Transaction Fraud detection based on BPs using Biometric Authentication and Invisible virtual keyboard.

Prof. Deepti Deshmukh,Tushar Mahamuni, Nihal Londhe, Tejashri Magade
D.Y.Patil Institute Of Engineering And Technology Ambi, Pune

Abstract: With the popularization of on-line searching, group action fraud is growing seriously. Therefore, the study on fraud detection is attention-grabbing and significant. An important manner of detective work fraud is to extract the behavior profiles (BPs) of users supported their historical group action records, then to verify if Associate in Nursing incoming group action could be a fraud or not in sight of their bits per second and verify the Fingerprint details and Invisible Keyboard. Mark off chain models are fashionable to represent bits per second of users, that is effective for those users whose group action behaviors ar stable comparatively. However, with the development and popularization of on-line searching, it's additional convenient for users
to consume via the web, that diversifies the group action behaviors of users. Therefore, Mark off chain models are unsuitable for the illustration of these behaviors. during this paper, we have a tendency to propose Fingerprints BP that is a total order-based model to represent the relation of attributes of transaction records. supported Fingerprints and users group action records, we can reckon a path-based transition likelihood from Associate in Nursing attribute to a different one. At an equivalent time, we have a tendency to define Associate in Nursing data entropy-based diversity co- efficient so as to characterize the variety of group action behaviors of a user. additionally, we have a tendency to define a state transition rob ability matrix to capture temporal options of transactions of a user. Consequently, we are able to construct a BP for every user then use it to verify if Associate in Nursing incoming group action could be a fraud or not. Our experiments over a true knowledge set illustrate that our technique is better than 3 progressive ones. during this project we have a tendency to propose a way to extract users bits per second supported their group action records, that is employed to detect group action fraud within the on-line searching state of affairs. OM overcomes the shortcoming of Mark off chain models since it characterizes the variety of user behaviors. Experiments additionally illustrate the advantage of OM.
Keywords: Behavior profile (BP), e-commerce security, fraud detection, online transaction

Introduction:

The volume of the electronic dealings has raised significantly in recent years thanks to the popularization of on-line searching (e.g., Amazon, eBay, and Alibaba). the worldwide e-commerce market is foreseen that it'll be value a staggering US$ twenty four trillion by 2019. Credit cards square measure wide employed in online searching, and card-not-present transactions in master card operations becomes a lot of and a lot of widespread since internet payment gateways (e.g., Pay- Pal and AliPay) become widespread. However, there has been a coincident growth of dealings fraud which ends up during a dramatic impact on users. A survey of over one hundred sixty corporations reveals that the amount of on-line frauds is twelve times on top of that of the bovid frauds, and also the losses will increase yearly at double-digit rates by 2020. A physical card isn't needed within the situation of on-line searching and solely the knowledge of the cardboard is enough for a transaction. Therefore, it's a lot of easier for a fraudster to create a fraud. There are many ways by that fraudsters will lawlessly get the cardboard data of a user: phishing (cloned websites), pseudo base station, Trojan virus, collision attack, malicious business executive, and so on. Therefore, it's terribly attention-grabbing and significant to check the ways of fraud detection.

Literature Survey

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

Description: This paper starts by presenting a broad, multidisciplinary survey of insider threat capturing contributions from computer scientists,

psychologists, criminologists, and security practitioners. Subsequently, the BAIT (Behavioral Analysis of Insider Threat) framework, in which detailed experiment involving 795 subjects on Amazon Mechanical Turk in order to gauge the behaviors that real human subjects follow when attempting to ex filtrate 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, develop bootstrapping algorithms that learn from highly imbalanced data, mostly unlabeled, and almost no history of user behavior from an insider threat perspective. Here develop and evaluate 7 algorithms using BAIT and show that they can produce a realistic (and acceptable) balance of precision and recall.
Insider threat is a growing problem in many organizations. Although recent episodes in the press such as the leaks caused by the Wiki leakers, Bradley Manning and Edward Snowden, have made headlines in the global press, the problem of insider threats has long threatened companies in many different sectors

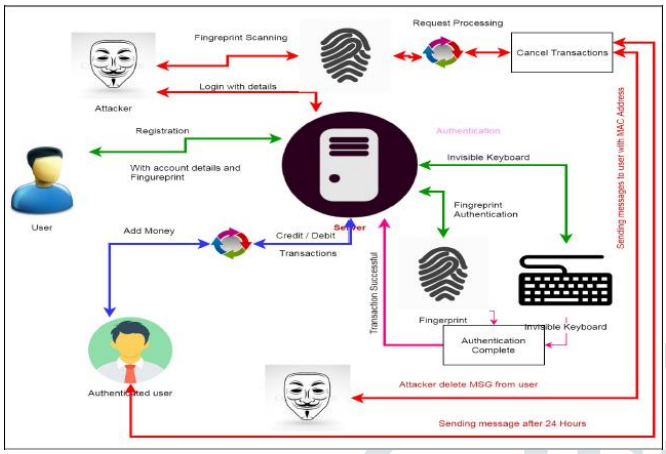
Paper(2). Business intelligence and analytics: From big data to big impact
Description: Business intelligence and analytics (BI&A) has emerged as an important area of study for both practitioners and researchers, rejecting the magnitude and impact of data-related problems to be solved in contemporary 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 BIA is analyzed and challenges and opportunities associated with BIA research and education are identified. A bibliometric study of critical BIA 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 BIA
research framework. Through BI&A 1.0 initiatives, businesses and organizations from all sectors began to gain critical insights from the structured data collected through various enterprise systems and analyzed by commercial relational database management systems. Over the past several years, web intelligence, web analytics.

Paper(3). Clustering in Metric Spaces for the KDD Practitioner
Description: Approaches for clustering records in real-world databases are discussed. Particular attention is paid to defining similarity when the fields are correlated and to the problem then posed by databases where fields are of differing types.
This paper presented a critical review of the current concepts and methods used for discovering comprehensible and interesting (novel or surprising) patterns in data.

Paper(4). Fraud Detection System: A survey
Description: In this paper 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 FPSs might 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. Here 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. Fraud cases have increased in recent years, particularly in important and sensitive technical areas. Hence, there is a dire need to combat fraud. Fraud prevention and detection are the proper protection

mechanism against fraud. Fraud prevention alone is not sufficient. Fraud detection is proposed to protect vital services in the technical systems.

System Architecture:



Algorithm Details:

1. Scan Line Algorithm

Add polygon edges to the Global Edge table(GET)
Set Y to the Smallest Y coordinates in the GET.
Initially active edge table (AET) to be empty.
Repeat until AET and GET are empty.
a. Add edges from the GET and AET in which y=y;
b. Remove edges from the AET.
c. Sort AET on x.
d. Fill pixel between pair of intersection in AET.
e. for each edge in the AET, replace x with x+1
f. set y=y+1 to the move to the next scan line.

2. Behavioral Profile

1. Look for an unusual behavior among users.
2. Monitor that users behavior profile with their information such as username, password specified, and user key etc.,
3. Tracing of login passwords.
4. During document access, the user key specified is tracked along with the type of operation i.e., valid or invalid.
5. Classify profile as valid or invalid using the following mathematical operation: P (4) = count (invalid operations/operations), If the result of P is above a threshold parameter then the profile is categorized as invalid and the user is redirected to the decoy module.

3. Mark over

We have seen that when a sequence of chance experiments forms an independent trials process, the possible outcomes for each experiment are the same and occur with the same probability. Further, knowledge of the outcomes of the previous experiments does not influence our predictions for the outcomes of the next experiment. The distribution for the outcomes of a single experiment is sufficient to construct a tree and a tree measure for a sequence of n experiments, and we can answer any probability question about these
experiments by using this tree measure.

Screen shots:

Conclusion:

In this project, we tend to propose a technique to extract users rate supported their transaction records, that is employed to notice dealings fraud within the on-line shopping state of affairs by exploitation the Fingerprints. overcomes the defect of Mark off chain models since it characterizes the range of user behaviors. Experiments additionally illustrate the advantage of OM. the long run work focuses on some machine-learning strategies to mechanically classify the values of dealings attributes in order that our model will characterize the users personalized behavior additional exactly. additionally, we tend to conceive to extend BP by considering different information like users comments. 3 sorts of technique that try and overcome some limitations of a data-driven approach based mostly solely on applied math properties of the info are mentioned, in particular: (a) a "meta-learning" technique employing a classification algorithmic program to find out that combination of data-driven rule powerfulness measures best predicts the user's rule interest; and strategies destined towards the invention of peculiar patterns.

References:

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. Subrahmanian, Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data, IEEE Trans. Computer. Social Syst., vol. 1, no. 2, pp. 135155, Jun. 2014.