Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 1 (2012) 2733–2742

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Computational Science, ICCS 2010

A Novel Hybrid Artificial Immune Inspired Approach for Online Break-in Fraud Detection

R. Huang*, H. Tawfik, and A.K. Nagar

Faculty of Business and Computer Sciences, Liverpool Hope University, Liverpool, United Kingdom

Abstract

This paper proposes a new hybrid model for online fraud detection of the Video-on-Demand System, which is aimed to improve the current Risk Management Pipeline (RMP) by adding Artificial Immune System (AIS) based fraud detection for logging data. The AIS based model combines two artificial immune system algorithms with behavior based intrusion detection using Classification and Regression trees (CART). Immune inspired algorithms include the improved version of negative selection called Conserved Self Pattern Recognition Algorithm (CSPRA) and a recently established algorithm inspired by Danger Theory (DT) called Dendritic Cells Algorithm (DCA). The hybrid method based on stacking-bagging demonstrates higher detection rate lower false alarm, and handles high dimensional data set better when compared to the results achieved using only CSPRA, DCA, and CART.

Keywords: Artificial Immune System; Fraud Detection; Dendritic Cells Algorithm.

1. Introduction

There is money, there is fraud. This has been true for decades. As E-Commerce has become a dynamic force, changing all kinds of business operations world-wide, new forms of fraud based on Internet has been invented. In comparison with traditional fraud, online-fraud poses more challenges in terms of prevention and detection. Consequently, fraud detection remains an interesting research issue.

Fraud detection is about identifying fraud as soon as possible and responding to it. Limitations in exchanging ideas and data sets about fraud undisclosed to the public hamper e-fraud research and make it more difficult to develop new fraud detection methods. At present, there are a number of different methods applied for fraud detection such as auditing [1], expert systems [2], fuzzy logic [3], neural networks [4], pattern recognition [5], statistics [6], decision tree [7], regression [8] etc. These algorithms focus only on very specific types of their applications, and do not try to implement an extensible approach to the prevention of different kinds of online fraud. Hence, more efficient techniques for E-fraud detection need to be developed.

* Rentian Huang. Tel.:+44 0151 291 3599.
E-mail address:huangr@hope.ac.uk.

1877-0509
doi:10.1016/j.procs.2010.04.307

Phua et al. suggested for labeled fraud training data, it is better to employ hybrid algorithms to output suspicion scores, rules and/or visual anomalies on evaluation data [9]. This paper proposes an improved approach of current online fraud detection system. This approach is focused on logging data since many systems have logging for accounting purposes. Artificial immune systems are one of the most rapidly emerging biologically motivated computing paradigms and proved very powerful in addressing computational problems. In our paper, a novel hybrid artificial immune inspired approach is introduced for detecting online fraud in the Video-on-Demand system. The approach combines the Dendritic Cell Algorithm (DCA), Conserved Self Pattern Recognition Algorithm (CSPRA) and CART model [10, 11, 12]. Due to the different characteristics of each method, our empirical results demonstrate that detection rate can be improved, and the false alarm can be reduced much more than when using the three algorithms separately.

2. Our Proposed Online Fraud Detection System

The current Risk Management Pipeline System shown in Fig 1 for online fraud management is well established, mainly depending on the computerized methods which can be subdivided into validation service and purchase device tracing. Some merchants also apply decision and rules systems to determine whether the transaction should be accepted, rejected or suspended for manual review [13].

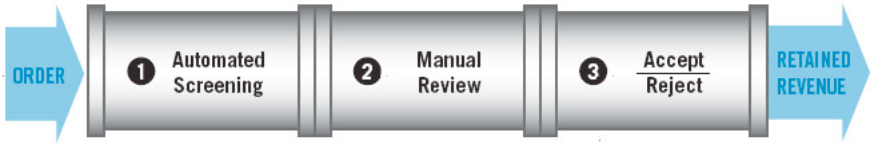

Fig 1. Framework of Risk Management Pipeline

Fig 2 showed our E-fraud detection system. Our approach focuses on improving the current risk management pipeline by adding AIS based E-fraud detection on logging data since many systems have logging for accounting, billing purposes. Systems may also have some kind of logging to monitor the status of the system. Those logging sources can then provide signs of suspicious user action, give information that clarifies the nature of the user actions, the identity or location of the user, or any other useful information about the fraud.

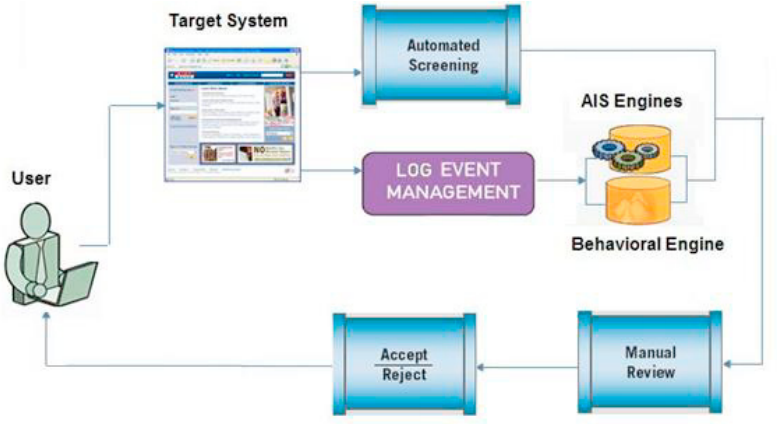

Fig 2. Proposed Fraud Detection System

Since RMP is a well established fraud management tool, to develop a system to use AIS based fraud detection techniques to log, event data is the main task of the paper (Fig 3).

Fig 3. AIS based fraud detection system

2.1. Target system

Our target system is a Video-on-Demand (VoD) system. This system consisted of a number of components, shown in Fig 4. Each user had a set-top-box (stb) at home, which can be connected to the Internet using a fast xDSL connection. When the set-top-box was turned on, the user will be allowed to contact the service providers DHCP server (Dynamic Host Configuration Protocol server), eventually a dynamic IP address will be allocated to the user.

Then, the user can login to the application server, browse the video database and order a movie. When the user provides correct identity and billing information to the server, the application server will generate an authentication ticket for the user. The VoD server then starts delivering the chosen movie after verification of the ticket. The simulation model to generate synthetic data can be found in [14].

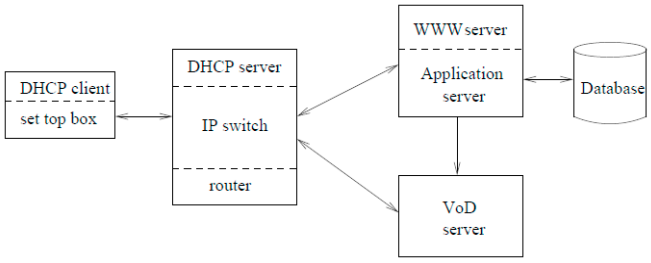

Fig 4. Video on Demand System's Structure

2.2. Log, event management

After data pre-processing for each fraud case in our system, three more useful and summarized information are extracted from the raw logs produced by the VoD system. As shown in Table 1 , data record file will start with Event Index is an integer number from 0, 0 means set-top-box on, 1 means set-top-box off, 1 and other numbers mean events within the session. Event Information will show the results of some activities, such as successful login or not, successful order or not. Billing and delivery don't have event information since they only generated when the action is completed.

Table 1. Record file format

Events Index	Event Date	Event Time	IP Address	Event Info	Event Name

The second file called router daily logs, which contains one line per day for the information of the date, time, user IP address, uploaded bytes and downloaded bytes. Based on the useful and summarized information from raw log, event data, the sum of all input events (over an interval) of the user will feed to the inputs of the fraud detection methodologies. For simplicity, we used an interval of 1440 minutes (24 hours). This allowed our detection scheme to detect fraud with a granularity of 24 hours, which should be sufficient for most service environments using fraud detection. The selected events were assigned to detection techniques as follow:

1. Sum of failed login attempts
2. Sum of successful login attempts
3. Sum of failed movie order
4. Sum of successful movie orders
5. Sum of movie delivery notifications
6. Sum of billing notifications
7. Ratio between upload & downloaded (bytes)

Since the user's behavior is changing over time, an exponential trace memory to maintain a moving average of pass input: $\bar{x}_i(t) = (1-\mu_i)x_i(t) + \mu_i \bar{x}_i(t-1)$ is introduced. The configurable μ allows for the representation of averages spanning various intervals of time. We used 0.7 in our detection tests, which proved to provide a sufficient decay rate for our purposes.

The simulation resulted in synthetic data for 7 months containing 600 normal users, 100 break-in fraudsters. The break-in frauds mimic a user who has taken over the identity of a legal user by hacking the user's set-top-box. The real user may use the service without knowing that they had a break-in. After data pre-processing, 3 datasets are generated for each fraud case, each dataset has more than 100,000 examples.

2.3. Behavioral engine

The finite state machine of our Video-on-Demand System showed in Fig 5 includes the possibility of the user's behaviour. The number 0 to 5 in the Fig 5 plus 6 for billing notification and 7 for delivery notification are recorded for the behaviour analysis. Behavioural engine operates on the account level, comparing sequences of actions to detect a change in behaviour of a particular user. The sequences of actions accumulated together can represent the behaviour of the user.

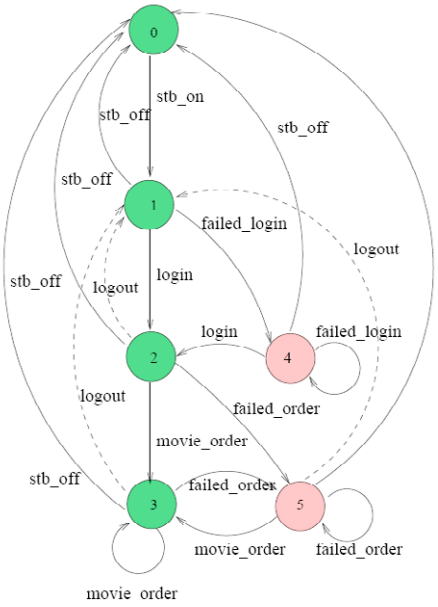

Fig 5. Finite State Machine

CART is implemented for training and testing the behavioral data of users extracted from log and event management component. One advantage of classification trees is that they are non-parametric, assuming neither a linear, nor even a continuous, nonlinear relationship between the classifiers and the dependent variable. Another important advantage is its simplicity [12].

2.4. AIS based engines

The AIS detection engines implements AIS based algorithms which can classify input data as normal or fraudulent. In our case study, the AIS detection engines will include Conserved Pattern Self Recognition Algorithm (CSPRA) [11] and Dendritic Cells Algorithm (DCA). We will investigate the usability of both algorithms for solving the E-fraud problem before hybrids them.

2.4.1. CSPRA for break-in fraud

CSPRA is inspired by the biological Pattern Recognition Receptor (PRRs) model published by Janeway [15]. PRRs can be viewed as an improved version of the negative selection suggested that the Antigen Presenting Cells (APCs) can recognize evolving pathogens.

The implementation of CSPRA consisted of two phases. In an initial phase, the CSPRA learns about behaviour of the normal user in the system (Fig 6). At the end of this learning phase, the system will be able to select the conserved pattern and generate an APC detector. Also the system runs the negative selection process and creates its antibodies (detectors).

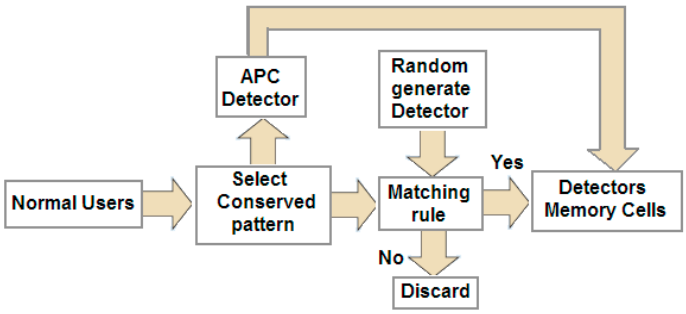

Fig 6. Phase 1: CSPRA training phase for break-in fraud detection

After the initial phase, the system enters the second phase where detection and classification are done. In this phase shown in Fig 7, the system may be exposed to fraud users. Detectors are used for checking if newly collected antigens represent the behaviour of good or bad users. Detectors generated by negative selection and APC detector will work together to classify the antigen into a normal user or a fraudster. The matching rule implemented here are the Euclidean distance.

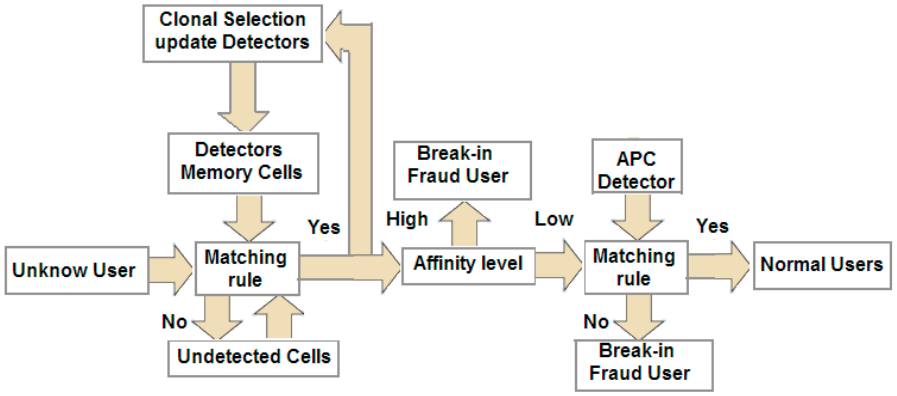

Fig 7. Phase 2: CSPRA detection phase for break-in fraud detection

Since some detectors will detect more matched antigens than others, the detectors with the highest scores will enter the clonal selection process, in which each of them will produce one new additional detector. The selected detectors will go through 2 clonal operations called cloning and mutation. Each new detector generated after clonal selection will be eliminated if they match some of the self antigens. This is repeated until one mutated clone survives the CSPRA. The new detectors and will replace the detectors which had the worse score in detection process. After updating the detector memory cells, the undetected antigen will go through the system again. The clonal selection details can be found in our previous paper [16].

2.4.2. DCA for break-in fraud

The original DCA was developed during the Danger Project leading by University of Nottingham [17]. The idea of DCA is to correlate disparate data-streams in the form of antigen and signals and label groups of identical antigen as normal or anomalous. It is not a traditional classification algorithm, but shares properties with certain filtering techniques. It provides information representing how anomalous a group of antigen is, not simply if a data item is anomalous or not. It has been applied into different domains including computer security [18, 19, 20, 21], scheduling process [22], robotic [23] etc. The DCA has 4 main phases:

- **Initialization Phase:** In the initialization phase, DCA selects useful information from the Video on Demand system. The antigen here represents the collected user's data. Each antigen (data) has its own signal matrix, such as the 7 inputs in our system. Typically, the data is normalized and categorized into the corresponding signal categories such as Pathogen Associated Molecular Patterns (PAMP), danger and safe signals.

- **Sampling Phase:** In the sampling phase, there is a set of immature dendritic cells (DCs). Each immature DC has three functions to perform as shown in Fig 8. Firstly they sample the antigen randomly and is placed in its own storage; then the DC collects the values of the different signals; finally at each iteration, the DC calculates the value that be the CSM (costimulatory) signal, semi-mature signal, and mature signal based on the current received input signals. If the CSM exceed its own migration threshold, the sampling phase is completed for this DC.

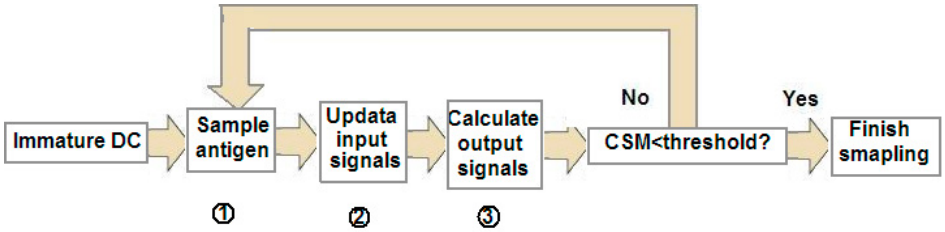

Fig 8. Sampling phase flowchart

- **Maturation phase:** Each cell has its own CSM threshold value, only when the CSM exceeds the migration threshold, the immature DC will enter the maturation phase. Immature DC will change its terminal state to semi-mature if it is greater than the resultant mature signal value. Otherwise, immature DC will terminate as mature.

- **Result phase:** The multiple DCs means antigen is sampled multiple times. If a single DC presents incorrect information, it becomes inconsequential provided that the majority of the DCs population derived from the correct cell context. Different combination of data sampling result in two different antigen context, dependent upon the combination of input signal value. Semi-mature antigen context implies antigen data was collected under normal conditions, whereas a mature antigen context signifies a potentially anomalous data. The response is decided by the measurement of the number of DCs that terminated from immature to mature, represented by a coefficient termed the mature context antigen value (MCAV). The value of MCAV is between 0 and 1; and can be used to assess the degree of anomaly of a given antigen. For example, a value close to 1 means the antigen is probably anomalous data.

2.5. Risk score

Risk score component can automate the results generated by the AIS detection engines, behavioural engine and determine whether the transaction should be accepted, rejected, or suspended for manual review. As there are 3 models used in the system, how to employ automated systems to interpret and weigh the multiple results in order to produce the final decision become increasingly important. Obviously, combining the output of different models will make the decision more reliable and increase predictive performance than a single model.

3. Experimentation

In this section, the implementations of different models are briefly described. All the parameters setting are based on experiments. Our training experiments randomly select 2000 normal and fraud samples that follow the distribution of 50:50 which demonstrate better performance. The first 1000 samples will be used for training and the rest 1000 are for testing. The classification results will compare with the perfect classification results (in the testing stage since they are not comparable in the training stage), to assess the true positive (TP), false positive (FP), true negative (TN) and false negative (FN).

3.1. CART experiment setup

In the CART model for behavioural engine, selecting correct splits and determines when to stop will affect the predictive accuracy. For classification problems, CART gives the user the choice of several impurity measures: The Gini index, entropy or misclassification. There are also two options that can be used to keep a check on the splitting process, namely Minimum n and Fraction of objects [12]. Table 2 are the summary of the 30 repeated tests with different impurity measure (Minimum n) based on the testing data. The results show that Gini index gave the best performance.

Table 2. Results for CART models

Impurity	TP%	TN%	FP%	FN%
Gini	81	85	15	19
Entropy	70	98	2	30
Misclassification	45	100	0	55

3.2. DCA experiment setup

The DCA is an unsupervised learning algorithm which does not require training; but it still has a large number of parameters and stochastic elements. Setting these parameters to the appropriate values has always been somewhat arbitrary.

Five experiments are performed to investigate how the key parameters will affect the classification results which include Signal Mapping, Number of DCs created, Migration Threshold Range, Antigen Multiplier, and Number of DC antigen receptors. The best scenario for the parameters setting is shown in Table 3 below which exhibit excellent performance with TP=78%, TN= 90%, FP=10%, FN=22%. Details of signal mapping, parameters investigation and other information can be found in our previous paper [24].

Table 3. Best parameters setting for DCA

Parameters	Value
Number of Cells	300
Number of DC antigen receptors	1
Antigen Multiplier	65
Migration Threshold Range	0.5-1.2
Max Cycle	100

3.3. CSPRA experiment setup

The first task for CSPRA is to select the conserved self pattern. In our system, successful order and fail order are selected as conserved self patterns. The details of the selection and generation of the APC detector can be found in [3]. A range of experiments of the CSPRA are decided carefully in order to evaluate the performance of the algorithm and analyze the experimental results. The experiments assist in clarifying the affect of different parameters, and fall into four categories:

1. Selecting the data dimensions
2. Selecting the number of T detectors
3. Selecting the T detector threshold and APC detector threshold
4. Selecting the Clonal selection update percentage
5. Selecting the Clonal mutation rate

The experimental results show that the parameters in the Table 4 gave the best performance with TP=81%, TN= 89%, FP=11%, FN=16%, and 3% failed to classified.

Table 4. Parameters values used in the experiments

Parameters	Value
Data dimensions	4
Self detector threshold	0.08
T-detector threshold	0.2
APC detector threshold	0.08
T-detector size	700
Clonal selection update %	15
Clonal mutation rate	0.1

4. Hybrid Algorithm

The hybrid algorithm is for combining multiple outputs of different models to achieve more reliable decisions and increase predictive performance over single model. Three approaches include bagging, stacking, and stacking-bagging are been investigated and experiments shown that, stacking -bagging is the best model for our case.

The Stacking-bagging trains the simplest algorithm first, followed by the complex ones (Fig 9). In our case, the CART classifier has the quick analysis ability which will compute first, followed by DCA and CSPRA which take longer training time. As most of the work has been done by the base classifiers, the simple and fast one which is CART will be reused for the meta-classifier. In order to select the most reliable base classifiers, stacking-bagging uses stacking to learn the relationship between classifier predictions and the correct class. For a data, these chosen base classifiers' predictions contribute their individual votes and the class with the most votes is the final prediction.

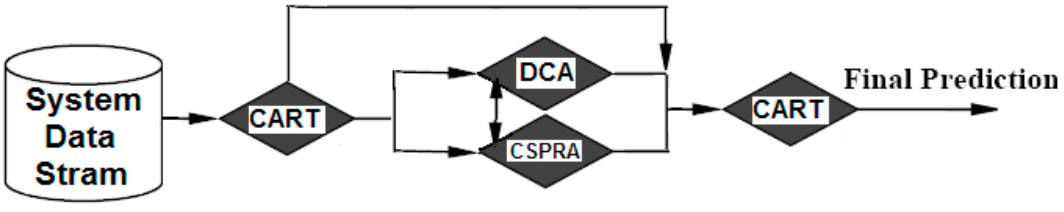

Fig 9. Hybrid based on Stacking & Bagging

The behaviour of the user will be firstly passed to the CART model and be classified as either 0 for normal or 1 for fraudulent. The CART will be first trained with the samples, and results will not only pass to help DCA and CSPRA for classification, but also save for the final prediction. The training results of CART, DCA, and CSPRA will gather together to be the inputs of the CART model again; and the output is the output of samples.

In CSPRA training, a pool of qualified detector candidates is generated. The DCA is further deployed to acquire the optimal detectors with danger are used for CSPRA. In the classification, a question will naturally raise the APC detectors classified a new sample as self data, but T detector recognizes the new samples as non-self. How does the system make the final decision? The solution in the previous section claimed that the APC detector will not be conducted until the detection from T detectors becomes unsure. But the performance of the algorithm will rely on the application domain since the definition of a suspicious antigen is not always in accordance with a specific application. In this situation, the output of the CART will help the CSPRA to classify the new sample as self or non-self data to resolve the conflicts.

For DCA, the output of the CART can become an additional danger signal or PAMP signal for the DCA depends on the classification result of the CART model. A threshold (in our case 0.7) also needs to be defined in order to classify the output of the CART model as a PAMP signal (>0.7) or danger signal (<0.7).

The testing results for hybrid model and CSPRA, CART, DCA are shown in Table 5 below.

Table 5. Results for hybrid method and individuals

Algorithms	TP%	TN%	FP%	FN%
CART	81	85	15	19
CSPRA (3% undetected)	81	89	11	16
DCA	78	90	10	22
Stacking Bagging	89	95	5	11

The results of hybrid approach demonstrate significant performance improvements in the testing over the CART, CSPRA, and DCA models. It shows a significantly better positive predictive value of fraud detection than what is achieved by three single approaches on the same data.

5. Conclusions

This paper proposes an improved approach of E-fraud detection by using logging data sets. The proposed approach can help e-commerce better understand the issues and plan the activities involved in a systemic approach to E-fraud. This approach is focused on logging data since many systems have logging for accounting purposes. In order to obtain sufficient quality data for fraud detection system, a Video-On-Demand system is used for this purpose.

The paper has investigated the potential usage of the CSPRA and DCA for online fraud detection and proved they are two efficient and reliable techniques to classify normal and fraud users in an online environment. Finally, a novel hybrid model for online fraud detection, which combines two artificial immune system algorithms with behaviour based intrusion detection using CART model is proposed. Based on the experimental results, our proposed methods demonstrate higher detection rate, lower false alarm and handle high dimensional data set better when compared with the results achieve by only using CSPRA, DCA, and CART as individual algorithms.

The present study contributes to researches in the fraud detection and prevention area by suggesting hybrid supervised and unsupervised algorithms can exhibit better performance for online fraud detection. Our research is not only focus on very specific application, we are trying to implement a more portable and extensible approach to prevention and detection of online fraud treatment in the online world faces many new challenges.

Acknowledgements

Thanks to Emilie Lundin Barse for providing the data, valuable discussions and suggestion for the paper.

References

1. Qian Liu, Tong Li, and Weixu, A subjective and objective integrated method for fraud detection in financial system, In Proceedings of Machine Learning and Cybernetics, (2009), 1339-1345.
2. Rozsnyai, S, Schiefer, J, and Schatten, A, Solutionarchitecture for detecting and preventing fraud in real time, In proceeding of Digital Informatino Management, ICDIM'07, (2007), 152-158.
3. Wei Chai, Hoogs, B.K., Verschueren, B.T., Fuzzy Ranking of Financial Statements for Fraud detection, In proceeding of International Conference on Fuzzy System, (2006), 152-158.
4. Tao Guo, Gui-Yang Li, Neural data mining for credit card fraud detection, In proceeding of International Conference on Machine Learning and Cybernetics, (2008), 3630-3634.
5. Jianyun Xu, Sung, A.H., Qingzhong Liu, Tree Based Behaviour Monitoring for Adaptive Fraud Detection, In proceeding of International Conference on Pattern Recognition, (2006), 1208-1211.
6. Z. Ferdousi, and A. Maeda, Unsupervised Outlier Detection in Time Series Data, In Proceedings of 22nd International Conference on Data Engineering Workshops, (2006).
7. E. Kirkos, C. Spathis, and Y. Manolopoulos, Data mining techniquesfor the detection of fraudulent financial statements, Expert Systems with Applications, (2007), 23: 32.
8. C. Spathis, Detecting false financial statements using published. data: some evidence from Greece, Managerial Auditing Journal, vol. 17, no.4, (2002), 179-191.
9. S Clifton Phua, Vincent Lee, Kate Smith & Ross Gayler, A Comprehensive Survey of Data Mining-based Fraud Detection Research, Artificial Intelligence Review (2005).
10. J. Greensmith, J. Twycross, and U. Aickelin, Dendritic cells for anomaly detection, In IEEE Congress on Evolutionary Computation (2006), 664-671.
11. Senhua Yu and Dipankar Dasgupta , Conserved Self Pattern Recognition Algorithm, ICARIS, LNCS 5132, (2008) 279-290
12. Breiman, L., J. H. Friedman, R. A. Olshen, and C. J. Stone, Classification and regression trees. Monterey, Calif., U.S.A.: Wadsworth, Inc (1984).
13. CyberSource, Online Fraud Report. Also available on http://forms.cybersource.com/forms/FraudReport2009NACYBSwww020309 (2009)
14. Emilie Lundin, Hakan Kvarnstr ¨om and Erland Jonsson. A synthetic fraud data generation methodology. In Proceedings of the Fourth ICICS 2002, Singapore, December 9-12,(2002). Volume 2513 of LNCS, Springer-Verlag.
15. Janeway, C. A., How the immune system recognizes invaders, Scientific American, vol. 269, no. 3, (1993), 72–79.
16. Rentian Huang, Hissam Tawfik, and Atulya Nagar, Licence Plate Character Recognition Using Artificial Immune Technique, In Proceedings of the 8th ICCS, Krakow, (2008) LNCS, 823-832, Springer-Verlag
17. U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod. Danger theory: The link between AIS and IDS. ICARIS, LNCS 2787, pp.147–155. (2003), Springer-Verlag.
18. J. Greensmith, U. Aickelin, and J. Feyereisl, The DCA SOMe comparison: A comparative study between two biologically-inspired algorithms. Evolutionary Intelligence: Special Issue on Artificial Immune Systems, (2008).
19. J. Greensmith, U. Aickelin, and G. Tedesco, Information fusion for anomaly detection with the DCA. (2008) Information Fusion.
20. J. Greensmith, J. Twycross, and U. Aickelin Dendritic cells for anomaly detection. In Proc. of the CEC, (2006) 664–671.
21. Jungwon Kim, Peter Bentley, and Christian Wallenta, Danger Is Ubiquitous: Detecting Malicous Activities in Sensor Networks Using the Dendritic Cell Algorithm, ICARIS, LNCS 4163, (2006) 390-403.
22. N. Lay and I. Bate, Improving the reliability of real time embedded systems using innate immune techniques. Evolutionary Intelligence: Special Issue on Artificial Immune Systems (2008).
23. R. Oates, J. Greensmith, U. Aickelin, J. Garibaldi, and G. Kendall, The application of a dendritic cell algorithm to a robotic classifier. In Proc. of the 6th ICARIS, LNCS 4628, (2007) 204–215.
24. Rentian Huang, Hissam Tawfik, and Atulya Nagar, Artificial Dendritic Cells Algorithm for Online Break-in Fraud Detection, In Proceedings of the 2nd International Conference on Developments in eSystems Engineering, Abu Dhabi, UAE, (2009), 181-189.