INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1785-1788

www.ijprems.com
editor@ijprems.com

e-ISSN : 2583-1062
Impact Factor : 7.001

AI POWERED FRAUD DETECTION IN FINANCIAL TRANSACTION

Prutha Sakhare[1], Khushboo Gondane[2], Monalisa Meshram[3], Siddhant Bodele[4]

[1,2,3,4]Student, Department Of Information Technology, Nagpur Institute Of Technology, Nagpur, Maharastra, India.

ABSTRACT

Globally, credit card fraud is a serious threat to people, businesses, and financial institutions. With the rise of online transactions, fraudsters have developed clever ways to take advantage of loopholes in payment systems. Traditional fraud detection methods based on manual inspections and rules-based systems are unable to counteract this new and evolving risk. As a result, the use of data analytics and machine learning has become a viable option for real-time detection and prevention of credit card fraud. The paper looks at using machine learning algorithms such as logistic regression, decision trees, random forests, neural networks, etc. to detect fraudulent transactions We go over the importance of data sources and components, analytical metrics, and how fraud detection on the effectiveness of examples. In addition, we list the current challenges and directions in which credit card fraud detection is likely to continue, including the use of blockchain technology and sophisticated AI techniques. Overall, this study highlights the importance of credit card theft detection and the promise of machine learning in mitigating this ubiquitous problem financial institutions use advanced machine learning algorithms and analytics function to detect fraudulent behaviour, protect customer interests, and maintain payment environment integrity to improve their capabilities.

Keywords: Credit Card Fraud Detection, Machine Learning, Anomaly Detection, Performance Metrics.

1. INTRODUCTION

Credit cards provide consumers and businesses with unmatched ease and flexibility in today's interconnected digital economy, helping to facilitate a wide range of transactions. But in addition to the advantages of using credit cards, there is a constant and widespread risk in the shape of credit card theft. Financial institutions, retailers, and cardholders throughout the world face serious difficulties because of this danger, which includes a variety of illegal activities such as identity theft, unauthorized transactions, and account takeover. Technology advancements and the growing popularity of online shopping have made credit card fraud even more complex by giving thieves access to more advanced methods for targeting weaknesses in the payment system.

These tactics consist of, but are not restricted to, pointof-sale terminal card skimming devices, scams attack at gullible customers, and advanced malware intended to steal cardholder information. Because of this, the financial sector constantly must fight to keep ahead of scammers and safeguard the integrity of the payment system

2. METHODOLOGY

1. Data collection
2. Data pre-processing
3. Data visualization
4. Feature extraction
5. Evaluation model

1 Data Collection:

Data used in this paper is a set of product reviews collected from credit card transactions records. This step is concerned with selecting the subset of all available data that you will be working with. ML problems start with data preferably, lots of data (examples or observations) for which you already know the target answer. Data for which you already know the target answer is called labelled data.

2 Data Pre-processing

Pre-processing is the process of three important and common steps as follows:

- **Formatting:** It is the process of putting the data in a legitimate way that it would be suitable to work with. Format of the data files should be formatted according to the need. Most recommended format is .csv files.
- **Cleaning:** Data cleaning is a very important procedure in the path of data science as it constitutes the major part of the work. It includes removing missing data and complexity with naming category and so on. For most of the data scientists, Data Cleaning continues of 80% of work.

Sampling: This is the technique of analyzing the subsets from whole large datasets, which could provide a better result and help in understanding the behavior and pattern of data in an integrated way

3 Data visualization

Data Visualisation is the method of representing the data in a graphical and pictorial way, data scientists depict a story by the results they derive from analysing and visualising the data. The best tool used is Tableau which has many features to play around with data and fetch wonderful results.

4 Feature extraction

Feature extraction is the process of studying the behavior and pattern of the analyzed data and draw the features for further testing and training. Finally, our models are trained using the Classifier algorithm. We use classify module on Natural Language Toolkit library on Python. We use the labelled dataset gathered. The rest of our labelled data will be used to evaluate the models. Some machine learning algorithms were used to classify pre-processed data. The chosen classifiers were Random forest. These algorithms are very popular in text classification tasks.

5 Evaluation model

Model Evaluation is an essential part of the model development process. It helps to find the best model that represents our data and how well the selected model will work in the future. Evaluating model performance with the data used for training is not acceptable in data science because it can effortlessly generate overoptimistically and over fitted models. To avoid overfitting, evaluation methods such as hold out and cross-validations are used to test to evaluate model performance. The result will be in the visualized form. Representation of classified data in the form of graphs. Accuracy is well-defined as the proportion of precise predictions for the test data. It can be calculated easily by mathematical calculation i.e. dividing the number of correct predictions by the number of total predictions.

3. SYSTEM ARCHITECTURE

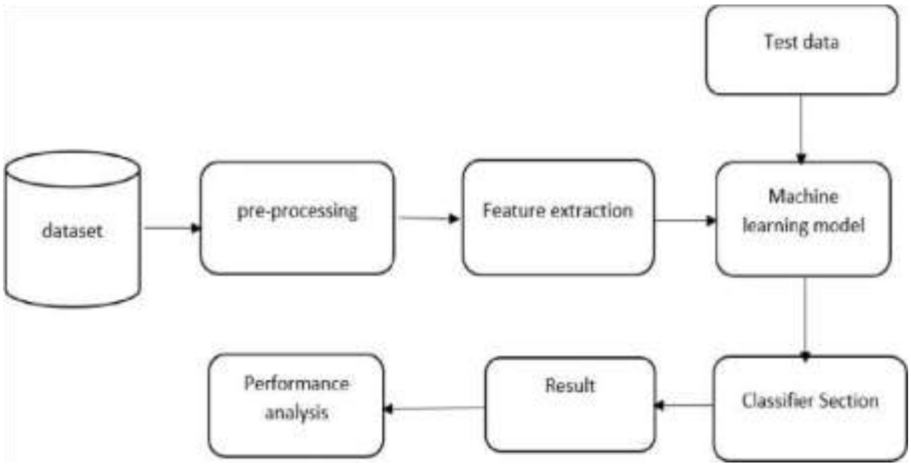
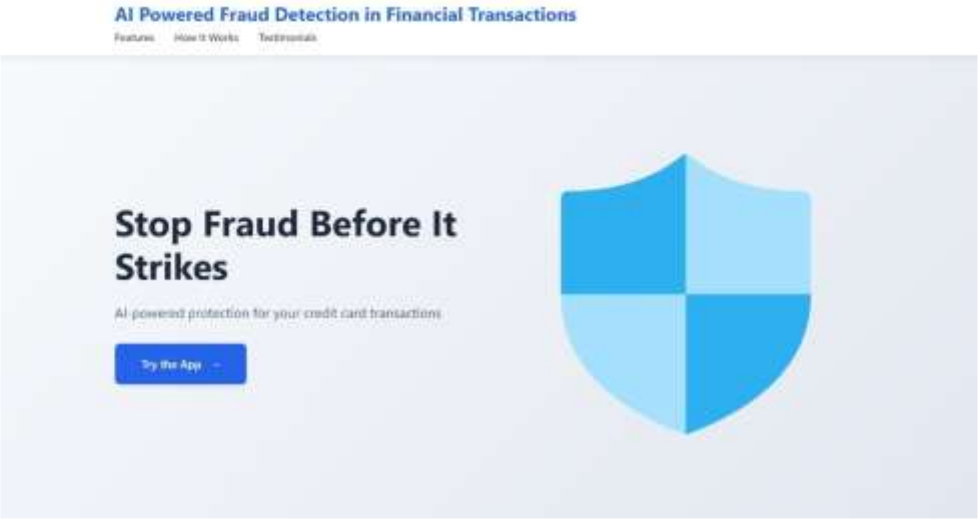


Figure 1: System Architecture.

4. RESULTS AND DISCUSSION

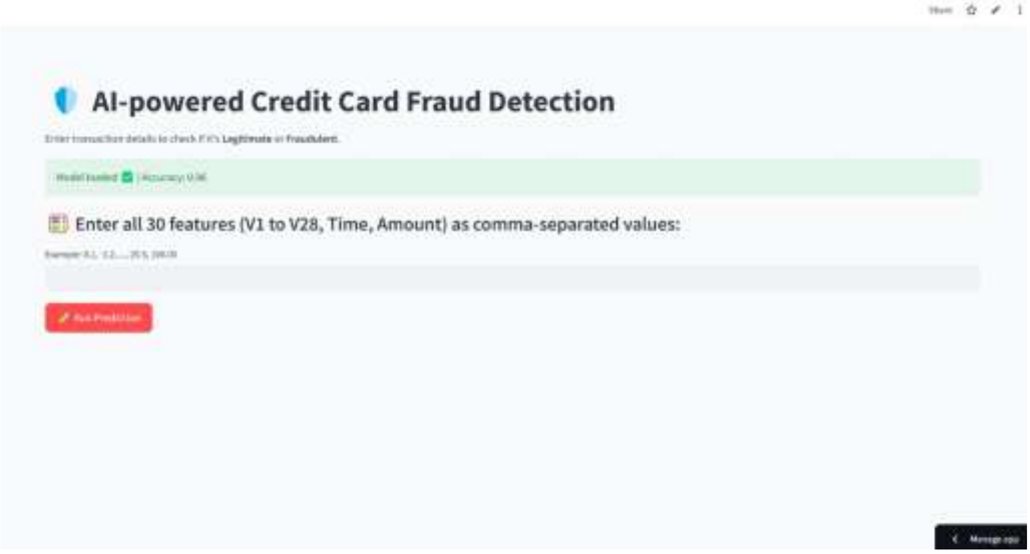
In this Section results and discussion of the study is written. They may also be broken into subsets with short, revealing captions. This section should be typed in character size 10pt Times New Roman.


AI Powered Fraud Detection in Financial Transactions

Stop Fraud Before It Strikes

AI powered protection for your credit card transactions

Figure 2: Landing Page - Secure Credit Card



AI-powered Credit Card Fraud Detection

Enter transaction details to check if it's Legitimate or Fraudulent.

Model loaded ✅ | Accuracy: 0.96

Enter all 30 features (V1 to V28, Time, Amount) as comma-separated values:

Example: 0.1, -1.2, ..., 25.5, 100.0

Figure 3: Working of Model

Unless or otherwise specified specific gravity values reported shall be based on water at 270C. So the specific gravity at 27^{0}C = K Sp. gravity at Tx^{0}C. The specific gravity of the soil particles lie with in the range of 2.65 to 2.85. Soils containing organic matter and porous particles may have specific gravity values below 2.0. Soils having heavy substances may have values above 3.0.

5. CONCLUSION

In conclusion, this research paper examined the essential significance of machine learning within the improvement of credit card fraud detection systems. A detailed assessment of the literature and analysis of numerous machine learning algorithms exhibits that machine learning procedures have excellent capability for detecting and blocking off fraudulent transactions in real time.

The paper emphasised the significance of characteristic engineering, model selection, and evaluation metrics in developing powerful fraud detection systems. Furthermore, the incorporation of current machine learning strategies including deep learning and ensemble approaches has confirmed promise in enhancing the accuracy and efficiency of fraud detection algorithms.

The report additionally emphasised the barriers and boundaries of credit card fraud detection, together with uneven datasets, converting fraud patterns, and computational complexity. Addressing these problems includes ongoing research at and the development of novel techniques to conform to changing fraud dynamics.

Overall, the information provided in these studies highlight the need of the usage of machine learning in combatting credit card fraud. Financial establishments may improve the safety of their customers' budget and hold consider in the digital price surroundings by of leveraging the power of data-driven techniques and constantly improving algorithms. As machine learning advances, it has significant capacity to enhance fraud detection systems and reduce the risks linked with monetary fraud.

ACKNOWLEDGEMENTS

We would like to express our heartfelt gratitude to all those who have contributed to this project. Your support, guidance, and encouragement have been invaluable throughout this journey. First and the foremost we, express our deep sense of gratitude, sincere thanks to Dr. Anil Warbhe for the best support, opinion, views, comments, and thoughts that have been extremely helpful.

6. REFERENCES

[1] Sailusha, R., Gnaneswar, V., Ramesh, R., and Rao, G.R., 2020, May. Credit card fraud detection using machine learning. In *2020 4th international conference on intelligent computing and control systems (ICICCS)* (pp. 1264-1270). IEEE.

[2] Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., and Singh, A.K., 2021. Credit card fraud detection using machine learning: a study. *arXiv preprint arXiv:2108.10005*.

[3] Trivedi, N.K., Simaiya, S., Lilhore, U.K. and Sharma, S.K., 2020. An efficient credit card fraud detection model based on machine learning methods. *International Journal of Advanced Science and Technology*, *29*(5), pp.3414-3424.

[4] Alarfaj, F.K., Malik, I., Khan, H.U., Almusallam, N., Ramzan, M. and Ahmed, M., 2022. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access*, *10*, pp.3970039715.

[5] Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A. and Aljaaf, A.J., 2020. A systematic review on supervised and unsupervised machine learning algorithms for data science. *Supervised and unsupervised learning for data science*, pp.3-21.

[6] Janiesch, C., Zschech, P. and Heinrich, K., 2021. Machine learning and deep learning. *Electronic Markets*, *31*(3), pp.685-695.

[7] Lai, J.P., Chang, Y.M., Chen, C.H. and Pai, P.F., 2020. A survey of machine learning models in renewable energy predictions. *Applied Sciences*, *10*(17), p.5975.

[8] Chatzimparmpas, A., Martins, R.M., Jusufi, I., Kucher, K., Rossi, F. and Kerren, A., 2020, June. The state of the art in enhancing trust in machine learning models with the use of visualizations. In *Computer Graphics Forum* (Vol. 39, No. 3, pp. 713-756).

[9] Amr, T., 2020. *Hands-On Machine Learning with scikit-learn and Scientific Python Toolkits: A practical guide to implementing supervised and unsupervised machine learning algorithms in Python*. Packt Publishing Ltd.

[10] Ileberi, E., Sun, Y. and Wang, Z., 2022. A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1), p.24.

[11] Khatri, S., Arora, A., and Agrawal, A.P., 2020, January. Supervised machine learning algorithms for credit card fraud detection: a comparison. In *2020 10th international conference on cloud computing, data science & engineering (confluence)* (pp. 680-683). IEEE.