Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity

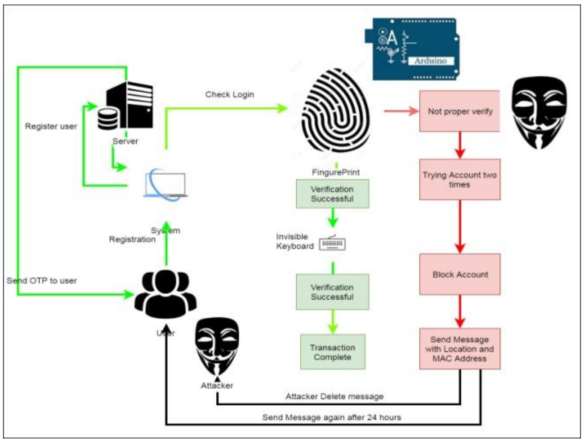
Tushar Mahamuni, Nihal Londhe, Tejashri Magade, Prof. Pallavi Mathur
Institute Of Engineering And Technology, Ambi

Abstract: With the popularization of on-line searching, dealings fraud is growing seriously. Therefore, the study on fraud detection is fascinating and important. a very important approach of police investigation fraud is to extract the behavior profiles (BPs) of users supported their historical dealings records, then to verify if AN incoming dealings may be a fraud or not see able of their BPs. Mark off chain models area unit in style to represent bits per second of users, that is effective for those users whose dealings behaviors area unit stable comparatively. However, with the event and popularization of on-line searching, it's additional convenient for users to consume via the net, that diversifies the transaction behaviors of users. Therefore, Mark off chain models are unsuitable for the illustration of those behaviors. In this paper, we have a tendency to propose logical graph of BP (LGBP) that may be a total order-based model to represent the relation of attributes of dealings records. supported LGBP and users' dealings records, we will work out a path-based transition chance from AN attribute to a different one. At constant time, we define an data entropy-based diversity constant so as to characterize the range of dealings behaviors of a user. In addition, we have a tendency to outline a state transition chance matrix to capture temporal options of transactions of a user. Consequently, we can construct a BP for every user then use it to verify if an incoming dealings may be a fraud or not. Our experiments over a real knowledge set illustrate that our technique is healthier than 3 state-of-the-art ones.

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

Introduction: THE volume of the electronic dealing has raised considerably in recent years because of the popularization of online searching (e.g., Amazon, eBay, and Alibaba). The global e-commerce market is expected that it'll be price a staggering US$ twenty four trillion by 2019. Credit cards are wide used in on-line searching, and card-not-present transactions in master card operations becomes additional and additional fashionable since net payment gateways (e.g., PayPal and Ali Pay) become popular. However, there has been a coinciding growth of transaction fraud which ends in an exceedingly dramatic impact on users. A survey of over one hundred sixty corporations reveals that the amount of on-line frauds is twelve times more than that of the offline frauds, and also the losses will increase yearly at double-digit rates by 2020. A physical card isn't needed within the state of affairs of on-line shopping and solely the knowledge of the cardboard is enough for a dealing. Therefore, it's a lot of easier for a fraudster to make a fraud. There are some ways by that fraudsters can illicitly acquire the cardboard data of a user: phishing (cloned websites), pseudo base station, Trojan virus, collision attack, malicious corporate executive, and so on. Therefore, it's terribly fascinating and vital to check the methods of fraud detection.

Architecture Diagram:



Literature Survey:

Paper 1. Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data.

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

Description: The problem of insider threat is receiving increasing attention both within the computer science community as well as government and industry. This paper starts by presenting a broad, multidisciplinary survey of insider threat capturing contributions from computer scientists, psychologists, criminologists, and security practitioners. Subsequently, we present the BAIT (Behavioral Analysis of Insider Threat) framework, in which we conduct a detailed experiment involving 795 subjects on Amazon Mechanical Turk in order to gauge the behaviors that real human subjects follow when attempting to exfiltrate data from within an organization. In the real world, the number of actual insiders found is very small, so supervised machine learning methods encounter a challenge. Unlike past works, we develop bootstrapping algorithms that learn from highly imbalanced data, mostly unlabeled, and almost no history of user behavior from an insider threat perspective. We develop and evaluate 7 algorithms using BAIT and show that they can produce a realistic (and acceptable) balance of precision and recall.

Paper 2. BUSINESS INTELLIGENCE AND ANALYTICS: FROM BIG DATA TO BIG IMPACT

Author Name : Hsinchun Chen

Description: Business intelligence and analytics (BI&A) has emerged as an important area of study for both practitioners and researchers, reflecting the magnitude and impact of data-related problems to be solved in contemporary business organizations. This introduction to the MIS Quarterly Special Issue on Business Intelligence Research first provides a framework that identifies the evolution, applications, and emerging research areas of BI&A. BI&A 1.0, BI&A 2.0, and BI&A 3.0 are defined and described in terms of their key characteristics and capabilities. Current research in BI&A is analyzed and challenges and opportunities associated with BI&A research and education are identified. We also report a bibliometric study of critical BI&A publications, researchers, and research topics based on more than a decade of related academic and industry publications. Finally, the six articles that comprise this special issue are introduced and characterized in terms of the proposed BI&A research framework.

Paper 3. Clustering in Metric Spaces for the KDD Practitioner

Author Name: V. J. Rayward-Smith

Description: Clustering is one of the most widely used techniques in Knowledge Discovery in Databases (KDD) but it is arguably one of the most di±cult to accomplish well. In non-hierarchical clustering, the database is partitioned into separate sets of similar records; in hierarchical clustering, there are multiple levels of decomposition resulting in a tree structure with the database at the root and, at each level, a set of records being partitioned into further subsets. This paper only addresses non-hierarchical clustering. In partitional, non-hierarchical clustering.

Paper 4. Fraud Detection System: A survey

Author Name : Aisha Abdallah, Mohd Aizaini Maarof and Anazida Zainal

Description: The increment of computer technology use and the continued growth of companies have enabled most financial transactions to be performed through the electronic commerce systems, such as using the Credit card system, Telecommunication system, Healthcare Insurance system, etc. Unfortunately, these systems are used by both legitimate users and fraudsters. In addition, fraudsters utilized different approaches to breach the electronic commerce systems. Fraud prevention systems (FPSs) are insufficient to provide adequate security to the electronic commerce systems. However, the collaboration of FDSs with FPSsmight be effective to secure electronic commerce systems. Nevertheless, there are issues and challenges that hinder the performance of FDSs, such as Concept Drift, Supports Real Time Detection, Skewed Distribution, Large Amount of Data etc. This survey paper aims to provide a systematic and comprehensive overview of these issues and challenges that obstruct the performance of FDSs. We have selected five electronic commerce systems; which are Credit card, Telecommunication, Healthcare Insurance, Automobile Insurance and Online auction. The prevalent fraud types in those E-commerce systems are introduced closely. Further, state-of-the-art FDSs approaches in selected E-commerce systems are systematically introduced. Then a brief discussion on potential research trends in the near future and conclusion are presented.

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 have a tendency to propose a way to extract users' BPs supported their group action records, that is employed to detect group action fraud within the on-line looking state of affairs. OM overcomes the disadvantage of Markov process models since it characterizes the range of user behaviors. Experiments also illustrate the advantage of OM. the longer term work focuses on some machine-learning strategies to mechanically classify the values of group action attributes in order that our model will characterize the user's customized behavior additional exactly. In addition, we have a tendency to decide to extend BP by considering alternative information such as user's comments.

References:

[1] W. van der Aalst, T. Weijters, and L. Maruster, "Workflow mining: Discovering process models from event logs," IEEE Trans. Knowl. Data Eng., vol. 16, no. 9, pp. 1128–1142, Sep. 2004.
[2] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," J. Netw. Comput. Appl., vol. 68, pp. 90–113, Jun. 2016.
[3] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based associative classification data mining," Expert Syst. Appl., vol. 41, no. 13, pp. 5948–5959, 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. 21–29, 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. Subrahmanian, “Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data,” IEEE Trans. Comput. Social Syst., vol. 1, no. 2, pp. 135–155, Jun. 2014.

[7] V. Bhusari and S. Patil, “Application of hidden Markov model in credit card fraud detection,” Int. J. Distrib. Parallel Syst., vol. 2, no. 6, pp. 203–210, 2011.

[8] R. Brause, T. Langsdorf, and M. Hepp, “Neural data mining for credit card fraud detection,” in Proc. IEEE Int. Conf. Tools Artif. Intell., 1999, pp. 103–106.

[9] T. Carter, An Introduction to Information Theory and Entropy, S. Fe, Eds. CiteSeer, 2007.

[10] R. C. Chen, S. T. Luo, X. Liang, and V. C. S. Lee, “Personalized approach based on SVM and ANN for detecting credit card fraud,” in Proc. Int. Conf. Neural Netw. Brain, Oct. 2005, pp. 810–815.