Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Intelligent System to Detect Admission Fraud in Colleges of India

Harpreet Kaur*
Computer Science Department
North West Institute of Engineering &Technology, Moga, India

Dr. Mohita Garag
Computer Science Department
Principal of North West Institute of Engineering &Technology, Moga, India

Harbhajan Kaur
Computer Science Department
North West Institute of Engineering &Technology, Moga, India

Abstract—Due to continuously increase of fraud in whole world, affects the daily life of people's and also economic conditions of each country. Different modern fraud detection techniques have been applied to prevent frauds in various fields. In today's world, education is one of the famous fields where cases of fraud admissions, fraud degree certificates are occurring continuously. Fraudsters are continuously playing with life of students. However many techniques have been applied but still it needs to be improve. In this paper, the survey of different fraud detection techniques has been presented. The goal of this paper is to review different existing techniques used to detect frauds.

Keywords—Fraud Detection, Expert System, Neural Networks, Data Mining

I. INTRODUCTION

The Association of Certified Fraud Examiners (ACFE) defined fraud as the use of one's occupation for personal enrichment through the deliberate misuse or application of the employing organization's resources or assets [1]. Now days, with advancement in technology, the cases of fraud are also increasing in various fields. The fraudsters are using technology for wrong purposes instead of right. These frauds are now very common in fields of banking, insurance, education, computers, industries and other private sectors. Educational field is one of the fields that make every person perfect. The whole life of person and his achievements in life depends on education. But in todays world, education system is totally corrupted by fraudsters. To prevent these frauds, fraud detection has become serious issue to be discussed.

Fraud detection is the method to detect fraud as soon as possible, when it happens. These methods need to be developed continuously to defend crime of fraud. But with advancement of new technology, it is becoming more challenging task to detect fraud immediately, because fraudsters are also using this technology to find new ways of fraud. Although prevention technologies are the best way to reduce fraud, to catch fraudsters. Statistics and machine learning, distributed deep learning provide effective technologies for fraud detection and also has been applied in fields to detect activities such as financial fraud detection, computer intrusion etc.

II. TYPES OF FRAUDS

A. CREDIT Card Fraud:- Credit card fraud is divided into two types: offline fraud and online fraud. Offline fraud is committed by using a stolen physical card at storefront or call center. In most cases, the institution issuing the card can lock it before it is used in a fraudulent manner. Online fraud is committed via web, phone shopping or cardholder not present. Only the card's details are needed, and a manual signature and card imprint are not required at the time of purchase [11].

B. Computer Intrusion:- Intrusion is defined as the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable. Intruders may be from an outsider (or hacker) and an insider who knows the all about layout of the system that where the valuable data is and what security precautions are in place. Computer intrusion can be classified into two categories: misuse intrusions and anomaly intrusions. Misuse intrusions are well-defined attacks on known weak points of a system. Anomaly intrusions are based on observations of deviations from normal system usage patterns. These include attempted break-ins, masquerade attacks, leakage, denial of service, and malicious use [4].

C. Telecommunication Fraud:- Fraud is costly to a network carrier both in terms of lost income and wasted capacity. The various types of telecommunication fraud can be classified into two categories: subscription fraud and superimposed fraud. Subscription fraud occurs from obtaining a subscription to a service, often with false identity details, with no intention of paying. Cases of bad debt are also included in this category. Superimposed fraud occurs from using a service without having the necessary authority detected by the appearance of unknown calls on a bill. This fraud includes several ways, for example, mobile phone cloning, ghosting (the technology that tricks the network in order to obtain free calls), insider fraud, tumbling (rolling fake serial numbers are used on cloned handsets so that successive calls are attributed to different legitimate phones), and etc [13].

D. Educational Fraud:- In reputed educational universities or colleges, the crowd of admissions is increasing day by day according to the level of competition. The students have two ways to take admissions either consoling or management quota. As the admissions for new session starts, rush of students can be noticed at university or college campus. Everyone wants to get admission directly or indirectly. It can be noticed that students use each way to get admissions. However students get admission in these colleges or universities on the basis of merit list. The students having highest percentage or high ranks in competitive exams are preferred firstly. Apart from this, some seats are also reserved for different quotas like SC, BC, and Army etc. From last few years, it can be noticed that with expansion of technology, fraud is also increasing. In the field of education, the complaints of fraud admissions are growing rapidly. The fraudsters are providing fake degrees, certificates to students and students pay them high amount of money to get all theses certificates.

III. TECHNIQUES OF FRAUD DETECTION

A. Neural Networks:- A neural network is a set of interconnected nodes designed to imitate the functioning of the human brain. Each node has a weighted connection to several other nodes in adjacent layers. Individual nodes take the input received from connected nodes and use the weights together with a simple function to compute output values. Neural networks come in many shapes and forms and can be constructed for supervised or unsupervised learning. The user specifies the number of hidden layers as well as the number of nodes within a specific hidden layer. Depending on the application, the output layer of the neural network may contain one or several nodes [5].

B. Model-based Reasoning:- Model-based detection is a misuse detection technique that detects attacks through observable activities that infer an attack signature. There is a database of attack scenarios containing a sequence of behaviors making up the attack. Garvey and Lunt combined models of misuse with evidential reasoning. The system accumulates more and more evidence for an intrusion attempt until a threshold is crossed; at this point, it signals an intrusion attempt. **A** pattern matching approach based on Colored Petri Nets to detect misuse intrusion is proposed by Kumar and Spafford [10]. It uses audit trails as input under UNIX environment.

C. Data Mining:- Data mining approaches can be applied for different fraud detection. The main advantage of data mining approach is that it can create a new class of models to identify new attacks even before they have been detected by human experts. Classification model with association rules algorithm and frequent episodes has been developed for anomaly intrusion detection. This approach can automatically generate concise and accurate detection models from large amount of audit data. However, it requires a large amount of audit data in order to compute the profile rule sets. Moreover, this learning process is an integral and continuous pat? Of an intrusion detection system because the rule sets used by the detection module may not he static over a long period of time. A team of researchers at Columbia University proposed the detection models using cost-sensitive machine learning algorithms. Audit data is analyzed by association rules algorithm in order to determine static features of attack data [13].

D. Expert Systems:- An expert system is defined as a computing system has the capacity to represent and reasoning about some knowledge-rich domain to solve problems and to give advice . Expert system detectors used if-then rules to encode knowledge about attacks**.** NIDES developed by SRI uses the expert system approach to implement intrusion detection system that performs real-time monitoring of user activity [3]. NIDES consist of statistical analysis component for anomaly detection and rule based analysis component for misuse detection.

IV. CONCLUSIONS

In this paper, different type of frauds has been discussed and also the techniques to detect frauds have been studied. Different techniques are best for different type of frauds. The study shows that educational frauds are serious issue of whole world but work done to detect frauds in educational field is very less. In modern society, education is very important for every person. Even, person learns good and bad thoughts through education. So, it is very important to prevent frauds in educational field.

REFERENCES

[1] M. S. Beasley, "An empirical analysis of the relation between the board of director composition and financial statement fraud," The Accounting Review, vol. 71, no. 4, pp. 443-465, 1996.6.

[2] J. V. Hansen, J. B. McDonald, and W. F. Messier, "A generalized qualitative-response model and the analysis of management fraud., " Management Science, vol. 42, pp. 1022-1032, 1997.

[3] M. M. Eining, DS. R. Jones, and J. K. Loebbecke, "Reliance on decision aids: an examination of auditors' assessment of management fraud.," Auditing: A Journal of Practice and Theory, vol. 16, pp. 1-19, 1997.

[4] B. P. Green, and J. H. Choi, "Assessing the risk of management fraud through neural network technology," Auditing, vol. 16, pp. 14-28, 1997.

[5] K. Fanning and K. Cogger, "Neural network detection of management fraud using published financial data," International Journal of Intelligent Systems in Accounting, Finance & Management, vol. 7, no. 1, pp. 21-24, 1998.

[6] M. D. Beneish, "Incentives and penalities related to earnings overstatements that violate GAAP," Accounting Review, vol. 4, no. 4, pp. 425-457, 1999.

[7] L. J. Abbott, S. Parker, and G. F. Peters, G.F. "Audit committee characteristics and financial misstatement: A study of the efficacy of certain blue ribbon committee recommendation," Proceedings of the Auditing Section of the AAA Meeting, 2001.

[8] K. Fanning, K., Cogger, and R. Srivastava, "Detection of management fraud: a neural network approach", International Journal of Intelligent Systems in Accounting, Finance & Management, vol. 4, no. 2, pp. 11326, June 1995.

[9] T. Bell and J. Carcello, "A decision aid for assessing the likelihood of fraudulent financial reporting". Auditing: A Journal of Practice & Theory, vol. 9, no. 1, pp. 169– 178, 2000.

[10] C. Spathis, M. Doumpos, and C. Zopounidis, "Detecting falsified financial statements: a comparative study using multicriteria analysis and multivariate statistical techniques". The European Accounting Review, vol. 11, no. 3, pp. 509–535, 2002.

[11] Fu, K., Cheng, D., Tu, Y., & Zhang, L. (2016, October). Credit Card Fraud Detection Using Convolutional Neural Networks. In International Conference on Neural Information Processing (pp. 483-490). Springer International Publishing.

[12] Rana, Priya J., and Jwalant Baria. "A Survey on Fraud Detection Techniques in Ecommerce." International Journal of Computer Applications, Vol. 113, Issue 14, 2015.

[13] Lata, Lutfun Nahar, Israt Amir Koushika, and Syeda Shabnam Hasan. "A Comprehensive Survey of Fraud Detection Techniques.", International Journal of Computer Applications (0975 – 8887) Volume 113 – No. 14, March 2015.

