JOURNAL FOR INNOVATIVE DEVELOPMENT IN PHARMACEUTICAL AND TECHNICAL SCIENCE

Volume-2,Issue-4 (April-2019)
ISSN (O) :- 2581-6934

Highly Secured Credit Card Transactions using Fingerprint Authentication

Ms. R.A. MABEL ROSE [1] , SUBHASINI A [2]
[1] Assistant Professor M.E ,[2] Student M.E
[1 2] Computer Science and Engineering, Rajas International Institute of technology for women

Abstract:- ***With the rapid development of electronic commerce, the number of transactions by credit cards are increasing rapidly. As online shopping becomes the most popular transaction mode, cases of transaction fraud are also increasing. In this paper, we propose a novel fraud detection method that composes of four stages. To enrich a cardholder's behavioral patterns, we first utilize the cardholders' historical transaction data to divide all cardholders into different groups such that the transaction behaviors of the members in the same group are similar. We thus propose a window-sliding strategy to aggregate the transactions in each group. Next, we extract a collection of specific behavioral patterns for each cardholder based on the aggregated transactions and the cardholder's historical transactions. Then we train a set of classifiers for each group on the base of all behavioral patterns. Finally, we use the classifier set to detect fraud online and if a new transaction is fraudulent, a feedback mechanism is taken in the detection process in order to solve the problem of concept drift. The results of our experiments show that our approach is better than others.***

Index Terms—Behavioral patterns; sliding window; concept drift; credit card fraud; machine learning

I. INTRODUCTION

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect, collect and exchange data. IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internetenabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled. With the arrival of driverless vehicles, a branch of IoT, i.e. the Internet of Vehicles starts to gain more attention. IoT (Internet of Things) is an advanced automation and analytics system which exploits networking, sensing, big data, and artificial intelligence technology to deliver complete systems for a product or service. These systems allow greater transparency, control, and performance when applied to any industry or system. IoT systems have applications across industries through their unique flexibility and ability to be suitable in any environment. They enhance data collection, automation, operations, and much more through smart devices and powerful enabling technology.

On the other hand, both of them are not aware of the adaptive capacity of the model. For example, a person may involve some new transaction behaviors in a specific period which has never happened in his/her history. Most of the proposed methods just keep the recent instances for model training, but do not consider the adaptiveness of the model.

Facing the above challenges, we extract the transaction behaviors of a cardholder using both his/her historical transaction data and the data of some similar cardholders. Further more ,we propose a feedback mechanism which can adapt to the cardholder's transaction behaviors seasonally. Our work can be summarized as the following four aspects:

1) By using clustering method, all cardholders are divided into three groups based on transaction amount, i.e., high, medium and low.

2) We propose a sliding-window-based method to aggregate the transactions in every group, i.e., derive a set of additional features from windows to characterize a cardholder's behavioral patterns.

3) After preprocessing features, we train a set of classifiers for each group using the data consisting of each specific behavioral pattern and extracted fraud features.

4) Finally, the classifier set trained for a group is assigned to each cardholder in the group as his/her own behavioral patterns, and the classifier with the highest rating score is viewed as his/her recent behavioral pattern.

Based on the three classifier sets, we propose a fraud detection method in which a feedback mechanism is taken in order to solve the concept drift problem.

EXISTING SYSTEM

As e-commerce continues to grow, so does the opportunity for perpetrating online fraud. As a result, many researches have been conducted to make online transactions possible in a risk free environment by proposing different fraud detection methods. Concept drift is an inherent feature in many data streams such as electronic financial transactions. Hence, many fraud detection techniques have tried to detect and preferably manage concept drift. A new concept drift management framework has been proposed. A temporary profile has been introduced in order to retain new concepts in the incoming data stream independently from historical profile. When the historical profile reaches a different decision from the temporary profile this is an indication that most probably a concept drift has occurred. A window based method is applied as a strategy for managing concept drift. The ability to adapt normal profiles systematically makes this concept drift management framework applicable to any profile based fraud detection method. Simulation results indicate that the proposed scheme is able to reduce the false positives (FPs) of a typical fraud detection method to 4.3% on average in the presence of a wide variety of concept drifts in the incoming transactions. This is an average of 85.7% reduction in FPs for this fraud detection technique.

Disadvantages

• The result was not accurate.

• Time consuming

• Behavior of cardholder was not identified.

PROPOSED SYSTEM

With the popularization of mobile devices, online shopping becomes a popular mode of daily purchases. However, the Internet environment is open, online shopping systems have bugs, and criminals can use some bad techniques such as Trojan and pseudo base-station. All these result in a serious increasing of credit card fraud events. When a criminal steals or cheats the information of the credit card of a cardholder, the criminal can use the credit card to consume. Facing the above challenges, extract the transaction behaviors of a cardholder using both his/her historical transaction data and the data of some similar cardholders. Furthermore, a feedback mechanism was proposed which can adapt to the cardholder's transaction behaviors seasonally. Our work can be summarized as the following four aspects:

• By using clustering method, all cardholders are divided into three groups based on transaction amount, i.e., high, medium and low.

• A sliding-window-based method to aggregate the transactions in every group, i.e., derive a set of additional features from windows to characterize a cardholder's behavioral patterns was proposed.

• After preprocessing features, train a set of classifiers for each group using the data consisting of each specific behavioral pattern and extracted fraud features.

• Finally, the classifier set trained for a group is assigned to each cardholder in the group as his/her own behavioral patterns, and the classifier with the highest rating score is viewed as his/her recent behavioral pattern. Based on the three classifier sets, propose a fraud detection method in which a feedback mechanism is taken in order to solve the concept drift problem.

Advantages

The advantages of the proposed system are,

• Avoid fraudulent.

• Accurate result

• More efficient

ISSN:- 2581-6934 |www.jidps.com

SYSTEM DESIGN

Systems design is the process of defining the architecture, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. There is some overlap with the

disciplines of systems analysis, systems architecture and systems engineering. System design provide the following designs

Architectural design

The architectural design of a system emphasizes the design of the system architecture that describes the structure, behavior and more views of that system and analysis.

Logical design

The logical design of a system pertains to an abstract representation of the dataflows, inputs and outputs of the system. This is often conducted via modelling, using an over-abstract model of the actual system. Logical design includes entity-relationship diagrams.

Physical design

The physical design relates to the actual input and output processes of the system. This is explained in terms of how data is input into a system, how it is verified/authenticated, how it is processed, and how it is displayed.

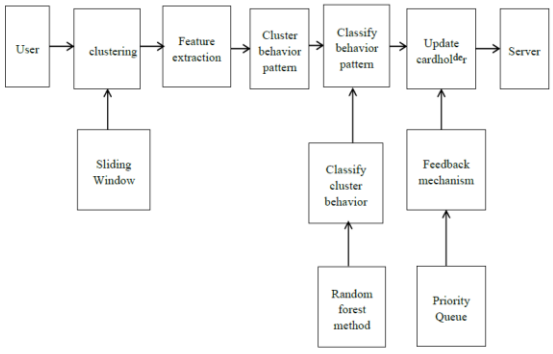

Fig: Architecture Diagram

the user behavior was grouped by using sliding window the feature was extracted. The classification of the behavior patter was provided by random forest method and then upload the cardholder behavior by using the feedback mechanism.

SYSTEM IMPLEMENTATION

5.1 MODULES

• Preprocessing

• Clustering Cardholder behavior

• Classifying Cardholder behavior

• Updating Cardholder behavior

PREPROCESSING

Cardholder Clustering: First use the clustering method k-means to divide all cardholders into three similar groups which are respectively labelled as high (h), medium (m) and low (l) based on transaction amount. Therefore, assume that V = {l,m.h} and |V | = 3. Note that l, m and h can be viewed as three sets of id's of all cardholders in the corresponding group and id is the identification of the cardholder. Transaction data of all cardholders in a group are more helpful to solve the sparse problem of data compared with the transaction data of a single cardholder. More importantly, each cardholder's behavioural patterns can be composed of two parts: his/her own behaviors reflected by his/her historical transactions, and other behaviors recommended by other members in the same group which may happen in the future but are not reflected by his/her historical transactions. The latter can enrich a cardholder's behaviors and improve the adaptiveness of individual model.

Sliding Window: After dividing all users into three similar groups, propose a sliding-window-based algorithm to aggregate the transactions and then derive some new amount-related/time-related features from the aggregated data in order to characterize the behavioral patterns of a cardholder more precisely. The sliding-window-based algorithm is an incremental mining technique and often used to detect the image objects. Furthermore, due to the fixed window size, this algorithm can quickly drop the first element and append the next new element to do data statistics by using the partial information from the previous window.

Feature Extraction: After the aggregation process, use these new windows to derive some new features. It is important to assume that some fraudsters are not familiar with the transaction behaviors of a cardholder. They are trying to get the most profits by performing high value transactions. Hence, four features are needed to extract the maximum, minimum, average amount and the amount of the last transaction in a window.

ISSN:- 2581-6934 |www.jidps.com

In addition, more cautious fraudsters try to imitate a cardholder's transaction behaviors and perform low value transactions in a short time. Therefore, analyzing some time-related features. Set p-1 time intervals which are respectively calculated from a transaction and its previous transaction in a window. Finally, label each window as normal or abnormal by using the label of the last transaction and the label function is yidi = LABEL(Tidi).Finally, for each cardholder obtain two datasets: Gid and Fid where Gid is the normal feature set of the cardholder and Fid is the abnormal feature set.

CLUSTERING CARDHOLDER BEHAVIOR

After extracting new features from each window, Xidi can be regarded as a single behavior pattern of a cardholder and Gid is the set of all behavioral patterns of the cardholder with id. It is difficult to classify the normal feature set to specific behavioral patterns. The reason is that the definition of behavioral patterns may be obscure when they are concluded by using human domain knowledge. However, it's more convenient to use a clustering method to solve this unsupervised learning problem which can automatically organize high-level abstract knowledge. For example, Bl is the behavioral pattern set of the low consumption group. Each cluster can be thought of as the specific behavioral patterns of group j. In other words, those aggregated transactions in a fixed cluster are of similar features.

CLASSIFYING CARDHOLDER BEHAVIOR

Several specific behavioral patterns are obtained from those aggregated transactions for each group. In each group, there are several normal behavioral patterns but there is still have no ability to predict the incoming transaction due to the lack of abnormal features. Hence, collect all abnormal features from the three groups and form an abnormal feature set:

F = [UidcVFid]

For each bi, F and their labels, utilize Random Forest to training a classifier ci. Random Forest is one of the state-of-the-art ensemble methods. This method can produce a classifier that is constructed by combing several different independent-base classifiers. This technique is known as bagging, or bootstrap aggregation which has a significantly lower risk of overfitting. By using multiple trees based on a majority voting on the individual predictions, reduce the error rate and variance of a classifier which is more accurate than a single-base classifier. After training, obtain a set of classifiers for each group: Cj . Here, each classifier can be viewed as a profile of single behavioral pattern. Next the classifier set Cj will be assigned to each cardholder in group j. Thus, each group member has many specific profiles from the similar group. By using group's profiles instead of using individual profiles, enrich a cardholder's behavioral patterns, some of which may not occur in his/her historical transactions but may happen in the future. Finally, for each cardholder u in group j, our method will choose the most suitable classifier from set Cu_j as the cardholder's recent profile. This can always keep the trends of the cardholder's transaction behaviors and the outdated behaviors can be forgotten.

UPDATING CARDHOLDER BEHAVIOR

The True label of a transaction in test dataset has never been used to update the profile of the cardholder. Note that the True label information is useful because it can reflect the changes of a cardholder's transaction behaviors indirectly. Hence, our proposed method uses feedback mechanism to update the profile of each cardholder when a new transaction comes. Each cardholder u in group j has a set Cu_j = {c1; c2; … ;ck}. A rating score will be assigned to each classifier. Priority Queue is used to choose a classifier with the highest rating score, which is highlighted as the gray block. Once the method produces a wrong prediction, it considers that the recent transactions cannot conform to the newest profile of the cardholder. The True label of the incoming transaction will be used to change the rating score of the classifier and our method tries to find out the most suitable classifier that is as the newest profile of the cardholder. Hence, a feedback mechanism was proposed for updating the rating score. The incoming transaction inconsistent with the newest profile will be input to each classifier, and the classifier ci will be rewarded (i.e., ri = ri+1) if it predicts correctly, else it will be punished (i.e., rj = rj-1). By using this feedback mechanism, the next transaction can be predicted by a classifier c*such that r*is the highest rating score in {r1; r2;:::;rk }. The feedback mechanism makes the on-

ISSN:- 2581-6934 |www.jidps.com

line method have the ability to adapt to the cardholder's transaction behaviors.

CONCLUSION

Novel fraud detection method was proposed to utilize the behavioral patterns from the similar cardholders to build a recent behavioral profile of a cardholder for solving the adaptive capacity of the model. A feedback mechanism can make full use of the true label information from transactions in order to solve the concept drift problem. The classifier will adjust its own rating score according to a series of incoming transactions. This on-line fraud detection method can dynamically change its parameters to adapt to a cardholder's transactions behaviors timely.

FUTURE ENHANCEMENT

The future work aims to design an individual periodic time window p in order to continue to improve the performance of fraud detection. Fraud detection methods are continuously developed to defend criminals in adapting to their strategies. In Fraud detection, identifying Fraud as quickly as possible once it has been done through fraud detection techniques, is now becoming easier and faster. The techniques which were studied here, through which credit card fraud can be detected quickly and fast and the crime can be stopped.

REFERENCES

[1]. A.C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten (2016), "Feature engineering strategies for credit card fraud detection," Expert Systems with Applications an International Journal, vol. 51, no. C, pp. 134-142.

[2]. T.K. Behera, and S. Panigrahi(2015), "Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network," in Proc. IEEE Int. Conf. Advances in Computing and Communication Engineering, Dehradun, India, pp. 494-499.

[3]. V.R. Ganji, and S.N.P. Mannem(2012), "Credit card fraud detection using anti-k nearest neighbor algorithm," International Journal on Computer Science & Engineering, vol. 4, no. 6, pp. 1035.

[4]. M. Masud, J. Gao, L. Khan(2015), "Classification and Novel Class Detection in Concept-Drifting Data Streams under Time Constraints" IEEE Transactions on Knowledge & Data Engineering, vol. 23, no. 6, pp. 859-874.

[5]. Shen, R. Tong, and Y. Deng (2007), "Application of Classification Models on Credit Card Fraud Detection," in Proc. IEEE Int. Conf. Service Systems and Service Management, Chengdu, China, pp. 1-4.

[6]. Srivastava, A. Kundu, S. Sural, and A. Majumdar(2008), "Credit Card Fraud Detection Using Hidden Markov Model," IEEE Transactions on Dependable & Secure Computing, vol. 5, no. 1, pp. 37-48.

[7]. L. Seyedhossein, and M.R. Hashemi (2011), "Mining information from credit card time series for timelier fraud detection," in Proc. IEEE Int. Conf. Telecommunications (IST), Tehran, Iran, pp. 619-624.

[8]. Q. Wei, Z. Yang, Z. Junping, and W. Yong(2003), "Mining multi label concept drifting data streams using ensemble classifiers," in Proc. IEEE Int. Conf. Fuzzy Systems and Knowledge Discovery, Tianjin, China, pp. 275-279.

[9]. C. Whitrow, D.J. Hand, P. Juszczak (2009), "Transaction aggregation as a strategy for credit card fraud detection," Data Mining & Knowledge Discovery, vol. 18, no. 1, pp. 30-35.