Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2022, 9(7):72-80

Research Article ISSN: 2394 - 658X

Comparative Analysis On implementation in fraud detection systems Based on Machine Learning Methods

Kartheek Pamarthi

Kartheek.pamarthi@gmail.com

ABSTRACT

In this work, we look at how various machine learning models perform when faced with highly skewed datasets in an effort to detect credit card fraud. The three models that we examined in detail were Multilayer Perceptron (MLP), Random Forest, and Logistic Regression. We made use of a dataset that included 555,719 transactions, with 22 attributes recorded for each. The accuracy and hyperparameter tuning reliance of Random Forest were assessed, while MLP's capacity to detect non-linear patterns was put to the test. Logistic Regression was used as a baseline. We used ROC AUC, Matthews Correlation Coefficient (MCC), and precision-recall curves to assess the models' ability to detect fraudulent transactions. When it came to handling class imbalances and complex data linkages, the Random Forest model performed significantly better than others, with a ROC AUC of 0.9868 and an MCC of 0.6638. Despite its usefulness as a benchmark, Logistic Regression had limitations due to its high false positive rate. Although MLP had promise, it had a high false positive rate, indicating that the model may use some improvement.

Keywords: Machine Learning, Fraud detection, Security.

INTRODUCTION

In 1996, Citibank and Wells Forgo Bank were the first US banks to offer consumers online banking [1]. Prior to this, users could only access their accounts in person. People started using credit cards online as internet banking became widely available. Social media, internet banking, online shopping, and electronic payment systems are just a few of the many developments in the past decade that have played a role in this.

This is why criminals are stepping up their efforts to steal money from people making purchases online using different payment methods. New digital technologies, especially those that facilitate currency transactions, have altered people's day-to-day approaches to managing their finances. Many payment systems have made a massive shift from using physical payment stations to using digital platforms [2]. A lot of economists have turned to digital transactions, which leverage technology, to keep productivity and competitive advantage going. Consequently, consumers have found that using their credit cards for online banking and other transactions is a simple way to handle their finances and other banking needs without leaving the comfort of their homes or offices.

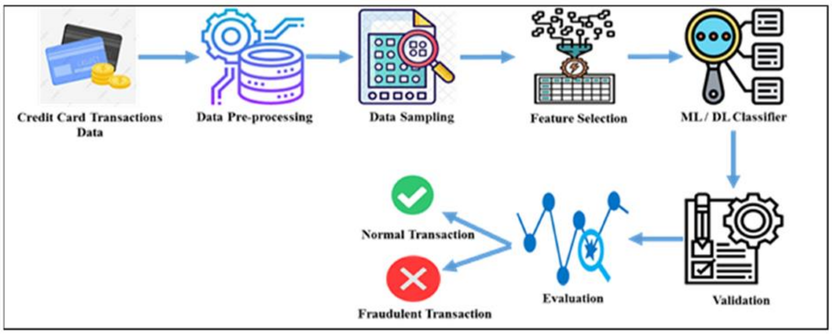

Figure 1: The process of finding fraudulent credit cards.

This is one way to find credit card scams. In order to pay with a credit card, the user or customer must provide the right information.

To check for fraudulent processing, the transaction data is first sent to a verification module, which labels them as non-fraud or fraud (Figure 1). Credit cards allow customers to make purchases at any time and in any place they want by storing their personal information on a plastic card that is provided by a financial institution [3]. Credit card fraud is when someone illegally gets money or things by using someone else's credit card, either online or in person. Credit card fraud is a common occurrence that frequently results in substantial monetary losses. Online transactions no longer necessitate physical cards; instead, just the card's information is needed to finalise a purchase, making fraud easier to pull off than in the past. The advent of credit cards, according to [4], has transmitted not only monetary policy but also the strategies and tactics employed by both large and small firms. The Bank of Ghana (BoG) lost about 1.26 million cedis ($250,000) to credit card theft in 2019. The loss went up to 8.20 million cedis ($1.46 million) in 2020 (BoG, 2021). This was a 548.0% bigger loss than the previous year.

While fraud has been on the rise across all payment methods in recent years, it has been most noticeable in online purchases. Payment fraud can occur in many forms, including but not limited to: house transfers, automated clearing, online payments, automated bill payments, P2P, wire transfers, automated clearing houses, debit and credit card transactions, and ATM transactions. It can be difficult to capture criminals because they often use aliases and free software like Anchor to establish Virtual Private Network (VPN) tunnel connections or commit physical robberies from obscure locations. Compliance and risk management firms that operate online have also demonstrated a strong interest in AI and ML models for fraud detection. Models such as Decision Tree, Logistic Regression, Random Forest, Ada Boost, XG Boost, Support Vector Machine (SVM), and Light GBM are just a few examples [5].

This is essential since identifying fraudulent charges on credit cards is a classification and prediction issue. The methods described earlier have shown that supervised machine learning models are the most effective at detecting fraud. This is going to serve as the basis for our comparison of three methods for identifying fraudulent financial transactions: Decision Tree, Logistic Regression, whereas Random Forest.

LITERATURE REVIEW

Machine Learning Techniques for Credit Card Fraud Detection:

Credit card fraud detection was the focus of this study's evaluation of multiple ML approaches [6]. Among these methods were logistic regression, random forests, decision trees, and support vector machines.

Out of all the solutions they studied, ensemble methods—which include random forests—were shown to be the most efficient and accurate. Several machine learning models were evaluated in a comparative research [7] for their ability to identify credit card fraud. Logistic regression, k-nearest neighbours, and artificial neural networks were among the models included in this set.

Neuronal networks outperformed other methods in detecting fraud and handled complicated patterns better, according to the study. A further study examined the efficacy of various ML algorithms in detecting credit card fraud [8]. These algorithms included deep learning models, gradient boosting machines, and support vector machines. The results showed that convolutional neural networks and other deep learning models performed far better than other methods when it came to detecting fraudulent transactions.

The article included a proposal for an adaptable method for detecting idea drift using Hoeffding Adaptive Trees (HAT) [9].

When compared to more conventional batch learning methods, the HAT algorithm performed better when it came to detecting credit card fraud using concept drift. In order to detect credit card fraud, Adaptive Random Forest (ARF) was proposed as a new method to handle concept drift in [10].

In order for the model to adjust to changing fraud trends, ARF integrates ensemble learning with incremental learning. Results showed that ARF kept detection accuracy high and successfully dealt with idea drift. In order to identify instances of credit card fraud, a combination of online learning and change detection methods was proposed in [11].

This method used statistical change detection approaches to identify concept drift and continuously updated the model with incoming data. When compared to more conventional batch learning techniques, the hybrid strategy performed better. A machine learning solution's efficacy and efficiency are typically impacted by the data's properties and the learning algorithms' performance. Developers of data-driven systems can save time and effort by using one of many machine learning methods, including clustering, regression, classification, feature engineering, dimensionality reduction, association rule learning, reinforcement learning, and many more [12]. Deep learning, a branch of machine learning, has its roots in artificial neural networks (ANNs). That is why picking a learning algorithm that works in a specific area isn't always a sinch.

Because each learning algorithm has its own unique goal, and because even within a single category, results can change based on data properties [13]. "Applications of Machine Learning" gives a brief summary of numerous practical domains where knowledge of the concepts and implementations of various machine learning algorithms might be useful. A few examples of these fields are context-aware systems, sustainable agriculture, healthcare, cybersecurity, smart cities, and COVID-19.

Considering the significance and possibilities of "Machine Learning" in assessing the mentioned data, this article offers a thorough synopsis of several machine learning algorithms that might improve the intelligence and capacities of an application. An explanation of the concepts and potential uses of various machine learning algorithms in the aforementioned real-world domains is, thus, the principal contribution of this research.

Consequently, the purpose of this work is to provide academics and business professionals with a solid grounding in machine learning and its practical applications to the study, research, and creation of intelligent systems that are driven by data.

TYPES OF MACHINE LEARNING TECHNIQUES

Supervised, unsupervised, semi-supervised, and reinforcement learning are the four basic types of machine learning algorithms (Fig. 2) [14]. This article will take a look at the different learning methods and how they could be applied to real-world issues.

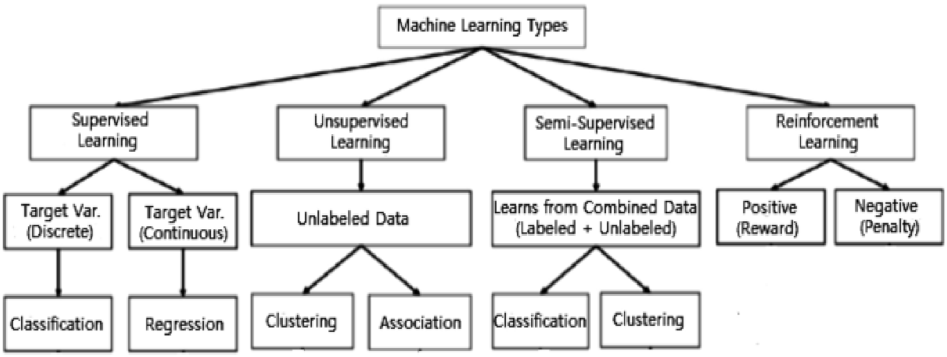

Figure 2: Different Machine Learning Approaches

Supervised: In machine learning, supervised learning usually entails using input-output pairs as examples to develop a function that converts one type of data into another. It uses a collection of training examples and labelled training data to infer a function. One type of supervised learning is a task-driven approach, which uses a predefined set of inputs to achieve certain goals [15]. The "classification" function is employed for data categorization, whereas the "regression" function employs data fitting. Both of these tasks are common in the supervised workforce. Text categorization, in which a piece of text like a tweet or a review of a product is used to forecast its class label or mood, is one use of supervised learning.

Unsupervised: An example of a data-driven process, unsupervised learning examines datasets that are not labelled [16]. This is frequently employed for exploratory reasons, finding significant trends and structures, extracting generative features, and grouping findings. Clustering, dimensionality reduction, identifying association rules, anomaly detection, feature learning, density estimation, and so forth are among the most prevalent unsupervised learning tasks.

Semi-supervised: By utilising both labelled and unlabeled data, semi-supervised learning mixes supervised and unsupervised methods to produce predictions [17]. Learning "without supervision" and learning "with supervision" are thus complementary. Practical applications of semi-supervised learning include situations when labelled data is few and unlabeled data is abundant. An ideal semi-supervised learning model would outperform its labelled data-only counterpart when it comes time to make predictions. Applications of semi-supervised learning include machine translation, text categorization, data labelling, and fraud detection.

Reinforcement: The application of reinforcement learning—a machine learning technique—by software agents and computers to autonomously ascertain the best course of action in every given situation is an example of an environment-driven strategy [18]. Using the insights provided by eco-activists, this reinforcement learning approach aims to maximise reward and avoid risk. It is a fantastic tool for training AI models for complex systems like supply chain logistics, autonomous driving, manufacturing, and robots, but it isn't effective for tackling fundamental or simple problems.

CYBER FRAUD DETECTION TECHNIQUES

Here we address RQ1, which searches for the ML/DL techniques used to detect cyber crime on credit cards from 2019 to 2021.

Machine Learning

Machine learning was recognised as a technique applicable to numerous issues, particularly in fields that demand processing and analysis of data. The imbalanced dataset can be corrected using machine learning (ML), which can be categorised as supervised, unsupervised, or reinforced ML. Machine learning (ML) methods are highly effective in identifying and avoiding fraud due to their capacity to automatically recognise trends across large datasets.

Differentiating between legal and fraudulent conduct becomes easier with the right ML models. These astute systems might eventually adjust to covert fraud methods. This can only happen if thousands of calculations are done accurately in milliseconds. In order to better detect cyber fraud, the next generation of fraud defences should include supervised and unsupervised technology.

Machine learning (ML) algorithms are trained using supervisory learning, which utilises labelled data sets and adjustable data sets with known variable targets.

Among the many applications of supervised learning are classification, regression, and inference. The most popular machine learning (ML) approach is supervised learning, which uses a huge dataset of correctly tagged transactions to train models. There are two possible outcomes for every given transaction: fraudulent and genuine. The models are taught to mimic real behaviour by feeding them massive amounts of tagged transaction data.

Unsupervised learning is the method of choice for training ML algorithms when the dataset contains variables with unclear definitions. The model's goal, when fed data, is to extract meaningful patterns. Unsupervised learning methods include things like cluster segmentation and dimension extraction.

Hybridising supervised and unsupervised learning, semi-supervised learning involves training a model using unlabeled data. This method finds the optimum data representation with the help of the unsupervised learning attribute and then utilises the directed learning attribute to look for relationships inside it and make predictions.

Various supervised, unsupervised, and semi-supervised ML methods were employed in the aforementioned experiments. To demonstrate how often the methodology is used, Table 1 shows how often ML and DL techniques appear in the literature that was evaluated. It is important to note that multiple articles used multiple ML/DL approaches.

Table 1: The number of times ML and DL are used in credit card scams.

Learning type	Technique	Usage frequency	Reference
Supervised	Logic regression (LR)	52	Adityasundar et al. (2020), .
	Naive Bayes (NB)	42	Sujatha (2019), Soni (2021)
	Decision tree (DT)	49	Dornadula & Geetha (2019)
	Random forest (RF)	74	Amusan et al. (2021)
	K-near neighbor (KNN)	39	Asha & Suresh Kumar (2021)
	Support vector machine (SVM)	56	Al Rubaie (2021).
Unsupervised	Hidden Markov model (HMM)	7	Singh et al. (2019).
	K-means	7	Palekar et al. (2020).
	Isolation forest	19	Dornadula & Geetha (2019),
Semi-supervised	Semi-supervised learning	3	Dzakiyullah, Pramuntadi & Fauziyyah (2021)
Reinforcement	Reinforcement	1	Dang et al. (2021)
Ensemble learning	ADA Boost	20	Krishna, Nagini & Tatayyanaidu (2019),
	RUSBoost	2	Al-Faqeh et al. (2021), Arora et al. (2020).
Deep learning	CNN	7	Carrasco & Sicilia-Urbán (2020)
	DNN	4	Sireesha et al. (2020)
	DCNN	4	Nguyen et al. (2020).
	Long short-term memory (LSTM)/BILSTM	8	Benchaji, Douzi & El Ouahidi (2021)
Sampling technique	Synthetic minority over sampling technique (SMOTE)	17	Choubey & Gautam (2020) et al. (2020)
	The adaptive synthetic (ADASYN)	3	Vijay Rahul et al. (2021)

Random Forest

Classification is where random forest really shines as a machine learning system. It works with data that is linear and data that is not. When dealing with unbalanced datasets, random forest outperforms all other machine learning algorithms. When dealing with an uneven dataset, it is impossible to use a single basic classifier. The suggested approach use random forest to identify instances of fraud in an imbalanced dataset with a lower frequency of frauds. Even with the unbalanced sample, the authors here used random forest. They employed two datasets, one with a fixed amount of fraud cases and one with a variable amount of cases. The suggested model, however, has an RF algorithm that is more accurate than its predecessors. RF uses a combination of decision trees, with a majority vote deciding the ultimate outcome. Additionally, it deals with the issue of overfitting. A notable imbalance ratio exists in the training sample, with a minority:majority ratio of 0.001:0.999. Traditional classifiers might not cut it in this scenario. Using RF in this way has the added benefit of making full use of all available data while preserving crucial information about the majority class.

Linkage of Blockchain with Machine Learning in the Proposed Model

Over the last several years, blockchain technology has been utilised to bolster privacy and security in a variety of networks. Blockchain is still susceptible to fraudulent activity, despite its intriguing features. The bad actors might use techniques like a double-spending assault to conduct illegitimate and fraudulent transactions. The proposed solution combines blockchain and machine intelligence to tackle this problem. The underlying study makes use of the bitcoin transaction database to train the proposed ML model. We look at the database's transaction pattern for when we need to refer back to it. All of these transactions are taking place simultaneously on the Ethereum network. Assumption: These transactions will reflect the typical pattern of bitcoin transactions. An additional feature of Ethereum is that the machine learning model is taught with each new transaction. To decipher it, we look at how it compares to the Bitcoin transaction pattern. The new transaction is considered legitimate or malicious if its pattern is identical to the other transaction's pattern. The proposed method is tested in the underlying study using a double-spending attack. As seen in Figure 3, a machine learning model confirms a transaction that is based on the blockchain. If the transaction is legitimate or malicious, this model will reveal it. The prediction is based on the machine learning model's performance during training and testing on a dataset that includes bitcoin transactions.

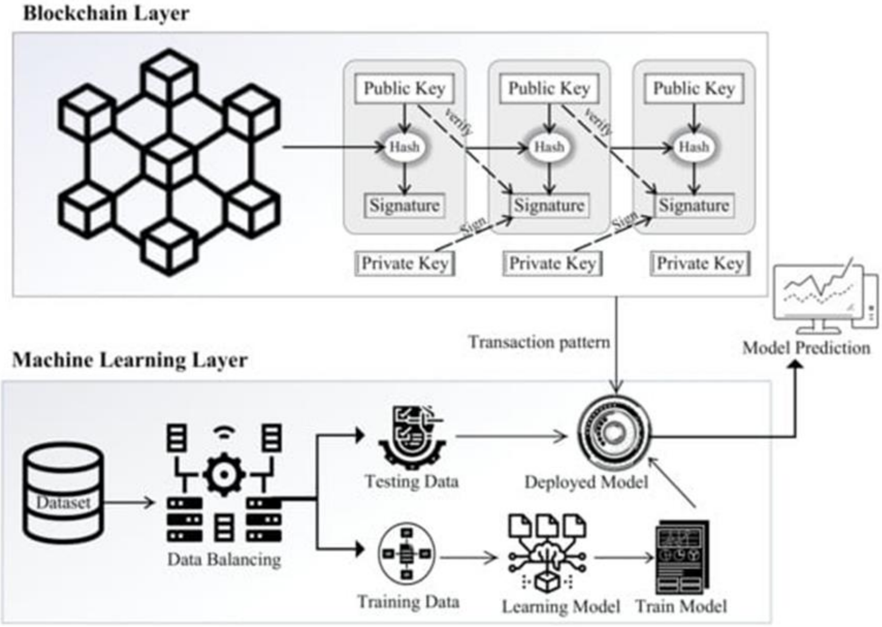

Figure 3: Blockchain and ML as a system mode.

Data Balancing Using SMOTE

Data imbalance, namely the unequal distribution of classes, is a big issue in machine learning. Uneven data makes machine learning systems less accurate. If there are more instances of one class than the other, it will increase. As a result, SMOTE is used to generate synthetic samples at random for the minority class.

When data is randomly oversampled, overfitting might occur; this method prevents it. The method relies on selecting a single data point from the minority group at random. After that, its neighbours are given random weights and then added to the initial samples. Combining samples from underrepresented groups is SMOTE's primary objective. When data is balanced, machine learning algorithms work better and produce better outcomes. Because the data's class distribution is skewed, Algorithm 1 employs SMOTE to level the playing field. The initialization, input, and output of the variables are displayed on lines 1 through 6. You can see how SMOTE balances data in lines 7–16. Using the K-nearest neighbour pattern, SMOTE is able to create artificial data. Step one is for SMOTE to pick data at random from the minority group. The second step is to locate the K-nearest neighbours of the dataset. Finally, the data that has been randomly selected is used in conjunction with K-nearest neighbours to create synthetic data.

RESULTS AND DISCUSSION

Here we show the outcomes of our suggested model's simulations before moving on to show the results after subjecting the system to two recent cyberattacks—the Sybil assault and the double-spending attack.

See Figures 4 and 5 for evidence of the extremely skewed nature of the chosen dataset. An imbalance in the data causes the classification models to favour the majority class.

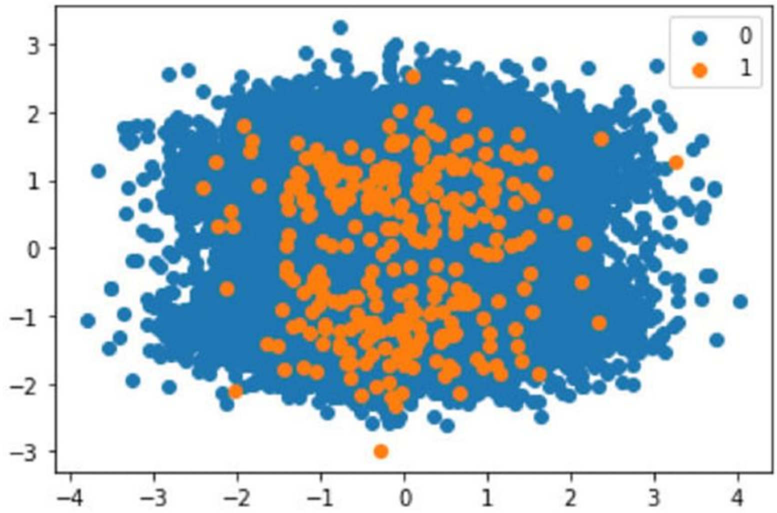

Figure 4: Imbalanced data.

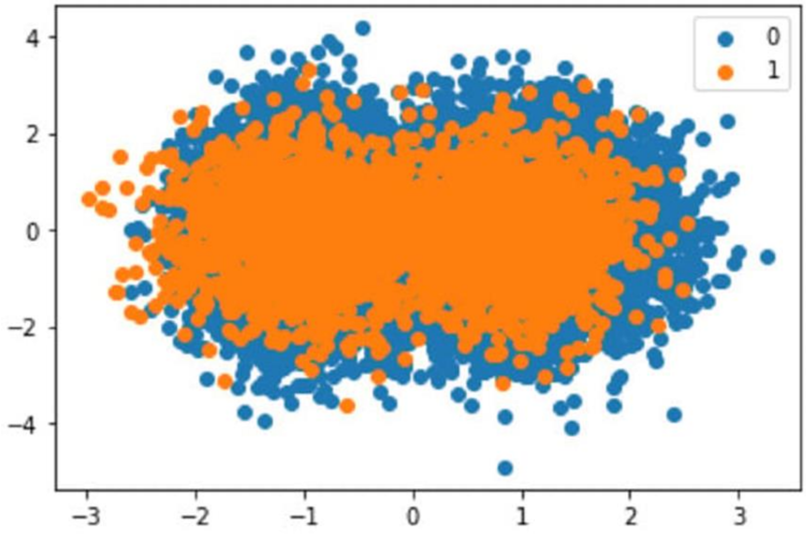

Figure 5: Balanced data.

Both legitimate and dishonest transactions can be seen in Figure 4. The figure clearly shows that there are more legitimate transactions than fraudulent ones. A bias in the classification results from the data's uneven nature. This difficulty is solved by using synthetic data. Using SMOTE, the harmful entities are oversampled. To reduce the model's categorization bias, the synthetic transactions are included in the dataset. Figure 5 displays the outcomes that were achieved by the utilisation of SMOTE.

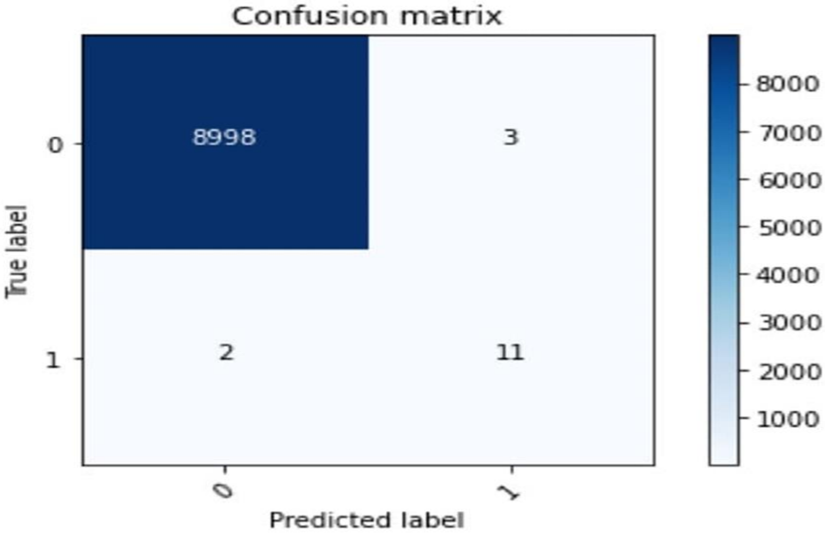

Figure 6: Confusion matrix through random forest.

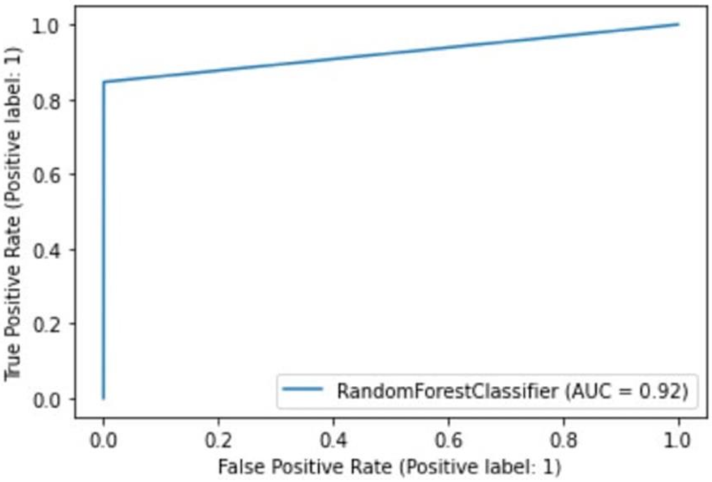

Figure 7: Accuracy of random forest.

The confusion matrix that was created via RF is displayed in Figure 6. With 9009 accurate predictions, random forest picks 9014 samples at random from this matrix. Thus, the proposed paradigm effectively separates nefarious from lawful interactions. True negatives, with a probability of 99%, produce the maximum values, as seen in the matrix. The number of values is lower in the other three circumstances as well. That the suggested methodology can effectively identify genuine negative transactions is demonstrated here. When it comes to categorization, the random forest model performs better thanks to the phenomena of majority voting. A random forest's area under the curve (AUC) is displayed in Figure 7. The area under the curve (AUC) shows how accurately the model separates the positive and negative categories. The AUC number jumps up to nearly 0.85 at the start, which is rather noticeable. Following that, there is a steady rise up to the maximum value of 0.92 AUC. The random forest model captures both valid and fraudulent transactions well, with an AUC of 0.92.

CONCLUSION

Credit card cyber fraud detection using ML/DL methods was the major emphasis of this assessment. There are three perspectives from which we assessed ML/DL models: technique, learning-based fraud detection, and ML/DL performance valuation. The years 2019, 2020, and 2021 were selected as the primary research years for this study. In order to address the four research questions, we combed through 181 academic articles. This in-depth analysis has covered all you need to know about deep learning and machine learning, including how they work, how to pick the right approaches, and how to spot credit card cyber theft. Cyber credit card fraud detection trends, gaps, future directions, and limits are all included in the report. Researchers and the financial industry can use this thorough evaluation to create innovative solutions for cyber fraud detection, in our opinion. Our findings from this analysis lead us to believe that unsupervised and semi-supervised learning methods need further investigation. Our findings leads us to believe that DL methods might benefit from additional study in the fight against cybercrime involving credit cards. We encourage more study into how to integrate ML/DL algorithms for better detection results. Because the datasets are so skewed, researchers should also apply under sampling and oversampling approaches. In addition, it would be helpful if researchers could provide credit to the datasets and performance measures used to convey the results. For the sake of future study, banks should also make public datasets including information on various fraudulent acts that have occurred around the country.

REFERENCES

[1]. S. Madan, S. Sofat, D. Bansal, Tools and Techniques for Collection and Analysis of Internet-of-Things malware: A systematic state-of-art review, J. King Saud Univ. - Comput. Inf. Sci. (2021) xxxx, http://dx.doi.org/10.1016/j.jksuci.2021.12.016.

[2]. F.C. Yann-a, Streaming active learning strategies for real-life credit card fraud detection: Assessment and visualization, 2018.

[3]. V. Nath, ScienceDirect credit card fraud detection using machine learning algorithms credit card fraud detection using machine learning algorithms, Procedia Comput. Sci. 165 (2020) 631–641, http://dx.doi.org/10.1016/j.procs.2020.01. 057.

[4]. T. Pencarelli, The digital revolution in the travel and tourism industry, Inf. Technol. Tourism (2019) 0123456789, http://dx.doi.org/10.1007/s40558-019- 00160-3.

[5]. S.B.E. Raj, A.A. Portia, A. Sg, Analysis on Credit Card Fraud Detection Methods. (2011) 152–156

[6]. Bhattacharyya, S., Ghosh, M., and Sural, S., (2010). Credit Card Fraud Detection: A Fusion Approach Using Dempster-Shafer Theory and Bayesian Learning. Decision Support Systems, 48(2), 282-291, doi: 10.1016/j.dss.2009.07.005

[7]. Yang, C., Liu, G., Yan, C., & Jiang, C. (2021). A clustering-based flexible weighting method in AdaBoost and its application to transaction fraud detection. Science China Information Sciences, 64, 1-11.

[8]. Harwani, H., Jain, J., Jadhav, C., & Hodavdekar, M. (2020). Credit card fraud detection technique using hybrid approach: An amalgamation of self-organizing maps and neural networks. International Research Journal of Engineering and Technology (IRJET), 7(2020).

[9]. Jagdish, S., Singh, M. and Yadav, V. (2020). Credit Card Fraud Detection System: A Survey, Journal of Xidian University, 14(5). doi: 10.37896/jxu14.5/599.

[10]. Li, C., Ding, N., Dong, H., & Zhai, Y. (2021). Application of credit card fraud detection based on CS-SVM. International Journal of Machine Learning and Computing, 11(1), 34-39.

[11]. Lucas, Y., Portier, P. E., Laporte, L., Calabretto, S., He-Guelton, L., Oblé, F., & Granitzer, M. (2019, June). Dataset shift quantification for credit card fraud detection. In 2019 IEEE second international conference on artificial intelligence and knowledge engineering (AIKE) (pp. 97-100). IEEE.

[12]. Lucas, Y., Portier, P. E., Laporte, L., He-Guelton, L., Caelen, O., Granitzer, M., & Calabretto, S. (2020). Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. Future Generation Computer Systems, 102, 393-402.

[13]. Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M. S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. IEEE Access, 7, 93010-93022.

[14]. Adityasundar et al. (2020) Adityasundar N, SaiAbhigna T, Lakshman B, Phaneendra D, MohanKumar N. Credit card fraud detection using machine learning classification algorithms over highly imbalanced data. Journal of Science and Technology. 2020;5(3):138–146. doi: 10.46243/jst. 2020.v5.i3.pp138-146

[15]. Sujatha (2019) Sujatha M. A comparative study of credit card fraud detection using machine learning for United Kingdom dataset. International Journal of Computer Science and Information Security (IJCSIS) 2019;17(9):2019.

[16]. Dornadula & Geetha (2019) Dornadula VN, Geetha S. Credit card fraud detection using machine learning algorithms. Procedia Computer Science. 2019; 165:631–641. doi: 10.1016/j.procs.2020.01.057

[17]. Amusan et al. (2021) Amusan E, Alade O, Fenwa OD, Emuoyibofarhe JO. Credit card fraud detection on skewed data using machine learning techniques. Lautech Journal of Computing and Informatics. 2021;2(1):49–56

[18]. Asha & Suresh Kumar (2021) Asha RB, Suresh Kumar KR. Credit card fraud detection using artificial neural network. Global Transitions Proceedings. 2021;2(1):35–41. doi: 10.1016/j.gltp.2021.01.006.

[19]. Al Rubaie (2021) Al Rubaie EMH. Improvement in credit card fraud detection using ensemble classification technique and user data. International Journal of Nonlinear Analysis and Applications. 2021;12(2):1255–1265. doi: 10.22075/IJNAA.2021.5228.

[20]. Singh & Jain (2019) Singh A, Jain A. Financial fraud detection using bio-inspired key optimization and machine learning technique. International Journal of Security and Its Applications. 2019;13(4):75–90. doi: 10.33832/ijsia.2019.13.4.08

[21]. Palekar et al. (2020) Palekar V, Kharade S, Zade H, Ali S, Kamble K, Ambatkar S. Credit card fraud detection using isolation forest. International Research Journal of Engineering and Technology (IRJET) 2020;7(3):1–6.

[22]. Dornadula & Geetha (2019) Dornadula VN, Geetha S. Credit card fraud detection using machine learning algorithms. Procedia Computer Science. 2019; 165:631–641. doi: 10.1016/j.procs.2020.01.057.

[23]. Dzakiyullah, Pramuntadi & Fauziyyah (2021) Dzakiyullah NR, Pramuntadi A, Fauziyyah AK. Semi-supervised classification on credit card fraud detection using autoencoders. Journal of Applied Data Sciences. 2021;2(1):1–7. doi: 10.47738/jads. v2i1.16

[24]. Dang et al. (2021) Dang TK, Tran TC, Tuan LM, Tiep MV. Machine learning based on resampling approaches and deep reinforcement learning for credit card fraud detection systems. Applied Sciences. 2021;11(21):10004. doi: 10.3390/app112110004

[25]. Krishna, Nagini & Tatayyanaidu (2019) Krishna NM, Nagini MVV, Tatayyanaidu G. A new hybrid method for credit card fraud detection on financial data. International Journal of Science Engineering and Advance Technology. 2019;7(7):2019

[26]. Al-Faqeh et al. (2021) Al-Faqeh AWK, Zerguine A, Al-Bulayhi MA, Al-Sleem AH, Al-Rabiah AS. Credit card fraud detection via integrated account and transaction submodules. Arabian Journal for Science and Engineering. 2021;46(10):10023–10031. doi: 10.1007/s13369-021-05856-5.

[27]. Carrasco & Sicilia-Urbán (2020) Carrasco RSM, Sicilia-Urbán MÁ. Evaluation of deep neural networks for reduction of credit card fraud alerts. IEEE Access. 2020;8 doi: 10.1109/ACCESS.2020.3026222. 186421–186432.

[28]. Sireesha et al. (2020) Sireesha M, Jyothirmayi K, Divya B, Kalyan GS. Master card fraud detection using arbitrary forest. International Journal for Recent Development in Science and Technology (IJRDST) 2020;4(7):2020

[29]. Nguyen et al. (2020) Nguyen TT, Tahir H, Abdelrazek M, Babar A. Deep learning methods for credit card fraud detection. ArXiv preprint. 2020.

[30]. Benchaji, Douzi & El Ouahidi (2021) Benchaji I, Douzi S, El Ouahidi B. Credit card fraud detection model based on LSTM recurrent neural networks. Journal of Advances in Information Technology. 2021;12(2):113–118. doi: 10.12720/jait.12.2.113-118.

[31]. Choubey & Gautam (2020) Choubey R, Gautam P. Combined technique of supervised classifier for the credit card fraud detection. Shodah Sarita. 2020; 7:27–32.

[32]. Vijay Rahul et al. (2021) Vijay Rahul A, Gowda A, Sunhith P, Pasha MSM. Using machine learning to detect credit card fraudulent transactions. International Research Journal of Modernization in Engineering Technology and Science. 2021; 3:2582–5208.