system, system will immediately block the credit card as soon as it detects and finds it unusual.
- The Existing system checks for the country, while the proposed system has limited that to the state making it much more secure.
- In existing system, the pattern is not considered, but new systems have come which has implemented the pattern system but has chose to take an average and take 50% of it, which is too high. The hackers or intruders are smart, so the proposed system has taken it down by 20%.
- In the Existing System it is the same pin or 3D Secure Code, which is very easy for an intruder to get it, while Secure Code is rarely used only in the case of some unusual encounters, less possibility to be known by anyone else.

VI. CONCLUSION

Through this paper, we are just giving an ideology of Behaviour and Location Analysis (BLA) which uses different sources to indentify the user. There are many such similar Systems already at function. The main advantage here is it stores the different patterns and the pattern is made by the user itself and not by the system. And drastic reduction in the number of False Positive Transactions identified as malicious by a Fraud Detection System although they are actually genuine.

REFERENCES

[1]. http://www.consumer-action.org/downloads/english/Chase_CC_Fraud_Leaders.pdf
[2]. https://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2008/sentinel-cy2008.pdf
[3]. V. Bhusari , S. Patil, "Application of Hidden Markov Model in Credit Card Fraud Detection", Department of Computer Science, Department of Computer Technology, College of Engineering, Bharati Vidyapeeth, Pune, India, 400011, Nov.2011
[4]. https://www.gifttool.com/support/Page?BID=10&AID=279