Vol.15, Issue No 2, 2025

Financial Risk Assessment Credit Cards using Machine Learning

[1]MULAPARTHI ANU, [2]NAIDU RENUKA MADHAVI, [3]CHANDU TEJASRI, [4]MANTENA NAGA VENKATA SAI KRISHNAMRAJU,[5]Dr. A. RAMA MURTHY

[1234]Student, Department of CSE, DNR College of Engineering & Technology, Balusumudi, Bhimavaram, India.

[5] Professor, Department of CSE, DNR College of Engineering & Technology, Balusumudi, Bhimavaram, India.

Abstract—

The major problem that customers face in the financial industry, according to this research, is the false crediting of monies. Conversely, credit card fraud has been there since the beginning of the industry. When faced with such a complex set of factors, many rule-based approaches to fraud detection were inadequate. On the other hand, detecting fraud is critical for preventing clients from paying for further credit. The government is now promoting digital money and is using machine learning methods to fight corruption. Credit and ATM cards are widely used, however many individuals do not realize that they might be victims of fraud. Every year, criminals steal personal data and use it to conduct fraudulent financial transactions, costing businesses and consumers billions of dollars. It is possible to reduce losses by using efficient algorithms that identify fraud. Those looking into fraud may find these algorithms' usage of complex machine learning techniques beneficial. Terms—Savings, Credit, Machine Learning, and Consumer Finance.

INTRODUCTION

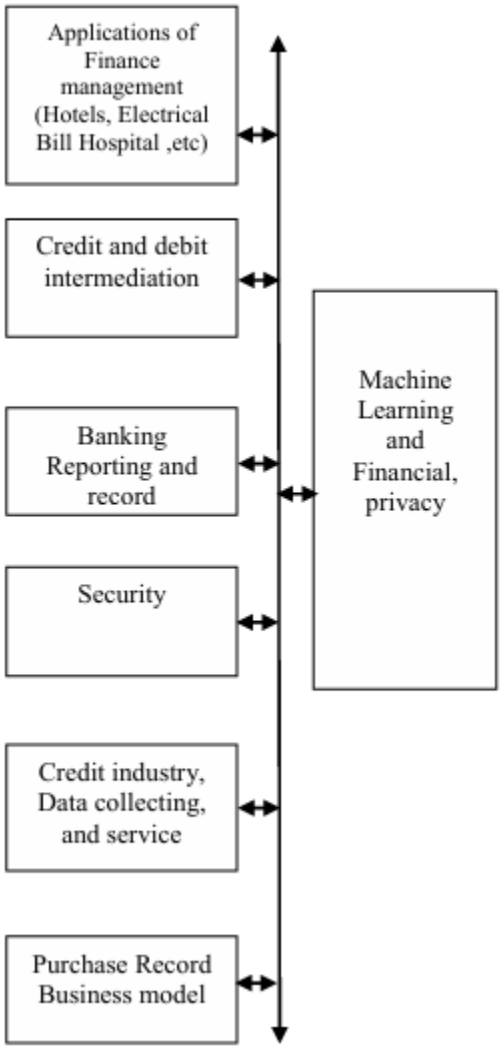
Using Supervised Learning to Accept Credit Cards In order to resolve the issue and have the credit card accepted, this study employs the Supervised Learning approach. Additionally, many specified criteria are used to compare the product's accuracy using Supervised Learning methods [1]. From the results, we can deduce that 84.32% is the sweet spot for Naive Bayes, 98.13% for KNN, 99.62% for Decision Trees, and 98.50% for Logistic Regression.

APPLICATIONS

Figure 1: Research on credit The credit industry's business model and model architecture were investigated via research and literature review in relation to label generation utilizing big data from energy. This included data collection, model design, service purposes, fees, and profit model [2]. In their research, they found that corporate credit—the bedrock of the social credit system—is essential to national life and the expansion of the commercial sector [3]. Furthermore, the basis for credit assessment is a power credit label that is generated using power data, unique application conditions, and power attributes [4]. Because of this, the study makes use of energy big data (such as transaction tariffs, sales figures, and consumers' power use) together with other technologies such as statistical modeling, clustering algorithms, mining algorithms, and expert rules.

PREDICTING CREDIT CARD DEFAULT SYSTEM

In order to generate a reliable credit score, credit card companies compile the personal details and financial records of new applicants. Machine learning has been extensively studied for its potential to analyze and predict credit ratings [5].



However, previous research failed to enhance prediction accuracy by using single approaches such as ensembles or deep learning[6]. Nor did it handle the problem of varied card histories used by the same customer. This work proposes a hybrid solution to these problems by combining heterogeneous ensembles with TabNet, a deep learning method that specializes in tabular data.

PREVENT CREDIT CARD FRAUD AS A SECURITY MEASURE

Figure 2 shows The increase in cybercrime has led to a surge in the need for cyber security solutions [7]. A company's top priorities should be protecting sensitive customer data and crucial data from cyberattacks while also preserving a favorable public image [8]. People are losing a lot of money, personal information, and privacy.

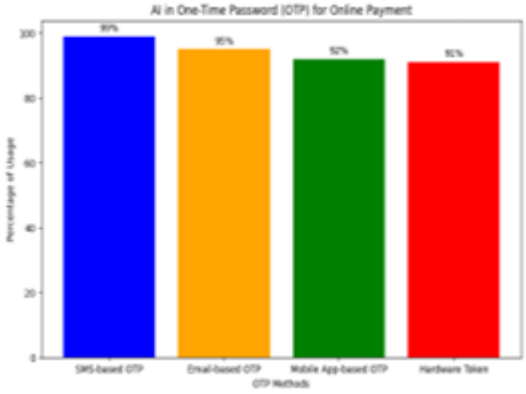


Fig. 2. Output Online Security Payment

PREDICTING CREDIT LOAN DEFAULT USING DATA MINING

Basic data, social interactions, and consumption habits are all part of this statistical package. One piece of information retrieved from the mountains of consumer data gathered for the benefit of borrowers is their address[9]. All of these things come together to build a model that can accurately forecast an individual's credit risk [10]. The results show that XGBoost is the most accurate model when compared to Random Forest and Logistic Regression.

OUTPUT ANALYSIS OF PRIVACY IN CREDIT CARD TRANSACTIONS

One of the most pressing problems in the modern world (see fig.3) is data leakage, which includes sensitive user information (such as credit card numbers). Data providers are targeted by hackers who steal sensitive personal information, including purchase history, geolocation details, and medical records [11]. An efficient credit card rating system is critical to guarantee that banks and cardholders get the same benefits. Information researchers also have challenges in obtaining several approaches since banks are not allowed to share their data due to security issues. The data from the gadget is also very skewed and not spread uniformly, which is a problem.

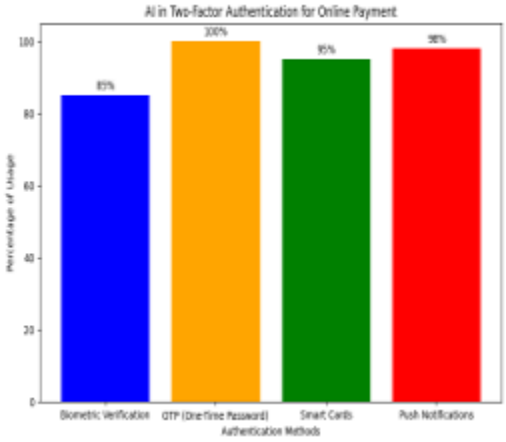


Fig. 3. Output analysis Artificial intelligence User Two-Factor Authentication Online Payment VII.

ARTIFICIAL INTELLIGENCE BASED FRAUD DETECTION ON CREDIT CARDS

The way web-based companies function is being transformed by the increasing number of online clients. An increasing amount of fraud is being seen in transactions conducted over the internet. When criminals access another person's charge card information, they are committing a kind of wholesale fraud known as credit card theft. The yearly worldwide loss due to online fraud is in the millions of dollars, and it's just getting worse. For this reason, developing and implementing procedures to aid in fraud detection is of the utmost importance. Every single credit card transaction will be validated with precision using this model [12]. An efficient analysis of data is possible because of the algorithm's design. The database is not balanced. To make the necessary changes, it is recommended to up-sample the database. Then, after examining the random forest techniques' 99.88% accuracy, a confusion matrix is built. The quick innovations and enhancements that make buying more convenient for consumers fuel the growth[13]. The present difficulties, especially online business transaction fraud, are exacerbated by the enormous amount of online commercial transactions. Additionally, there has been a consistent rise in the number of cases of fraud involving internet enterprises from around the year [14]. Extortion cost businesses 5.65 cents out of every $100 in online transactions in 2013, according to a report. Cheating has surpassed 70 trillion USD as of 2019 [5]. Cheat identification is one tool that may be used to measure the prevalence of cheating in online commercial transactions [15]. From artificial intelligence (AI) fraud detection to deep learning (DL) cheat location, the field of credit card cheat detection has grown swiftly in recent years [16]. Credit card fraud detection is still in its infancy, and studies on the origins of online transaction fraud are few and few between. In order to ascertain the likelihood of online transaction fraud, cheat detection studies focusing on web-based enterprises mostly include validating traits and qualities [17].

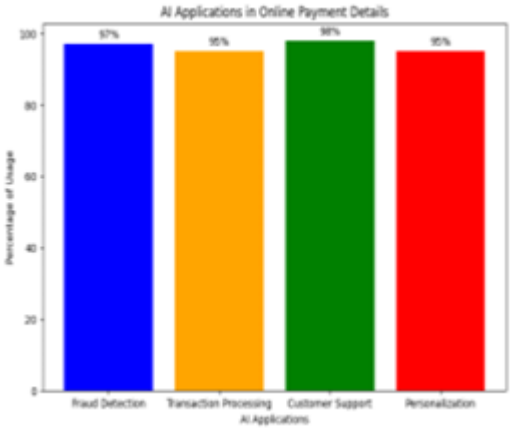


Fig. 4. Artificial intelligence applications

Payment information for online transactions A variety of credit card fraud detection methods based on actual transactions are already on the market. The accuracy of the cheating incidence has been determined by current models using a variety of methodologies, including neural networks, logistic regression, Naive Bayes, and others [18]. A model or system to detect fraudulent credit card swaps is being developed in this proposed research.

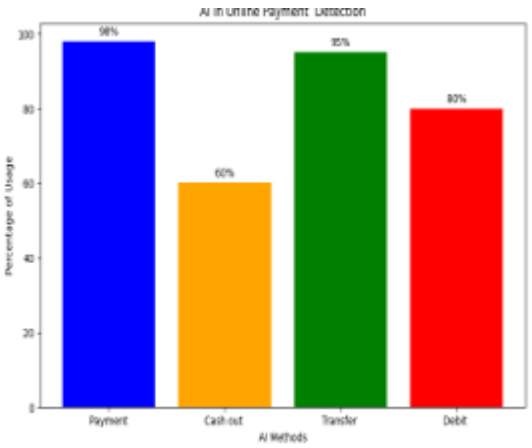


Fig. 5. Artificial intelligence applications

Electronic Funds Transfer Taking the time to double-check each and every credit card purchase [19]. The software needs to examine the data from Figure 5 effectively. The authentication process must be safe and quick. Developing a model with increased working precision. This research aims to improve upon existing models by developing one that can detect fraudulent activity in online business transactions with more precision. Multiple methods exist for distinguishing legitimate from fraudulent transactions based on their behavior. The aforementioned research delves further into the uses and benefits of prominent machine learning algorithms. Although several models have been developed using the random forest approach, none of them have achieved 100% accuracy [20]. This is why we came up with the idea for a model that can spot cheat transactions faster and more precisely than what's currently available. Artificial intelligence has shown to be a valuable resource for data sets that automate the analysis of massive volumes of complex data. Artificial intelligence has also been a major Its ability to lessen over-fitting while yet producing the same outcome makes it superior to the existing decision trees. An "Irregular Forest" is a system of interconnected computational investigations. The "Forest" creation procedure typically involves collecting all decision trees and getting them ready for the "stashing" phase. Improved efficiency, rapid query assessment (even with bigger databases), accurate exchange validation, and efficient data analysis are all benefits of the proposed method. Machine learning algorithms work well with bigger datasets but may not be as precise with smaller ones. The ingenious methods used by fraudsters to undermine the system will provide a substantial challenge. Pieces that are not similar are marked with the marks Time, Amount, and Class. Both the big transaction and the one before it show signs of slowing down as time goes on. It is calculated how much money was spent in total. Legitimate commerce uses class 0 labels, whereas unethical trade uses class 1 labels. There is an imbalance in the "CreditCard.csv" database that was utilized by Kaggle. There were around 2,84,315 legitimate deals, out of which 492 were fraudulent.

CONCLUSION

Using a customer's credit card to extort money is undeniably dishonest. In this experiment, they used the most famous deceit strategy to test their detection technique. The study has also provided a detailed explanation of how AI may be used to enhance fraud detection. The proposed model failed to establish a connection between the goal of 100% accuracy and the fraud location region, but it did create a system that, when given enough data and access, would provide outcomes that are very near to the aim. Similarly, comparable activities may find success here. Enhancements are doable with the addition of more estimations to the framework. The results of these computations should, nonetheless, follow a pattern consistent with the others. The database could need additional data to improve. Although shown above, the kind of expanded database determines the accuracy of the estimates. Therefore, it is clear that the accuracy of the framework in detecting extortion and cheating is enhanced with more data. Nevertheless, administrative backing from trustworthy financial institutions is necessary for this.

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, 10.1109/INOCON57975.2023.10101137. pp. 1-5, doi:

[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, 10.1109/ICIDCA56705.2023.10100266. pp. 791-796, doi:

[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, 10.1109/CVIDL58838.2023.10165721. pp. 518-521, doi:

[18]. [Guo et al., "Credit Default Prediction on Time-Series Behavioral Data Using Ensemble Models," 223 International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia, 2023, pp. 0109, 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, 10.1109/WCONF58270.2023.10235116. pp. 1-7, doi:

[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.