IOP Conf. Series: Materials Science and Engineering **263** (2017) 042045 doi:10.1088/1757-899X/263/4/042045

Fraud prevention in paying portal

Sandhu P S and Senthilkumar N C

School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: ncsenthilkumar@vit.ac.in

Abstract The purpose of presenting this paper is to give the idea to prevent the fraud in finance paying portals as fraud is increasing on daily basis and mostly in financial sector. So through this paper we are trying to prevent the fraud. This paper will give you the working algorithm through which you can able to prevent the fraud. Algorithm will work according to the spending amount of the user, which means that use will get categories into one of the low, medium, high or very high category.

1. Introduction

The Association of Certified Fraud Examiners (ACFE) characterized extortion as "the utilization of one's occupation for individual advancement through the consider abuse or use of the utilizing association's assets or resources" [1]. Cheat exercises are ominously influencing organizations. As an impact of which it has turn out be a stuff of huge touchy and required to be investigated. The varying techniques which are by and by being worned for cheat discovery are Statistics, Data Mining, Neural Network and Artificial Intelligence. Issues in the improvement of new techniques for misrepresentation discovery: Limitation of trade of thoughts, inaccessibility of informational indexes and concealed aftereffects of investigation. Cheat is uncovered by sieving the peculiarities in information and examples. Utilizing bookkeeping, reviewing and investigative abilities alongside scientific, measurable and information mining models find fakes.

Resource misappropriation, kickbacks and so forth are incorporated into Internal Financial Fraud. Outside Financial Fraud incorporates distortion of organization's budgetary position to partners. According to the writing distributed so far one might say that the majority of research is done on recognition of External Financial Fraud. Sadly next to no work is done on interior budgetary extortion. Strategies like Artificial Neural Network, Genetic Algorithm, Rough and Fuzzy set, Rule Discovery, Cluster Analysis and calculated relapse are audited for finding fakes. Learning Driven Internal Fraud Detection (KDIFD) system is proposed for finding inside budgetary extortion in paper [3]. This system helps the reviewers in at long last affirming whether plausibility of extortion is or not.

Money related extortion discovery (FFD) is essential for the counteractive action of the regularly wrecking outcomes of budgetary misrepresentation. FFD includes recognizing deceitful monetary information from misleading information, in this manner uncovering false conduct or exercises and empowering leaders to create proper systems to diminish the effect of misrepresentation.

When all is said in done, the target of extortion identification is to amplify amend expectations and keep up mistaken forecasts at a worthy level[3]. A high right demonstrative likelihood can be inferred by limiting likelihood of undetected misrepresentation and false alerts. Some specialized terms are depicted as takes after. False alert rate (or false positive rate) is the rate of honest to goodness exchanges that are inaccurately recognized as fake. Misrepresentation getting rate (or genuine positive rate or discovery precision rate) is the rate of deceitful exchanges that are effectively recognized as false.

The method for individuals purchasing the assortment of things, utilizing charge card changed the example of buying the items. Already, if the client needs to buy something, he needs to convey the cash to every one of the spots. Card banking gives all the data identified with the Visas and extra elements of their charge cards, which makes the client or client astutely, to choose which Visa must be chosen.

Rest of the section are arranged as follows:

1. This section will give you the brief research done before actual implementation of this project I.e literature survey.

2. This section will describe the algorithm, in which you will understand the working principle behind this algorithm.

3. This section will describe the modules of the project.

4. This section will throw light on the future work of this project and highlight the conclusion for this as well as upcoming projects.

2. Literature review

During our survey, we have analyze that fraud cases in financial sector is evolving bigger and broader every day. Now days companies are spending more amount of money on detecting and preventing frauds rather than spending on infrastructure and on the quality of their product. They are more worried about the security of the data and their reputation in the market.

Fraud detection using data mining techniques by shivakumar swamy N [1] in 2014 gives a way to detect fraud using supervised, unsupervised, hybrid and semi supervised approaches. After creating fraud detection model, they establish data model with ID3 decision tree claims the fraud detection model.

A survey on financial fraud detection methodologies by pankaj richariya [2] in 2012 gives the detail view of financial fraud techniques used by the companies to detect and prevent the fraud. They have concluded in their survey that in house fraud activities are also paying major role in increasing fraud.

Credit card fraud detection by suman published in IJCTT [3] in 2013 stated that all the different techniques used by the agencies or criminals to make the fraud activities true are describe very deeply in the paper so that you can get a lot more to know about the technologies and how they’re using it.

An effective fraud detection system using data mining techniques by syed ahsan shabbir [4] published in May 2013 in international journal of scientific research and publications stated the role of admin in the transaction, which will monitor all the records of the user and verify the card details of the user every time they are going to make the transaction from the card. They have implemented this whole program for a website, so that they can prevent fraud on their website.

A review of fraud detection technique by khyati choudhary, jyoti yadav and bhawna mallick [5] in 2012 published in international journal of computer applications stated that various types of techniques are used by the fraudster for fraud activities such as neural networks, machine learning, pattern matching etc in this paper they have shown the fraud combine coverage to minimize activities and high or low alarm rates.

3. Algorithm

This is the section where you will learn about the idea which we have come up with and how it works. Algorithm is as follows:-

a. user will enter into paying portal

b. If user is already a member, then only sign in is required

c. If user is not a registered user, then he needs to register himself in to the new user column

d. After registering, he can log in now to pay the price for whatever they are registered.

Now, actual algorithm start from this area

a. Whenever any user log in to the portal, algorithm will generate patterns from the user history.

b. After generating the patterns and analysis of the data, users will fall under one of the following category:-

-- LOW

-- MEDIUM

-- HIGH

-- VERY HIGH

c. This categories are demonstrated using 2 factors:

-- spending limit

-- time frequency

d. According to the category of the user, he is allowed to do the respective transactions.

e. If anyhow user tries to change its category means for example low category user is doing high category transaction, maybe he is the authentic user only but there is a chance of fraud also. So, users have to follow 3-tier high security process to process and complete the transaction.

So this is how our algorithm will work and hopefully we could able to restrict some of the fraud activities.

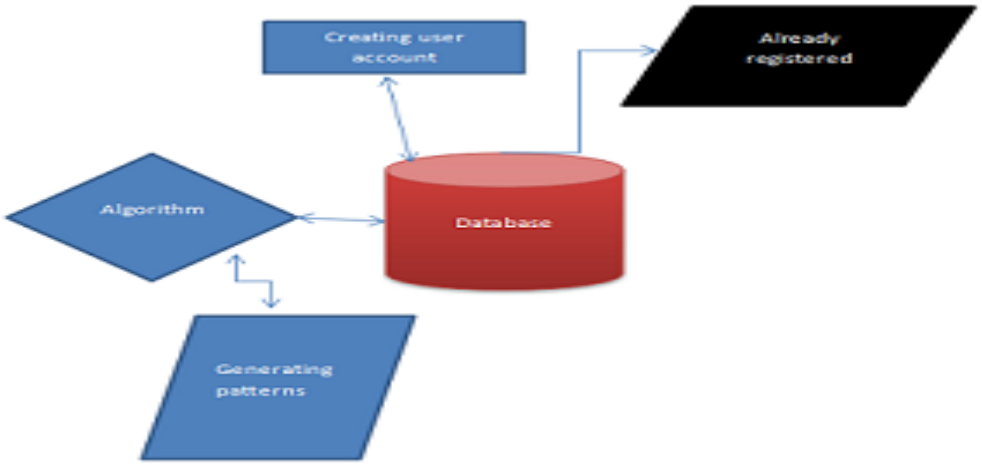

Fig 1. Flow Diagram

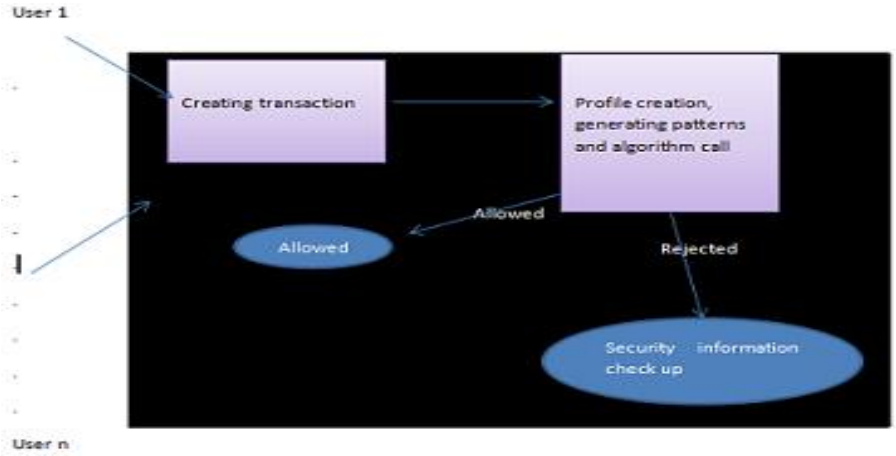

Fig 2 Transaction Diagram

4. Modules:

4.1 User Account

User account is the most important module of this whole system as this is the system which will work on the user's data and history of the user, which we can generate only from user records. This module will keep track on the user records I.e spending amount, contacts, name, user-id and passwords.

4.2 Profile creation

This is the module in which user have to create its profile and have to fill all the necessary details of the account for future reference and for eliminating any type of fraud activities

a. Name

b. User name

c. Password

d. mobile number

e. Alternate mobile number

f. e-mail

4.3 Card details

This is the module which will be activated only after user logged into the system and user is willing to pay or transact the amount. This module will ask for details of the card with which user is going to pay the amount.

4.4 Classifying user

This is the module in which user gets classified into one the 3 predefined categories:

High

Medium

low

These classification will be done on 2 factors:

Spending limit

Time Frequency

According to these 2 factors user gets classified and algorithm will work according to user's class. If any unusual behavior is identified then algorithm will run its security check up task.

4.5 Generating patterns

Now, classification is done. So pattern generation will take place.

Patterns will be generated by the server or machine according to the user's data and in which category he falls.

4.6 Security checkup

This is the routine which takes place, when user is willing to do any transaction and he has to follow normally OTP method to complete the transaction.

4.7 High security check up

This is module which gets activated when there is any detection of fraud. Fraud in this algorithm is defined as whenever user is changing its category allotted by the algorithm. In this module user has to undergo 3-tier security check up for making their transaction successful or else they can contact the branch.

Mobile OTP

MAIL-ID OTP

ALTERNATE NUMBER OTP

When user is able to complete these security check ups, then he will be able to complete his payments.

5. Conclusion and Future work

During the preparation of this project, we concluded that we can prevent fraud activities and even we can restrict them to most extent, fraud activities are at pace rate and they can reach billions of dollars by the end of 2020. According to the survey of 2015 they concluded that 15% of the mortgage cases involves fraud and 10% bank sector transactions using debit cards and credit cards or net banking involves fraud. So this is very important for us to control these types of activities and secure our data as well as organization's data. We have been doing research on improving this algorithm and we will try to come up with whole new algorithm taking base from this algorithm only, so that we could able to do something more to protect our data and prevent fraud activities. We try to publish as soon as possible regarding our next research on fraud prevention.

Fraud activities are the major threat to bank reputation also, if the authentic user is not doing any transaction and he is still losing his money, sooner or later he will contact bank branch only. Then they have to be answerable to the authentic user. Bank unable do anything at that moment because transaction is already done.

References

[1] Swamy S N and Lingareddy S C 2014 Fraud detection using data mining techniques *International Journal of Innovations in Engineering and Technology* **4**(1) 2319 - 1058
[2] Richariya P and Singh P K 2012 A survey on financial fraud detection methodologies *International Journal of Computer Applications* **45**(22) 15-22
[3] Suman and Nutan 2013 Credit card fraud detection *International Journal of Computer Trends and Technology* **4**(7) 2207-2215
[4] Shabbir S A and Kannadasan R 2013 An effective fraud detection system using data mining technique *International Journal of Scientific and Research Publications* **3**(5) 2250 - 3153
[5] Chaudhary K, Yadav J and Malick B 2012 A review of fraud detection techniques: credit card *International Journal of Computer Applications* **45**(1) 39-44