A Survey on credit Card Fraud Detection using machine and Deep Learning

Megha Nayak[1], Prof. Satendra Sonare[2]

[1]Reseacrh Scholar, Department of CSE, Gyan Ganga Institute of Technology and Sciences, Jabalpur, M.P.
[2]Professor, Departmet of CSE, Gyan Ganga Institute of Technology and Sciences, Jabalpur, M.P.

---***---

Abstract –

Recent developments in e-commerce and telecommunications have increased the use of credit cards for both online and everyday transactions. However, cases of credit card fraud are on the rise, causing financial institutions to incur huge losses every year. Establishing effective fraud detection systems is critical to reducing these losses, but is difficult due to the instability of most credit card information. Additionally, credit card fraud using traditional machine learning algorithms is ineffective as their structure consists of a static map from input vectors to vectors. For this reason, customers who use credit cards cannot transfer their purchases. A clustering-based transformation using a neural network as the learner is adopted. The performance of the plan has been confirmed using evidence available in the credit card world.

***Keywords**:* Detection of fraud; tracking of fraud; Fraud transaction understanding, Neural Network, Adaptive Learning.

1. INTRODUCTION

Electronic commerce in general has increased over time due to the popularity of e-commerce such as online stores such as Amazon, eBay and Alibaba. Credit/debit cards are widely used in electronic transactions. Recently, card-not-present transactions[1] have become more common in the credit card industry, ultimately through online payment systems such as paypal and alipay. The display value of global e-commerce is expected to reach $24 trillion by 2019 [2]. But at the same time, fraud occurs, which affects the economy. A study of more than 160 companies found that the number of online frauds each year is 12 times greater than offline frauds [4]. Since there is no need for a physical card in the e-commerce environment and almost all of the information on the card is sufficient for transactions, fraudsters need the information in this letter to gain power. For example, after scammers obtain card account numbers and passwords from honest cardholders, they use them to purchase certain products. Fraudsters often obtain card information through a variety of means: hijacking attempts to send letters containing the latest releases, copy-pasting of card information by copiers, phishing (clone websites), or from unknown credit card companies. 5]. Due to the complexity of the environment and population base, it is inevitable that all legitimate card holders will be robbed. The best way to identify this type of strain is to analyze each account's payment pattern and identify errors associated with "normal" transaction design [6]. Unauthorized transaction by someone other than the owner of the credit card or account. A stolen, lost or fraudulent credit card may result in cancellation. As online shopping has increased, cardless extortion or the use of credit cards in e-commerce has become more common. The spread of frauds such as ccf resulting from the proliferation of electronic banking and, in some cases, online payments leads to losses of billions of dollars each year. In the era of computer programming, ccf detection has become one of the most important goals. As a business owner, it doesn't matter if long-term transportation is moving towards a money-free culture. As a result, traditional payment strategies may not be available in the future and may not be suitable for business continuity. Customers do not need to come into the store with cash in their pockets. They now charge bills and credit cards. Therefore, companies need to adapt their environments to enable them to accept a variety of payments. This situation is expected to continue for a long time [7]. CCF was the top source of theft recorded this year, after government documents and financial support [9]. In 2020, 365,597 attempts were made to spend money using an unused credit card [10]. The number of theft-related conduct complaints increased 113% from 2019 to 2020; this includes a reported 44.6% increase in credit card identity theft [11]. Payment card theft cost the global economy $24.26 billion last year. Elaborate credit card skimming incidents accounted for 38.6% of incidents in 2018, making these states the least protected from credit card theft. Therefore, examining the use of money should be the priority of the use of inheritance. The program must identify fake and non-fake swaps and use this information to decide whether a future swap is fake or not. This problem includes major problems such as the operating speed of the system, attracting attention, and prioritization. Machine learning is a field of visual science that uses computers to make predictions based on early data patterns. Machine learning models have been used in many studies to solve many problems. Deep learning (dl) applications include computer network organizations, anomaly detection, financial management, protection, portable cellular systems, medical ransomware discovery, recovery and malware discovery, video surveillance discovery, zone tracking, android malware discovery, home robotization and heart disease prediction. . For data classification, inverse vector machines (svm) can be a training method. It has been used in many fields, including image recognition [12], credit scoring [9], and public safety [13]. Svm can solve two problems, both direct and unclassified, and finds a broad plane to separate input data into support vectors, which is important for other distributions. Neural systems were the first technique used to detect credit card robberies in the past [8]. So ml division (dl) now focuses on dl method. In the long run, deep learning methods have attracted widespread attention due to their high efficiency and effectiveness in different applications such as computer vision, general language processing, and speech. However, as some have thought, the use of deep tissue in identifying ccfs has been explored [7]. It uses a lot of deep learning to identify ccfs. Anyway, in this case we select the neural network and its layers to determine the initial ransom as a valid exchange of suitable datasets. There are some operations in the configuration file that are labeled as errors and are said to be faulty.

We propose a neural network display with additional criteria to extract and classify credit card transactions as fraudulent or fake. Use the element finder to find the best features in arrayed data. Some deep learning models are then used to identify ccfs.

1.1 Fraud Detection Approaches Currently, there are two kinds of approaches of fraud detection: (1) misuse detection and (2) anomaly detection [14]. Figure 1.1 below shows the types of Fraud detection methods.

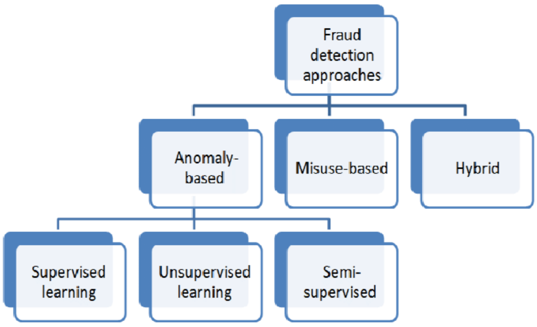

Figure 1.1: Fraud Detection Methods.

The first should collect a large database of incorrect signs and use this as a reference to distinguish existing (mis)use. This approach often requires prior malware knowledge to obtain different ransomware designs. Different techniques such as neural systems, selection trees, iterative computations, and inverse vector machines have been used for localizing credit card skimming [15]. But they have two disadvantages: first, it is more difficult to get all the cheats; secondly, all the cheats are harder to get. In addition, it is not possible to distinguish power usage that was not detected in previous sources today [16]. The difference is that the previously mentioned profile creates different exchange patterns based on transaction evidence, and the latter flags exchanges that differ from the "average" of "normal" historical profiles as potential fraud. Most irregularity-based credit card skimming detection techniques [17] attempt to eliminate actual rules-based behavior patterns and calculate the similarity of these behavior patterns with future transactions. The most important thing to consider this way is that people have different personalities, specific salaries, specific motivations, etc. They will have different personal shopping depending on their preferences. Adams et al. In [18] there is a reliable design of changing behavior from week to week and month to month. A complete description of the design of time variation is presented in [18]. A proof of blackmail based on the cover markov proof (the well) was proposed by srivastava et al. [13] Teamwork in credit card payment is well modeled. Amlan et al. In this policy, the cardholder's behavior changes confirmed to have been triggered by the integration and the integration time are used to determine what the future change of the credit card will be for the actual cardholder's past transactions of the transaction. The association of certified racketeering analysts (acfe) defines blackmail as "the deception or copying of a product or person knowing that it will provide an illegal benefit." Money laundering accounts for approximately 10 percent of white-collar crimes, according to the acfe. When misaccounting occurs, differences must be made to ensure agreement. Considering that the effect of money causes serious harm to thinking people, many studies have been conducted in the field using learning strategies such as ann [19], dt [20], svm [21] and content mining. Meanwhile, other extortion issues such as credit card blackmail [22], insider trading, and extortion prevention have also been studied. Given the unique characteristics of each type of financial withdrawal, specific strategies have been developed.

1.2 Data mining process

The data mining process breaks down into some steps. First, organizations collect data and load it into their data warehouses. Next, they store and manage the data. Business analysts, management teams and information technology professionals access the data and determine how they want to organize it. Then, application software sorts the data based on the user's results, and finally, the end user presents the data in the form of graph. The Data mining process is shown in figure 1.2.

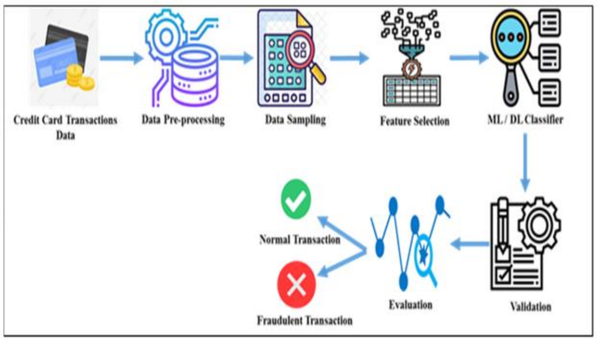

Figure 1.2: Data Mining Process for fraud detection.

A. Classification

Classification can be a mining technique that places items in a collection into classes or groups. The purpose of classification is to predict the target process for each case in the data. For example, categorical guidelines can be used to classify potential candidates as low credit risk, medium credit risk, or high credit risk. The classification process begins with providing information about the curriculum. For example, the distribution shows that loan duration can be predicted based on analysis of many top candidates over time. When linked to a credit report, this information can track employment history, home ownership or rent, time spent at home, number and type of jobs, and more. Credit evaluation will be objective, other quality will be expert and each customer profile will constitute a case. The classification is discrete and no order is extracted. Floats will always indicate numerical targets rather than categorical targets. Presciently, the objective function of number is not categorical counting but repetitive counting.

B. Prediction

Forward-looking analytics involves a variety of real-time techniques, such as modeling, machine learning, and data mining that analyze current and actual facts to create predictions about the future or other conditions that are uncertain. Prescient patterns in business create abuses present in evidence and are useful in discerning the dangers of time. The model captures the connection between different variables to assess the risk or potential associated with a particular process to guide the selection of candidates for change. One of the advantages of this professional system is that the forecast is given to everyone (customers, employees, medical facilities, vehicles, equipment, machines or other organizations) along with forecast points (needs) to determine, clarify or influence the situation. He took part in many missions related to the organization of people, such as testimony, economic evaluation, torture, production, health care and government affairs, including law. Evidence of my information is stored in the archive. The database can store all location information, customer identification information, click history information and transaction information. Although the data distribution area is very large, the capacity of the feature can ensure that my data is good.

2. LITERATURE REVIEW

Some research has been done in the field of ccf space. This chapter presents a specific research strategy regarding the rotation of the ccf program. We also clearly show the investigation of blackmail sites in the context of controversial topics. There are many strategies for different credit cards. Therefore, groups such as dl, ml, ccf discovery, clothing and emphasis localization, and customer identification may be the most common methods to examine the most important work in this field [23], [24]. Figure 2.1 shows how a credit card authorization system can be used for credit card verification. There are two authentication methods: password and biometric authentication. Biometric-based authentication can be divided into three categories: physiological and behavioral authentication and federated authentication [25], [26].

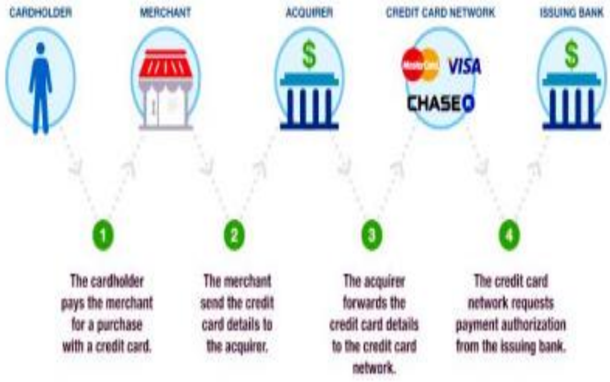
CARDHOLDER
MERCHANT
ACQUIRER
CREDIT CARD NETWORK
ISSUING BANK
$
MasterCard
VISA
CHASE
$
1
The cardholder pays the merchant for a purchase with a credit card.
2
The merchant send the credit card details to the acquirer.
3
The acquirer forwards the credit card details to the credit card network.
4
The credit card network requests payment authorization from the issuing bank.

Figure 2.1: Payment card authorization process.

2.1 Supervised Machine Learning Approaches

There are many branches of machine learning, each performing a different type of learning. However, machine learning has its own unique system. The ml method provides a ccf plan like arbitrary forest area (rf). The collection of selected trees is arbitrary forestry [24]. Most analysts use radio frequency. We can use (rf) in addition to the research setup to combine the display. This concept is called apat [23]. Analysts can use specialized machine learning techniques such as control learning and unsupervised techniques. Ml calculations such as lr, ann, dt, svm and nb are often used for ccf determination. Analysts can combine these methods with written methods to produce robust findings [26]. The connection between many neurons and the central nervous system is called nervous tissue. The feedforward perceptron multilayer consists of several layers: an output layer, an output layer, and one or more layers. The main process has access points to represent the search. The access process is copied at what weight and changed considering the coexistence of each hub layer. Meanwhile, connections work to produce the results of each neuron, which are then passed on to the next layer. Finally, the revenue layer gives the algorithm's answer. The main system used weights liberally and at one point used a system designed to limit errors. All these weights are balanced by special calculations such as back expansion [27], [28]. The real justification for the unity of processes is called bayesian belief organization. The liberal theory in naive bayes is that it is designed to relax and let things happen. When the conditions of events emerge in the form of curves of spaces, changes arise from spaces. Meetings are associated with each connected hub, causing the value of the node to vary according to the value of the parent [29], [30]. The working principle of the binary branching system (bbn) is as follows: finding the development of this system is the first step: it is requested by human experts and specific calculations are made using the data. Once this topology organization begins, clearly fit the competition to naive bayes using the data that can be collected to confirm significant and meaningful effects. In bbn, each hub must be independent from its children, i.e., The parent of each hub is in the diagram [31]. This is often considered a markov case. Direct classification shows potential support vector machines (svms) and problem duplication. When converted to svm calculation, we found the focus closest to a straight line in both groups [32]. These foci are called rotation vectors. This article focuses on the integration of unsupervised techniques with directed techniques for CCF localization.

2.2 Deep Learning Approaches

Dl computation is important, including convolutional neural network (cnn) computation, and further computations are deep belief (dbns) and deep autoencoders; there are different technical methods, learning methods and classification systems [33]. The purpose of deep learning is to consider artificial neural systems. The proposed method respects the predictive neural system and is considered a backward representation [34]. The effectiveness of backcomputation is greatly reduced, thus the depth of the brain is expanded, which can cause problems such as undershooting and shrinking of nearby targets. The long-term plan should be seen as a success. It is thought that they can significantly solve the problem of unplanned development [35], [36]. Compiled by shenzhen engineering co., Ltd. It is generally considered the main story of shenzhen engineering co., Ltd. Normal count ml such as svm, dt and lr are expanded into the ccf field. These calculations are not specific to big data. In 1dcnn, some channels moved in the test group profile instead of moving to the right as in 2dcnn [35], [36]. Raghavan describes autoencoders as actual neural tissue. An autoencoder can encode data the same way it decodes the data. In this concept, autoencoder is recommended to avoid abnormal analysis. According to the established line, crimes are reported and classified as “fraud” or “non-fraud”, indicating that the framework is not yet ready and better criminalization is needed [37], [38]. However, values slightly above the upper limit or threshold are considered characteristic. This concept is also used in [30], an autoencoder-based nonlinear detection network. Machine learning performance can be a useful feature when two neural networks work together to improve their predictions. Gans often learns to use zero-sum game systems without supervision. The main category of deep learning is gan [39], and the recognition of the progress it can make in deep learning is the most promising. Gan has two main modes. In the preparation phase, all modules create a dl demo which can be a neural network. The two most commonly used strategies are generator (g) and discrimination (d). The generator's organization can generate recycled data, and the difference between the recycled data and the target data determines the manager, so that true and false information is created around the virtual information. Finally, modeling can produce better data to prepare for data generation [40] , [41] . Vae is a variable autoencoder with a continuous planning cycle to ensure that the area it covers has sufficient resources to help us generate new data. Vae is created by increasing the diversity depending on the position of the autoencoder. Vgg and gan are surprisingly comparable. Again, the aim is to modify and integrate traffic data to create a virtual data close to the target [40]. In general, the number of tests is proportional to the number of infections. If everything checks out, the work will be perfect. So analysts always use the brain to smooth out the brutality and fine-tuning of the transmission. Short-term (lstm) is a recurrent neural array (rnn) designed for use in dl models [42], [43]. Lstm organization is consistent with the classification, execution and generation of forecasts based on time records. The most common rnn type is lstm. Standard neural networks (nn) cannot store information from previous learning each time they are run. In very simple terms, rnn with memory can be a neural network [44], [45]. Rnns tend to have short memory due to the horizon angle issue. The neural spine spreads back as the starting angle reduces the weight loss of the replacement tissue. In rnns, the incline backfires as it moves the spine in line, and then the weight increases slightly. These small changes are influenced by previous processes in planning. They can no longer learn and mn lose the ability to recall information before long-term planning, resulting in short-term memory organization [46]. And lstm can handle large datasets and is therefore suitable for image classification, natural language processing (nlp) and rbm. The way these dl strategies perform ccf classification is important for this decision [47]. Additionally, data preprocessing is an important organization in machine learning. The impact of preliminary information on work distribution during credit card approval is another question that needs to be answered. These factors must be complete and sufficient to cover all aspects of the company's operations. For example, velocity ratio and revenue ratio show the change in growth, while earnings per share show the efficiency of the business; subsequently, the phonetic aspects of mds are used in scientific research. Petr hajek found that fake companies had slightly more negative reviews in their annual reports than non-fake companies. So fake companies often use bad words. The number of fake companies used in previous studies has ranged from tens to thousands, and research methods in each country have differed slightly.

2.3 Existing survey

Technological developments such as e-commerce and new financial technologies (fintech) have begun to increase the number of online credit cards day by day. Because of this, credit card skimming cases have occurred, affecting card issuers, carriers, and banks. That's why it's important to create products that guarantee the security and discretion of credit card transactions. In research [48], we implemented a machine learning (ml)-based credit card skimming localization system using real-world suspicious data generated by european credit card holders. To demonstrate the shyness issue, we resample the data using a minimally invasive procedure (fractionation). The system is evaluated using machine learning techniques: inverse vector machine (svm), repeated counting (lr), random forest (rf), custom angle boosting (xgboost), tree selection (dt), and tree addition (and). These ml calculations are combined with various boosting (adaboost) programs to increase classification efficiency. Model sensitivity was evaluated using precision, censoring, precision, matthews correlation coefficient (mcc), and range of inflection (auc). Additionally, the proposed method was applied on the controversial credit card ransomware before the results obtained in this research were allowed. Test results show that the use of adaboost has a positive impact on the success of the proposed strategy. Note that improved models are more efficient than existing methods.

Recent developments in e-commerce and telecommunications have resulted in the widespread use of credit cards both online and in business models. Despite this, the fake credit card business, for example, is on the rise and causes financial institutions to incur huge losses every year. Improvements in successful extortion site calculations are important to reduce these frustrations, but are difficult because most credit card information sets are inconsistent. Additionally, using machine learning models for credit card skimming detection is wasteful because their inputs include poor performance of the input vectors for the generated vectors. After that, they cannot adapt to the credit card customer culture. This paper [49] presents an effective method to detect credit card skimming using neural permutation addition classifiers and cross-information resampling strategies. The cluster group is used to use a short-term (lstm) neural network as the learner base in the general boost algorithm (adaboost). During this period, a revolutionary change was achieved by using the minority building strategy and the updated neighbor (smote-enn) strategy. The feasibility of the proposed strategy is demonstrated by using data exchange in the free world. The success of the scheme was evaluated by the following calculations: inverse vector machine (svm), multilayer perceptron (mlp), tree selection, traditional adaboost and lstm. Test results show that the classifier performs better when planning to use repeated data, and the lstm tool outperforms other calculations with sensitivity and specificity of 0.996 and 0.998, respectively. > Developments such as e-commerce and fintech (financial technology) applications

have begun to increase the number of online credit card transactions day by day. As a result, credit card extortion incidents occurred that affected credit card companies, merchants and banks. In this way, it is important to create content that guarantees the security and speed of credit card transactions. In this work [50], we use machine learning (ml) as a credit card extortion site uses real-world data generated by european credit card holders. To account for the hard-to-solve problem, we resample the data using the proposed minority (distortion) strategy. The system is evaluated using machine learning techniques: inverse vector machine (svm), repeated counting (lr), arbitrary forest (rf), hyper angle boosting (xgboost), selection tree (dt) and contribution tree (et). These machine learning methods are combined with multiple boosting (adaboost) techniques to expand its classification. Model sensitivity, censoring, accuracy were evaluated using matthews correlation coefficient (mcc) and area under the curve (auc). Additionally, the proposed method has been applied to different credit card skimming profiles in order to support the compatibility of the results obtained in this research. Research results show that the use of adaboost has a positive impact on the success of the planning strategy. Note that the extended model leads to results that check existing ideas. Machine learning (ml) algorithms are used in credit card fraud. However, the dynamic business model of credit card holders and the problem of different classes make it difficult for machine learning classes to achieve optimal performance. To solve this problem, this paper [51] proposes a deep learning method based on the learner base level in the joint process, consisting of short-term (lstm) and gated recurrent unit (gru) neural network. Multilayer perceptron (mlp) as a meta-learner. At the same time, hybrid synthetic minority oversampling technique and modified nearest neighbor (smote-enn) method were used to balance the class distribution in the dataset. Experimental results show that the integration of deep learning with the smote-enn method achieves sensitivity and specificity of 1.000 and 0.997, respectively, outperforming other ml classifiers and methods in the literature. Advances in processing and communications technology have made credit cards the most popular form of payment for both online and offline purchases, so app interactions with these businesses are expanding. Credit card fraud is a huge loss to businesses and consumers every year, and fraudsters are constantly trying to find new ways to fake business.

3. CONCLUSION

CCFS pose a serious threat to financial institutions. Scammers are constantly finding new ways to scam people. A strong product can withstand fraudulent changes. Estimating the true extent of fraud and reducing false positives are the most important aspects of fraud detection. The effectiveness of machine learning techniques varies with each marketer. The type of data input is the main driving variable of machine learning. For the ccf test, the number of features, the number of variables and the relationship between features are important factors that determine the performance of the model. It is associated with deep learning, text processing, and underlying models such as cnns and layers. Using this method to identify credit cards is more effective than traditional algorithms.

REFERENCES

[1] Gupta S and Johari R. A new framework for credit card transactions involving mutual authentication between cardholder and merchant. In Communication Systems and Network Technologies, pages 22–26. IEEE, 2011.

[2] C. Arun. Fraud: 2016 & its business impact. Technical report, 11 2016.

[3] Vronique Van Vlasselaer, Cristin Bravo, Olivier Caelen, Tina Eliassi-Rad, Leman Akoglu, Monique Snoeck, and Bart Baesens. Apate: A novel approach for automated credit card transaction fraud detection using network-based extensions. Decision Support Systems, 75:38–48, 2015.

[4] Suvasini Panigrahi, Amlan Kundu, Shamik Sural, and A. K. Majumdar. Credit card fraud detection: A fusion approach using dempstercshafer theory and bayesian learning. Information Fusion, 10(4):354–363, 2009.

[5] Jon T. S Quah and M Sriganesh. Real-time credit card fraud detection using computational intelligence. Expert Systems with Applications An International Journal, 35(4):1721–1732, 2007.

[6] Abhinav Srivastava, Amlan Kundu, Shamik Sural, and Arun Majumdar. Credit card fraud detection using hidden markov model. Dependable & Secure Computing IEEE Transactions on, 5(1):37–48, 2007.

[7] Y. Abakarim, M. Lahby, and A. Attioui, "An efficient real time model for credit card fraud detection based on deep learning," in Proc. 12th Int. Conf. Intell. Systems: Theories Appl., Oct. 2018, pp. 1–7, doi: 10.1145/3289402.3289530.

[8] A. O. Balogun, S. Basri, S. J. Abdulkadir, and A. S. Hashim, "Performance analysis of feature selection methods in software defect prediction: A search method approach," Appl. Sci., vol. 9, no. 13, p. 2764, Jul. 2019, doi: 10.3390/app9132764.

[9] B. Bandaranayake, "Fraud and corruption control at education system level: A case study of the Victorian department of education and early childhood development in Australia," J. Cases Educ. Leadership, vol. 17, no. 4, pp. 34–53, Dec. 2014, doi: 10.1177/1555458914549669.

[10] V. N. Dornadula and S. Geetha, "Credit card fraud detection using machine learning algorithms," Proc. Comput. Sci., vol. 165, pp. 631–641, Jan. 2019, doi: 10.1016/j.procs.2020.01.057.

[11] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," 2015, arXiv: 1512.03385

[12] D. Molina, A. LaTorre, and F. Herrera, "SHADE with iterative local search for large-scale global optimization," in Proc. IEEE Congr. Evol. Comput. (CEC), Jul. 2018, pp. 1–8, doi: 10.1109/CEC.2018.8477755.

[13] J. Kim, H.-J. Kim, and H. Kim, "Fraud detection for job placement using hierarchical clusters-based deep neural networks," Int. J. Speech Technol., vol. 49, no. 8, pp. 2842–2861, Aug. 2019, doi: 10.1007/s10489-019-01419-2.

[14] Wen Hua Ju and Yehuda Vardi. A hybrid high-order markov chain model for computer intrusion detection. Journal of Computational & Graphical Statistics, 10(2):277–295, 2004.

[15] V. Dheepa and R. Dhanapal. Behavior based credit card fraud detection using support vector machines. Ictact Journal on Soft Computing, 2(4), 2012.

[16] Z. Zojaji, R. E. Atani, A. H. Monadjemi, et al. A survey of creditcard fraud detection techniques: Data and technique oriented perspective. arXiv preprint arXiv:1611.06439, 2016.

[17] Thuraya Razooqi, Pansy Khurana, Kaamran Raahemifar, and Abdolreza Abhari. Credit card fraud detection using fuzzy logic and neural network. In Communications & NETWORKING Symposium, 2016.

[18] Giovanni Montana David J. Weston Niall M. Adams, David J. Hand. Craud detection in consumer credit. Expert Update SGAI, Special Issue on the 2nd UK KDD Workshop, 2(1), 2006.

[19] Wang, L. and C. Wu, A Combination of Models for Financial Crisis Prediction: Integrating Probabilistic Neural Network with Back-Propagation based on Adaptive Boosting. International Journal of Computational Intelligence Systems, 2017. 10(1): p. 507.

[20] Kotsiantis, S., et al., Forecasting fraudulent financial statements using data mining. Enformatika, 2006. 3(2): p. 104-110.

[21] Huang, S.Y., Fraud Detection Model by Using Support Vector Machine Techniques. International Journal of Digital Content Technology & Its Applic, 2013.

[22] Olszewski, D., Fraud detection using self-organizing map visualizing the user profiles. Knowledge-Based Systems, 2014. 70(C): p. 324-334.

[23] Y. Abakarim, M. Lahby, and A. Attioui, "An efficient real time model for credit card fraud detection based on deep learning," in Proc. 12th Int. Conf. Intell. Systems: Theories Appl., Oct. 2018, pp. 1–7, doi: 10.1145/3289402.3289530.

[24] V. Arora, R. S. Leekha, K. Lee, and A. Kataria, "Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence," Mobile Inf. Syst., vol. 2020, pp. 1–13, Oct. 2020, doi: 10.1155/2020/8885269.

[25] A. O. Balogun, S. Basri, S. J. Abdulkadir, and A. S. Hashim, "Performance analysis of feature selection methods in software defect prediction: A search method approach," Appl. Sci., vol. 9, no. 13, p. 2764, Jul. 2019, doi: 10.3390/app9132764.

[26] B. Bandaranayake, "Fraud and corruption control at education system level: A case study of the Victorian department of education and early childhood development in Australia," J. Cases Educ. Leadership, vol. 17, no. 4, pp. 34–53, Dec. 2014, doi: 10.1177/1555458914549669.

[27] H. Abdi and L. J. Williams, "Principal component analysis," Wiley Interdiscipl. Rev., Comput. Statist., vol. 2, no. 4, pp. 433–459, Jul. 2010, doi: 10.1002/wics.101.

[28] J. Błaszczyński, A. T. de Almeida Filho, A. Matuszyk, M. Szelg,, and R. Słowiński, "Auto loan fraud detection using

dominance-based rough set approach versus machine learning methods,'' Expert Syst. Appl., vol. 163, Jan. 2021, Art. no. 113740, doi: 10.1016/j.eswa.2020.113740.

[29] B. Branco, P. Abreu, A. S. Gomes, M. S. C. Almeida, J. T. Ascensão, and P. Bizarro, ''Interleaved sequence RNNs for fraud detection,'' in Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2020, pp. 3101–3109, doi: 10.1145/3394486.3403361.

[30] F. Cartella, O. Anunciacao, Y. Funabiki, D. Yamaguchi, T. Akishita, and O. Elshocht, ''Adversarial attacks for tabular data: Application to fraud detection and imbalanced data,'' 2021, arXiv: 2101.08030.

[31] S. S. Lad, I. Dept. of CSE Rajarambapu Institute of Technology Rajaramnagar Sangli Maharashtra, and A. C. Adamuthe, ''Malware classification with improved convolutional neural network model,'' Int. J. Comput. Netw. Inf. Secur., vol. 12, no. 6, pp. 30–43, Dec. 2021, doi: 10.5815/ijcnis.2020.06.03.

[32] V. N. Dornadula and S. Geetha, ''Credit card fraud detection using machine learning algorithms,'' Proc. Comput. Sci., vol. 165, pp. 631–641, Jan. 2019, doi: 10.1016/j.procs.2020.01.057.

[33] X. Hu, H. Chen, and R. Zhang, ''Short paper: Credit card fraud detection using LightGBM with asymmetric error control,'' in Proc. 2nd Int. Conf. Artif. Intell. for Industries (AII), Sep. 2019, pp. 91–94, doi: 10.1109/AI4I46381.2019.00030.

[34] J. Kim, H.-J. Kim, and H. Kim, ''Fraud detection for job placement using hierarchical clusters-based deep neural networks,'' Int. J. Speech Technol., vol. 49, no. 8, pp. 2842–2861, Aug. 2019, doi: 10.1007/s10489-019-01419-2.

[35] M.-J. Kim and T.-S. Kim, ''A neural classifier with fraud density map for effective credit card fraud detection,'' in Intelligent Data Engineering and Automated Learning, vol. 2412, H. Yin, N. Allinson, R. Freeman, J. Keane, and S. Hubbard, Eds. Berlin, Germany: Springer, 2002, pp. 378–383, doi: 10.1007/3-540-45675-9_56.

[36] N. Kousika, G. Vishali, S. Sunandhana, and M. A. Vijay, ''Machine learning based fraud analysis and detection system,'' J. Phys., Conf., vol. 1916, no. 1, May 2021, Art. no. 012115, doi: 10.1088/1742-6596/1916/1/012115.

[37] R. F. Lima and A. Pereira, ''Feature selection approaches to fraud detection in e-payment systems,'' in E-Commerce and Web Technologies, vol. 278, D. Bridge and H. Stuckenschmidt, Eds. Springer, 2017, pp. 111–126, doi: 10.1007/978-3-319-53676-7_9.

[38] Y. Lucas and J. Jurgovsky, ''Credit card fraud detection using machine learning: A survey,'' 2020, arXiv: 2010.06479.

[39] H. Zhou, H.-F. Chai and M.-L. Qiu, ''Fraud detection within bankcard enrollment on mobile device based payment using machine learning,'' Frontiers Inf. Technol. Electron. Eng., vol. 19, no. 12, pp. 1537–1545, Dec. 2018, doi: 10.1631/FITEE.1800580.

[40] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M.-S. Hacid, and H. Zeineddine, ''An experimental study with imbalanced classification approaches for credit card fraud detection,'' IEEE Access, vol. 7, pp. 93010–93022, 2019, doi: 10.1109/ACCESS.2019.2927266.

[41] I. Matloob, S. A. Khan, and H. U. Rahman, ''Sequence mining and prediction-based healthcare fraud detection methodology,'' IEEE Access, vol. 8, pp. 143256–143273, 2020, doi: 10.1109/ACCESS.2020.3013962.

[42] I. Mekterović, M. Karan, D. Pintar, and L. Brkić, ''Credit card fraud detection in card-not-present transactions: Where to invest?'' Appl. Sci., vol. 11, no. 15, p. 6766, Jul. 2021, doi: 10.3390/app11156766.

[43] D. Molina, A. LaTorre, and F. Herrera, ''SHADE with iterative local search for large-scale global optimization,'' in Proc. IEEE Congr. Evol. Comput. (CEC), Jul. 2018, pp. 1–8, doi: 10.1109/CEC.2018.8477755.

[44] M. Muhsin, M. Kardoyo, S. Arief, A. Nurkhin, and H. Pramusinto, ''An analyis of student's academic fraud behavior,'' in Proc. Int. Conf. Learn. Innov. (ICLI), Malang, Indonesia, 2018, pp. 34–38, doi: 10.2991/icli-17.2018.7.

[45] H. Najadat, O. Altiti, A. A. Aqouleh, and M. Younes, ''Credit card fraud detection based on machine and deep learning,'' in Proc. 11th Int. Conf. Inf. Commun. Syst. (ICICS), Apr. 2020, pp. 204–208, doi: 10.1109/ICICS49469.2020.239524.

[46] A. Pumsirirat and L. Yan, ''Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine,'' Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 1, pp. 18–25, 2018, doi: 10.14569/IJACSA.2018.090103.

[47] P. Raghavan and N. E. Gayar, ''Fraud detection using machine learning and deep learning,'' in Proc. Int. Conf. Comput. Intell. Knowl. Economy (ICCIKE), Dec. 2019, pp. 334–339, doi: 10.1109/ICCIKE47802.2019.9004231.

[48] E. Ileberi, Y. Sun and Z. Wang, "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost," in IEEE Access, vol. 9, pp. 165286-165294, 2021, doi: 10.1109/ACCESS.2021.3134330.

[49] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba and G. Obaido, "A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection," in IEEE Access, vol. 10, pp. 16400-16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[50] E. Ileberi, Y. Sun and Z. Wang, "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost," in IEEE Access, vol. 9, pp. 165286-165294, 2021, doi: 10.1109/ACCESS.2021.3134330.

[51] I. D. Mienye and Y. Sun, "A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection," in IEEE Access, vol. 11, pp. 30628-30638, 2023, doi: 10.1109/ACCESS.2023.3262020.

[52] A. A. Taha and S. J. Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine," in IEEE Access, vol. 8, pp. 25579-25587, 2020, doi: 10.1109/ACCESS.2020.2971354.