Transaction Fraud Detection using Invisible Keyboard and Questions Queries

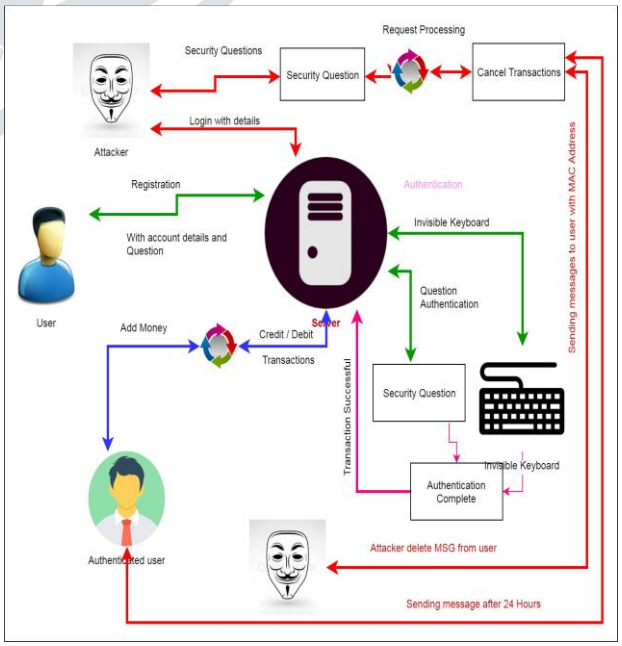
Ashvini Jive, Sonali Gade, Shivkashi karamunge, Rupam Kumar, Prof. Nilesh Madke
Department of computer engineering,
Genba sopanrao moze college of engineering balewadi,

Abstract: With the popularization of online shopping, transaction fraud is growing seriously. Therefore, the study on fraud detection is interesting and sign cant. An important way of detecting fraud is to extract the behavior roles (BPs) of users based on their historical transaction records, and then to verify if an incoming transaction is a fraud or not in view of their BPs and verify the Security question details and Invisible Keyboard. Markov chain models are popular to represent BPs of users, which is effective for those users whose transaction behaviors are stable relatively. However, with the development and popularization of online shopping, it is more convenient for users to con some via the Internet, which diverse the transaction behaviors of users. Therefore, Markov chain models are unsuitable for the representation of these behaviors. In this paper, we propose Security Questions BP which is a total order-based model to represent the logical relation of attributes of transaction records. Based on Security Questions and users transaction records, we can compute a path-based transition probability from an attribute to another one. At the same time, we dine an information entropy-based diversity coefficient in order to characterize the diversity of transaction behaviors of a user. In addition, we dine a state transition probability matrix to capture temporal features of transactions of a user. Consequently, we can construct a BP for each user and then use it to verify if an incoming transaction is a fraud or not. Our experiments over a real data set illustrate that our method is better than three state-of-the-art ones.

Keywords: Behavior profile (BP), e-commerce security, fraud detection, online transaction

Introduction: The volume of the electronic transaction has raised significantly in recent years due to the popularization of online shopping (e.g., Amazon, eBay, and Alibaba). The global e-commerce market is predicted that it will be worth a staggering US$ 24 trillion by 2019. Credit cards are widely used in online shopping, and card-not-present transactions in credit card operations becomes more and more popular since web payment gateways (e.g., PayPal and AliPay) become popular. However, there has been a simultaneous growth of transaction fraud which results in a dramatic impact on users. A survey of over 160 companies reveals that the number of online frauds is 12 times higher than that of the online frauds, and the losses can increase yearly at double-digit rates by 2020. A physical card is not required in the scenario of online shopping and only the information of the card is enough for a transaction. Therefore, it is much easier for a fraudster to make a fraud. There are many ways by which fraudsters can illegally obtain the card information of a user: phishing (cloned websites), pseudo base station, Trojan virus, collision attack, malicious insider, and so on. Therefore, it is very interesting and significant to study the methods of fraud detection.

Architecture Diagram:



Literature Survey

1. Paper name: Discovering process models from event logs

Author: W. van der Aalst, T. Weijters, and L. Maruster,

Description: Contemporary progress management systems ar driven by express method models, i.e., a totally nominative progress design is needed so as to enact a given progress method. Making a progress style could be a difficult long method and, typically, there ar discrepancies between the particular progress processes and therefore the processes as perceived by the management. Therefore, we've got developed techniques for locating progress models. The start line for such techniques could be alleged "workflow log" containing info regarding the progress method because it is truly being dead. we tend to gift a brand new algorithmic rule to extract a method model from such a log and represent it in terms of a Petri internet. However, we'll additionally demonstrate that it's not possible to get discretionary progress processes. During this paper, we tend to explore a category of progress processes which will be discovered. We show that the -algorithm will with success mine any progress diagrammatic by a alleged SWF-net.

2. Paper name: Survey of fraud detection techniques

Author: Yo-Ping Huang

Description Due to the dramatic increase of fraud which ends in loss of billions of greenbacks worldwide every year; many trendy techniques in sleuthing fraud are frequently evolved and applied to several business fields. Fraud detection involves monitoring the behavior of populations of users in order to estimate, detect, or avoid undesirable behavior: Undesirable behavior could be a broad term as well as delinquency): fraud, intrusion, and account defaulting. This paper presents a survey of cement techniques utilized in credit card fraud detection, telecommunication 9aud detection, and pc intrusion detection. The goal of this paper is to produce a comprehensive review of different techniques to notice frauds

3. Paper name: Phishing detection based Associative Classification data mining

Author: Neda Abdelhamid , Aladdin Ayesh, Fadi Thabtah

Description Website phishing is taken into account one among the crucial security challenges for the net community because of the massive numbers of on-line transactions performed on a each day. web site phishing may be delineate as mimicking a trusty web site to get sensitive info from on-line users like usernames and passwords. Black lists, white lists and therefore the activity of search strategies area unit samples of solutions to minimize the risk of this downside. One intelligent approach supported data processing referred to as Associative Classification (AC) appears a possible resolution which will effectively notice phishing websites with high accuracy. According to experimental studies, AC usually extracts classifiers containing straightforward ''If-Then'' rules with a high degree of prognostic accuracy. During this paper, we tend to investigate the matter of web site phishing employing a developed AC methodology referred to as Multi-label Classifier primarily based Associative Classification (MCAC) to hunt its applicability to the phishing downside. we tend to additionally wish to spot options that distinguish phishing websites from legitimate ones. Additionally, we tend to survey intelligent approaches accustomed handle the phishing problem. Experimental results victimization real knowledge collected from totally different sources show that AC significantly MCAC detects phishing websites with higher accuracy than alternative intelligent algorithms. Further, MCAC generates new hidden information (rules) that alternative algorithms area unit unable to seek out and this has improved its classifiers prognostic performance..

4. Paper name Earnings Management: A Perspective

Author: By Messod D. Beneish

Description The paper provides a perspective on earnings management. I begin by addressing the following questions: what's earnings management? however pervasive is it? However

is it measured? Then, I discuss what we have a tendency to, as teachers, comprehend incentives to extend and to decrease earnings. The analysis bestowed relates to earnings management incentives streaming from regulation, debt and compensation contracts, trading and security issuances. I additionally discuss problems concerning issues in measurement the extent of earnings management and propose extensions for future work.

5. Paper name: Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data

Author: Amos Azaria, Ariella Richardson, Sarit Kraus, and V.S. Subrahmanian

Description Insider threat refers to the threat display to organizations by people UN agency have legitimate rights to access the interior system of a company. In a detailed study [1] of twenty three business executive threat incidents in the banking and finance sector between 1996 and 2002 that was applied put together by the North American country Secret Service and sure thing (at Carnegie-Mellon University), the authors found that business executive threat events enclosed fraud, thievery of material possession and tries to sabotage the organization's network. An equivalent organizations conducted an analogous study that specialize in 36 incidents within the government sector throughout the same timeframe that concerned document fraud, monetary fraud (embezzlement), fraud employing a laptop, theft of counsel and/or sabotage, and more. CERT's business executive threat page, http://www.cert. org/insider threat/, presents a wonderful outline and several reports description numerous styles of business executive threat. In an exceedingly similar vein, [2], quoting a North American country Justice Department survey, states that seventy four of all cyber-theft.

Mathematical Model :

System S as a whole can be defined with the following main components.

S= I, Ad, T, A, O

S=System

T=Transaction

Ad=admin

A= Account

Where,

Input1=Account details

Where,

Transaction= Transactions

Output O = Output1, Output2

Where,

O= Total Count

Conclusion

In this paper, we propose a method to extract users BPs based on their transaction records, which is used to detect transaction fraud in the online shopping scenario by using the Security Questions. Overcomes the shortcoming of Markov chain models since it characterizes the diversity of user behaviors. Experiments also illustrate the advantage of OM. The future work focuses on some machine-learning methods to automatically classify the values of transaction attributes so that our model can characterize the users personalized behavior more precisely. In addition, we plan to extend BP by considering other data such as users comments

Reference

1. W. van der Aalst, T. Weijters, and L. Maruster, Workow mining: "Discovering process models from event logs", IEEE Trans. Knowl. Data Eng., vol. 16, no. 9, pp. 11281142, Sep. 2004.
2. A. Abdallah, M. A. Maarof, and A. Zainal, Fraud detection system: A survey, J. Netw. Comput. Appl., vol. 68, pp. 90113, Jun. 2016.
3. N. Abdelhamid, A. Ayesh, and F. Thabtah, Phishing detection based associative classi_cation data mining, Expert Syst. Appl., vol. 41, no. 13, pp. 59485959, 2014.
4. N. M. Adams, D. J. Hand, G. Montana, D. J. Weston, and C. W. Whitrow, Fraud detection in consumer credit, Autumn, vol. 9, no. 1, pp. 2129, 2006.

5. C. Arun, Fraud: 2016 its business impact, Assoc. Certified Fraud Examiners, Austin, TX, USA, Tech. Rep., Nov. 2016.
6. A. Azaria, A. Richardson, S. Kraus, and V. S. Subramanian, Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data, IEEE Trans. Compute. Social Syst., vol. 1, no. 2, pp. 135155, Jun. 2014.