Advances and Applications in Mathematical Sciences
Volume 20, Issue 12, 2021, Pages 3365-3378

A COMPREHENSIVE REVIEW OF FRAUDULENT ACTIVITY TRACKING AND DETECTION TECHNIQUES

N. PRABHA and S. MANIMEKALAI

Research Scholar
School of Computer Science
Thiruvalluvar University
Serkadu, Vellore, India

Department of Computer Science
Theivanai Ammal College for Women (Autonomous)
Villupuram, Tamil Nadu, India
E-mail: nprabhamca@gmail.com

Abstract

This review paper represents the various automated fraud detection techniques to categorize and comparison of important published articles. There are different methods and techniques are used to detect the multiple fraud activities in network security and online transactions. Nowadays, online fraud activities main issue in the network society. Because every second's thousands of activities online fraudulent activities held in the society. The fraudulent detection techniques classified as proactive and reactive methods. Based on the analysis of existing research the fraud detection techniques are implemented in the concepts of data mining, graph flow control, artificial intelligence, machine learning, Blockchain Technology and IoT etc. The novelty of this paper is presenting the type of relevant data-mining, graph flow techniques and electronic fraud-based fraud detection techniques and it's a comparison of standard methods with multiple parameters presented in this article. The parameters compared with classification, types of problems and predictions etc. The finally various issues, challenges and future feasible possible methodologies are presented.

1. Introduction

Fraud detection activities have been performed using different methods. In this review paper, the various types of frauds, and corresponding

2010 Mathematics Subject Classification: 68.

Keywords: Fraudulent Detection Techniques- data mining- Artificial intelligence- machine learning- Graph based prediction.

Received November 20, 2020; Accepted December 15, 2020

prevention methods are described using other techniques. The different kinds of fraud activities including insurance frauds, credit card frauds, web-based network fraud, customs frauds, telecommunication frauds etc. As per the report of javelin strategy and research [1] every time some fraudulent online activities going on in the online. So, a massive number of online prediction and tracking mechanisms are needed to society. As per the javelin research [1], the statistical report of fraudulent activities and other activities shown in figure 1 and top five fraudulent activities as per the report 2019 [1] shown in table 1.

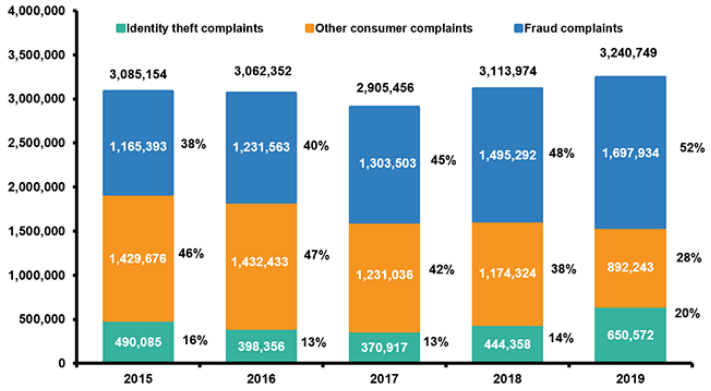

Figure 1. The statistical report of fraudulent activities [source: 1].

Table 1. Top five fraudulent activities.

S.No.	Top five Fraud Activities	Number of Reports	% of total top Five Activities
1	Credit card fraud- new accounts access	2,46,763	45.70%
2	Miscellaneous identity theft	1,66,875	30.9
3	Mobile telephone -new accounts access	44,208	8.2
4	Business or personal loan	43,919	8.1
5	Auto loan or lease	38,561	7.1

Different types of fraud detection techniques are grouped as per the activities of predictions. Some of the leading prediction classifications [4] are i. proactive ii. Reactive iii. Inductive detection and iv. deductive detection methods etc. The proactive [2] techniques find the fraud activates based on the symptoms of fraud, and before happening the fraud activities, this method is analysed. Some of the methods used in proactive approaches [3]

are Fourier transform and wavelength transform etc. The proactive strategy provides the solution after the fraudulent activity held. This method is used to find the source of the attractions or activities. The inductive method [4] searches the anomalies based on data mining techniques and digital analysis. This inductive method has a low cost, but the time complexity is very high. The Deductive processes higher cost compared to the inductive approach. The outcome of the deductive approach yields good results. The different models are used to identify fraud activities. The significant models of fraud activities are shown in figure 2.

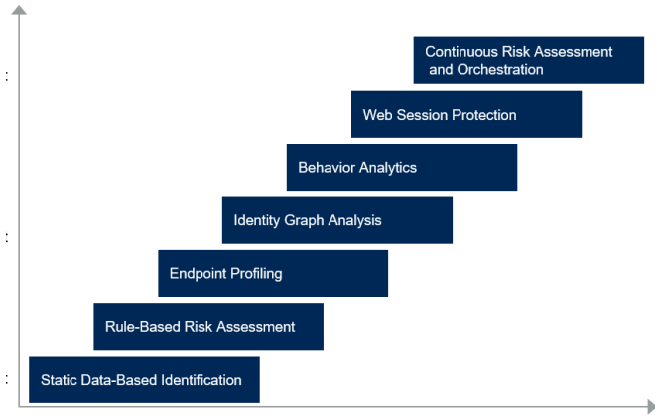

Figure 2. Different Models for Fraud detections.

As per the Albrecht et al. [4], three phases used to identify the risk such as Fraud search, Identify fraud investigation and fraud detection. The flow representation of three-phase risk identification is shown in figure 3. The fraud search is used to identify the fraud risk, symptoms and search the symptoms. The fraud investigation used to investigate the signs and pieces of evidence. The fraud detection used to identify and find the perpetrators and extend the activity tracking. The proactive Reactive Inductive detection and deductive detection methods are used different techniques and algorithms are used to trace the fraud detection. The trending techniques are data mining concepts, Artificial Intelligence (AI), Machine learning and Deep learning and Internet of Things (IoT). Those are some of the effective techniques mostly used to identify and trace the fraud detection. Each method used different parameters to trace and compare it with other methods. The author's john et al. [5] are mentioned some of the significant parameters for comparison for

tracing and fraudulent finding. The different researchers are proposed other comparison methods, but the time complexity, classification, and network overhead are the significant parameters to consider the comparisons.

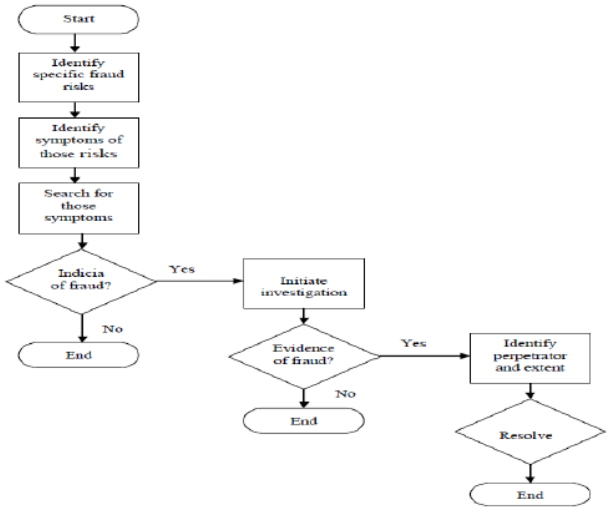

Figure 3. Phases of identifying the fraud.

The rest of this review paper organised as follows: Section II has provided different data mining techniques article and its comparison. Section III has artificial intelligence and machine and deep learning and its comparisons. Section IV has IoT techniques and its comparison. Section *V* has different future research directions in fraud detection, and finally, section VI has a conclusion.

II. Data Mining Techniques for Fraud Detection

Different data mining and associated techniques are used for finding fraud detection activities. The different authors are presented the various surveys related to fraud detection and tracing activities [5, 8]. In this section present various activities related data mining fraud detection techniques and its advantages and limitations. The B. Bai, J. Yen [6] presented the false financial statements generation in china and Asian countries. The object of this work is Classification and Regression Tree (CART), finding the false financial statements. The L. Bermudez [7] proposed simulation-based approach with Monte Carlo Bayesian Gibbs sampling for identifying

insurance fraud activities predictions using sample datasets. This approach is identified similar activities predicted using asymmetric logistic model. Mark Cecchini [9] proposed support vector machine (SVM) techniques for detecting fraud data using financial data with the help of machine learning. In this work various non-linear properties are used to found the fraud activities from the public organizations. P. Dechow et al. [10] proposed to find mismatching statements using logistic probability. The different dimensions are used to find such as accrual quality, non-financial measures, market-based measures, financial performance and off-balance sheet. The authors of [11, 12] predicted fraudulent financial statements using SOM and *K*-Means algorithm. The experimental and da predictions only past data used and not used real time data. The authors of [13, 14] used detecting the errors in the insurance claim and found the insurance fraud data predictions. The cost sensitive learning approach is used to find the data insurance data using past claim and past record data. The implementation purpose U. S health insurance data is used. The author proposed computational model for detecting fraud activities from the report. The analytical automation method is used to find and implementations 10-k filled past data used. The Holton C proposed text mining techniques for employee's fraud activities. Using this problem provided simple solutions for multiple problem.

The Ping-Feng Pa et al. [17] proposed SVM and CART method for analysis and predicting top management people fraud activities. This method is applied into various financial sectors such as banking and stock market etc. The implementation purpose the Taiwan stock market data is used. The Authors Suvasini Panigrahiet et al. [18] used find the credit card fraud detection using Fusion Approach: Dempster-Shafer and Bayesian Method with the help of past data. In this method four components are used such as rule adder, Dempster-Shafer, past database and Bayesian method. Using these four methods incoming, outgoing, normal, abnormal activities are detected and predicted. The authors Jon T. S. Quah [19] proposed real time credit card fraud detection with the help of intelligence techniques. The SOM and filter method are used to analysis the behaviour of the transactions. In this method implemented using the real time transactions of credit card. The authors D. Sanchez [20] proposed rule-based credit prediction using real time transactions with the help of behaviour analysis. The various methods used

for comparison in data mining techniques. In the table 1 it's summarized and the proposed method techniques of advantages and disadvantage are mentioned.

Table 1. Comparison of various methods.

S.No.	Techniques and References	Advantages	Limitations
1	Classification and Regression Tree (CART) [6].	Finding false financial statements and accuracy is improved.	Tracing mechanism not used.
2.	Simulation based approach using Monte Carlo Bayesian Gibbs sampling [7].	Identifying similar Insurance fraud activities.	The researches proposed to identify likelihood data to identify. Different situations it is not feasible.
3	Support Vector Machine [9]	Detected fraud data using non-linear properties.	The result of the Prediction used only historical data. The real data is not used.
4	Logistic Probability[10]	Mismatching between the statements in financial institution are found	The reasons for mismatch is not introduced.
5	Self-organising and K-Means, [11, 12]	Predicted fraudulent financial statements	Only past records are used to predict.
6	Cost Sensitive learning Approach [14]	Predicted insurance false claim and insurance fraud prediction.	Implementation U.S based past health insurance data is used.
7	Computational Model for fraud detection.[15]	The analytical method is used to predict and analysis the fraudulent and non- fraudulent data or file.	The 10-k filling data used to analysis and classifications' this method also used only past existing data
8	Text mining Techniques and naïve Bayes model [16]	Text mining techniques are used to identify the employee's fraud risk	The archived e-mail data and untapped data is used for implementations.
9	SVM Techniques and CART [17]	Detected top Management team fraud	The Implementations Taiwan 75 firms stock mark

		data. This method applied in banking and financial institutions.	data is used.
10	Fusion Approach: Dempster–Shafer and Bayesian Method [18]	Credit Card fraud Prediction	The implementation and result, the past data is used.
11	SOM and Filter [19]	Credit card fraud transactions Prediction	Real Time Prediction but not proactive method.
12	Association Rules [20]	Credit card fraud transactions using behaviour analysis	Real time Prediction but not proactive method

III. Graph Based fraud Detection

In recent years a number of methods have been introduced to predict the receipt of fraudulent complaints. Graph-based fraud detection [GBFD] is one of the most important ways to predict corruption and diversity [21]. Some of the research literature on fraud detection [22-24] and graph-based applications have been published [25, 26, 27, 28]. This section summarizes the unpredictable predictions of the graph. Chandola et al. [21], different exploration strategies are explored in different ways, using different schemes and challenges. Similarly, the authors Bhattacharyya et al., Abdallah et al. [22], [23], and Ngai et al. [24], which specifically examined fraudulent detection strategies to detect fraud in various details between different financial sectors, also belongs to a different domain. Our focus on discovery studies that do not incorporate graph-based methods is consistent with studies conducted by Savage et al. [25], Akoglu et al. [26], Anand et al. [27], no Ranshous et al. [28]. The review by Savage et al.'s [25] focuses on existing computerized techniques for detecting different types of variations (such as anomalous nodes, edges, or subgraphs) on online social networks (OSNs). They summarize the process of differential detection by OSNs in two steps: (i) the selection and calculation of network features and (ii) the separation of visuals from this feature space. Due to the lack of publicly available data, reviewers also noted that the proposed solutions were tested on a limited number of data points. This limitation has led them to question whether the solutions are likely to be "extremely adequate" for a particular type of anomaly, therefore, the results may not apply to a wide range of data or

problems. Akoglu et al. [26] also examined GBAD methods with a focus on them the difficulties involved in finding inaccuracies and the importance of graphical approaches to solving proposed challenges. They analysed the technical aspects and interpretations of these methods and discussed the use of GBAD methods in specific real-world contexts, including the discovery of fraud. In their conference paper, Anand et al. [27] reviewed several studies on the detection of OSN malpractice and divided them into two main categories: behavioural-based methods, user performance analysis and interaction, and architectural-based methods, focusing on identifying specific types of network structures, such as structures, clusters or communities, stars, and ego networks. In a review of Ranshous et al.'s [28], negative findings on dynamic social networks were the main focus, which included a critical discussion of the technical aspects of existing methods and types of problems identified. However, none of these updates have scrutinized the graph-based approach to finding fraud to identify the latest problems and challenges, a gap this paper aims to close. In a systematic review of the literature, we list the research practices, methods, and key challenges when using GBAD methods for detecting fraud.

Our review of existing activities contributes to four areas of GBAD research on fraud detection. First, we propose a framework for categorizing GBAD research studies and identification challenges. The proposed framework provides a systematic investigation of investigators as well provides an in-depth understanding of how GBAD strategies can be used to Analyze and detect fraud. Secondly, we include the availability of existing index documents so that users can inform connections between their data network type, types of malfunctions, and appropriate graph-based approaches to their app's site requirements. IV Electronics Card fraud Detection Techniques Credit card fraud strategies are divided into two general categories: fraud analysis (malicious detection) and user behaviour analysis (malicious detection). The first group of strategies deals with targeted segregation work at the transaction level. In these methods, the transaction is labelled as deceptive or standard based on prior historical data. This database is used to create segment models that can predict the status (normal or fraud) of new records. There are many ways to create a model for common classification functions such as law enforcement [29], cutting trees [30] and neural networks [31].

The second method involves unregulated methods based on account behaviour. In this way the transaction is obtained if it is contrary to the normal behaviour of the user. This is because we do not expect fraudsters to behave in the same way as the account holder or know the owner's behaviour model [32]. For this purpose, we need to remove the official user behaviour model (e. user profile) from each account and detect fraudulent activities according to it. Comparing the new behaviour with this model, activities that are sufficiently different are classified as fraudulent. Profiles may contain account activity details; such as vendor types, price, location and transaction time, [33]. This method is also known as anonymous acquisition. It is important to highlight the major differences between user behavioural analysis and fraud analysis methods. The method of fraud analysis can detect known fraudulent tactics, with a low positive rate lie. These programs issue the signature and model of fraud strategies displayed in the oracle database and can easily detect any fraud, the system is currently dealing with. If the test data does not have fake signatures, no alarm is raised. Therefore, the false positive rating can be greatly reduced. However, since the study of the deceptive analysis system (e.g. classification) is based on limited and defined fraud records, it is impossible to detect novel fraud. As a result, lies can be very high depending on how clever the fraudsters are. User behavioural analysis, on the other hand, focuses more on the problem of finding novel tricks.

These methods do not require fraudulent patterns, but instead compare the revenue functions with a structured model of legal user behaviour. Any activity that is different from the model will be considered a possible fraud. Or, the methods of user behaviour analysis are powerful at discovering new tricks, they actually suffer from high levels of false alarms. Moreover, if fraud occurs during training, these deceptive behaviours will be introduced into the basic mode and considered normal in further analysis [34, 35]. In this section we will briefly present some of the current fraudulent scams used in credit card fraud operations, and the pros and cons of each method will be discussed.

V. Future Direction of Research in Fraud Detection

Different techniques and methods are introduced to solve and trace the fraud detection problems. But different issues and difficulties are open for future research. The different researchers are mentioned some of the difficulties [36, 37]. In this section, present various issues in the credit fraud detection, challenges, difficulties and future direction of research are mentioned below.

A. Various Issues and Challenges of fraud Detection: Imbalanced data: The data has imbalance in nature because small data and transactions also fraudulent. In this situation's prediction level is very risk [38].

Misclassification importance: The prediction of misclassification is very important because normal mistake and classification between randomly doing mistake is very important in the fraud detection [39].

Overlapping data: In many transactions the false positive, false negative classification detection is very difficult and it is the key challenging in fraud detection [40]. Proactive and Reactive Detection: The most of the existing system based on only reactive approach. But the tracing of proactive is very difficult and level of finding also one of the challenging one [40, 41].

Lack of adaptability: Behaviour-based Analysis is used to find the fraud detection. Based on the classification, it is very difficult to detect the new patterns of normal, and abnormal behaviours in prediction.

B. Future Direction of Research: The challenges and issues are resolved using different research methodologies. Some of the trending research methodologies for solving these issues are as follows;

1. Data Mining and Classification Techniques: The different financial and fraud activities are predicted using data mining and classification techniques. Some of the main techniques to predict are discriminant analysis, NN analysis, Naïve Bayes, Profit model, etc.

2. AI, Machine Learning and Deep Learning: The AI, Machine learning and deep learning are some of the trending methodologies. Using these methodologies different data analysis and predicted in different situations such as Past, current and future positions of data [43-45].

3. Blockchain Technologies: Using the current blockchain technologies already applied into cryptocurrencies and record of all transaction of data. With the help of blockchain easily we can predict and analysis the different data in transactions.

4. Other Methodologies: The other methodologies are such as graph flow, decision-making system, fuzzy system and IoT are some of the methods that are used to predict and Analyze the data in the transaction. Especially, graph flow used to predict proactive and reactive methods.

VI. Conclusion

Each and every second's thousands of financial fraud activities occurs in the world, to rectify the fraud activities using fraud detection techniques. It's classified into two methods proactive and reactive. The proactive methods are used to prevent fraud activities before it occurs. The reactive activities are used to trace when it is occurs. There are various techniques used to predict fraud activities such as data mining and AI techniques, Graph-based tracing are the most dominating techniques to trace. The techniques of the existing research the past data is used for implementation and to simulate the fraud statements. The real-time fraud data prediction is an important one because the necessary actions to be taken immediately, or the card to be stopped immediately. The different issues, future direction of the research and feasible methodologies presented in section

References

[1] https://www.experian.com/blogs/news/2019/01/30/global-identity-and-fraud-report/

[2] Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks.

[3] H. R. Davis, Fraud 101: Techniques and Strategies for Detection. NY: John Wiley and Sons, Inc. 2000.

[4] W. S. Albrecht, C. Albrecht and C. Albrecht, Fraud Examination and Prevention, H. Mason, Thomson Southwestern 2006.

[5] A. John and T. Sivakumar, DDoS: Survey of Traceback Methods, International Journal of Recent Trends in Engineering ACEEE (Association of Computer Electronics and Electrical Engineers) 1(2) (2009).

[6] B. Bai, J. Yen and X. Yang, False Financial Statements: Characteristics of China's Listed Companies and CART Detecting Approach, International Journal of Information Technology and Decision Making 7 (2008), 339-359.

[7] L. Bermúdez, J. Pérez, M. Ayuso, E. Gómez and F. Vázquez, A Bayesian Dichotomous Model with Asymmetric Link for Fraud in Insurance, Insurance: Mathematics and Economics 42 (2008), 779-786.

[8] S. Bhattacharyya, S. Jha, K. Tharakunnel and J. C. Westland, Data Mining for Credit Card Fraud: A Comparative Study, Decision Support Systems 50 (2011), 602-613.

[9] M. Cecchini, H. Aytug, G. Koehler and P. Pathak, Detecting Management Fraud in Public Companies, Management Science 56 (2010), 1146-1160.

[10] P. Dechow, W. Ge, C. Larson and R. Sloan, Predicting Material Accounting Misstatements, Contemporary Accounting Research 28 (2011), 1-16.

[11] Q. Deng and G. Mei, Combining Self-Organizing Map and *K*-Means Clustering for Detecting Fraudulent Financial Statements, In IEEE International Conference on Granular Computing (2009), 126-131.

[12] C. Gaganis, Classification Techniques for the Identification of Falsified Financial Statements: A Comparative Analysis, International Journal of Intelligent Systems in Accounting and Finance Management 16 (2009), 207-229.

[13] A. Gepp, J. H. Wilson, K. Kumar, S. Bhattacharya, A Comparative Analysis of Decision Trees Vis-a-vis Other Computational Data Mining Techniques in Automotive Insurance Fraud Detection, Journal of Data Science 10 (2012), 537-561.

[14] R. Ghani and M. Kumar, Interactive Learning for Efficiently Detecting Errors in Insurance Claims, In Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data mining (2011), 325-333.

[15] F. H. Glancy and S. B. Yadav, A Computational Model for Financial Reporting Fraud Detection, Decision Support Systems 50 (2011), 595-601.

[16] C. Holton, Identifying Disgruntled Employee Systems Fraud Risk Through Text Mining: A Simple Solution for a Multi-Billion Dollar Problem. Decision Support Systems 46 (2009), 853-864.

[17] P. F. Pai, M. F. Hsu and M. C. Wang, A Support Vector Machine-Based Model for Detecting Top Management Fraud, Knowledge-Based Systems 24 (2011), 314-321.

[18] S. Panigrahi, A. Kundu, S. Sural and A. Majumdar, Credit Card Fraud Detection: A Fusion Approach Using Dempster-Shafer Theory and Bayesian Learning, Information Fusion 10 (2009), 354-363.

[19] J. T. Quah and M. Sriganesh, Real-Time Credit Card Fraud Detection Using Computational Intelligence, Expert Systems with Applications 35 (2008), 1721-1732.

[20] D. Sánchez, M. Vila, L. Cerda and J. Serrano, Association Rules Applied to Credit Card Fraud Detection, Expert Systems with Applications 36 (2009), 3630-3640.

[21] V. Chandola, A. Banerjee and V. Kumar, Anomaly detection: a survey, ACM Comput. Surv. 41(3) (2009), 1-58.

[22] S. Bhattacharyya, S. Jha, K. Tharakunnel and J. C. Westland, Data mining for credit

card fraud: a comparative study, Decis. Support. Syst. 50(3) (2011), 602-613.

[23] A. Abdallah, M. A. Maarof and A. Zainal, Fraud detection system: a survey, J. Netw. Comput. Appl. 68 (2016), 90-113.

[24] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen and X. Sun, The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature, Decis. Support. Syst. 50(3) (2011), 559-569.

[25] D. Savage, X. Zhang, X. Yu, P. Chou and Q. Wang, Anomaly detection in online social networks, Soc. Networks 39 (2014), 62-70.

[26] L. Akoglu, H. Tong and D. Koutra, Graph based anomaly detection and description: asurvey, Data Min. Knowl. Disc. 29(3) (2015), 626-688.

[27] K. Anand, J. Kumar and K. Anand, Anomaly detection in online social network: a survey, ICICCT 2017, IEEE, (2017), 456-459.

[28] E. Ranshous, S. Shen, D. Koutra and S. Harenberg, Anomaly detection in dynamic networks: a survey, Comput. Stat. 7(3) (2015), 223-247.

[29] Khyati Chaudhary, Jyoti Yadav and Bhawna Mallick, A review of Fraud Detection Techniques:Credit Card, International Journal of Computer Applications 45(1) (2012).

[30] Michael Edward Edge, R. Pedro and Falcone Sampaio, A survey of signature based methods forfinancial fraud detection, Journal of Computers and Security 28 (2009), 381-394.

[31] Linda Delamaire, Hussein Abdou and John Pointon, Credit card fraud and detection techniques: a review, Banks and Bank Systems 4(2) (2009).

[32] Salvatore J. Stolfo, David W. Fan, Wenke Lee and Andreas L. Prodromidis, Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results; Department of Computer Science Columbia University, 1997.

[33] Maes S. Tuyls K. B. Vanschoenwinkel and B. Manderick, Credit Card Fraud Detection Using Bayesian and Neural Networks, Vrije University Brussel-Belgium; 2002.

[34] Andreas L. Prodromidis and Salvatore J. Stolfo, Agent-Based Distributed Learning Applied to Fraud Detection; Department of Computer Science-Columbia University; 2000.

[35] Salvatore J. Stolfo, Wei Fan, Wenke Lee and Andreas L. Prodromidis, Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAM Project, 0-7695-0490-6/99, 1999 IEEE.

[36] Tahereh Pourhabibi et al., Fraud detection: A systematic literature review of graph-based anomaly detection approaches, Decision Support Systems 133 2020.

[37] Z. Zojaji, R. E. Atani and A. H. Monadjemi, A survey of credit card fraud detection techniques: data and technique oriented perspective, Cryptography and Security, 2016.

[38] Roy, Abhimanyu, et al., Deep Learning Detecting Fraud in Credit Card Transactions, 2018 Systems and Information Engineering Design Symposium (SIEDS), 2018, doi:10.1109/sieds.2018.8374722.

[39] Jiang, Changjun et al., Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism, IEEE Internet of Things Journal 5 (2018), 3637-3647.

[40] Salvatore J. Stolfo, David W. Fan, Wenke Lee and Andreas L. Prodromidis, Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results, Department of Computer Science Columbia University; 1997.

[41] Michael Edward Edge and Pedro R. Falcone Sampaio, A survey of signature based methods for financial fraud detection, computers and security 28 (2009), 381-394.

[42] Yufeng Kou, Chang-Tien Lu and Sirirat Sinvongwattana, Survey of Fraud Detection Techniques, Proceedings of the 2004 IEEE International Conference on Networking, Sensing and Control.

[43] A. John, M. Sugumaran and R. S. Rajesh, Performance analysis of the past, present and future indexing methods for spatio-temporal data, 2nd International Conference on Communication and Electronics Systems (ICCES), p.no: 645-649, IEEE, 2017.

[44] John Ayeelyan, Sugumarn Muthukumarasamy and Rengan Sivagurunathan Rajesh, DTNH Indexing Method: Past Present and Future Data Prediction for Spatio-Temporal Data, International Journal of Intelligent Engineering and Systems 10(3) (2017) DOI: 10.22266/ijies2017.0630.48.

[45] John and T. Sivakumar, Ddos: Survey of traceback methods, International Journal of Recent Trends in Engineering 1(2) (2009).