International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms

M. Srividya[1], K. Sumedha[2], M. Shraddha[3], V.Veda Samhitha[4]

[1]Assistant Professor, Matrusri Engineering College
[2,3,4]Students, Information Technology Department, Matrusri Engineering College.

Abstract:
This research study aims to detect credit card frauds, such as accessibility of public data, high-class imbalance data, changes in fraud nature, and high rates of false alarm. Machine learning and deep learning algorithms have been used to detect frauds, but there is still a need to apply state-of-the-art deep learning algorithms to reduce fraud losses. Comparative analysis of both machine learning and deep learning algorithms was performed to find efficient outcomes. The European card benchmark dataset was used to evaluate the proposed model, which outperformed the state-of-the-art machine learning and deep learning algorithms.

Keywords: Fraud detection, deep learning, machine learning, online fraud, credit card frauds, transaction data analysis.

INTRODUCTION

Credit card fraud (CCF) is a type of identity theft in which someone else makes an unlawful transaction using a credit card or account details. Increased fraud has resulted from the expansion of e-banking and online payment environments, resulting in annual losses of billions of dollars. In 2020, there were 393,207 cases of CCF out of 1.4 million total reports of identity theft. The number of identity theft complaints has climbed by 113% from 2019 to 2020, with credit card identity theft reports increasing by 44.6%. Payment card theft cost the global economy $24.26 billion last year.

LITERATURE REVIEW

3.1 An efficient real time model for credit card fraud detection based on deep learning:

Machine Learning has revolutionized data processing and classification, making it possible to create real-time interactive and intelligent systems. This paper focuses on a fraud detection system based on a deep neural network technology. The proposed model is based on an auto-encoder and can classify credit card transactions as legitimate or fraudulent in real-time. The Benchmark shows promising results for the proposed model.

3.2 Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence:

Machine learning has the potential to automate financial threat assessment for commercial firms and credit agencies. This study aims to build a predictive framework to help the credit bureau by modelling/assessing

credit card delinquency risk. Evaluation metrics include sensitivity, specificity, precision, F scores, and area under receiver operating characteristic and precision recall curves.

3.3 Performance analysis of feature selection methods in software defect prediction: A search method approach:

Software Defect Prediction (SDP) models are built using software metrics derived from software systems. High dimensionality is one of the data quality problems that affect the performance of SDP models. Feature selection (FS) is a proven method for addressing the dimensionality problem, but the choice of FS method for SDP is still a problem. This paper evaluated four filter feature ranking (FFR) and fourteen filter feature subset selection (FSS) methods over five software defect datasets obtained from the NASA repository. The experimental analysis showed that the application of FS improves the predictive performance of classifiers and that the performance of FS methods can vary across datasets and classifiers. However, FFR methods are more stable in terms of predictive performance.

METHODOLOGY

Financial institutions should prioritise the installation of an automated fraud detection system. The purpose of supervised CCF detection is to build a machine learning (ML) model based on previously collected transactional credit card payment data. The model should be able to differentiate between fraudulent and nonfraudulent transactions and utilise this information to determine whether or not an incoming transaction is fraudulent. The challenge covers a number of basic issues, such as the system's rapid response time, cost sensitivity, and feature pre-processing. ML is an artificial intelligence area that use a computer to generate predictions based on previous data patterns.

Advantages:

1. Improved results in accuracy, f1-score, precision, and AUC Curves with optimised settings.
2. For credit card recognition challenges, the proposed model outperforms state-of-the-art machine learning and deep learning methods.
3. The offered methodologies are practical for detecting credit card fraud in the real world.

Disadvantages:

1. Card-not-present fraud, or the use of your credit card information in e-commerce transactions, has also grown more widespread as online purchasing has increased.
2. The rise of e-banking and many online payment environments has led in increased fraud, such as CCF, causing in yearly losses in the billions of dollars.

This research study aims to identify frauds using machine learning and deep learning algorithms. A comparative examination of both machine learning and deep learning methods was conducted using the European card benchmark dataset. Three convolutional neural network-based designs were used to increase fraud detection performance. An empirical investigation was conducted by varying the number of hidden layers, epochs, and models.

5. DESIGN SYSTEM

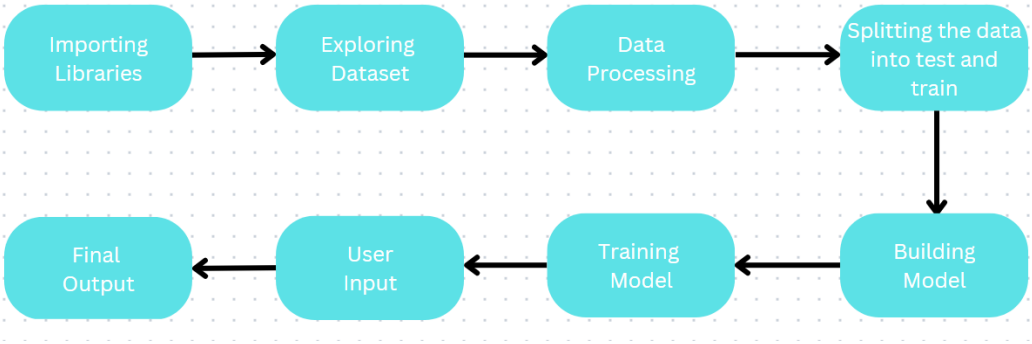

Fig.3: Design system

IMPLEMENTATION

SVM:

SVM is a supervised machine learning technique that may be used for both classification and regression. Though we call them regression issues, they are best suited for categorization. The SVM algorithm's goal is to identify a hyperplane in an N-dimensional space that clearly classifies the input points.

Random Forest:

Random forest is a kind of Supervised Machine Learning Algorithm that is often used in classification and regression issues. It constructs decision trees from several samples and uses their majority vote for classification and average for regression.

KNN:

The k-nearest neighbours method, often known as KNN or k-NN, is a non-parametric, supervised learning classifier that employs proximity to classify or predict the grouping of a single data point.

Decision Tree:

A decision tree is a non-parametric supervised learning approach that may be used for classification as well as regression applications. It has a tree structure that is hierarchical and consists of a root node, branches, internal nodes, and leaf nodes.

RESULT

The result of the project is detecting weather the credit card transaction is fraudalant or non-fraudalant by using machine learning and deep learning algorithms.

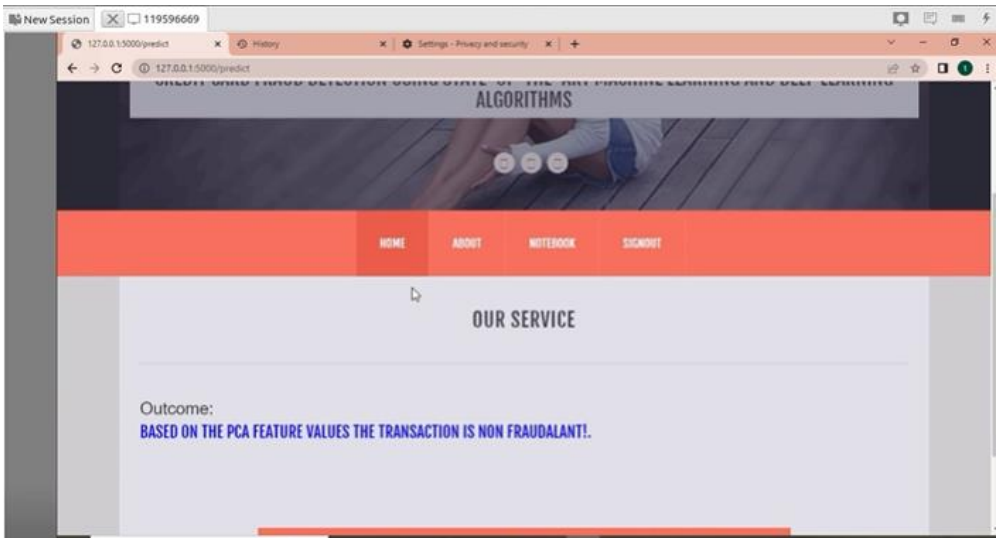

Fig.4: Prediction result

CONCLUSION

CCF is a growing threat to financial institutions, and a strong classifier is needed to accurately forecast fraud instances and decrease false-positive cases. ML algorithms vary depending on the business case, but CNNs and their layers outperform existing algorithms when it comes to detecting credit cards. Future work may investigate the use of more cutting-edge deep learning algorithms.

REFERENCES

1. Y. Abakarim, M. Lahby, and A. Attioui, ‘‘An efficient real time model for credit card fraud detection based on deep learning,’’ in Proc. 12th Int. Conf. Intell. Systems: Theories Appl., Oct. 2018, pp. 1–7, doi: 10.1145/3289402.3289530.
2. H. Abdi and L. J. Williams, ‘‘Principal component analysis,’’ Wiley Interdiscipl. Rev., Comput. Statist., vol. 2, no. 4, pp. 433–459, Jul. 2010, doi: 10.1002/wics.101.
3. V. Arora, R. S. Leekha, K. Lee, and A. Kataria, ‘‘Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence,’’ Mobile Inf. Syst., vol. 2020, pp. 1–13, Oct. 2020, doi: 10.1155/2020/8885269.
4. A. O. Balogun, S. Basri, S. J. Abdulkadir, and A. S. Hashim, ‘‘Performance analysis of feature selection methods in software defect prediction: A search method approach,’’ Appl. Sci., vol. 9, no. 13, p. 2764, Jul. 2019, doi: 10.3390/app9132764.