2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) | 979-8-3503-4367-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICAECT60202.2024.10469399

Analysis of Machine Learning Based Credit Card Transaction and its Applications

S.Venkatachalam [a*], P.Priyadarsini [b], K.Jayasree [c], Vikas Bhimrao Pawar [d], R. Sasikala [e], S. Loganathan [f]

[a] Department of Management, Karpagam Academy of Higher Education, Coimbatore, INDIA
[b] Department of Management Studies, Tagore Engineering College, Chennai, INDIA
[c] Department of Master of Business Administration, Panimalar Engineering College, Chennai, INDIA
[d] Department of Applied Science, Bharati Vidyapeeth College of Engineering, Navi Mumbai, INDIA
[e] Department of MBA, S. A. Engineering College (Autonomous), Chennai -600077, India
[f] CSE, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, India
**srisvenkatachalam@gmail.com*

Abstract—**In this paper fraudulent crediting of amounts is the primary challenge that clients encounter in the finance sector. On the other side, frauds have accompanied credit card innovation since it began. Many rule-based techniques that were used in the past to identify fraud were ineffective at managing the large number of variables. However, in order to prevent customers from paying for more credit, it is imperative to detect fraud. Machine learning techniques in an effort to combat corruption, the government is also pushing digital currency in this day and age. Although many people use credit cards and ATM cards to complete their transactions, they are not aware of the potential for fraud. An attacker utilizes the information of others to perform a fraudulent transaction, which results in billions of dollars' worth of losses annually. To lower the losses, effective fraud detection algorithms can be applied. The sophisticated machine learning methods these algorithms rely on can be useful to fraud investigators.**

Keywords—Credit, Customers Finance, Machine learning, Savings.

I. Introduction

Acceptance of Credit Cards through Supervised Learning this work uses the Supervised Learning method to solve the problem, which needs to be implemented in order for the credit card to be approved. Furthermore, Supervised Learning techniques are employed to compare the accuracy of the product against multiple established criteria[1]. The outcome demonstrates that the optimal accuracy for Naive Bayes, KNN, Decision Trees, and Logistic Regression is 84.32%, 98.13%, 99.62%, and 98.50%, respectively.

II. Applications

Fig 1Investigations on credit Label creation using big data from electricity examined the business model and model architecture of credit rating in the credit industry, including data collecting, model design, service aims, fees, and profit model, through research and literature study[2]. The discovered that the cornerstone of national life and the growth of the commercial economy is corporate credit, which serves as the basis for the social credit system[3]. Additionally, power credit uses power characteristics, specific application circumstances, and values derived from power data to produce a power credit label that serves as the foundation for credit evaluation[4]. Thus, this paper uses big data on electricity (i.e., transaction tariff, electricity sales, electricity consumption customers, etc.) and other technologies like expert rules, statistical modeling, mining algorithms, clustering algorithms, and other mining algorithms.

III. Predicting credit card default System

Credit card firms use new applicants' personal information and credit data to establish an accurate credit score. Many researches have used machine learning to examine and forecast credit scores[5].

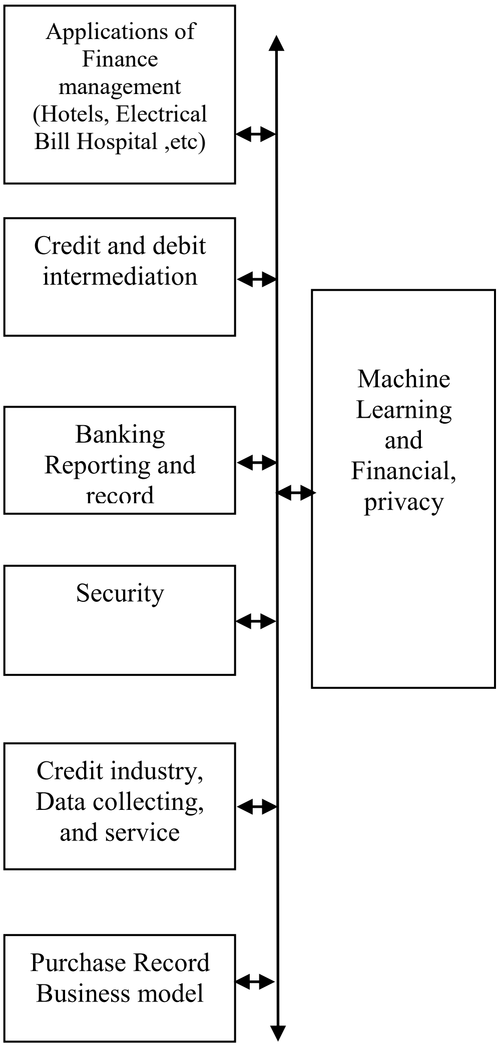
Applications of Finance management (Hotels, Electrical Bill Hospital ,etc)
Credit and debit intermediation
Banking Reporting and record
Security
Credit industry, Data collecting, and service
Purchase Record Business model
Machine Learning and Financial, privacy

Fig. 1. Block diagram

But prior work could not address the issue of various histories of the same consumer using different cards, nor could it improve prediction accuracy using single methods like ensembles or deep learning[6]. To solve these challenges, this paper presents a hybrid approach that combines a deep learning algorithm specialized in tabular data, TabNet, with heterogeneous ensembles.

IV. Prevent Credit Card Fraud as a Security Measure

Fig 2 Cyber security is in high demand as a result of the rise in cybercrime[7]. Businesses must defend themselves against attacks, maintain a positive public image, and, most importantly, safeguard critical data and confidential user information[8]. Individuals are suffering significant financial, privacy, and data losses.

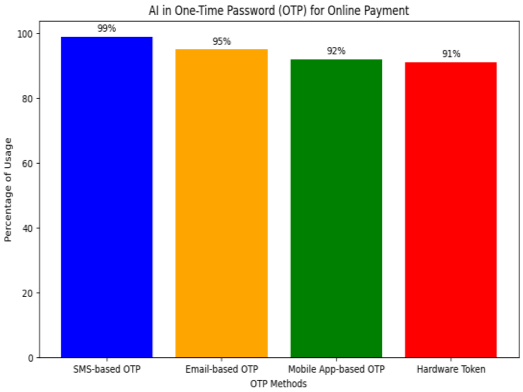

Fig. 2. Output Online Security Payment

V. Predicting Credit Loan Default Using Data Mining

This statistics includes basic information, social relationships, and consumption patterns. Address information is one such piece of information that is extracted from the vast amounts of customer data that are mined on behalf of borrowers[9]. These factors are combined to form a model that effectively predicts personal credit risk[10]. The findings demonstrate that the XGBoost model outperforms the Random Forest and Logistic Regression models in terms of prediction accuracy.

VI. Output Analysis of Privacy in Credit Card Transactions

In the present world fig 3, one of the most important issues is data leakage, which involves user personal information, including credit card information Hackers steal personal data such as purchase histories, geolocation information, and health information from data providers who handle and store it[11]. To ensure that credit cardholders and banks benefit equally, an effective credit card rating system is necessary. Moreover, banks are prohibited from sharing their data for security concerns, which makes it challenging for information researchers to obtain several approaching. Additionally, it be discovered to facilitate the device data is not evenly distributed and is highly skewed.

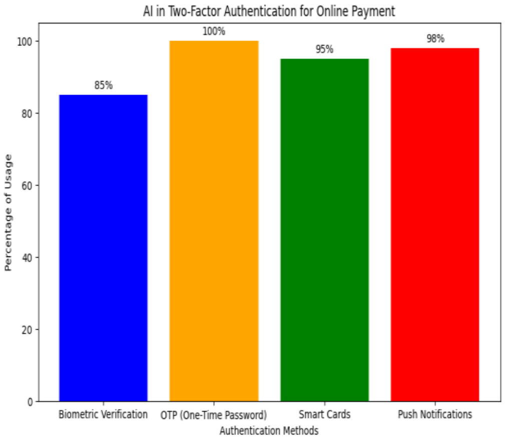

Fig. 3. Output analysis Artificial intelligence User Two-Factor Authentication Online Payment

VII. Artificial Intelligence Based Fraud Detection on Credit Cards

The number of online customers is gradually changing how web-based businesses operate. It has been observed that there is a growing degree of fraud in web-based exchanges. One type of wholesale fraud is credit card theft, in which thieves obtain funds from the charge card account of another customer. Online fraud incidents are on the rise and cause millions of dollars' worth of losses annually on a global scale. Therefore, it's critical to create and implement processes that can support fraud detection. The purpose of this model is to precisely validate every credit card transaction[12]. The algorithm is built in a way that allows for effective data analysis. There is an imbalance in the database. It should up-sample the database in order to make adjustments. Afterwards, a confusion matrix is constructed, analyzing the 99.88% accuracy of the random forest methods.

The rapid advancements and improvements that make shopping more comfortable for customers sustain the development[13]. Enormous volume of online business transactions, which raises the bar for current problems, specifically fraud in online business transactions. The number of frauds related to online businesses has also been steadily increasing since approximately[14] .A 2013 survey stated that 5.65 pennies were lost for every $100 in web-based business exchanged due to extortion. Up to 2019 [5], cheat has reached above 70 trillion dollars. One way to gauge the amount of cheating that occurs in web-based business dealings is through cheat recognition[15].

The fig 4 area of credit card cheat detection has expanded rapidly, from AI-based fraud identification to deep learning-based cheat location [16]. Regrettably, there is still a dearth of research on fraud location for online transactions, and fraud detection for credit card exchanges is still relatively new. Cheat discovery research on web-based businesses is merely limited to verifying features and attributes [17], which will be used to determine whether or not there is a possibility of fraud in online transactions.

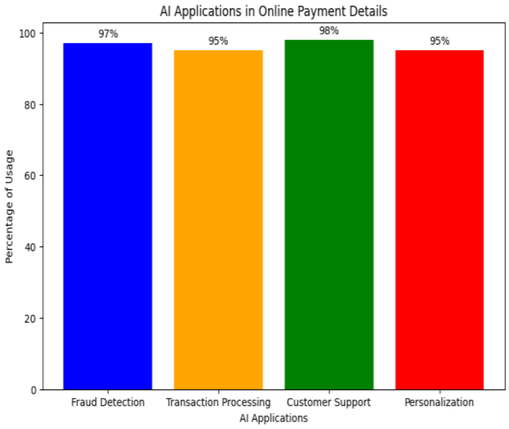

Fig. 4. Artificial intelligence applications Online Payment details

Currently, there are a number of transaction-practice-based models available for the identification of credit card fraud. Neural networks, Nave Bayes, logistic regression, and other techniques have been employed by existing models to determine the accuracy of the cheating incident[18]. This proposed study develops a model or system to identify fraudulent credit card swaps.

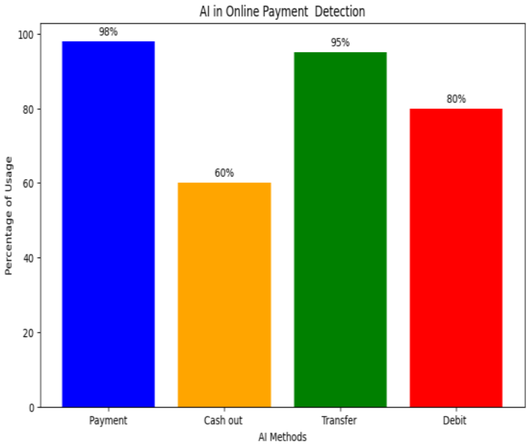

Fig. 5. Artificial intelligence applications Online Payment

Verifying the accuracy of every credit card transaction [19]. The fig 5 data must be efficiently analyzed by the program. The verification needs to be secure and swift. Developing a model with improved working accuracy. The purpose of this study is to create a new model with more exactness or accuracy than the current ones that can identify fraud in web-based commercial transactions.

Based on transaction behavior, there are several ways to identify or categorize genuine transactions from fraudulent ones. Aforementioned studies provide a thorough explanation of the applications and performance enhancements of major machine learning algorithms. Despite the fact that the random forest technique has been used to create numerous models, none of them have demonstrated 100% accuracy[20]. This is what inspired the proposal of a model that will detect cheat exchanges more rapidly and accurately than the current methods. Artificial intelligence has shown to be a useful tool for funding data sets that automate the study of enormous amounts of confusing data. Additionally, AI has played a significant role in the identification of MasterCard extortion in online transactions

The main idea outlined here is to use the Random Forest algorithm to arrange transactions that have both genuine and fraudulent exchanges coming under the database. For directed learning calculations, the Random Forest computation has been widely used. It is applied intended for together categorization and deterioration. Still, categorization harms are the main application for this approach. Since most forests are made up of trees, decision-making for example information is made using Random Forest computation, which results in expectations being met for all example information. Random Forest computation represents the directed learning approach.

It is far better than the current choice trees since it reduces over-fitting in terms of achieving an equivalent result. The term "Irregular Forest" describes a coordinated computational investigation. When a "Forest" is created, all decision trees are gathered and usually prepared for the "stashing" process. The suggested approach is superior because it provides increased efficiency, assesses queries fast even with larger databases, precisely validates exchanges, and analyzes data effectively. Machine learning algorithms provide good results when applied to larger databases, but their accuracy may suffer when used to smaller databases.

A significant obstacle will be the fraudsters' inventive ways of subverting the system. The markers Time, Amount, and Class are applied to non-identical fragments. Time shows a slowdown in both the main trade and the previous one. The total amount of money spent is determined. Class 0 labels are used for legal trade, while class 1 labels are used for dishonest trade. The "CreditCard.csv" database from Kaggle is being used, and it is out of balance. This includes roughly 2,84,315 valid trades, of which 492 are fraudulent trades.

VIII. Conclusion

Without a doubt, bank card extortion has served as evidence of unlawful dishonesty. This study tested their detection technology in conjunction with the most well-known deception tactic. Additionally, this research has explained in great depth how artificial intelligence can be used to improve fraud detection. Although the suggested model was unable to link the objective of 100% accuracy under the fraud location area, it did manage to develop a system that, given sufficient access and data, will yield results that are extremely close to the objective. Similarly, there may be an opportunity to succeed here for similar endeavors. By adding more estimates to the framework, it is feasible to make improvements. Regardless, the output of these calculations should have a similar design to the others. There could be more volume for advancement in the database. Despite being shown in advance, the accuracy of the estimations depends on the type of extended database. Higher data therefore undoubtedly improves the framework's accuracy in identifying extortion and cheating. However, this will require administrative support from reputable banks.

REFERENCES

[1] Y. R. M. R, K. A, R. D, R. Reshma, D. R. Santhosh and N. Mekala, "An Analytical Approach to Fraudulent Credit Card Transaction Detection using Various Machine Learning Algorithms," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2023, pp. 1400-1404, doi: 10.1109/ICEARS56392.2023.10085157.

[2] E. C. D. Del Pilar and M. F. Bongo, "Towards the Improvement of Credit Card Approval Process Using Classification Algorithm," 2023 8th International Conference on Business and Industrial Research (ICBIR), Bangkok, Thailand, 2023, pp. 461-465, doi: 10.1109/ICBIR57571.2023.10147636.

[3] A.N. Ahmed and R. Saini, "Detection of Credit Card Fraudulent Transactions Utilizing Machine Learning Algorithms," 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/INOCON57975.2023.10101137.

[4] A. Mahajan, V. S. Baghel and R. Jayaraman, "Credit Card Fraud Detection using Logistic Regression with Imbalanced Dataset," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 339-342.

[5] K. Goyal, S. Singh, M. Gulati and A. Suresh, "An Ensemble Of Machine And Deep Learning Models For Real Time Credit Card Scam Recognition," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-4, doi: 10.1109/ICCCI56745.2023.10128473.

[6] W. Lee, S. Lee and J. Seok, "Credit card default prediction by using Heterogeneous Ensemble," 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France, 2023, pp. 907-910, doi: 10.1109/ICUFN57995.2023.10199756.

[7] H. P. N, P. D. Rathika and P. A, "Privacy Preservation Using Federated Learning for Credit Card Transactions," 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS), Coimbatore, India, 2023, pp. 398-403, doi: 10.1109/ICISCoIS56541.2023.10100577.

[8] T. Padmavathi, P. Pavitra, M. P. Neeraja, P. Murali, G. Ramachandran and B. V. F. Justin, "An Innovative Analysis of Assistive Technology Emergency Situations Android and IoT based Telemedicine Nursing Monitoring Management," 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2023, pp. 1317-1322, doi: 10.1109/ICAAIC56838.2023.10140617.

[9] V. Sudha, , "Artificial Intelligence Energy Efficiency in Low Power Applications," 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 2023, pp. 1-5, doi: 10.1109/INCET57972.2023.10170102.

[10] Dawar, N. Kumar, G. Kaur, S. Chaturvedi, A. Bhardwaj and M. Rana, "Supervised Learning Methods for Identifying Credit Card Fraud," 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 2023, pp. 791-796, doi: 10.1109/ICIDCA56705.2023.10100266.

[11] S. Asthana and S. Rai, "Toward improvement of credit card fraud detection based on Machine learning Techniques," 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2023, pp. 587-591, doi: 10.1109/CICTN57981.2023.10140298.

[12] T. Zheng, J. Chen, Z. Zhang, Z. Gong and Y. Chen, "Bank Credit Score Card Selection and Threshold Determination Based on Quantum Annealing Algorithm and Genetic Algorithm," 2023 IEEE 5th International Conference on Power, Intelligent Computing and Systems (ICPICS), Shenyang, China, 2023, pp. 588-594, doi: 10.1109/ICPICS58376.2023.10235447.

[13] J and A. Senthilselvi, "Detection of Credit Card Fraud Detection Using HPO with Inception Based Deep Learning Model," 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2023, pp. 70-77, doi: 10.1109/ICIRCA57980.2023.10220771.

[14] P. Thongthawonsuwan, T. Ganokratanaa, P. Pramkeaw, N. Chumuang and M. Ketcham, "Real-Time Credit Card Fraud Detection Surveillance System," 2023 IEEE International Conference on Cybernetics and Innovations (ICCI), phetchaburi, Thailand, 2023, pp. 1-7, doi: 10.1109/ICCI57424.2023.10112320.

[15] H. Wang, Q. Liang, J. T. Hancock and T. M. Khoshgoftaar, "Enhancing Credit Card Fraud Detection Through a Novel Ensemble Feature Selection Technique," 2023 IEEE 24th International Conference on Information Reuse and Integration for Data Science (IRI), Bellevue, WA, USA, 2023, pp. 121-126, doi: 10.1109/IRI58017.2023.00028.

[16] Wang, W. Liu, Y. Kou, D. Xiao, X. Wang and X. Tang, "Approx-SMOTE Federated Learning Credit Card Fraud Detection System," 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), Torino, Italy, 2023, pp. 1370-1375, doi: 10.1109/COMPSAC57700.2023.00208.

[17] F. Chen, X. Wei, S. Yu, P. Ma and S. He, "Customer Churn Prediction based on Stacking Model," 2023 4th International Conference on Computer Vision, Image and Deep Learning (CVIDL), Zhuhai, China, 2023, pp. 518-521, doi: 10.1109/CVIDL58838.2023.10165721.

[18] Guo et al., "Credit Default Prediction on Time-Series Behavioral Data Using Ensemble Models," 2023 International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia, 2023, pp. 01-09, doi: 10.1109/IJCNN54540.2023.10191783.

[19] A. Yadav, A. Adhikary, A. Kainth and R. Kumar, "Performance Evaluation of Machine Learning Methods for Detecting Credit Card Fraud," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 2023, pp. 1-7, doi: 10.1109/WCONF58270.2023.10235116.

[20] M V, S. Siva Priyanka, A. S. Kumar, S. Prahasita and G. Sahithi, "Credit Card Fraud Detection with Auto Encoders and Artificial Neural Networks," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10308011.