**Research Paper- Identification of Fraud with Credit Cards Using Hybrid Machine Learning Model**

**A PROJECT REPORT**

***Submitted by***

**Shubham Singh**

**ACKNOWLEDGEMENT**

First, I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to Dr. Sandip Mal, Head of the Department, School of

Computer Science and Engineering for much of his valuable support and encouragement in carrying out this work.

I would like to thank my internal guide Dr. Sandeep Mal for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School of Aeronautical Science, who extended directly or indirectly all support.

Last, but not least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

**List of Abbreviations:**

1. CCFDS – Credit Card Fraud Detection System
2. CNN – Convolutional Neural Networks
3. SVM - Support Vector Machine

**LIST OF FIGURES**

| **FIGURE NO.** | **TITLE** | **PAGE NO.** |
| --- | --- | --- |
| 1 | Project Coding flow | 8 |
| 2 | Libraries | 10 |
| 3 | Dataset | 10 |
| 4 | Cleaning the Null values | 11 |
| 5 | Legitimate Entries | 11 |
| 6 | Fraud transactions | 11 |
| 7 | Training Datasets | 12 |
| 8 | Output | 12 |

**LIST OF TABLES**

| **TABLE NO.** | **TITLE** | **PAGE NO.** |
| --- | --- | --- |
| 1 | Accuracy Table | 10 |

| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| --- | --- | --- |
|  | List of abbreviations  List of figures  List of tables | iii.  iv.  v. |
| 1. | **Introduction**  1.1 Introduction  1.2 Motivation for the work  1.3 Software implemented  1.4 Hardware implemented  1.5 Problem Statement  1.6 Objective of the work  1.7 Organization of thesis | 7  7  7  8  8  8  8  8  9 |
| 2. | **Experimental Data** | 10 |
| 3. | **Outputs** | 12 |
| 4. | **Conclusion** | 13 |
| 5. | **References** | 14 |

**Introduction**

In the digital age, the use of credit cards has revolutionized the way we conduct financial transactions, offering unparalleled convenience and flexibility. However, this convenience has also made credit card transactions an attractive target for fraudulent activities. Credit card fraud poses a significant threat to financial institutions and individuals, necessitating the development of advanced, dynamic, and accurate fraud detection systems.

As traditional rule-based systems have proven inadequate in keeping pace with the evolving tactics of fraudsters, the integration of machine learning techniques has emerged as a promising solution. Machine learning algorithms, powered by their ability to adapt and learn from data, offer the potential to enhance the accuracy and efficiency of credit card fraud detection systems.

By leveraging a blend of supervised and unsupervised learning methods, this approach allows for the identification of known fraud patterns while also detecting emerging threats and anomalies. In the following sections, we will see the methodology employed in constructing our hybrid architecture, explore the types of machine learning algorithms integrated into the system, and present an in-depth analysis of the results and performance metrics.

**Motivation for the work**

The strategies used by fraudsters to take advantage of flaws in financial systems evolve along with technology. Fraudulent credit card transactions can have severe financial losses and psychological effects for both people and institutions. We want to provide a strong defense against these nefarious acts by creating an effective and precise fraud detection system. This study adds to the larger field of data science and machine learning use in real-world scenarios in addition to addressing the urgent need for proactive fraud prevention. Our dedication to developing an effective fraud detection technology is motivated by the potential to have a significant influence on safeguarding financial transactions and fostering trust in digital payment systems.

**Software Implemented**

1. Tensorflow
2. Scikit- learn
3. Matplotlib
4. Pandas
5. Numpy
6. Keras
7. Google Colab

**Hardware Implemented**

1. Laptop

**Problem Statement**

The aim was to study and analyze the patterns of transactions with credit cards and warn about any sudden suspicious activities and transactions with the help of deep learning.

**Objective of work**

The main objective of this project is to develop a fraud detection system with the help of a ‘Hybrid model’ of machine-learning algorithms that identify patterns in legitimate and fraudulent transactions to minimize false positives and false negatives to improve accuracy.

**Organization of thesis**

The credit card fraud detection system (CCFDS) is used to manage and track any fraudulent activity in credit card transactions. But Fraudsters have managed to bypass the traditional CCFDS. Hence there is a need for the new system to detect any suspicious activity such as unusual transactions using regular credit card.

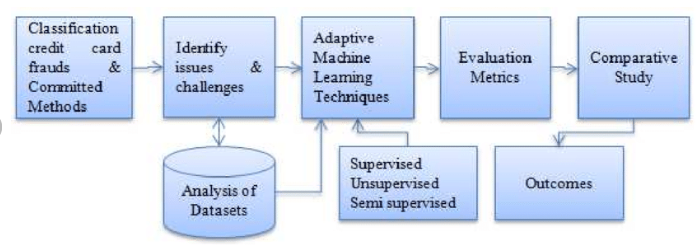
****

Fig1

Machine learning and deep learning can help in this as the unusual patterns can be identified using different models, and ‘Hybrid architecture’ can be used to improve the accuracy.

**Experimental Data**

There are various machine-learning algorithms available which can be used to create different models for fraud detection. These algorithms are categorized into supervised and unsupervised machine learning algorithms. Depending on the requirement, respective algorithms are used. However, any one algorithm is not sufficient for a strong CCFDS.

We searched and discussed various models that can be used for fraud detection and came to the conclusion that the following are some of the best algorithms for CCFDS.

Following are the Models we studied :

1. Decision Tree

2. SVM Model

3. Logistic Regression

4. CNN

5. Gradient Boosting

6. Random Forest

Accuracy Table:

| Algorithm | Accuracy |
| --- | --- |
| DECISION TREE | 94% |
| SVM | 95.99% |
| LOGISTIC REGRESSION | 97.2% |
| GRADIENT BOOSTING | 99.801% |
| CNN | 99.901% |
| RANDOM FOREST | 99.90% |

Table 1

From the models, CNN and Random Forest have the highest accuracy.

Hybrid architectures can be more interpretable. This is because normal machine learning algorithms are often easier to interpret than deep learning algorithms. By combining a deep learning model with a traditional machine learning algorithm, it is possible to create a hybrid architecture that is both accurate and interpretable.

**Implementation of code**

Importing Libraries:

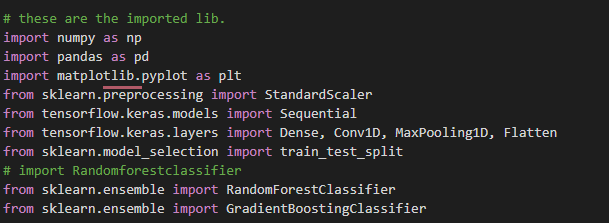


Fig.2

Reading the datasets:



Fig.3

Cleaning the datasets:



Fig.4

Removing Null Values:



Fig.5

Counting legitimate Entries:



Fig.6

Counting Fraud transaction:



Fig.7

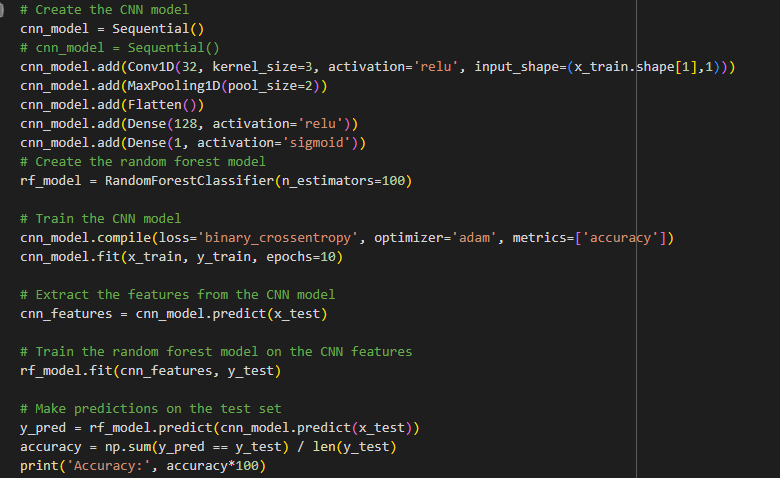
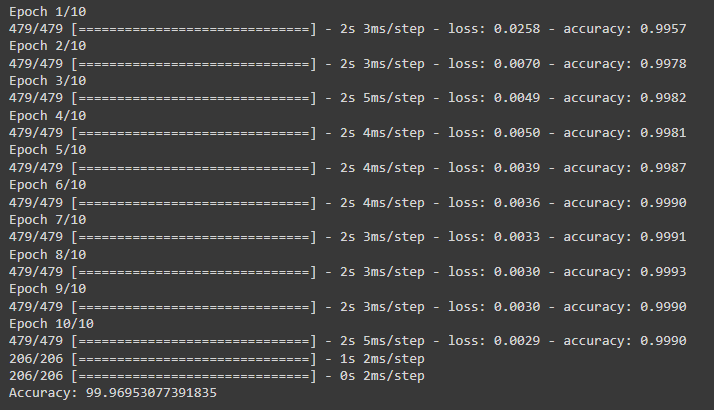
Creating and training Models:

Fig.8

Outputs:

Fig.9

After training the model, the accuracy was 99.969%.

Conclusion

The **hybrid model, with an accuracy of 99.97%,** outperforms other algorithms that had an accuracy of up to 99.908% at detecting credit card fraud. The combination of two powerful algorithms Random Forest and Gradient Boosting resulted in a hybrid model is the best solution for Credit card fraud detection. It is not only suitable for one dataset and can manage a variety of data types being the best solution in fraud detection

**References**

1. Kumar, Sheo & Gunjan, Vinit & Ansari, Mohd Dilshad & Pathak, Rashmi. (2022). Credit Card Fraud Detection Using Support Vector Machine. 10.1007/978-981-16-6407-6\_3.
2. Sai Kiran, Jyoti Guru, Rishabh Kumar, Naveen Kumar, Deepak Katariya, Maheshwar Sharma (2018). Credit card fraud detection using Naïve Bayes model based and KNN classifier. International Journal of Advance Research, Ideas and Innovations in Technology, 4(3) [www.IJARIIT.com](https://www.ijariit.com/).
3. Mohammed, Emad, and Behrouz Far. “Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study.” IEEE Annals of the History of Computing, IEEE, 1 July 2018, doi.ieeecomputersociety.org/10.1109/IRI.2018.00025.
4. Randhawa, Kuldeep, et al. “Credit Card Fraud Detection Using AdaBoost and Majority Voting.” IEEE Access, vol. 6, 2018, pp. 14277–14284., doi:10.1109/access.2018.2806420. <https://link.springer.com/chapter/10.1007/978-981-16-3675-2_40>

<https://www.grafos.cl/Articulos/HandwritingAnalysisforDetectionofPersonalityTraitsusingMachineLearningApproach.pdf>

1. <https://thesai.org/Downloads/Volume11No12/Paper_65-Fraud_Detection_in_Credit_Cards.pdf>
2. <https://www.webology.org/data-cms/articles/20220922064230pmPaper103.pdf>
3. <https://www.ijrti.org/papers/IJRTI2304141.pdf>
4. https://www.researchgate.net/publication/357728400\_Credit\_Card\_Fraud\_Detection\_Using\_Support\_Vector\_Machine