ISSN 2278-3091
Volume 8, No.3, May - June 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse96832019.pdf
https://doi.org/10.30534/ijatcse/2019/96832019

Online Banking Fraud Detection System: A Review

Kanika[1], Jimmy Singla[2]
[1] School of CSE, Lovely Professional University, Punjab, India, kanikadhanjal@gmail.com
Associate Prof., School of CSE, Lovely Professional University, Punjab, India, jimmy.21733@lpu.co.in

ABSTRACT

The volume of online banking transactions is expanding day by day resulting in fraudulent transaction cases as well, producing losses in money for banking sector and financial institutions every year. Hence, there is an urgent need for a reliable mechanism which can efficiently identify and prevent such fraud transactions. Data mining and machine learning helps in detecting the patterns among data attributes i.e. to detect whether a transaction is fraudulent or not. This review paper compares the performance parameters retrieved from various methods used in various existing studies to detect the online banking fraud and presents the best methods used to detect the fraudulent transactions.

Key words : Banking Fraud Detection System, Fraudulent Transactions, Online Banking, Credit Card Fraud.

1. INTRODUCTION

With the development of information technology and banking sector, the majority of modern commerce is depending upon the online banking and cashless payments. Online banking services such as telephone bank, mobile bank etc. have provided great convenience to the banking customers. They provide easier, seamless and comfortable option to businesses.

However, security is also one of the major concerns for the online banking customers. Due to rise in online transactions, fraudsters are also inventing new techniques on regular basis. Whenever any fraudulent transaction occurs, customers suspect the security of online banking system after losing their precious money. To address this problem, a fraud detection system should be built to retain the customers by banking institutions. There is also a crucial need to develop an efficient and dynamic technique to address the security concern of online banking fraud.

In fraud detection system, the transactions are categorized into two classes i.e. fraudulent and non-fraudulent. Fraud detection systems are designed in a way to verify the transactions by comparing with the past spending history of the customers.

Thus, a transaction will be labelled as fraudulent if it is deviating from the normal spending history of the customers.

An efficient fraud detection system is the one which is effective to detect the high-risk frauds which lead to the huge money loss to banking sector and which is also able to deal the changes occurring in fraudulent techniques or patterns used by the fraudsters. Data science and big data may also play important role in this. [12,13]

The rest of paper is presented into two sections: Section 2 provides the summary on related works for the detection of online banking fraud. Section 3 describes the conclusion and future studies to be performed.

2. RELATED WORKS

This section consists of the reviews of various technical and review articles based on different techniques applied to detect online banking fraud.

- Q. Lu and C. Ju [1] have established a banking fraud detection system using credit card transactions which is based on Weighted Support Vector Machine algorithm. They have used Principal Component Analysis (PCA) and SVM-Imbalance Class Weighted algorithm on high dimensional real dataset from a bank and demonstrated that their proposed model is efficient for detecting credit card fraud.

- S. Kovach and W. V. Ruggiero [2] have proposed an online banking fraud detection system which takes into account of global and local observations of users' behaviour. They have used differential analysis to acquire local affirmation of banking fraud. A remarkable variation from usual behaviour of users point out a possible fraud. The user's global behaviour affirms the confirmation of fraud. The affirmation of fraud is based on a probability value deviating over time. They have applied the Dempster's rule of combination to these affirmations for final intuition of fraud. They have presented an online banking fraud detection method based on helpful recognition of devices which were used to access the user' accounts and so that the fraud can be detected by keeping track of various accounts accessed by each and every device. Figure 1 shows the mainstream design of the online banking fraud detection system.

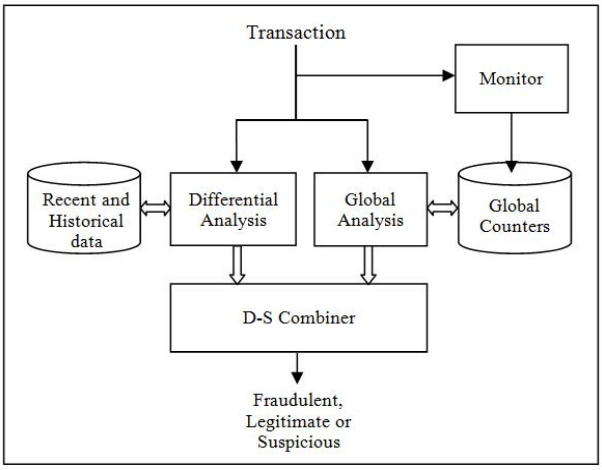

Figure 1: The mainstream design of the online banking fraud detection system [2].

- M. Carminati et al. [3] have described a system named as BankSealer for detection of online banking fraud. It is based on the semi-supervised and supervised approach. During the initial training phase, BankSealer support system builds straight forward models for spending habits of customers based on their previous transactions. BankSealer is also able to support data analysts at runtime as it provides ranking to the new banking transactions which show variation from the learned training profiles with an output which is easy to understand and has instant statistical meaning. It detects the banking fraud with 98% accuracy and the maximum time for calculation is 4 minutes.

- S. Nami and M. Shajari [4] have developed a method to detect fraudulent transactions. They have demonstrated a similarity measure on the basis of transaction time which assigns more weightage to recent transactions. They have used random forest algorithm in initial detection in the beginning and later minimum risk model has been applied in payment fraud detection involving costs. The experimental results performed on the real dataset taken from a bank showed that the recent transactions done by the cardholders have more impact to identify that whether the transaction is fraudulent or non-fraudulent.

- C. Guo et al. [5] have proposed a novel risk monitoring system for e-banking transactions. They have combined the score rules for online real-time transactions and offline historical transactions for the detection of fraud. They have integrated parallel big data frameworks Spark, Kafka and MPP Gbase with random forest machine learning algorithm to handle huge offline transaction logs. The proposed system shows effectiveness in handling real dataset of e-banking transactions.

- A.D. Pozzolo et al. [6] demonstrated the performance measures to detect credit card fraud detection. They have proposed a learning methodology that handles class imbalance and verification latency. They have put emphasis on training the classifier using the feedbacks received. They have illustrated the effect of class imbalance and concept drift on a real large dataset containing millions of credit card transactions.

- Z. Zhang et al. [7] have used convolutional neural network for detecting on online transaction fraud. They have presented a model in which convolutional neural network uses low dimensional features as input which saves the computational time. Their proposed model shows a significant improvement in the precision and recall as compared with the existing convolutional networks used for detection of fraud.

- A. Kumar and G. Gupta [8] has applied supervised machine learning techniques on the credit card transactions to detect the fraud. They have applied nearest neighbour, logistic regression, linear SVM, decision tree, random forest, naïve Bayes, RBF SVM in which the logistic regression outperforms all others.

- L. Zheng et al. [9] have proposed a logical graph of behavioural profiles of users based on their transactional history which detects whether a transaction is fraudulent or not. Their proposed method performs better than Markov chain models because it outlines the dissimilarities of user's behavioural profiles.

- G. Parthasarathy et al. [10] have applied various machine learning techniques like SVM, Random Forest, Decision Tree and back propagation classifiers on imbalanced datasets consisting of credit card transactions. SVM, Random Forest and Decision Tree classifiers show a very high accuracy in detection of fraud in credit card transactions.

- B. Lebichot et al. [11] have presented two methods that are based on deep neural networks. In first method, predictive and distribution related e-commerce features are merged to the face to face transactions to improve fraud predictions. The second one optimises the basic feature layer from the fraud tag predictor i.e. fraudulent vs genuine and the domain tag i.e. e-commerce vs face to face. Both methods were tested on a five month's real transactions dataset containing million transactions obtained from a large credit card issuer with three other methods. The second proposed method performs better than all the considered methods in terms of run time and performance.

The related works discussed so far have also been summarized in the following table.

Table 1: Comparison table on existing systems for detection of online banking fraud.

S. No.	Authors	Year	Method	Type of Fraud Detection System
1	Q. Lu and C. Ju [1]	2011	Weighted Support Vector Machine and Principal Component Analysis	Credit card fraud detection
2	S. Kovach and W. V. Ruggiero [2]	2011	Differential Analysis and Dempster's Rule	Fraud detection system for online banking
3	M. Carminati et al. [3]	2015	BankSealer	A decision support system for online banking fraud analysis and investigation
4	S. Nami and M. Shajari [4]	2018	Dynamic Random Forest and k-nearest neighbours	Cost-sensitive payment card fraud detection
5	C. Guo et al. [5]	2018	Kafka, Spark and MPP Gbase with random forest machine learning algorithm	A risk monitoring system for e-banking transactions
6	A.D. Pozzolo et al. [6]	2018	A novel learning strategy to effectively addresses concept drift, class imbalance and verification latency	Credit card fraud detection
7	Z. Zhang, X. Zhou, X. Zhang, L. Wang, and P. Wang [7]	2018	Convolutional Neural Network	Online Transaction Fraud Detection
8	A. Kumar and G. Gupta [8]	2018	Nearest Neighbour, Logistic Regression, Linear SVM, Decision Tree, Random Forest, Naïve Bayes, RBF SVM	Fraud Detection in Online Transactions
9	L. Zheng, G. Liu, C. Yan, and C. Jiang [9]	2018	Logical Graph	Transaction Fraud Detection System
10	G. Parthasarathy et al. [10]	2019	SVM, Random Forest, Decision Tree and back propagation classifiers	Credit card fraud detection
11	B. Lebichot et al. [11]	2019	Deep Neural Network	Credit card fraud detection

3. CONCLUSION

This review paper presents the various methods used for detection of online banking transactions fraud. It provides the insight of various research works conducted in the detection of online banking fraud which can be effectively applied to provide the solutions to the problems inherent in the detection and prevention of fraud. In future studies, the machine learning algorithms may be used with different combinations of input and output parameters for the detection of fraudulent banking transactions.

REFERENCES

1. Q. Lu and C. Ju, "**Research on credit card fraud detection model based on class weighted support vector machine**," *J. Converg. Inf. Technol.*, vol. 6, no. 1, 2011. https://doi.org/10.4156/jcit.vol6.issue1.8

2. S. Kovach and W. V. Ruggiero, "**Online banking fraud detection based on local and global behavior**," in *Proc. of the Fifth International Conference on Digital Society, Guadeloupe, France*, 2011, pp. 166–171.

3. M. Carminati, R. Caron, F. Maggi, I. Epifani, and S. Zanero, "**BankSealer: A decision support system for online banking fraud analysis and investigation**," *Comput. Secur.*, vol. 53, pp. 175–186, 2015. https://doi.org/10.1016/j.cose.2015.04.002

4. S. Nami and M. Shajari, "**Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors**," *Expert Syst. Appl.*, vol. 110, pp. 381–392, Nov. 2018. https://doi.org/10.1016/j.eswa.2018.06.011

5. C. Guo, H. Wang, H.-N. Dai, S. Cheng, and T. Wang, "**Fraud Risk Monitoring System for E-Banking Transactions**," in *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, 2018, pp. 100–105. https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00030

6. A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "**Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy**," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 8, pp. 3784–3797, Aug. 2018. https://doi.org/10.1109/TNNLS.2017.2736643

7. Z. Zhang, X. Zhou, X. Zhang, L. Wang, and P. Wang, "**A Model Based on Convolutional Neural Network for Online Transaction Fraud Detection**," *Security and Communication Networks*, 2018. [Online]. Available: https://www.hindawi.com/journals/scn/2018/5680264/abs/. https://doi.org/10.1155/2018/5680264

8. A. Kumar and G. Gupta, "**Fraud Detection in Online Transactions Using Supervised Learning Techniques**," in *Towards Extensible and Adaptable Methods in Computing*, S. Chakraverty, A. Goel, and S. Misra, Eds. Singapore: Springer Singapore, 2018, pp. 309–321. https://doi.org/10.1007/978-981-13-2348-5_23

9. L. Zheng, G. Liu, C. Yan, and C. Jiang, "**Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity**," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 3, pp. 796–806, Sep. 2018. https://doi.org/10.1109/TCSS.2018.2856910

10. G. Parthasarathy, L. Ramanathan, Y. JustinDhas, J. Saravanakumar, and J. Darwin, "**Comparative Case Study of Machine Learning Classification Techniques Using Imbalanced Credit Card Fraud Datasets**," *Available SSRN 3351584*, 2019. https://doi.org/10.2139/ssrn.3351584

11. B. Lebichot, Y.-A. Le Borgne, L. He-Guelton, F. Oblé, and G. Bontempi, "**Deep-Learning Domain Adaptation Techniques for Credit Cards Fraud Detection**," in *INNS Big Data and Deep Learning conference*, 2019, pp. 78–88. https://doi.org/10.1007/978-3-030-16841-4_8

12. B.Manoj, K.V.K.Sasikanth, M.V.Subbarao and V Jyothi Prakash, **Analysis of Data Science with the use of Big Data,** *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, volume 7 no 6, pp-87-90, 2018 https://doi.org/10.30534/ijatcse/2018/02762018

13.Apoorva Deshpande, Ramnaresh Sharma, **Multilevel Ensembler Classifier using Normalized Feature Based Intrusion Detection System,** *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, volume 7 no 5, pp 72-76, 2018. https://doi.org/10.30534/ijatcse/2018/02752018