International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Survey on Exception Rules and Anomaly Detection

S. SenthilKumar[1] , Dr. S. Mythili[2]
[1] Ph.D. Research Scholar, Department of Computer Science
[2]Associate Professor & Head, Department of Information Technology,
[1&2]Kongunadu Arts and Science College,(Autonomous), Coimbatore, Tamil Nadu, India

ABSTRACT

This paper discusses about literature survey of exception rules and anomaly detection. This survey provides an overview of the research on anomaly detection. There exists a great variety of tools used for detecting outliers, exceptions or anomalies: expert systems, neural networks, clustering techniques, and association rules are some of them.

Keywords: Anomaly Detection, Anomalous Rule, Exception Rule.

I. INTRODUCTION

Anomalies is used for a variety of reasons, such as malicious activity, e.g., credit card fraud, cyber-intrusion, terrorist activity or breakdown of a system, but all have a common characteristic that they are interesting to the analyst. The "interestingness" or real life relevance of anomalies is an important feature of anomaly detection. Anomalies result in malicious actions, often adapt themselves to make the anomalous observations appear like normal, Anomalies define normal behaviour more difficult.

II. APPLICATIONS WHERE ANOMALY DETECTION USED ARE

- Cyber-Intrusion Detection
- Fraud Detection
- Medical Anomaly Detection
- Industrial Damage Detection
- Image Processing
- Textual Anomaly Detection
- Sensor Networks

ANOMALY DETECTION IN CREDIT CARD FRAUD

Credit card fraud, anomaly detection techniques are applied to detect fraudulent credit card applications or fraudulent credit card usage (associated with credit card thefts). Detecting fraudulent in credit card applications is identical to detecting insurance fraud. Many credit card companies are now employing data mining techniques to discover the abnormalities (anomalies) in pattern of the spending habits of their customers [8].

ANOMALY DETECTION IN MOBILE PHONE FRAUD

Mobile phone fraud detection is a distinct activity monitoring problem. The task is to scan a large set of accounts, examining the calling behaviour of each, and to issue an alarm when an account appears to have been misused [8].

ANOMALY DETECTION IN INSURANCE CLAIM FRAUD

An important problem in insurance industry is claims fraud, e.g. automobile insurance fraud. Individuals and group of claimants and providers manipulate the claim processing system for unauthorized and illegal claims. Detection of such fraud has been very important to avoid financial losses [8].

ANOMALY DETECTION IN MEDICAL

Anomaly detection in the medical and health areas work with patient records. The data can have anomalies

due to many reasons such as abnormal patient condition, instrumentation errors and recording errors. Several techniques have focussed on detecting disease outbreaks in a specific area. Hence the anomaly detection is a very critical problem in medical domain and requires high degree of accuracy [8].

ANOMALY DETECTION IN INDUSTRIAL DAMAGE

Anomaly detection techniques have been applied in this domain to detect damages. Industrial damage detection can be classified into two domains, one which deals with defects in mechanical components such as motors, engines, etc., and the other deals with defects in physical structures [8].

ANOMALY DETECTION IN IMAGE PROCESSING

Anomaly detection technique in images deals with any changes in an image or motion detection or in regions which appear abnormal or illegal on the image. The anomalies may be caused by motion or insertion of new object or instrumentation errors [8].

ANOMALY DETECTION IN TEXT DATA

Anomaly detection technique detects novel topics or events or news stories in a collection of documents or news articles. The anomalies are caused because of new interesting event or an anomalous topic [8].

ANOMALY DETECTION IN SENSOR NETWORKS

Anomalies in data collected from a sensor network can be caused due to one or more sensors are faulty, or they are detecting events (such as intrusions) that are interesting for analysts. Hence anomaly detection in sensor networks can capture sensor fault detection or intrusion detection or both [8].

Table (1) Merits and De-merits of Existing algorithms/methodology used and their outcome

Manuscript Title & Author(s)	Algorithm Used	Methodology / Technique Used	Outcome or Analysis of Previous Research	Merits	De-merits
Banking Fraud Analysis and Decision Support System,AyeshaAzeema. Maniyar, Chaitra. L. Mugali, Padma. Dandannavar, August 2015[1].	Density-Based Spatial Clustering of Applications with Noise (DBSCAN)" Cluster-Based Local Outlier Factor (CBLOF)" Histogram Based Outlier Score (HBOS)	The proposed approach is split into two stages of development including the training phase and the runtime. During the training phase, it creates a profile for each user on the basis of its prior transactions. The training phase takes as input aseries of transactions. It differentiates each user by using a *local, global and temporal profile*.	It provides the analysts with a ranked list of fraudulent transactions, along with the anomaly score of each user. The goal is to measure the effectiveness of this system in correctly identifying the transactions that are fraudulentand are not seen before in its prior transactions. sorted in decreasing order.	Well defined, manageable and well understood financial fraud monitoring system	Overcoming the limitations of this system requires more complicated datasets
Enhanced Fraud Miner: Credit Card Fraud Detection using Clustering Data Mining	LINGO clustering Data mining algorithm	Apriori and Lingo algorithm	Fraud Miner were having highest fraud detection rate than other classifiers with very less false alarm rate.	Fraud Miner recorded highest fraud detection and lowest false	In case of identical transactions exist both in Legal and

Techniques, Mohamed Hegazy, Ahmed Madian, Mohamed Ragaie, September 2016[2].				alarm rates when compared to other classifier.	Fraud patterns (overlapping) that's leads to unable to recognize fraud transactions.
A multi-algorithm data mining classification approach for bank fraudulent transactions,OluwafolakeAyano and Solomon O. Akinola, June 2017[3].	Density-Based Spatial Clustering of Applications with Noise (DB SCAN) combined with a rule base algorithm	The proposed model is a hybridized technique that combines DBSCAN classifier with rule-base algorithm to determine fraudulent transaction dynamically and reduce classification mismatch.	The result shows that the hybridized model has the tendency to perform better than a single model as it combines the strengths of the models used to come up with a better result.	The research aimed at detecting fraudulent transactions using multi-algorithm techniques to achieve higher accuracy.	Fraud card detection has not been tried with a combination of DBSCAN and RULE BASE before.
Data Mining Techniques for Credit Card Fraud Detection: Empirical Study, Marwan Fahmi, AbeerHamdy, KhaledNagati, November 2016[4].	SVM , Naive Bays, Decision trees and K-nearest neighbours	SVM , Naive Bays, Decision trees and K-nearest neighbours	The results showed that there is no data mining technique that is universally better than others.	Performance improvement could be achieved through developing a fraud detection model using a combination of different data mining techniques.	Only Four metrics were used in evaluating their performances
A novel anomaly detection algorithm for sensor data under Uncertainty, RaihanUl Islam, Mohammad ShahadatHossain, Karl Andersson, November 2016[5].	BRBAR (Belief-Rule-Based Association Rule)	A novel anomaly detection algorithm for sensor data based on BRBAR is proposed.	It can be observed that BRBAR combined with Web-BRBES (Web-BasedBelief-Rule-Based Expert System) provides better result of detecting metrological condition for anomaly-free data than from the anomalous data	The novel BRBAR technique will improve anomaly detection approach for other application areas such as, surveillance, environmental monitoring and disaster management under uncertainty. This new anomaly detection algorithm will also improve the prediction of different expert systems as anomalous	The performance of the algorithm needs to be tested by using more data from different types of sensor to ensure its efficiency and robustness.

				data can be removed more efficiently.	
Discovering Fuzzy Exception and Anomalous Rules M. Dolores Ruiz, Daniel S´anchez, Miguel Delgado, Maria J. Martin-Bautista, Aug 2016[6].	Fuzzy Exception Rule Search Algorithm (FERSA) & Fuzzy association rule mining	It computes the summary measures using the basic probability assignment associated to the support and certainty factor.	Fast and efficient method for detecting exception and the anomalous rules. Now we have developed an efficient algorithm based on the formalization that extracts jointly the common sense rules with their associated fuzzy exception and anomalous rules.	Useful in diverse domains such as in the security field	We need to develop Fast and efficient method for detecting this kind of information provided by the exception and the anomalous rules.
Anomaly detection using fuzzy association Rules, M. Dolores Ruiz, Maria J. Martin-Bautista, Daniel Sánchez, M. Amparo Vila March 2014 [10].	Fuzzy anomalous rules	The fuzzy version of the certainty factor for mining anomalous rules. Mining anomalies associated to a strong rule extracts the unusual and anomalous pattern.	Exception rules were first defined as rules that contradict the user's common belief (Suzuki, 1996). In other words, for searching an exception rule we have to find an attribute that changes the consequent of a strong rule. Anomalous rules are in appearance similar to exception rules, but semantically different. Anomalous association rule is an association rule that appears when the strong rule 'fails'.	Exception rules, that can be useful in several domains such as in the security field. The rules could be improved by parallelising the process.	Finding the fuzzy rules which algorithmically is more expensive than mining crisp rules. To overcome these problems we propose to use the algorithm fuzzy association rules
Firewall Anomaly Detection With A Model Checkerfor Visibility Logic, April 2012[9].	Visibility Logic(VL)	It used to express arbitrary patterns between rules inside a firewall model checker allows one to verify any formula expressed in visibility logic, of which traditional anomalies	Running times of under one second for 1,500 rules	The above Tool are efficient at detecting a predefined set of firewall anomalies,	The new logic can be likened (i.e.) Linear Temporal Logic can be used instead of Visibility Logic

III. CONCLUSION & FUTURE WORK

In this paper, a survey on various methods for exception and anomaly detection is discussed in an elaborate manner. The above table (1) shows the different existing methods used and their merits and de-merits. Some of the problems identified are:

(i) From the transaction database, the rule generation is not easier and the databases are incomplete hence we use Graph based technique and building sub graphs and we can find incomplete information.

Proposed Work:

Feature transformation - Discretization, filling missing values using normalization technique

Attribute selection - Gini index & information gain

Rule Generation

Rule pruning - Stepwise Regression analysis

Classification - Modified SVM based association classifier

(ii) For the proposed technique we can introduce Machine Learning Algorithms or Classification algorithm for Class Imbalance problems.

Proposed Work:

Feature transformation- Discretization,

Filling missing values using normalization technique

Attribute selection- Gini index, information gain and gain ratio

Rule generation

Rule pruning- Lasso Regression analysis

Classification using Enhanced Relevance Vector Machine based association classifier

(iii) Privacy is not concentrated in Transaction Database hence we can use k- anonymization technique and some modifications in Fuzzy algorithms are being introduced and privacy is enhanced so that owner of Transaction database may know all information's. To detect anomalous behaviour, we have to generate fuzzy rules and we have to calculate threshold value. Developing new approaches handling with imprecision or uncertainty for these new types of rules could be an interesting line for future research.

Proposed Work:

K-Anonymization technique is introduced for the privacy and Fuzzy SVM for based associative classifier.

IV. REFERENCES

[1]. Ayesha Azeema. Maniyar, Chaitra. L. Mugali, Padma. Dandannavar, Banking Fraud Analysis and Decision Support System, International Journal of Innovative Research in Advanced Engineering, Volume 2, Issue 8, August 2015.

[2]. Mohamed Hegazy, Ahmed Madian, Mohamed Ragaie, Enhanced Fraud Miner: Credit Card Fraud Detection using Clustering Data Mining Techniques, Egyptian Computer Science Journal, Volume 40, Issue 03, September 2016.

[3]. Oluwafolake Ayano and Solomon O. Akinola, A multi-algorithm data mining classification Approach for bank fraudulent transactions, African Journal of Mathematics and Computer Science Research, Vol. 10(1), June 2017.

[4]. Marwan Fahmi, Abeer Hamdy, Khaled Nagati, Data Mining Techniques for Credit Card Fraud Detection: Empirical Study, Sustainable Vital Technologies in Engineering & Informatics, November 2016.

[5]. Raihan Ul Islam, Mohammad Shahadat Hossain, Karl Andersson, A novel anomaly detection algorithm for sensor data under Uncertainty, Springer, November 2016

[6]. M. Dolores Ruiz, Daniel S´anchez, Miguel Delgado, Maria J. Martin-Bautista, Discovering Fuzzy Exception and Anomalous Rules, Vol:24,Issue:4,PP: 930 - 944 Aug 2016.

[7]. Raihan Ul Islam, Mohammad Shahadat Hossain, Karl Andersson, "A novel anomaly detection algorithm for sensor data under uncertainty", Soft Computing, 2016, ISSN 1432-7643.

[8]. Anomaly Detection : A Survey, Varun Chandola,ArindamBanerjee,VipinKumar,ACM Computing Surveys, PP: 1–72. September 2009.

[9]. Bassam Khorchani and Sylvain Hallé,Roger Villemaire, Firewall Anomaly Detection With A Model Checker for Visibility Logic, IEEE Network Operations and Management Symposium,PP:16-20,April 2012.

[10]. M. Dolores Ruiz, Maria J. Martin-Bautista, Daniel Sánchez, M. Amparo Vila, Anomaly detection using fuzzy association Rules, International Journal of Electronic Security and Digital Forensics, Volume 6, Issue 1, ISSN: 1751-911X, Pages 25-37, March 2014.