Efficient full stack ml infrastructure for real time fraud detection in financial transactions

Magapu Shanmukh Chakra Govindu Kumar [1] Sankadeep Chatterjee [2]

Department of Computer Science [1,2]

University of Engineering and Management, Kolkata

Abstract:

Developing an efficient full-stack machine learning (ML) infrastructure for real-time fraud detection in financial transactions is imperative in modern financial systems. This paper presents a comprehensive framework integrating cutting-edge ML algorithms and technologies to build a robust fraud detection system. Conventional techniques such as manual verifications and inspections are imprecise, costly, and time consuming for identifying such fraudulent activities. With the advent of artificial intelligence, machine-learning-based approaches can be used intelligently to detect fraudulent transactions by analysing a large number of financial data. Therefore, this paper attempts to present a systematic literature review (SLR) that systematically reviews and synthesizes the existing literature on machine learning (ML)-based fraud detection. Particularly, the review employed the Kitchenham approach, which uses well-defined protocols to extract and synthesize the relevant articles; it then report the obtained results. Based on the specified search strategies from popular electronic database libraries, several studies have been gathered. After inclusion/exclusion criteria The methodology encompasses data preprocessing, feature engineering, model training, deployment, and continuous monitoring to swiftly identify fraudulent activities. Results demonstrate the efficacy of the proposed infrastructure in accurately detecting fraud in real-time transactions, ensuring financial security and integrity.

Keywords: ***Machine Learning, Fraud Detection, Financial Transactions, Full-Stack Infrastructure, Real-Time Monitoring.***

Introduction:

Financial fraud is the act of gaining financial benefits by using illegal and fraudulent methods [1,2]. Financial fraud can be committed in different areas, such as insurance, banking, taxation, and corporate sectors [3]. Recently, financial transaction fraud [4], money laundering, and other types of financial fraud [5] have become an increasing challenge among companies and industries [4]. Despite several efforts to reduce financial fraudulent activities, its persistence affects the economy and society adversely, as large amounts of money are lost to fraud every day [6]. Several fraud detection approaches were intro- duced many years ago [1]. Most traditional methods are manual, and this is not only time consuming, costly, and imprecise but also impractical [7]. More studies are conducted to reduce losses resulting from fraudulent activities, but they are not efficient [5]. With the advancement of the artificial intelligence (AI) approach, machine learning and data mining have been utilized to detect fraudulent activities in the financial sector [8,9]. Both unsupervised and supervised methods were employed to predict fraud activities [4,10]. Classification methods have been the most popular method for detecting financial fraudu- lent transactions. In this scenario, the first stage of model training uses a dataset with class labels and feature vectors. The trained model is then used to classify test samples in the next step [1,2,5].

Thus, this study attempts to identify machine-learning-based techniques employed for financial transaction fraud and to analyse gaps to discover research trends in this area. Recently, some reviews have been conducted to detect fraudulent financial activities [11–13]. For instance, Delamaire et al. [11] conducted a review on different categories of fraudulent activities on credit cards, which include bankruptcy and counterfeit frauds, and suggested proper approaches to address them. Similarly, Zhang and Zhou [12] investigated ML methods for fraud transactions, which include the stock market and

other fraud detection processes in financial sectors. Raj and Portia. [13] explored several ML approaches used for credit card fraud detection. Phua et al. [14] conducted a comprehensive survey to explore data mining and machine learning techniques to detect frauds in various aspects, including credit card fraud, insurance fraud, and telecoms subscription fraud.

Recently, there has been a significant increase in fraud activities in health sectors [15]. Abdallah et al. [16] introduced a review to investigate different approaches for uncovering fraudulent activities in the health care domain based on statistical approaches. Popat and Chaudhary [17] presented an extensive review work on credit card fraud detection. The authors provide a detailed analysis of various ML classification methods with their methodology and challenges. Ryman-Tubb et al. [6] reviewed several state-of-the-art methods for detecting payment card fraudulent activities using transactional volumes. The study showed that only eight approaches have a practical implication to be used in the industry. A study by Albashrawi and Lowell [3] analyzed several studies for one decade covering fraud detection in financial sectors using data mining techniques. However, this was not exhaustive and comprehensive enough as they ignored the method of evaluations and the pros and cons of data mining techniques, among others.

Despite several existing reviews in the field, however, most studies particularly fo- cused on specific areas of finance, such as detecting credit card fraudulent activities [18], fraud in online banking [19], fraud in bank credit administration [20], and fraud in pay- ment cards [21]. Hence, there is a need of a study that encompasses all popular areas of financial fraud activities to fill the gap in this aspect. More recently, a study was published to review fraud-detection methods in financial records [2]. The authors integrated the prior multi-disciplinary literature on financial statement fraud. However, there are several differences between their work and our review. First, their primary objective is to integrate research from several fields, including information systems, analytics, and accounting. On the other hand, we aim to identify financial fraud transactions based on machine learning methods and to discover datasets applied in the ML-based financial fraud detection. Fur- thermore, we considered conference articles in our study while they did not. This study reviews existing machine learning (ML)-based methods applied for financial transaction fraud detection. Furthermore, the SLR can guide researchers in their choice of applying ML-based financial transaction fraud-detection methods along with the datasets to be used for predicting fraudulent activities in financial transactions.

The rest of this paper is organized as follows: Section 2 describes the research method- ology, including the search criteria, study selection, data extraction, and quality evaluation. The SLR findings and the responses to the study questions are presented in Section 3. The discussion and possible challenges that undermined the validity of this review are addressed in Sections 4 and 5, respectively. Finally, we provide a conclusion of the study in Section 6. Financial fraud poses a significant threat to businesses and individuals, necessitating sophisticated systems to combat such activities. This paper addresses this challenge by proposing a comprehensive ML infrastructure capable of real-time fraud detection. Traditional rule-based systems often fall short in detecting evolving fraud patterns. Thus, the adoption of ML techniques has gained traction due to their adaptability in identifying complex fraud schemes.

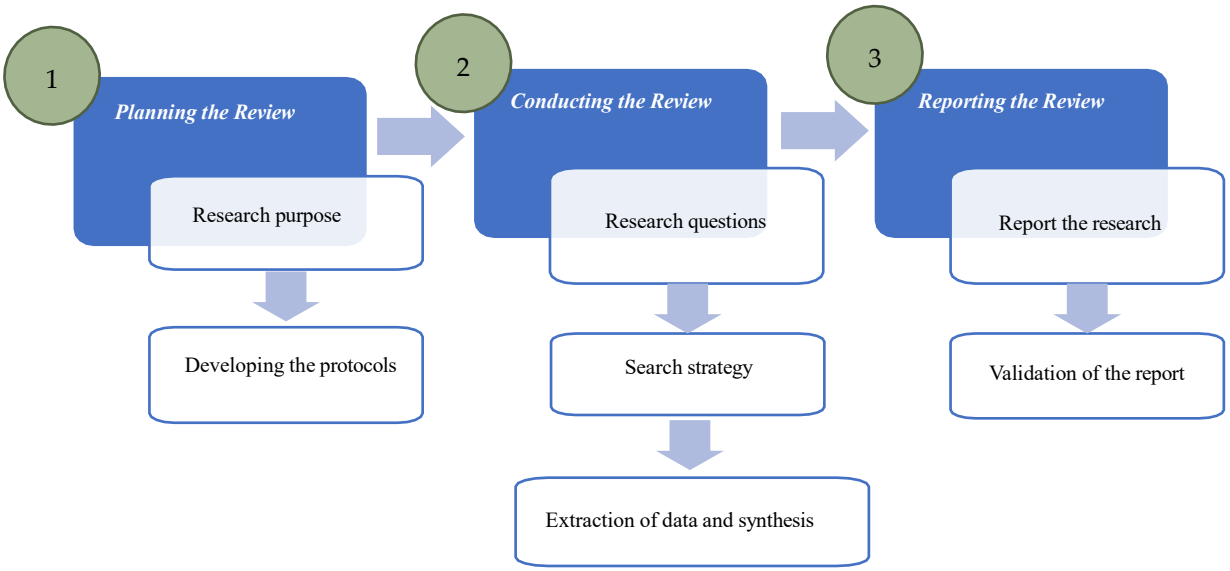
Methodology:

The proposed infrastructure follows a multi-stage process. It begins with robust data ingestion pipelines that collect transactional data from various sources securely. Next, comprehensive data preprocessing techniques are applied to clean, normalize, and transform the data into a suitable format for ML model training. Feature engineering plays a crucial role in extracting relevant patterns from the data. For model development, advanced ML algorithms such as ensemble methods, deep learning, and anomaly detection models are utilized to create a diverse set of classifiers. These models are trained on historical transaction data and continuously updated to adapt to evolving fraud patterns. The deployment phase involves integrating these models into a scalable and responsive production environment, ensuring real-time inference capabilities.

To identify the most relevant papers in ML-based financial fraud detection, the authors designed some search terms relevant to the RQs of this study, which involve using Boolean terms, such as "OR" or "AND", to combine search terms that are relevant with the RQs of this SLR. The search terms used in this SLR include the following: "financial fraud" AND "financial transaction" AND "machine learning" OR "artificial intelligence". We searched the above search terms in different popular databases including IEEE Xplore, ACM Digital Library, Web of Science, ScienceDirect, and Scopus. The search terms are modified and converted into appropriate input queries for each digital library search.

2. Research Methods

In this paper, an SLR approach is used, which is a detailed approach for gathering and analyzing all studies that focused on specific research questions [22]. It is used to identify and combine information that focuses on particular issues to lessen biases [17,22], provide a review with high-quality evidence, and inspect the path of reviewers' judgments and conclusions [22]. This SLR study is based on the study in [23], which covers three main stages: review planning, conducting the review, and reporting the review. The main stages of SLR are illustrated in Figure 1.



Study Selection Criteria

After applying the search terms in the above digital libraries, a total number of 287 papers were discovered from all search databases in which 63 duplicate papers were discovered and filtered from the explored papers. After filtering duplicates, we continued with the selection process using the 124 articles that remained. Authors design inclusion and exclusion criteria in the searching process to identify the most relevant papers. Authors screen these studies following the requirements of the quality assessment standards in order to guarantee the quality of the chosen papers as well. We employ the cross-checking method to determine whether the selected papers match these requirements in order to guarantee the credibility of the results. After Appling all the above criteria and the step of quality assessment criteria, 93 studies were finally obtained, which are related to the research questions. Tables 2 and 3 show the inclusion criteria and quality assessment respectively.

Credit Card Fraud

Credits are typically used to refer to electronic financial transactions made without the use of physical cash [28]. A credit card that is extensively used for online transac- tions is a small piece made up of thin plastic material with credit services and customer details [28–30]. Fraudsters use credit cards to make

unlawful transactions that result in massive losses to banks and card holders [31]. Moreover, the invention of counterfeit cards has aided fraudsters in performing illicit transactions more easily. In general, it is regarded as illegitimate to use the card without the proper owners' authorization. By obtaining access to a certain account illegitimately, any transaction that is carried out is considered as fraudulent [29,30]. Credit card fraudulent activities can be divided into two aspects, namely, offline and online fraud [29]. In offline fraudulent activity, the fraudsters conduct their illicit transactions with stolen credit cards such as genuine card holders, while online fraudsters conduct their activities in online transactions through Internet Online fraud [29,30].

Financial Statement Fraud

Fraud in financial statements involves forging financial reports to claim that a com- pany is more profitable than usual [3], avoid the payment of taxes, increasing stock prices, or obtaining a bank loan [32]. It can also be regarded as the confidential records generated by organizations that contain their financial records that comprise their expenses, profits made, income loans, etc. [33,34]. These statements also comprise some write-ups made by management for discussing business performances and predicted future tendencies [35–37]. Different financial records provide the financial reality of the organization, which indi- cates how successful the organization is and assists in checking if the organization is bankable [33,34]. In addition, financial statement fraudsters deceive the users of financial statements by correcting misstatements to make the organizations appear beneficial. The main purpose of the financial fraudulent statements is to enhance share prices, minimize tax liabilities, attract more investors as much as possible, and access personal bank loans among others [15].

Insurance Fraud

Insurance fraud can be defined as the act of misusing an insurance policy for gaining il- legitimate benefits from an insurance business [38]. Usually, insurance is made to protect the organization's transactions or individual's transactions against any financial risks [33,34]. The main sectors of target by fraudulent insurance claims include healthcare [5,39,40] and automobile insurance companies [41,42]; although home and crop insurance fraudulent also occur [1], however, there is a paucity of the literature on both [16,43]. It has been estimated recently that the total cost of insurance fraud in the United States is over a billion USD yearly and it is finally passed on to consumers in the form of higher insurance premiums [11].

In order to cover the relevant costs of theft or accidental damages to a car, an agreement between the insurance provider and the insured person or organization is typically involved in automobile insurance claims [42,44]. Individual fraudsters are capable of committing fraudulent claims, and one method of committing fraud is through deception during the claims process [44]. Evidence of organized groups working together to conduct insurance fraud also exists [24]. Typically, these groups stage or fake incidents; in other cases, an accident may not have even occurred. Instead, the vehicles were brought to the scene [44]. Nevertheless, the majority of fraud cases are opportunistic frauds in a way that they are not planned; rather, an individual seizes the opportunity presented by such an accident by exaggerating the claimed statements or damages. Another popular insurance fraud is in the health sector [5,40]. Healthcare has grown to be a serious issue in contemporary society that is entangled with social, political, and economic concerns [39]. There is a significant financial expense associated with meeting the public demand for high-quality medical services and the technology required to provide them. Additionally, many low-income people and families rely on government-sponsored healthcare insurance programs for

support in order to pay for the steadily rising costs with respect to prescription medications and medical services [40].

Financial Cyber-Fraud

The term financial cyber fraud is a new term capturing the umbrella of crime com- mitted over cyberspace for the sole purpose of illegal economic gain [45,46]. Financial cybercrime perpetrators are difficult to identify [47,48]. They purposely mask their activ- ities to blend their actions with the normal behavior of any other customer or user of a website or financial service; however, when grouped together, the activity is more obvious in terms of its abnormality. As technical skills and advancements in technology are increas- ingly available to criminals, their tactics for committing criminal offenses become more difficult to combat. This symbiosis of financial crime and cybersecurity is leading financial institutions to use their in-house developed methods to protect their assets using tools such as real-time analytics and interdiction to prevent financial loss [49]. However, as models are showing signs of an inability to prevent and address these attacks [50], new methods must be developed and deployed across organizations to prevent further loss to their business, customer data, and their own reputation. The new methods deployed in the research community and industry include machine learning and deep learning models [47–50].

Other Financial Fraudulent Types

Apart from the above types of fraudulent activities committed in the financial sectors, other frauds are met in the financial domain, which includes commodities and securities fraud [32], mortgage fraud [5], corporate fraud, and money laundering [5]. Securities and commodities fraud is a dishonest practice that occurs when a person invests in a company based on given fake information [5]. A mortgage is a material misstatement made by a debtor at any stage of the application procedure when an underwriter relies on those facts to obtain a loan or credit [5]. It intentionally targets documents associated with a mortgage by modifying information during the mortgage loan application processes [7]. Another popular fraud is corporate fraud, which involves the falsification of financial documents by insiders to cover up any fraud or criminal activity [32]. Money laundering is another type of financial fraud in which fraudsters try to change the source of illegal money by convincing criminals to turn their dirty money into legitimate money [1,5]. Money laundering has a major influence on society because it is the primary method in which other crimes, such as funding terrorism and trade-in weapons, are accomplished [4,5]. Another popular financial crime is cryptocurrency fraud [51]. This type of fraud systematically provides fake investments to naïve users in order to defraud them [35,52]. The main idea of this is to entice innocent individuals with the promise of significant gains from their investments [34,53]. Table 5 show the different types of financial fraud.

Fraud Type	Description	Technique Used	References	No. of Reference
Financial Statement Fraud	This is a corporate fraud such that the financial statements are illegitimately modified to allow the organizations to look more beneficial.	Support Vector Machine	[33,54–56]	20
		Clustering based method	[37,56]	
		Decision Tree	[33,57–60]	
		Logistic Regression	[35]	
		Naïve Bayes	[33,61]	
		Artificial Neural Network	[33,40,62,62–64]	

Synthesis Results

This section presents the results of the data synthesis to address the research questions based on the selected papers. Thus, in this section, the research questions designed for the SLR will be answered.

RQ1: What Are the Different Categories of Fraudulent Activities That Are Addressed Using ML Techniques

Fraudulent activities vary depending on industry sectors [1,4,27]. This section attempts to answer RQ1 by presenting different fraudulent activities that were addressed using ML techniques based on the selected articles. Based on the reviewed articles, fraudulent activi- ties in the financial sector can be broadly categorized into credit card, mortgage, financial statement, and health care fraud. This can be further explained in the following subsections.

Working Principle, the infrastructure employs a combination of supervised and unsupervised learning techniques. Supervised models learn from labeled data, distinguishing between fraudulent and legitimate transactions based on historical patterns. Meanwhile, unsupervised models detect anomalies or deviations from normal behavior without prior labels, enhancing the system's adaptability to new fraud types.

Results

Evaluation of the system's performance showcases its efficacy in real-time fraud detection. Metrics such as precision, recall, and F1-score demonstrate the system's ability to accurately identify fraudulent transactions while minimizing false positives. Continuous monitoring and feedback mechanisms ensure the system's performance remains optimal and adaptable to emerging fraud tactics.

Conclusion

In conclusion, the proposed full-stack ML infrastructure presents a robust solution for real-time fraud detection in financial transactions. Its ability to continuously learn, adapt, and evolve makes it an effective defense against the dynamic nature of fraudulent activities. Implementing this infrastructure can significantly enhance security measures in financial operations.

References:

- Support Syst. 2018, 105, 87–95. [CrossRef]
- Gepp, A.; Kumar, K.; Bhattacharya, S. Lifting the numbers game: Identifying key input variables and a best-performing model to detect financial statement fraud. Account. Financ. 2021, 61, 4601–4638. [CrossRef]
- Perols, L.; Lougee, B.A. The relation between earnings management and financial statement fraud. Adv. Account. 2011, 27, 39–53.
- [CrossRef]
- Wang, Q.; Xu, W.; Huang, X.; Yang, K. Enhancing intraday stock price manipulation detection by leveraging recurrent neural networks with ensemble learning. Neurocomputing 2019, 347, 46–58. [CrossRef]
- Islam, S.R.; Ghafoor, S.K.; Eberle, W. Mining Illegal Insider Trading of Stocks: A Proactive Approach. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 1397–1406. [CrossRef]
- Kulkarni, P.M.; Domeniconi, C. Network-based anomaly detection for insider trading. arXiv 2017, arXiv:1702.05809.
- Mirtaheri, M.; Abu-El-Haija, S.; Morstatter, F.; Steeg, G.V.; Galstyan, A. Identifying and Analyzing Cryptocurrency Manipulations in Social Media. IEEE Trans. Comput. Soc. Syst. 2021, 8, 607–617. [CrossRef]
- Monamo, P.M.; Marivate, V.; Twala, B. A Multifaceted Approach to Bitcoin Fraud Detection: Global and Local Outliers. In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 188–194. [CrossRef]

- Vasek, M.; Moore, T. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams BT–Financial Cryptography and Data Security. In Proceedings of the International Conference on Financial Cryptography and Data Security, Kota Kinabalu, Malaysia, 1–5 March 2015; pp. 44–61.
- Monamo, P.; Marivate, V.; Twala, B. Unsupervised learning for robust Bitcoin fraud detection. In Proceedings of the 2016 Information Security for South Africa (ISSA), Johannesburg, South Africa, 17–18 August 2016; pp. 129–134. [CrossRef]
- Li, X.; Ying, S. Lib-SVMs Detection Model of Regulating-Profits Financial Statement Fraud Using Data of Chinese Listed Companies. In Proceedings of the 2010 International Conference on E-Product E-Service and E-Entertainment, Henan, China, 7–9 November 2010; pp. 1–4. [CrossRef]
- Throckmorton, C.S.; Mayew, W.J.; Venkatachalam, M.; Collins, L.M. Financial fraud detection using vocal, linguistic and fi nancial cues. Decis. Support Syst. 2015, 74, 78–87. [CrossRef]
- Glancy, F.H.; Yadav, S.B. A computational model for fi nancial reporting fraud detection. Decis. Support Syst. 2011, 50, 595–601.
- [CrossRef]
- Mareeswari, V.; Gunasekaran, G. Prevention of credit card fraud detection based on HSVM. In Proceedings of the 2016 Inter- national Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 25–26 February 2016;
- pp. 1–4.
- Humpherys, S.L.; Mof, K.C.; Burns, M.B.; Burgoon, J.K.; Felix, W.F. Identi fi cation of fraudulent fi nancial statements using linguistic credibility analysis. Decis. Support Syst. 2011, 50, 585–594. [CrossRef]
- Li, X.; Xu, W.; Tian, X. How to protect investors? A GA-based DWD approach for financial statement fraud detection. In Proceed- ings of the 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC), San Diego, CA, USA, 5–8 October 2014;
- pp. 3548–3554. [CrossRef]
- Karlos, S.; Fazakis, N.; Kotsiantis, S.; Sgarbas, K. Semi-supervised forecasting of fraudulent financial statements. In Proceedings of the 20th Pan-Hellenic Conference on Informatics, Patras, Greece, 10–12 November 2016. [CrossRef]
- Özçelik, M.H.; Duman, E.; Is¸ik, M.; Çevik, T. Improving a credit card fraud detection system using genetic algorithm. In Pro- ceedings of the 2010 International Conference on Networking and Information Technology, Manila, Philippines, 11–12 June 2010;
- pp. 436–440.
- Rizki, A.; Surjandari, I.; Wayasti, R.A. Data mining application to detect financial fraud in Indonesia's public companies. In Proceedings of the 2017 3rd International Conference on Science in Information Technology (ICSITech), Bandung, Indonesia, 25–26 October 2017; pp. 206–211.
- Chen, S. Detection of fraudulent financial statements using the hybrid data mining approach. SpringerPlus 2016, 5, 1–16. [CrossRef]
- [PubMed]
- Yao, J.; Zhang, J.; Wang, L. A financial statement fraud detection model based on hybrid data mining methods. In Proceedings of the 2018 international conference on artificial intelligence and big data (ICAIBD), Chengdu, China, 26–28 May 2018; pp. 57–61. [CrossRef]
- Rajak, I.; Mathai, K.J. Intelligent fraudulent detection system based SVM and optimized by danger theory. In Proceedings of the 2015 International Conference on Computer, Communication and Control (IC4), Indore, India, 10–12 September 2015; pp. 1–4. [CrossRef]
    - Jeragh, M.; Alsulaimi, M. Combining Auto Encoders and One Class Support Vectors Machine for Fraudulant Credit Card Transactions Detection. In Proceedings of the 2018

Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 30–31 October 2018; pp. 178–184. [CrossRef]

- Kho, J.R.D.; Vea, L.A. Credit card fraud detection based on transaction behavior. In Proceedings of the TENCON 2017-2017 IEEE Region 10 Conference, Penang, Malaysia, 5–8 November 2017; pp. 1880–1884. [CrossRef]
- Behera, T.K.; Panigrahi, S. Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network. In Proceedings of the 2015 Second International Conference on Advances in Computing and Communication Engineering, Dehradun, India, 1–2 May 2015; pp. 494–499.
- HaratiNik, M.R.; Akrami, M.; Khadivi, S.; Shajari, M. FUZZGY: A hybrid model for credit card fraud detection. In Proceedings of the 6th International Symposium on Telecommunications (IST), Tehran, Iran, 6–8 November 2012; pp. 1088–1093.
    - Malini, N.; Pushpa, M. Analysis on credit card fraud identification techniques based on KNN and outlier detection. In Proceedings of the 2017 third international conference on advances in electrical, electronics, information, communication and bio-informatics (AEEICB), Chennai, India, 27–28 February 2017; pp. 255–258. [CrossRef]
- Benchaji, I.; Douzi, S.; ElOuahidi, B. Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection. In Proceedings of the International Conference on Advanced Information Technology, Services and Systems, Mohammedia, Morocco, 17–18 October 2018; pp. 1–5. [CrossRef]
- Case, B. Recognizing Debit Card Fraud Transaction Using CHAID and K-Nearest Neighbor: Indonesian Bank case. In Proceedings of the 2016 11th International Conference on Knowledge, Information and Creativity Support Systems (KICSS), Yogyakarta, Indonesia, 10–12 November 2016.
- Bhusari, V.; Patil, S. Study of Hidden Markov Model in credit card fraudulent detection. In Proceedings of the 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, India, 29 February–1 March 2016; pp. 1–4.
- Sahin, Y.; Bulkan, S.; Duman, E. A cost-sensitive decision tree approach for fraud detection. Expert Syst. Appl. 2013, 40, 5916–5923.
- [CrossRef]
    - Duman, E.; Ozcelik, M.H. Detecting credit card fraud by genetic algorithm and scatter search. Expert Syst. Appl. 2011, 38, 13057–13063. [CrossRef]
- Sahin, Y.; Duman, E. Detecting credit card fraud by ANN and logistic regression. In Proceedings of the 2011 International Symposium on Innovations in Intelligent Systems and Applications, Istanbul, Turkey, 15–18 June 2011; pp. 315–319.
- Ghobadi, F.; Rohani, M. Cost sensitive modeling of credit card fraud using neural network strategy. In Proceedings of the 2016 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), Tehran, Iran, 14–15 December 2016; pp. 1–5.
- Awoyemi, J.O.; Adetunmbi, A.O.; Oluwadare, S.A. Credit card fraud detection using machine learning techniques: A comparative analysis. In Proceedings of the 2017 international conference on computing networking and informatics (ICCNI), Ota, Nigeria, 29–31 October 2017; pp. 1–9. [CrossRef]
- Mishra, A.; Ghorpade, C. Credit Card Fraud Detection on the Skewed Data Using Various Classification and Ensemble Techniques. In Proceedings of the 2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 24–25 February 2018; pp. 1–5. [CrossRef]
- Kirlidog, M.; Asuk, C. A Fraud Detection Approach with Data Mining in Health Insurance. Procedia-Soc. Behav. Sci. 2012, 62,
- 989–994. [CrossRef]