Decision making scheme using Prisoner's dilemma: Fraud detection in financial transaction

Olofinlade, Victor Funmipe
School of Computing,
Federal University of Technology,
Akure, Nigeria
olofinladevf@futa.edu.ng

Adetunmbi, Adebayo Olusola[4]
Department of Computer Science
Federal University of Technology,
Akure, Nigeria
aoadetunmbi@futa.edu.ng

Alese, Boniface Kayode[2]
Department of Cyber Security
Federal University of Technology,
Akure, Nigeria
bkalese@futa.edu.ng

Thompson, Aderonke Favour-Bethy
Department of Cyber Security
Federal University of Technology,
Akure, Nigeria
afthompson@futa.edu.ng

***Abstract*— Financial institution are facing thoughtful challenges with loud rising number of credit card fraud occurrences across the globe. Although fraud has been a leading problem since the beginning of time, its operations in this present-day consent with various classes of people due to the availability of internet. Consequently, the matter of security is primary motivation as people begin to select their credit cards. Due to this fact, banks and credit card companies are looking into updating their systems to include more advanced mechanisms that can both detect and prevent fraud. By using current machine learning innovative idea that is shrewd to identify patterns and connections between transactions, activities, and fraud occurrences, financial institutions can find a smarter and more effective ways to detect and prevent fraudulent transactions. With this benefit, banks and financial institutions can automate the analysis of their customers' behavioral patterns for any signs of abnormality, giving them the ability to identify and flag fraudulent activity in real-time. Hence, the theory of rational choice becomes imperative in financial transaction decision making.**

Game theory represents a theoretical framework for conceiving social situations among competing players. It can also be described as science of strategy which make use of optimal decision-making scheme in independent and competing actors in a strategic setting. This classic Prisoner's Dilemma is a situation where the prisoners were to make individual simultaneous choices that cannot be undo. The independence of their choices was also ensured by putting the prisoners in separate cells, there by excluding any possibility for communication relevant to the choices that they were going to make. In doing so an uncommon situation is being set up in such a way that make people interact in manners that permit them to respond to each other's behavior or communicate about their choices.

Prisoner's dilemma is a modern game theory concepts used to represent a paradoxical decision analysis in which two individual acting in their own self-interest so not eventual produce the optimal outcome. A typical prisoner's dilemma describes a set up in which both parties individually choose to prioritize their own protection at the expense of the other participant. This simply describe the need for each partaker to defend their life from the havoc of the situation at hand, and it solemnly depends on the choice of decision by the individual player

Keywords-fraud, prisoner's dilemma, Game-theory; financial transaction

1. Introduction

With the extensive technology innovation and telecommunications, we have seen new financial distribution channels increasing rapidly both in numbers and form, from ATMs, telephone banking to PC banking and Internet Banking is the latest in the series of technological wonders of the recent past.

Cashless transactions such as online transactions, credit card transactions, and mobile wallet are becoming more popular in financial transactions nowadays. With increased number of such cashless transaction, number of fraudulent transactions are also increasing.

Fraud though being in existence even before the advent of technology, has taken unlimited variety of forms. The development of new technologies provides additional enhanced ways in which criminals may commit fraud. The use of credit cards is prevalent in modern day society and credit card fraud has kept on growing in recent years. Financial losses due to fraud affect not only merchants and banks (e.g. reimbursements), but also individual clients. Novell payment Methods and solutions has significantly increased the use of credit and debit cards. With the

enhancement in e-banking technology like credit Card, Debit Card, Mobile Banking, Internet Banking is the popular medium to transfer the money from one account to another and popularity increasing daily as well. Innovation, ease of payment and quest for increase in transaction volumes have seen products in form of various categories such as in online shopping, online bill payment like electricity, Insurance Premium and other charges, online recharges, and online hotel reservations [1].

With this surge in adoption and usage of payment system, there has been a rise in the incidence of fraud in Nigerian payments landscape of nearly 44 trillion naira in payments made across Nigeria in 2014, over 7billion naira was reported as the value of "attempted" fraud and 6.22 billion Naira was the actual loss value reported. the Nigeria Interbank Settlement System PLC (NIBSS) report also shows that the same year, ATM fraud was most attempted in 491 incidents and internet banking recoded the highest fraud value of 3.2 billion naira [2]. It is important to note that this statistic is not as a result of locale rather, the security of card payments and the trust of the general public in making card payments is a matter of concern for any bank in the world. Fraud with cards issued within SEPA stood at 1.3 billion of euros in 2012, *i.e.*, 0.038% of the value of card transactions [3].

The lack of face-to-face or voice interaction on the Internet makes fraudsters more daring by providing them with anonymity, which makes the detection and prevention of online frauds more difficult. Lists of stolen credit card numbers are also being posted on the Internet or sold in newsgroups and can be used by a variety of individuals to purchase goods online without the authorization of the credit card's owner [4].

Stolen credit cards are made available over the internet and to a larger group which uses the information to obtain goods and services in the name of the cardholder. Purchases through catalogues and mail orders are then often made using the victim's card number. They may select an unoccupied address to which their merchandise can be delivered, perhaps leaving a note asking the delivery service to simply put the package by the back door [5].

The actions however taken against fraud can be divided into fraud prevention, which attempts to block fraudulent transactions at source, and fraud detection, where successful fraud transactions are identified beforehand. Technologies that have been used in order to prevent fraud are Address Verification Systems (AVS), Card Verification Method (CVM) and Personal Identification Number (PIN). AVS involves verification of the address with zip code of the customer while CVM and PIN involve checking of the numeric code that is keyed in by the customer. For prevention purposes, financial institutions challenge all transactions with rule based filters and data mining methods. Any of these methods is applied to find out normal usage pattern of customers (users) based on their past activities.

Fraud detection technique such as expert driven approach uses the domain knowledge from fraud investigators or financial veterans to define a set of rules that are used to predict the probability of a new transaction to be fraudulent. While there are some notable advantages of expert driven rules such as: i) they are easy to develop and to understand, ii) they explain why an alert was generated and iii) they exploit domain expert knowledge. However, they have a number of drawbacks: i) they are subjective (if you ask 7 experts you may get 7 different opinions), ii) they detect only easy correlations between variables and frauds (it is hard for a human analyst to think in more the three dimension and explore all possible pattern combinations), iii) they are able to detect only known fraudulent strategies, iv) they require human monitoring/supervision (update in case of performance drop) and v) they can become obsolete soon due to fraud evolution [6].

However, fraudsters constantly change their strategies to avoid being detected, making traditional fraud detection tools –such as expert rules or machine learning static models– inadequate. Also, the change in fraudulent behaviour, disperse in distinct user profiles, and the spread across huge imbalanced real-world datasets (e.g., customer spending profiles, web logs, transaction logs) have made frauds often hard to detect and analyse. In this regard, one of the main challenges is to counteract the increasing fraud for “card-not-present” payments, especially in e-commerce activities [7].

While basic fraud prevention techniques have been more utilized in reducing card losses, financial institutions such as banks require more sophisticated techniques for detecting and preventing fraud.

Currently, Financial institution are facing thoughtful challenges with loud rising number of credit card fraud occurrences across the globe. Although fraud has been a leading problem since the beginning of time, its operations in this present-day consent with various classes of people due to the availability of internet. Consequently, the matter of security is primary motivation as people begin to select their credit cards. Due to this fact, banks and credit card companies are looking into updating their systems to include more advanced mechanisms that can both detect and prevent fraud. By using current machine learning innovative idea that is shrewd to identify patterns and connections between transactions, activities, and fraud occurrences, financial institutions can find a smarter and more effective ways to detect and prevent fraudulent transactions. With this benefit, banks and financial institutions are able to automate the analysis of their customers’ behavioural patterns for any signs of abnormality, giving them the ability to identify and flag fraudulent activity in real-time. Hence, the theory of rational choice becomes imperative in financial transaction decision making.

2. What is Game Theory?

Game theory represents a theoretical framework for conceiving social situations among competing players. It can also be described as science of strategy which make use of optimal decision-making scheme in independent and competing actors in a strategic setting. This classic Prisoner's Dilemma is a situation where the prisoners were to make individual simultaneous choices that cannot be undo. The independence of their choices was also ensured by putting the prisoners in separate cells, there by excluding any possibility for communication relevant to the choices that they were going to make. In doing so an uncommon situation is being set up in such a way that make people interact in manners that permit them to respond to each other's behaviour or communicate about their choices.

2.1. Prisoner's dilemma

Prisoners' dilemma game (PD) is primarily of two player problems with different choices. And the profit function of the game is given and fixed during the game. However, most of the problems is not in such simple scene but multiplayer deviations. Therefore, multiplayer formats afford the opportunity for a useful expansion of the prisoners' dilemma game.

2.2. Optional Prisoner's Dilemma (OPD)

The Optional Prisoner's Dilemma (OPD) game models a situation of conflict involving two players in game theory. It can be seen as an extension of the standard prisoner's dilemma game, where players have the option to "reject the deal", that is, to abstain from playing the game. The structure of the Optional Prisoner's Dilemma can be generalized from the standard prisoner's dilemma game setting. In this way, suppose that the each of the two players chooses to "Cooperate", "Defect" or "Abstain" [8]

Although the following condition must hold for the payoffs:
$T > R > L > P > S$

Canonical OPD payoff matrix			
	Cooperate	Defect	Abstain
Cooperate	R, R	S, T	L, L
Defect	T, S	P, P	L, L
Abstain	L, L	L, L	L, L

3. Motivation

A variety of secure payment systems have been proposed to thwart credit card fraud such as Address Verification Service (AVS), Card Verification Value. More sophisticated online financial fraud detection and prevention research and techniques have been proposed to overcome the flaws of the AVS technique. These have heavily relied on analysis of recorded transactions composed of different number of attributes (e.g., credit card identifier, transaction date, recipient, amount of the transaction).
Sequentially rule based or expert driven approach uses domain knowledge from fraud investigators to define rules that are used to predict the probability of a new transaction to be fraudulent. Typically, expert rules can be distinguished between scoring rules and blocking rules. The former assigns a score to a transaction based on the risk the investigators associate to a certain pattern; the latter can block the transaction because the risk of fraud is too high.

As highlighted, the advantages of expert rules are:
i) they are easy to develop and to understand
ii) they explain why an alert was generated and iii) they exploit domain expert knowledge.
However, they have a number of drawbacks:
i) they are subjective (if you ask 7 experts you may get 7 different opinions),
ii) they detect only easy correlations between variables and frauds (it is hard for a human analyst to think in more the three dimension and explore all possible pattern combinations)
iii) they are able to detect only known fraudulent strategies
iv) they require human monitoring/supervision (update in case of performance drop) and
v) they can become obsolete soon due to fraud evolution.

These approaches would largely be static in nature and fail in a scenario in which an attacker learns the methodology or strategy of the rules over a period of time in order to outdo it. Once aware of the strategy, the attacker can act to maximize his payoff. Conversely, the goal of the detection system is to be able to learn the moves of the attacker dynamically so as to minimize its own loss
Traditional security mechanisms are often found to be inadequate for protection against attacks by authorized users or intruders posing as authorized users. This has drawn interest of the research community towards intrusion detection techniques.
Many techniques have been designed to find ways to overcome credit card. As far as developing countries are concerned less work has been done to overcome this problem. Losses related with credit cards are quickly rising each year.
Still no technique can provide solution for all types of fraud.
This research model proposes a framework for "card not present" fraud. This fraud occurs mostly on internet or on phone when the user does not physically present his card to the merchant. "Card not present" fraud is much difficult to detect as compared to "card present" fraud

4. Methodology: Fraud detection using prisoner's dilemma

4.1. STEP 1: Profiling

Profiling is very important in fraud detection. This helps to determine the level of transaction fraudulence through the use of pattern matching based off of but not limited to the following metadata listed below

1 Full name
2 Location
3 Geolocation
4 Valid phone number
5 Credit card information
6 Commodity
7 Transaction amount frequency
8 Last amount spent
9 Location of last amount spent
10 Time of last transaction

4.2. STEP 2 Validation

Validations are done to be able to determine which metadata fails and which metadata passed such as

1 User must register with his full legitimate name. No nick names allowed
2 User IP and geo-location must be checked and stored at registration. No anonymous Ip or Ip behind proxy is allowed
3 User credit card financial institution must be in the same geo-location with the user
4 User must register with the phone number registered with the credit card financial institution
5 Credit card must be checked with previously linked accounts. No card must be linked twice
6 The BIN number and issuing bank must match. Fraudsters usually only have partial credit Card information except the issuing bank information.
7 User must not use a disposable e-mail domain and address
8 The username and password must not be too simple and generic
9 The credit card must not be a blacklisted credit card

4.3. STEP 3 Expert Rules

Following the validation, rules such as below are applied do determine the criticality of a transaction in terms of scale

1 Initial transaction for new consumers cannot exceed x value naira
2 No purchase/transaction can be made in two different geographical locations within 12 hrs.
3 Account that is registered in on geographical location and use in another geographical location should be flagged
4 IP and the billing address must be the same
5 IP address and the credit card address must match up

Algorithm
The following algorithm shows how t
For each user transaction get metadata [name, credit card, location, commodity, etc], store in the **METADATA DATABASE**

If user transaction < 10
Then check **FRAUD RULES**
If user transaction is legit
Then continue transaction
Else
Refuse transaction
Else if Transaction is greater than 10
Then check **DECISION TREE**
If user metadata is in **DECISION TREE**
Then continue transaction
Else
Check **EXCEPTION DATABASE**
If user metadata is in **EXCEPTION DATABASE**
Then Call client for confirmation
Continue Transaction
Else
Then flag transaction, check the **METADATA DATABASE**,
call client for suspicious transaction
If client confirm
Then add metadata to exception database
Else
Fraudulent Transaction, refuse

4.4. STEP 4 Pattern Matching

Supportive behavioral analysis of the spender in a real-world situation which cannot be quantified statistically is also critical in the decision of the fraudulence of transactions in the financial institutions. Such as below:

1. **Location**: Live in one place but make a purchase in another
2. **What you buy**: If your card is commonly used to buy your morning cup of coffee and then a tank of gas, and out of the blue is used to buy a pair of expensive designer shoes
3. **Spending amount**: If you typically spend N500 / month, and suddenly rack up N3000 in a week
4. **Spending frequency**: If your card is used to make a large number of purchases over a short period of time
5. **Large purchase after a smaller one**: Thieves typically test stolen credit cards with smaller purchases first, such as a song from iTunes; if the

card works, they will proceed to make another larger purchase, like an expensive camera, or television, or sound system

6. **Digital origins**: Ecommerce makes it easy for us to make purchases, but it also makes it easy for thieves to commit fraud; the digital origins of purchases are

4.5. STEP 5 Decision Making

1 We Define the following on a sample transaction T
FT: Fraudulent Traits
NFT: Non-Fraudulent Traits

2 2We set a threshold scale of 10 based on aggregated values of on Profiling, Validation, Rules and Pattern matching techniques

Set FT_SCALE = [1,10]
Set NFT_SCALE = [1,10]

3 We populate the payoff table within the scale of threshold scale following this condition T > R > L > P > S
We set R = P
Thus, condition becomes T > L > P = R > S

Legitimate Card Owner				
Fraud		Fraudulent	Not Fraudulent	Not Sure
	Fraudulent	1,1	1,7	3,3
	Not Fraudulent	7,1	1,1	3,3
	Not Sure	3,3	3,3	3,3

4 We Set Threshold for FT and NFT
Set Threshold for FT
Set Threshold for NFT

5 We calculate the Prisoner's confidence for both FT and NFT as:
PD Confidence_FT = (max (FT_SCALE) - Threshold for FT)/2
Set PD Confidence_ NFT = (max (NFT _SCALE) - Threshold for NFT)/2

6 We Check a Sample Transaction trait below with respect to their inverses
Sample Transaction ST [New_Val_NFT, New_Val_FT]
Highly Not Fraudulent = IF New_Val_NFT > Threshold for NFT || New_Val_NFT - Threshold for NFT > PD_Confidence_ NFT

Highly Fraudulent = IF New_Val_FT > Threshold for FT || New_Val_FT - Threshold for FT > PD_Confidence_ FT

Fraudulent / Non-fraudulent but not sure

IF New_Val_NFT > Threshold for NFT || New_Val_NFT - Threshold for NFT > PD_Confidence_ NFT

IF New_Val_FT > Threshold for FT || New_Val_FT - Threshold for FT > PD_Confidence_ FT

7 we apply prisoners Dilemna and we make our choices

5. Conclusion

The prisoner's dilemma (PD) game can be used as a model for many real-world situations involving supportive behavior. The states in which decisions must be made independent of other parties is a critical experience in financial institutions. Such as The following describes a typical game theory condition in cashless transactions. Analysis would be made to validate the effectiveness of the OPD on Financial transactions

6. References

[1.] Fraud Detection by Monitoring Customer Behavior and Activities. Parvinder Singh Assistant Professor MMICT and BM MM University, Mullana, Ambala, India 1.R. Kumars & Pranit-Lal A. (2016) Detecting denial of service attacks in the cloud, in: IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, pp. 309– 316.

[2.] A change in payment ecosystem interbank report

[3.] European Central Bank, Annual report (2015).520 European Central Bank, Card payments in europe – a renewed focus on sepa for cards (2014).

[4.] Krishna Modi & Reshma Dayma Review on fraud detection methods in credit card transactions (2017) Computer Department, L D College of Engineering, Ahmedabad, Gujarat, India

[5.] Andrea Dal Pozzolo Adaptive Machine Learning for Credit Card Fraud Detection Université Libre de Bruxelles, Computer Science Department Machine Learning Group

[6.] Jon Ander Gómez, Juan Arévalo, Roberto Paredes, Jordi Ninb, End-to-end neural network architecture for fraud scoring in card payments, Pattern Recognition Letters 105 (2018) 175–181

[7.] Ghosh, S., & Reilly, D. L. (1994). Credit card fraud detection with a neural network. Proceedings of the 27 Annual Hawaii International Conference on System Sciences, (pp. 621-630).

[8.] Wikipedia Contributors. "Optional Prisoner's Dilemma." Wikipedia, Wikimedia Foundation, 25 Nov. 2021, en.wikipedia.org/wiki/Optional_prisoner%27s_dilemma.