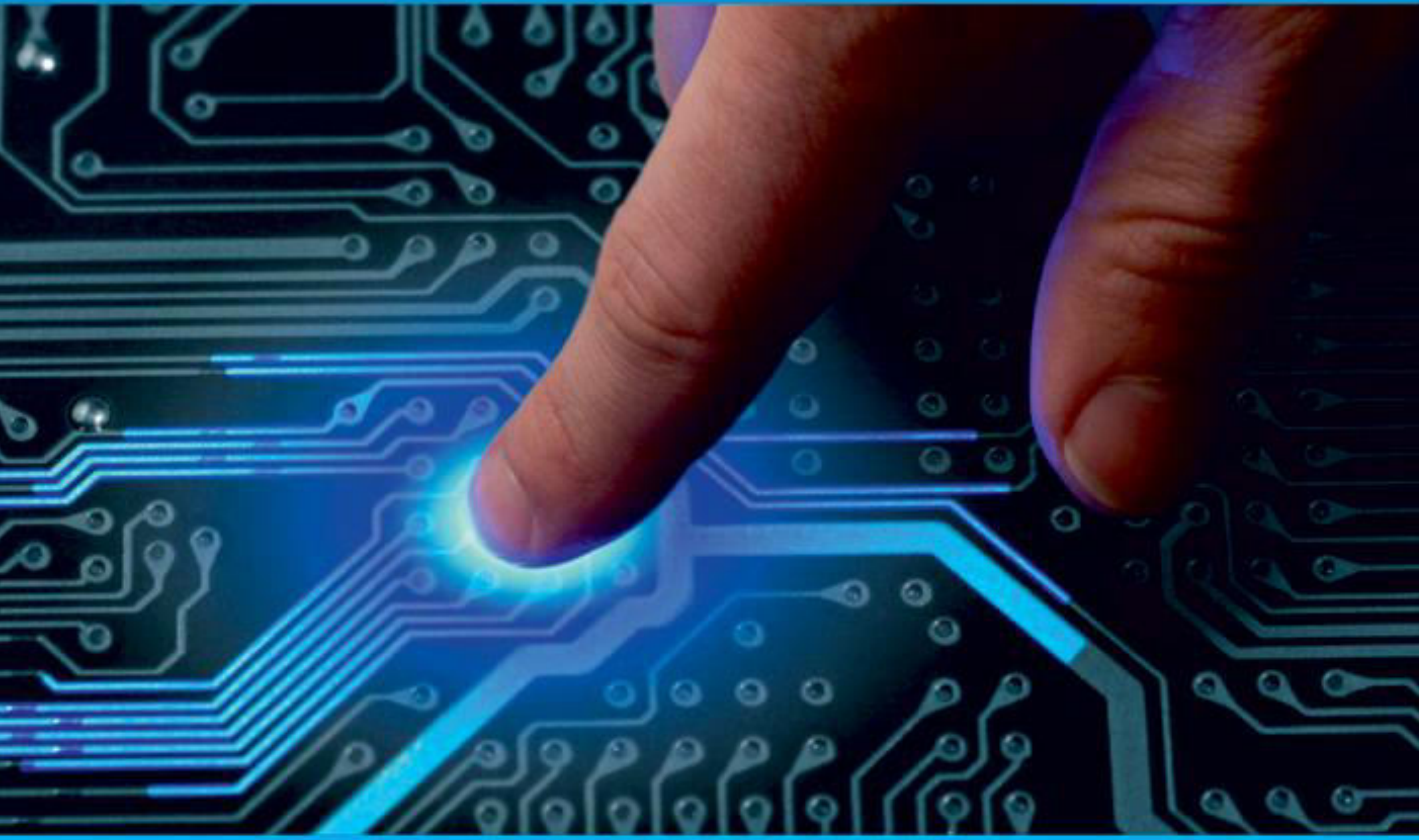
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 9, September 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Machine Learning in Financial Security: A Systematic Review of Credit Card Fraud Detection Methods

Ruchitha B, Snehalatha B, Manikantan R

Department of MCA, Surana College Kengeri, Bangalore, India

Department of MCA, Surana College Kengeri, Bangalore, India

Assistant Professor, Department of MCA, Surana College Kengeri, Bangalore, India

ABSTRACT: The article on credit card fraud detection uses both conventional and cutting-edge machine learning techniques to provide a comprehensive overview of the state of the field. The text discusses several approaches and their benefits and drawbacks. The following are some examples of machine learning techniques: Support Vector Machines, Fuzzy Logic-based Systems, Decision Trees, Hybrid Approaches, K-Nearest Neighbours, Neural Networks, Naive Bayes, Genetic Algorithms, and Privacy preserving Techniques. DTs give up They become more prone to overfitting when they trade interpretability for generalization ability. On the other hand, because LR is susceptible to outliers, its performance is compromised. Although NN is good at detecting complex patterns, it can be computationally demanding, and speed-loving NB compromises accuracy by breaking its feature independence assumption. When carefully incorporated into actual financial security frameworks, all of these numerous approaches present intricate trade-offs between accuracy, interpretability, scalability, and privacy concerns.

KEYWORDS: Credit Card Fraud, Machine Learning Support Vector Machines

I. INTRODUCTION

Both the customer and the retailer now have considerably easier lives thanks to electronic credit cards and internet shopping [1]. Unfortunately, there has been a sharp rise in credit card theft as a result of the digital revolution. Issues such as fraudulent transactions, identity theft, and account takeover are becoming major concerns for financial institutions and people worldwide [2]. Considering the financial ramifications and the decline in confidence in online payment methods, credit card theft is a significant problem for effective remedies.

Due to the emergence of sophisticated fraudulent schemes, rule-based systems and human evaluations are no longer sufficient for detecting swindling [3]. Manual evaluations are costly, time-consuming, and prone to human mistake. On the other hand, rule-based systems don't always provide the necessary flexibility to effectively combat new fraud trends.The banking sector has recently shown interest in creating increasingly complex and automated methods for detecting fraud, given the rise of machine learning algorithms. This study examines the current state of ML algorithms for credit card fraud detection while critically analyzing the benefits, drawbacks, and efficacy of various approaches

II. LITERATURE REVIEW

The prevalence of credit card fraud is growing, which is driving the need for greater resolution techniques to combat it [4]. Important conclusions and observations from in-depth research on credit card fraud detection are provided in this section.

A. Identification of Credit Card Fraud Prior to Machine Learning

Before ML techniques emerged, the field of CCFD depended primarily on these rule-based and heuristic-driven approaches. Even though these approaches were fulfilling their intended role, they were not without flaws. Specifically, they frequently displayed inconsistent performance for the goal of detecting fraudulent transactions. Some traditional approaches are

1) Rule-Based Frameworks: As soon as possible after the creation of rule-based systems, this technique for fraud detection was developed. The systems identified possible fraudulent financial transactions by using thresholds and other specified parameters. If an overseas transaction happened shorter than a predetermined amount of time following a domestic transaction, for example, a rule would trigger an alert. Although comprehending and executing rule-based systems is simple and clear, these systems were quite rigid and did not adapt to the changes that the fraud schemes experienced [5].
2) Threshold-Based Alerts: The number or count of transactions is limited by the threshold mechanism. When specific thresholds were exceeded in financial transactions, threshold systems alerted users. However, the rather high false positive rate that threshold-based approaches often generated was a fundamental problem. Lowering the criterion, for instance, would identify more fraudulent situations, but it might also choose more high-value, legal transactions.

B. Fraud Prevention and Mitigation

Prior to the development of machine learning, efforts to stop credit card fraud relied mostly on a mix of conventional methods, such as cardholder education and fraud investigation teams. Financial institutions have set up specialized teams to look into transactions and patterns that seem suspicious. In the course of their operations, these units usually collaborate closely with law enforcement organizations. Furthermore, cardholders have been provided with information regarding safe procedures, and their active verification of their own transactions has been essential in discouraging fraudulent activity. In addition to certain banks offering online transaction tracking, cardholders were asked to report suspicious behaviour right away.

C. Machine Learning Algorithms in Credit Card Fraud Detection

As demonstrated by the work of Dornadula and Geetha [6], the use of ML algorithms for CCFD has grown significantly in popularity recently. Its reputation stems mostly from the fact that it provides stable and adaptable solutions. The algorithms make use of data-driven decision making and cognitive reasoning to detect intricate patterns of fraudulent activity. Neural networks, deep learning, LR, DT, RF, and SVM Ultimately, learning models are a portion of the approaches that are applied in the sector.

1) LOGISTIC REGRESSION (LR): Mohammed and Maram [9] state that LR is one of the most often used techniques for resolving binary classification issues. At the same time, as credit cards have become the major method of payment in today’s world, fraudulent actions have proliferated. Thus, it has become evident that creating reliable fraud detection systems is essential. The reason LR is so commonly used is that it is simple to use and comprehend. Transaction features like amount, location, and merchant type can be utilized to identify credit card fraud, and LR has proved effective in doing so. Notwithstanding its benefits, LR could fail to identify intricate, nonlinear fraud schemes. Tanouz et al. examine the urgent need for an efficient fraud detection system in light of recent technological advancements. The study suggests using LR, random forest, and Naive Bayes, among other machine learning-based classification techniques, to address the issue of dataset imbalance in credit card fraud scenarios. ML must be used to combat the growing issue of credit card fraud. A few crucial metrics to assess these algorithms include recall, accuracy, precision, F1 score, confusion matrix, and Rocauc score [7]. This study examines four widely-used machine learning algorithms: Random Forest, Decision Tree, K-nearest neighbours, and LR, in the context of severely imbalanced datasets, which are commonly seen in credit card transaction data. Transactional aspects such as time, location, kind of purchase, value, vendor, and customer choice are examined in this work. To calculate the likelihood that a transaction is fraudulent, models utilizing statistical methods are supplied with all of these different data factors [8]. As previously mentioned, it is essential to have a solid ML This survey illustrates some of the strategies used to stop credit card theft. Two essential components of effective study in this field are extensive transactional data and meticulous comparisons of the various models.

2)DECISION TREES (DT)and RANDOM *FORESTS(RF):*

According to Zhang, there are no major issues with using DT and RF to manage non-linear data. Overfitting and data noise are well-known to be tolerated by RF, an ensemble learning technique based on several DT. Given that RF is a tree-growing technique that operates independently (as shown in figure 1.0), it may be used to a variety of fields, including CCFD, at a reasonable computing cost. As an ensemble method, RF makes use of the collective knowledge of several DT. Its innate capacity to successfully generalize into new data cases—to identify fraudulent credit card transactions—is provided by this combination of quite different trees, each of which was learnt on a different sample of the data. This allows it to adapt to noise and to shifting structural patterns. RF is made up of many different component trees and an ensemble structure. In other words, it poses a challenge to interpretability in light of all its uses. That is to say, its usefulness in accurately identifying fraudulent transactions is unaffected by the fact that it is more interpretative and complex than the other simple models. Numerous high-calibre studies attest to the effectiveness of RF in identifying credit card fraud. For example, Bhattacharyya et al. [10] used actual data from a global credit card operation in their analysis. Their findings demonstrated that, with a higher success rate and fewer false positives, RF outperformed other methods for detecting fraud. Dal Potzolo et al. [9] looked into RF-based models as a potential solution to the idea drift issue in credit card transaction data. Their tests using real-world datasets demonstrated appreciable increases in warning accuracy, demonstrating the method’s resilience to shifts in customer behaviour. Furthermore, other research (Dal Pozzolo et al., for example) compared RF with numerous other models, such as neural networks, SVMs, LRs, and KNNs. Christine and colleagues, Veronique and colleagues [11]. To the best of our knowledge, all those research show that when it comes to accuracy, AUC, and predictive power, RF is the best alternative.

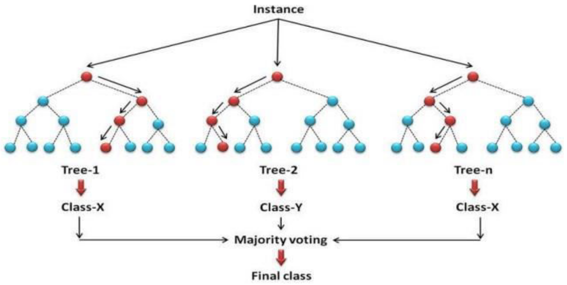


Fig. 1: Framework of RF

3) K NEAREST NEIGHBOUR (KNN):

One of the most widely used supervised machine learning techniques, KNN is effective at spotting instances of fraudulent credit card transactions. Its application in regression and classification research is its principal usage [12]. It provides an excellent detection facility with very few false-positive cases and works very well to get around fraudulent activity during transactions. To use this KNN-based method for fraud detection, two significant estimates must be produced, though: determining the links between transactions and calculating the distance between each transaction in the dataset. This approach is supported by the CCFD system since it has the ability to detect fraud instances when memory consumption is restricted. Finding anomalies in target variables is made possible by data separation and oversampling techniques, which improves the efficiency of handling datasets of various sizes. The KNN approach has several drawbacks in addition to its many advantages. Because source data sets have a high memory requirement and a propensity to highlight unimportant data properties, they present unique issues [13]. This is the CCFD process’s limitation, which may have an impact on the method’s accuracy and recall metrics.

4) SUPPORT VECTOR MACHINES (SVM):

Regression and classification studies have demonstrated the great utility of SVM, particularly in the field of CCFD [14]. Well-researched is the issue of intricate patterns in consumers’ credit card transaction behaviour. SVM techniques can be used to classify consumer behaviour as either lawful or illegal by providing extracted data sets pertaining to payment patterns. The SVM has exceptional performance and yields dependable classification outcomes, even when a limited number of attributes are eliminated from the dataset. However, there are disadvantages with huge datasets, which typically have more than 100,000 entries. This ensemble model’s performance was assessed using metrics such as accuracy, recall, and area under the curve. We are able to get approximately 95 percent accuracy effectiveness by combining SVM with RFC. The combined effect may reduce the quantity of transactions that are false positives and raise the sensitivity to 87 percent. Hence, by combining various methods for handling significant datasets, proper and improved fraud detection can be developed, [15]. The model's ability in detecting fraud has significantly improved, making privacy a metric of evaluation that is related to recall or accuracy and, consequently, should be related to the security of financial transactions.

It's crucial to remember that while the RFC approach can work well with small datasets, it has trouble scaling and producing good results with larger datasets. Therefore, the problem still lies in figuring out how to handle the massive amounts of data related to credit card transactions while maintaining an accuracy level that is acceptable in relation to operational efficiency. Generally speaking, SVMs perform well when it comes to the categorization of credit card transactions and when the number is modest. As a working scale increases, however, their performance deteriorates. Additional research utilizing certain appropriate methods for privacy-preserving models, such as federated learning and improved techniques for data privacy and accuracy—the best course of action for CCFD approaches. One method to handle imbalanced datasets could be to combine the RFC and SVM. It is capable of determining the decision boundary's ideal value in high-dimension space. Later on, hyperparameter tweaks and a customized kernel can change how effective SVM is.

5) NAIVE BAYES (NB):

NB classifiers are probabilistic classifiers that divide data into the classes that have the highest likelihood using Bayes conditional probability. Typically, fraud detection and prevention employ this strategy. The efficiency and interpretability of the classifiers make them appealing, especially when working with highly dimensional input data. They are more effective in making complicated decisions because they let experts' knowledge to be incorporated into ambiguous statements. On the other hand, the dataset's characteristics presumed conditional independence can dramatically reduce their predictive power. This assumption tends to produce lesser accuracy in datasets with redundant properties. In a study by Mohammed et al., the effectiveness of the NB classifier and other ML classifiers for the detection of credit card thefts in extremely big and unbalanced datasets was assessed.

Mahmud et al. [18] examined the efficacy of various machine learning algorithms in identifying instances of fraudulent credit card transactions. According to the study's findings, DT-based models outperformed NB methods in terms of classification accuracy. Lastly, Bahnsen et al. [19] presented a Bayes minimum risk strategy that takes into account the actual monetary costs associated with CCFD in order to address its financial impact. On a real-world transactional dataset, they showed that the suggested framework may be less expensive than more established methods like LR, DT C4.5, and RF. In a contribution, Mahmoudi and Duman assessed how well Linear Fisher discriminant analysis performed in comparison to NB, ANN, and DT. Using a real-world dataset from an unidentified Turkish bank, the When taken as a whole, these investigations show how subtle and successful NB classifiers are at detecting credit card fraud. While NB's speed and interpretability are quite good, they struggle to handle conditional independence of characteristics.

ire approach demonstrated its practical advantages over conventional measures by beating the state-of-the-art in both classical performance measures and maintaining the overall availability and limit. When taken as a whole, these investigations show how subtle and successful NB classifiers are at detecting credit card fraud. While NB's speed and interpretability are quite good, they struggle to handle conditional independence of characteristics. As a result, their implementations need careful thought, particularly in situations where fraud detection is crucial and a quick and dependable solution is needed.

6) GENETIC ALGORITHMS (GA):

The idea of GA was derived by John Holland from natural evolutionary processes. These algorithms function by sifting through a population of possibilities, often called chromosomes, which are encoded as strings of bits, in an effort to identify the most suitable answer. The work method of GA for effectively identifying potential instances of credit card theft is depicted in Figure 2.0. In order to increase security for credit card companies as well as their clients, these algorithms categorize credit card transactions as either suspicious or not. A genetic programming method that extended credit to reputable clients through a score system was presented by Bentley et al. Their results demonstrated that the generated rules had the best predictive performance when tested on a dataset of 4,000 transactions. In terms of classification accuracy, this method outperformed earlier Abased systems, especially when compared to models that relied on user behaviour, like Cha's algorithm.

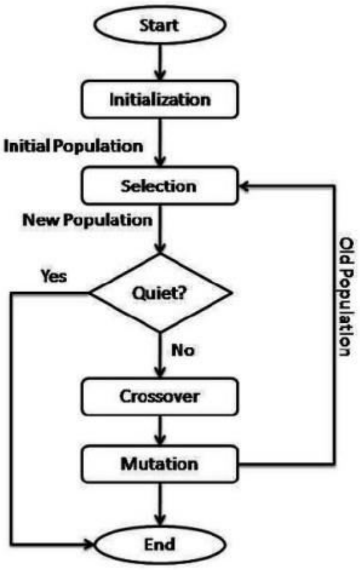


Fig. 2: Framework of RF

Prior research has mostly measured the rate of errors (False Negative Rate, or FNR) and the accuracy of forecasts (True Positive Rate, or TPR). But Chan et al. [20] offered a method for identifying suspicious activities by gauging cost-based models. In order to improve prediction capacity, Bei [21] suggested combining several algorithms. Numerous strategies, including diagnostic, resolution, best-match, density-selection, probabilistic-curve, and negative-selection procedures, are covered in some length in the publications. Results and probabilistic analysis have attested to the potential of neighbourhood-based algorithms as classification techniques. Additionally, researchers suggest employing diagnostic algorithms to compute confidence metrics, determine relative risk, and make decisions in ambiguous scenarios. The primary force behind GANNs, an integrated GA/NN method, is natural selection. By embedding the NN within the GA's DNA, GANN integrates the GA into the NN's architecture. In order to evaluate its parameter strings, a GANN approach first generates a pool of randomly chosen individuals. Next, the genetic data is used to train the NNs. GANN approaches compute the performance measure by using either the GA or the backpropagation training technique alone, and then they choose topologies that have a significant increase in fraud detection accuracy. To sum up, because GAs mimic the processes of evolution, they are a very powerful tool for searching and optimization. In the process of detecting credit card fraud, the algorithms have proven useful in improving accuracy, creating prognostic models, and streamlining decision-making processes. Fraud detection approaches can be greatly enhanced when NN is incorporated into GANN procedures.

7) HIDDEN MARKOV MODEL (HMM):

Through the application of transition probabilities, the HMM regulates the transitions between its small set of states [22]. As shown in Figure 3.0, each state is closely related to a probability distribution. The probability distribution in this formulation Conversely, this likelihood associated with specific states is employed to produce likely results or observations.

The reason the model is named HMM is because the states themselves are concealed, even though the data's obvious results are widely known. The CCFD system operates quickly and effectively because HMM has the innate capacity to process transactions at a high speed and identify fraudulent activity. One of the system's many advantages is that it can tell fraudulent from non-fraudulent transactions, which lowers the amount of false positive transactions [20]. The modelled component is essential since the HMM uses the cardholders' spending patterns as its major indicator of fraud. It is possible to effectively organize people's spending patterns by classifying these acts into several expenditure categories, typically denoted as low, moderate, and high. A technique for identifying possible fraudulent activity during credit card transactions is employed by the HMM-based fraud detection system. Of greater significance, the HMM model effectively reproduces the dynamic sequence and temporal pattern found in financial data. Using the sequential nature of the data, the system determines how to spot slight changes or anomalies in cardholder behaviour that might point to possible fraud. As a result of its ability to handle sequential data and behavioural patterns, the HMM is a very effective tool for identifying credit card theft situations [22]. Reducing the likelihood of false positives and accurately classifying various sorts of expenses make it essential for managing real-world credit card fraud detection difficulties.

8) FUZZY LOGIC BASED SYSTEM (FLBS):

In 1988, Zadeh made the first proposal for FLBS. By using fuzzy sets and numbers that describe values in an extremely easily understandable way, these systems offer a reliable way to handle uncertainty related to input and output variables. This framework offers a very clear classification system that ranks and groups transactions and processes into buckets according to their level of risk—low, moderate, or high. By bolstering security measures and enabling transactions to be categorized appropriately, fuzzy logic plays a critical role in CCFD [14]. It takes a significant amount of time and data to capture intricate patterns. Figure 4.0 depicts its structure. Sumanth et al. [16] have suggested a technique to enable the reliable identification of various types of credit card fraud, encompassing both in-store and online purchases, in light of the increased incidence of Valentine's Day scams and the startling increase in the use of debit cards for. A sizable credit card dataset is required for training and testing, as seen by the explosive growth of e-commerce. In conjunction with SVM, DNN, and NB algorithms, a deep neural network is used in this paper's comprehensive approach. This leads to a very accurate approach for identifying credit card fraud. Alarfaj et al. discuss the widespread issue of credit card fraud in online transactions within the same framework. This problem is exacerbated by the convenience and popularity of the previously described transaction kinds. the use of a range of machine learning techniques, including as XG Boost, DT, RF, SVM, LR, and Extreme Learning Method, to increase detection accuracy and lower fraud losses. The optimal CNN topologies, layering effects, and model combinations have been identified through thorough investigation and documentation in this study. Deep learning techniques are becoming more and more important in this field just by itself. The model that is suggested works better to.? No.? Journal of Entrepreneurship, Finance and Management, https://doi.org/10.1108/JEMPLARY02-2022-0046,Emerald Publishing Limited; 2022-01-??; doi: 10.1108/JF–02–2022–0046 15 compared to the current credit card ML and DL methods. A few considerations should be made in order to ensure security through thorough classification and quick fraud detection. Given that FDS may have a tendency to have a high computational intensity, more investigation and optimization are required. It appears that credit card fraud can be identified and categorized by the use of FLBS, which includes FNN and FDS. As they handle ambiguity and swiftly categorize transactions according to risk categories, they achieve a quantum leap in improving credit card security. Further study into the optimization of these systems and the reduction of computational complexity is necessary for enhanced efficacy and widespread application in financial fraud detection.

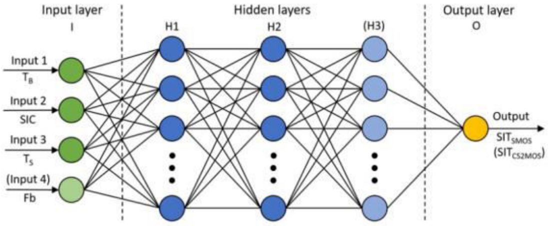


Figure 4.0: NN architecture [53]

Fig. 3: Framework of HMM [17]

9) NEURAL NETWORKS (NN) AND DEEP LEARNING (DL): Deep learning models such as Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs) have produced some very impressive outcomes [14]. This is due to the fact that intricate patterns must be recorded, which takes a significant amount of work and information. Figure 4.0 depicts its structure. Sumanth et al.'s [16] goal was to provide an accurate way of identifying credit card fraud cases in light of the growing number of Valentine scam cases and the significant shift in the use of debit cards for both in-store and online sales. Ecommerce's explosive growth confirms the need for a sizable credit card dataset for training and testing. This article presents a thorough approach that combines SVM, Deep DNN, and NB algorithms with a deep neural network. As a result, a system's ability to accurately detect credit card fraud can be highly enhanced. In this context, Alarfaj et al.'s attempt to address the widespread issue of credit card fraud in online purchases, which has been made possible by the simplicity and popularity of these kinds of transactions. The study looks into a variety of machine learning algorithms, including XG Boost, DT, RF, SVM, LR, and Extreme Learning Method, which are used to improve detection accuracy and lower losses caused by fraud. This study will go into great detail on various CNN topologies, layer effects, and model configurations in order to determine which combination works best and support the expanding significance of deep learning techniques. In comparison to existing ML and DL algorithms for credit card fraud, the model put forth here performs better; real data demonstrates accuracy of 99.9 percent, precision of 93 percent, f1-score of 85.71 percent, and AUC of 98 percent. Additionally, this study strives to lower false negatives and increase in-world efficacy; It reveals how successful these tactics are at combating credit card fraud. According to Esenogho et al, the increase in physical and online transactions brought about by Valentine's Day is one of the main fraud schemes that costs banks millions of dollars every year. Their novel approach helps them avoid the drawbacks of skewed credit card data sets and altered spending habits. They employ a hybrid data resampling technique that combines an LSTM neural network and an ensemble classifier with adaptive boosting, or AdaBoost.

III. RESEARCH FINDINGS OF MACHINE LEARNING APPLICATIONS FOR CREDIT CARD FRAUD DETECTION

The use of deep learning models, such as CNNs and RNNs, to address the issue of fraud detection in credit card systems is examined by Chen and Lai [23] in this study. Due to its capacity to detect intricate and constantly changing fraud schemes, deep learning models are said to be very useful in the battle against fraudulent deals. To address this specific issue, Afriyie et al. conducted research on the effectiveness of DT and RF in identifying fraudulent credit card transactions. The findings demonstrate that these algorithms perform exceptionally well in identifying intricate fraud patterns and in appropriately handling data nonlinearities. An academic caution exists regarding a condition known as overfitting. The employment of regularization processes is therefore given a lot of attention. Xia investigates the potential of SVM for detection. The capacity of SVM to quickly identify the best decision boundaries in high-dimensional feature spaces has been highlighted by the author. This capability aids in precisely identifying fraudulent activity. Additionally, a different study using an improved random forest approach to identify cases of credit card theft was conducted by Aftab et al. [88]. It is stressed that combating the tactics derived from frauds requires constant innovation in algorithms. Many academics have hypothesized that hybrid approaches—traditional approaches combined with machine learning algorithms—might offer an intermediary solution. Rule-based systems are combined with machine learning techniques in Socony et al.'s ensemble methodology. Such a combination is thought to have the ability to produce a strong and adaptable fraud detection system. Table 2.0 above also contains further relevant works on CCFD.

IV. CHALLENGES AND FUTURE DIRECTIONS

More work is still required to fully realize the potential of machine learning algorithms, despite their considerable promise. Authors also highlight the issue of class bias in the identification of credit card fraud. To combat this, researchers emphasize the use of cost-sensitive learning algorithms and resampling [24]. The problems with interpreting deep learning models' predictions are covered by Mishra et al. [25]. Although deep learning models are typically quite accurate, it can be difficult to communicate their decision-making processes and results to stakeholders in accordance with standards because of their opaque nature.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. CONCLUSION

There are many advantages and disadvantages to using both conventional and cutting-edge machine learning techniques in CCFD. Even if they are transparent and straightforward, traditional methods often fall short when dealing with intricate and ever-changing fraud practices. However, ML techniques such as DT lead to interpretable models but have overfitting issues. While effective, LR is susceptible to outliers. While NN are excellent at detecting patterns, they require a lot of computational power. NB appears to be quick, but its accuracy is compromised by underlying assumptions. There are dynamic choices regarding accuracy, interpretability, scalability, and privacy using GA, HMM, SVM, FLBS, and Hybrid Approaches. One must carefully weigh the benefits and drawbacks of accuracy, interpretability, and computing requirements when selecting algorithms in this maze.

REFERENCES

1. L. Einav, P. Klenow, J. Levin, and R. MurcianoGoroff, “Customers and Retail Growth.,” J. Monet. Econ., 2021, [Online]. Available: https://doi.org/10.1016/j.jmoneco.2021.09.004.
2. M. Dhone and G. Regulwar, “Learning For Anomaly Detection.,” J. Emerg. Technol. Innov. Res., 2020, [Online]. Available: https://doi.org/10.1201/b10867-5.
3. S. Daliri, “Using Harmony Search Algorithm in Neural Networks to Improve Fraud Detection in Banking System.,” Comput. Intell. Neurosci., 2020, [Online]. Available: https://doi.org/10.1155/2020/6503459.
4. A. Al-Faqeh, A. Zerguine, M. Al-Bulayhi, A. AlSleem, and A. Al-Rabiah, “Credit Card Fraud Detection via Integrated Account and Transaction Submodules,” Arab. J. Sci. Eng., vol. 46, pp. 10023–10031, 2021, [Online].Available: https://doi.org/10.1007/s13369-021-05856-5.
5. I. Sadgali, N. Sael, and F. Benabbou, “Human behavior scoring in credit card fraud detection.,” IAES Int. J. Artif. Intell., vol. 10, pp. 698–706, 2021, [Online]. Available: https://doi.org/10.11591/IJAI.V10.I3.PP698-706.
6. W. Hilal, S. A. Gadsden, and J. Yawney, “Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances,” Expert Syst. Appl., vol. 193, p. 116429, 2022, [Online]. Available: https://doi.org/10.1016/j.eswa.2021.116429.
7. J. Pan, “Deep Set Classifier for Financial Forensics: An application to detect money laundering,” 2022, [Online]. Available: https://doi.org/10.48550/arXiv.2207.07863.
8. T. Vairam, S. Sarathambekai, S. Bhavadharani, A. Dharshini, N. Sri, and T. Sen, “Evaluation of Na¨ıve Bayes and Voting Classifier Algorithm for Credit Card Fraud Detection.,” in 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), 2022, vol. 1, pp. 602–608, [Online]. Available: https://doi.org/10.1109/ICACCS54159.2022.9784968.
9. N. H. Mohammed and S. C. R. Maram, Fraud Detection of Credit Card Using Logistic Regression. 2022.
10. E. Ileberi, Y. Sun, and Z. Wang, “A machine learning based credit card fraud detection using the GA algorithm for feature selection.,” J Big Data, vol. 9, p. 24, 2022, [Online]. Available: https://doi.org/10.1186/s40537-022-00573-8.
11. Q. Zhang, “Financial Data Anomaly Detection Method Based on Decision Tree and Random Forest Algorithm,” J. Math., vol. 2022, no. 9135117, p. 10, 2022, [Online]. Available: https://doi.org/10.1155/2022/9135117.
12. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, “Data mining for credit card fraud: A comparative study.,” Decis. Support Syst., vol. 50, no. 3, pp. 602–613, 2011.
13. A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, “Credit card fraud detection and concept-drift adaptation with delayed supervised information.,” in In Neural Networks (IJCNN), 2015 International Joint Conference on IEEE, 2015, pp. 1–8.
14. F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, “Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms,” IEEE Access, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.
15. N. Rtayli and N. Enneya, “selection features and support vector machine for credit card risk identification.,” Procedia Manuf., vol. 46, pp. 941–8, 2020.
16. C. H. Sumanth, P. P. Kalyan, B. Ravi, and S. Balasubramani, “Analysis of Credit Card Fraud Detection using Machine Learning Techniques,” in 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2022, pp. 1140–1144, doi: 10.1109/ICCES54183.2022.9835751.

17. B.-J. Yoon, “Hidden Markov Models and their Applications in Biological Sequence Analysis,” Curr. Genomics, vol. 10, pp. 402-415., 2009, [Online]. Available: https://www.semanticscholar.org/reader/f7181dd96101b60fd397ef5d53c152b56fbff056.
18. M. S. Mahmud, P. Meesad, and S. Sodsee, “An evaluation of computational intelligence in credit card fraud detection.,” in In Computer Science and Engineering Conference (ICSEC), 2016 International, 2016, pp. 1–6.
19. A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. ¨orn Ottersten, “Cost sensitive credit card fraud detection using bayes minimum risk.,” in In Proceedings-2013 12th International Conference on Machine Learning and Applications, 2013, pp. 333–338.
20. et al. Chan, Philip K., “Distributed data mining in credit card fraud detection.,” in IEEE Intelligent Systems and Their Applications, 1999, pp. 67–74.
21. Y. Bei, “Detection and Resolution of Data Confliction in the Integration of Heterogeneous Information Sources.,” J. Beijing Univ. Technol., 2008.
22. M. Syeda, Y.-Q. Zhang, and Y. Pan, “Parallel granular neural networks for fast credit card fraud detection,” in 2002 IEEE International Conference on Fuzzy Systems. FUZZIEEE’02. Proceedings, 2002, vol. 1, p. 02CH37291.
23. J. Chen and K.-L. Lai, “Deep Convolution Neural Network Model for Credit-Card Fraud Detection and Alert.,” J. Artif. Intell. Capsul. Networks, vol. 3, pp. 101–112, 2021, doi: 10.36548/jaicn.2021.2.003.
24. M. Alamri and M. Ykhlef, “Survey of Credit Card Anomaly and Fraud Detection Using Sampling Techniques.,” Electronics, vol. 11, no. 23, p. 4003, 2022, [Online]. Available: https://doi.org/10.3390/electronics11234003.
25. R. Mishra, G. Reddy, and H. Pathak, “The Understanding of Deep Learning: A Comprehensive Review.,” Math. Probl. Eng., pp. 1–15, 2021.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details