Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Improving Crime Detection Using Service Discovery Methods

Vaishnavi.S *
Department of Computer Science and Engineering, Anna University-India

Dr.P.Ezhumalai
Head Department of Computer Science and Engineering, Anna University-India

Abstract—Now a day's credit cards usage has become hysterically. As credit card becomes the most famous in the form of amount for both online and regular purchase, in this cases fraud also increased. Credit card fraud is act of using credit card of authorized user by unauthorized user. To identity crime with adaptively and quality data in real time, a new multi-layered detection system with two additional layers: The first new layer is Communal Detection (CD) finds exact or similar matches between categorical data and The second new layer is Spike Detection (SD) selects the attributes for the suspicion score and updates the attribute weights for CD.SD strengthens CD by providing attribute weights which has following limitations: effectiveness, as scalability issues, extreme imbalanced class, and time constraints dictated the use of rebalances data. To overcome these limitations by proposes four service discovery method of ontology such as Service profile, Service model and Service grounding .Each service address set of parameter to improve quality of service during fraud detection.

Keywords— Credit card, Credit card fraud, detection system, service discovery.

I. INTRODUCTION

Credit card is process of transfer or debits the cash in bank organization. Credit card fraud is act of using credit card of authorized user by unauthorized user. There are various types of fraud and how to detect the fraud in order to providing security for the credit card holder in banking industry. Credit card frauds are robbing the card physical or stealing the user information like account number and password for illegal transactions. Anyone can apply for credit card by using valid details of card holder or can even use money from the card which is not known until complaint has hired. This criminal activity has been more complex and there is no safe for valid credit card holders. Fraudsters are artistic of criminal acts and innovating new way of steal cards. Nowadays organization use web to store real identity data and access confidential data through mails thus it provides hole for identity crimes. In recent days identity crime became eminent and identity data classified into two categories real identity and synthetic identity. In developed countries that do not have a nationally registered identity numbers, identity crimes are pervasive. Credit card fraud detection allows us to find a large number of well experienced and sophisticated fraudsters. They are tenacious because of high financial rewards and involve minimal risk and effort. The behaviour of duplicate differs from characteristics pattern of behaviour of original thus fraudsters using application is detected by the methods that are reported.

Web services are complete, self documenting, heterogeneous software components, reported by Web Service Description Language (WSDL). Web services are accessed through internet when it is installed in the service registry Universal Description Discovery and Integration .The two main issues in web service are Keyword-based syntactic search and Interface heterogeneity these issues are overcome by proposing semantic web services. Web Ontology Language for Services promoted by OWL-S coalition is the another service proposed. Most of the discovery methods in semantic web service are based on the service profile ontology of OWL-S. Web Service Description Language and Business Process Execution Language for Web Services are enhanced with semantic annotations by OWL-S. Web ontology act as the key mechanism to globally define and reference concepts. Web services are extended with a distinct description by relating the input and output parameters of the service to common concepts defined in Web Ontology by OWL-S.

II. LITERATURE REVIEW

The literature review regarding various algorithms and its techniques for detection of crime in bank organization. This survey also gives ideas that can be incorporated to the proposed to improve performances and decrease time delay during fraud identification. In the paper [2], to view the insurance fraud detection problem as a data gathering and data analysis problem using Principal Component Iterative Discriminate Technique or Principal component analysis of RIDIT Scores. Optimal ranking used for Fraud/no fraud claims and allocated investigative resources efficiently to insurance fraud. This leads to labour costs so more economical being consistent. In the paper [12], to successful detect anomalous patterns that are indicative of an anthrax release using what's strange about recent events (WSARE) Algorithms.WSARE Creates baseline distribution without taking trends. This leads to unacceptably high false positive counts during fraud detection which slow detection times. In the paper [11], to detect fraudulent transaction through the neural network along with the genetic algorithm and learning algorithm. It has being used in different areas due to its powerful capabilities of learning and predicting. There is no design controls credit card fraud before any real transaction is made. In the paper [1], The sequence of operations in credit card transaction processing using a Hidden Markov Model (HMM) and show how it

can be used for the detection of frauds by Baum-Welch algorithm. Initial transaction is detected fraudulent or not and ensure that genuine transactions are not rejected. Transaction has no profile information at all and the system shows some performance degradation.

In the paper [10], to accurate identification of fraudulent transactions in historical databases using supervised method. Anomaly detection process and identifying are become most useful but features would not necessarily be captured by outlier detection.

III. EXISTING SYSTEM

In current trends credit card frauds are restricted using non data mining defence layers. Each layer has its own distinctive strength and flaws. Initially business rules and score cards are used for defence. Each rule undergoes a test of 100 points in which rules should obtain sufficient point to get through the test by providing weighted documents in a formal meeting .Business rules involves enquiry of applicant over telephone. Thus business rules are efficient and drawback is they are human resource intensive Another technique in use these days is fraud matching. Here a list of known fraud applications is maintained as black list. Black list is periodically reported. The current applications are tested against blacklist for match. Since patterns are repeated it enables clear understanding of frauds. The issues in known frauds are time delays that is fraud detection takes long time may be over a month for fraud to reveal itself, and be reported and recorded. Hence frauds are given more time to operate the application. Another issue is the frauds are recorded manually. Thus known frauds can be inaccurately expensive, hard to maintain and likely to breach privacy.

The real-time credit application fraud detection uses unsupervised algorithms which uses class labels. Scalability and handling extreme imbalanced class in credit card application cannot be achieved by using support vector machines, logistic regression or neural networks. As the behaviour of fraud and legitimate user keeps on changing frequently, thus classifier will disintegrate rapidly and training on new data is required for supervised algorithms.

A. Communal Detection

Communal detection reduces suspicion score by detecting real social relationship and also damage resistant to synthetic relationships. Communal detection is a whitelist oriented approach it works over a set of attributes. When two credit card applications shows a match in certain attributes like contact information, mobile number, date of birth but only the name of applicant differs then this falls under three cases: a fraud trying to obtain multiple credit cards with synthetic identity or might be Twins applying for credit card or same person applying for a second card and typographical error in name.

In first case CD layers use similarity between the current applications and previous applications and interpret similar applications with suspicion score. According to second and third case the probability that applicant is a legitimate user is high thus it tries to reduce the suspicion score. The whitelist approach is a list of communal and self-relationships between applications .The two main issues in whitelist are: attacks over whitelist and the volume and ranks of whitelist attributes changes over time. This approach reduces the scores of legal behaviours and false positives. Communal relationships reflect social relationships that are like family bond transforms to casual acquaintances. The communal relations can be family members, neighbours, or friends. The relationship like husband wife, brother-sister, cousin, Father, mother as well as uncle-niece falls under family member relationship. The same applicant when applying for more than one credit card then this relationship is called as self relationship. The link between applicants are ranked by volume which contributes whitelist .The probability of communal relationship is directly related to the volume of links of applications in a whitelist.

B. Spike Detection

Spike detection accompaniments communal detection which is attribute oriented approach and variable size set of attribute.SD helps to increase suspicion score by spikes which has probe contrary attributes leads to reduces opportunity of finding fraudster in the SD score calculation. The redundant attributes leads either too sparse or too dense which have no pattern to detect or no values can be found. But these attributes continually filtered on selected attributes only based on SD suspicion score. Therefore these attributes are reduced because only limited (one or two) attributes attentively selected. For example, in the bank organization if new ladies platinum credit card is campaign to give as attractive but this leads to spike in the number of attentively credit card applications by women. Final the system became defectively understood as fraudster attack. CD has only limited match of values from data set and does not have real social relationship because some values (name and address) are not unique. It provides importance in attribute weights which is continually determined but it does not have any pattern for it so new ones occurs overall volume fluctuates and natural changes in attribute weights. Final CD decrease computation speed and more data errors. To overcome this duplicate in important values is done by SD detect.SD improves computation speed but degrades security so computation of each attributes is done parallel on multiple workstations. Limitations of CD and SD detection are degrades security, imbalanced class, scalability issues, not true finding fraudsters due to updated after every period and time delay during rebalanced data. The main limitation is time delay and degrades security is overcome in this paper by introducing service discovery method.

IV. PROPOSING METHODS

In existing system, communal and spike detection algorithm drawbacks are overcome by service discovery methods. There are many semantic web service discovery methods introduced based on service profile ontology of ontology web language. Using ontologically annotated process model introduced service discovery method by information system (IS) manager. IS manager helps to find relevant match from existing database.

Web Ontology Language for Services has defined four ontology are service, service profile, service model and service grounding.[9] The service provides as an upper ontology and others references to it.

A. Service Profile

The service profile characterized service work. It has three types such as details about the organization, operation which should be done by service and other characteristics. The operation defines operational parameter such as user details, score of each attribution, checking match of data and access or denied user. This list of parameters has information about geographic availability, response time, and quality of service which is increased during detection of fraud. When user apply for credit card with all detail specified by bank, organization should detect the user with details provided whether user is valid or not without any time delay and give the access to valid users only.

B. Service Model

The service model characterized service process operation. They split class into sub-class of each service model which consist various web services and it has complete process. Process is defined as how data flow through the organization specification. There are three types of processes: first, Atomic processes have particular method should be done for specified input and produced output for it. Second, Simple is same as atomic process but it does not have any particular method. Three, Composite processes decomposable all processes to destination by specified method and it is control constructs by OWL-S has split, if and else, any order, choice. When the bank organisation provides user details to administrative for finding fraud. User details are splitted to both communal and spike algorithm to check parallel, which is used to find valid user to access credit card.

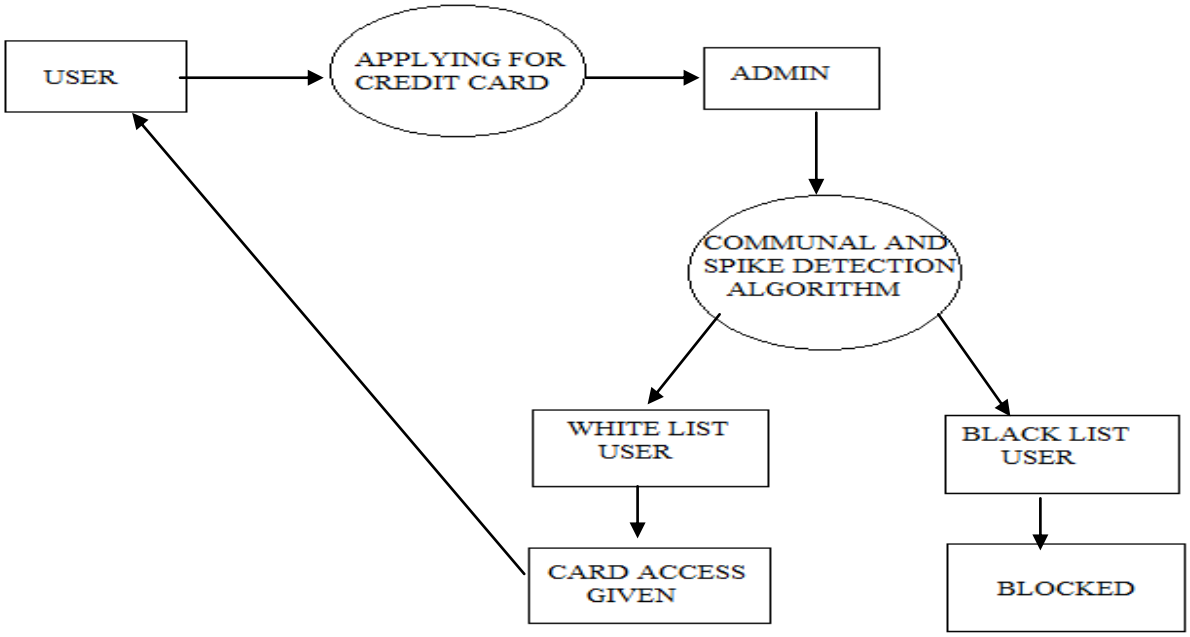

Fig. 1 System architecture diagram for Fraud Detection

C. Service grounding

The service grounding characterized service method which used to detect the fraud. It is binding between the service profile, the service model and the XML-based web service which is done by specification of organization how to execute the particular service. Using standard protocol called simple object access protocol (SOAP) for communicating between administration and other organization through internet. In fig1, user applying for credit card to particular bank with his/her details. These details of each attribute are converted into weight as specified separate weight percent to each attribute. Administration (admin) consists of centralized database weight of all other banks which is used to find fraud during applying credit card by matching weight of attribute using algorithms. After detecting user, valid user is moved to white list user who gets access of credit card and fraud user is moved to black list user who is blocked in the organization.

V. CONCLUSIONS

Presently, credit card fraud plays a major role in banking industry. There are various algorithms and techniques used to identify fraud but there consist of drawbacks like more time delay, many rules and score to calculate. This paper consist detection system with additional layer which are communal and spike detection algorithm for finding crime during applying for credit card in bank. Thus algorithms address various limitations during identification of fraud.Inorder to overcome limitation, proposing a service discovery method which has set of parameter to improve performance and decrease time delay.

ACKNOWLEDGMENT

The authors would like to the anonymous reviewers for their constructive and useful comments.

REFERENCES

[1] Abhinav Srivastava, Amlan Kundu, Shamik Sural, and Arun K. Majumdar, (January-March 2008), "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transactions On Dependable And Secure Computing, Vol. 5, No. 1,pp. 37 – 48,ISSN: 1545-5971.

[2] Brockett.P, R. Derrig, L. Golden, A. Levine, and M. Alpert, (2002), "Fraud Classification Using Principal Component Analysis of RIDITs," The J. Risk and Insurance,pp. 341-371.

[3] Clifton Phua, Member, Kate Smith-Miles Vincent Cheng-Siong Lee, and Ross Gayler, (March 2012), "Resilient Identity Crime Detection," IEEE Transactions on Knowledge and Data Engineering,pp. 533-546.

[4] Demian Antony D'Mello and V.S. Ananthanarayana, (February 2010), "Dynamic selection mechanism for quality of service aware web services", Enterprise Information Systems Vol. 4, No. 1,pp. 23-60.

[5] Hassan Issa, Chadi Assi, Mourad Debbabi and Sujoy Ray, (November 2009), "QoS-aware middleware for web services composition: a qualitative approach", Enterprise Information System Vol. 3, No. 4,pp. 449-470.

[6] Jackson.M, A. Baer, I. Painter, and J. Duchin, (2007), "A Simulation Study Comparing Aberration Detection Algorithms for Syndromic Surveillance," BMC Medical Informatics and Decision Making,pp. 1-11.

[7] Linda Delamaire , Hussein Abdou , John Pointon, (2009) , "Credit card fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2,pp. 57-68.

[8] NG Pavlidis, DK Tasoulis, NM Adams and DJ Hand (2012), "Adaptive consumer credit classification",Journal of the Operational Research Society,pp. 1645-1654.

[9] Paulraja. D, S. Swamynathan and M. Madhaiyan, (November 2012)," Process model-based atomic service discovery and composition of composite semantic web services using web ontology language for services (OWL-S)", Enterprise Information Systems Vol. 6, No. 4,pp. 445-471.

[10] R. Bolton and D. Hand, (2001), "Unsupervised Profiling Methods for Fraud Detection", Statistical Science,pp. 235-255.

[11] Raghavendra Patidar, Lokesh Sharma, (June 2011), "Credit Card Fraud Detection Using Neural Network", International Journal of Soft Computing and Engineering (IJSCE)ISSN: 2231-2307, Volume-1, Issue-NCAI2011.

[12] W. Wong, A. Moore, G. Cooper, and M. Wagner, (2003), "Bayesian Network Anomaly Pattern Detection for Detecting Disease Out breaks ",Proc. 20th Int'l Conf. Machine Learning (ICML),pp. 808-815.

