International Journal of Computer Sciences and Engineering
Vol.**11**, Issue.**8**, pp.**65-70**, August **2023**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Paper

Improved Credit Card Fraud Prediction using Edited Nearest Neighbors Learning Technique

Kajol Khan[1*], Poornima Dwivedi[2]

[1,2]Dept. of Computer Science and Engineering/NRI Institute of Research and Technology, Bhopal, India

Received: 06/Jul/2023; **Accepted**: 10/Aug/2023; **Published**: 31/Aug/2023. **DOI**: https://doi.org/10.26438/ijcse/v11i8.6570

Abstract: Cloud computing and mobile computing have increasing its performance with rapid manner through numerous area of applications, these are extending such as digital payments, storage and confidential information accessing. Current technology offers several internet applications by using cloud based electronic payment methods, therefore security and confidentiality is necessary. According to national herald in India 42% frauds are identified in various fields from 1990 to 2020. Like "no fraud" agency in USA identified around 30% frauds since 1990, every year these frauds are increases with high ratios. Frauds did not have particular patterns, also change their behavior at every time. These frauds are most probably recognized at cloud based e-commerce and trade business websites. A real and precise fraud detection system must be developed in order to reduce this fraud ratio. In this exploration with the assistance of profound and AI improvement strategies has been utilized to recognize the cloud based fakes. So many, existed works settle this issue yet precision, F-score, review and precession are exceptionally less. Due to this impediment, in this work is introduced deep learning mechanisms like fully Edited Nearest Neighbor (ENN) and deep neural network (DNN). The DNN with ENN is best technique for credit card fraud prediction and achieve good accuracy.

Keywords: Credit Card, Deep Learning, ENN, DNN, Accuracy

1. Introduction

Today, virtual organizations and the Internet are changing the landscape of traditional commerce. Online businesses are gaining popularity as the Internet provides a global marketplace, increases flexibility, and increases market competition. For web-based businesses, we also offer a variety of simpler and more comprehensive developments in the areas of banking and installment payments. It plays a fundamental role in fierce markets around the world. As the global market expands, people tend to focus on the computerized market instead of the traditional market. There are also many restrictions due to assigning offices to customers. Online payments are essential for online businesses and advanced markets. Interest in installment payments in the currency and banking sectors has become the norm these days as the overall market expands. Online payments allow you to make exchanges anytime, anywhere using the best gadgets such as PCs, portable devices, workstations and PDAs. A key aspect behind the development of electronic installment payments is to remove the limitations of traditional commerce. Customers do not have to wait in long queues and visit banks for currency exchange procedures. It offers a number of advantages, including: B. No need to go to the bank and wait in line because the exchange is done in an instant. There are two ways to make electronic installments: online or offline. Online installments can be distinguished as virtual installments. For online installment payment, the account holder name, PIN, card number, expiration date, etc. are required confidential data. You can recognize the disconnect rate as the actual rate. Installment payments require the cardholder and her PIN [1, 2].

These tricks can be done in many ways. Phishing, misrepresentation, skimming, use of lost or stolen cards, and card cloning are common online Visa fraud tactics. Apart from these tactics, there are other components that enable Mastercard's tricks, such as malware that can hack Visa and important lumberjacks. Due to the complexity of online transactions, credit cards are used to examine the complexity of business cards [3, 4].

Online installment payments don't require you to enter a tag or PIN on your card, but the process is easier. Most websites make use of map details and make them available to outside parties. Many scammers are accessible on the Internet, making it difficult to lure scammers into traps. The ATM framework and the POS framework are two systems that are typically fundamental to misrepresenting unrelated installments. Card duplication, card interception, counterfeit ATM or POS devices and mass fraud, lost or stolen cards, questionable systems, businesses, or devices [5]. For web-based exchanges that prevent customer fraud from duplicate installment card numbers, this creation includes trusted card numbers. Here are the steps to process installment cards:

- Customer selects a host and makes a web-based request. When submitting a web-based installment payment request, no card number is submitted.
- Traders enter the OrderID of the submitted request.
- The customer uses a private key to verify the details of the payment via the host; the merchant also requests payment verification via the host. Client and trader both confirm installment with a similar orderID.
- The host evaluates the secret key and looks up the order ID. The host obtains it along with the private key process and provides a partial card number.
- The host then sends an interest in the cardholder's share allocation. When the cardholder submits a reply to the installment check, the reply is returned to the merchant.
- Seller completes the request and submits it through the installment host.
- During web-based exchanges, all data is sent over SSL in encrypted structure and when it is received by the beneficiary it is sent in unencrypted structure.

2. Types of Cards

Payment cards are the part of payment system i.e. issued by payment organization or bank. There are number of different type of cards available in market. But most common card used by customer is either credit card or debit card. Consumer used it for payment purpose. It can be used either for physical payment or virtual payment. It removes the concept of carry paper money. Advantage of digital cash is no need to carry cash and merchant cannot refuse to accept it. Following chart shows the various types of card available in Mauritius market. Each and every card has its unique features. Customer can issue card from legal organization as per their needs.

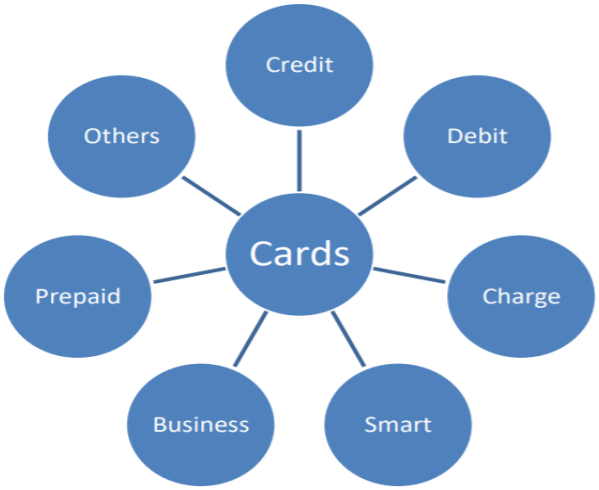


Figure 1. Type of cards

1. Credit card: It is a plastic material card, issued by bank or payment organization. It gives credit to customer for purchase goods or services. There is spending limit on card.

2. Debit card: It is plastic material card, issued by bank to their account holder. It is different from credit card, it directly withdrawal money from customer account. Normally used for cashless transaction.

3. Charge Card: Plastic cards are distinct from credit cards. It is provided to customers by a payment processor, and they are responsible for paying for the card. It permits client to do on the web or actual spending. Credit on the card is unlimited.

4. Brilliant Card: It is a chip based plastic card given by bank to their clients. There is no credit cap on this card. The cardholder will occasionally pay for their statement. Clients need to pay charges to card giving organization.

5. Business Card: A business card is similar to plastic material credit card. Card holder name, job title, business address, phone number, etc. information printed on card. Business card is used for business expenses at your home or abroad. It can be business debit card or credit card.

6. Prepaid Card: It is not like credit or debit card. Unlike credit or debit card, for prepaid card u does not require a bank account. The amount on the card must be entered beforehand. You can burn through cash that is stacked in your card for instalment. It is reusable card; ones stacked sum is utilized, customer can reload or toss the card.
7. Other Cards: Apart from all these types of cards, there are many different types of cards like cheque card, gift card, cash card, reward card, etc.

3. Proposed Methodology

The Artificial Consciousness Extortion Site (AIFD) as a high-level direct recurrence model is elaborated to decompose highly complex credit card exchange data sets containing several fixed points completely switched to other mathematical properties. made to The model results then determined that: This particular exchange was false: 1.0 or real: 0.0.

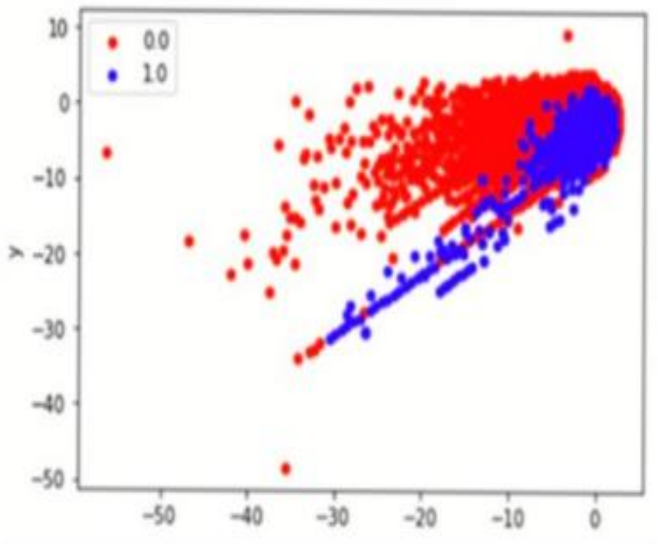


Figure 2. Credit Card dataset

A particular Mastercard dataset actively passes some Primary Part Exam (PCA) and ML strategies and contains 284807 transactions, fundamentally inconsistent with the cheat

dataset at 0.172%. I'm here. As such, the data is particularly skewed towards the valid 284315, with a trend around X = 0.0 (red).) to get a plot of the data, we showed the trend of 492 trades vs. mean around y = 1.0 (blue). The Mastercard dataset was plotted using a scatterplot with x and y functions. These generally show stress when extinguished ENNs are applied (Fig. 2).

The AIFD model was developed to test up to five layers of key brain networks and various skills that improve their accuracy (Figure 3).

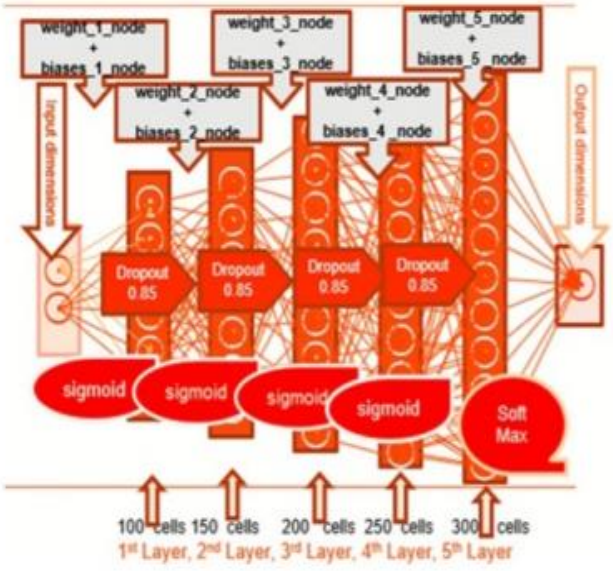


Figure 3. Visual representation of AIFD

Brain networks were first prepared and tested using natural information and then tested using Destroyed + ENN. We then inspected the accuracy of each layer to determine the optimal number of layers for AIFD productivity and added the number of cells per layer (L): L1=100, L2=150, L3=200, L4=250. , L5=300. Dropout Capacity: 0.85, Adam Smooth Specialist: 0.006, Age Number 1000 was set for best results.

Synthetic Minority Oversampling and Edited Nearest Neighbours

SMO-ENN computation applies over analysis (working framework) using annihilated and performs planned tests for minority imbalance class: 1.0 (IC), then a crossover approach using the cleanup strategy ENN.

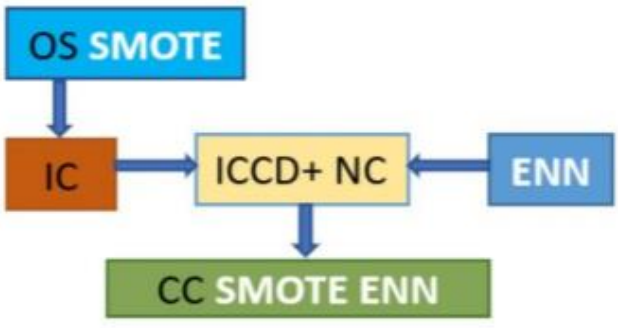


Figure 4. Visual representation of SMOTE ENN algorithm

Under estimates the emerging phenomenon: that is imbalanced Visa data (ICCD) corrupted his ENN dataset, even though newly created (NC) data generated bogus credit card data (CC) (Fig. 4).

Credit card records were preprocessed using ENN with DNN estimation with test strategy 0.5, augmented minority models when Obliterated was applied, discarded most models when nearest neighbors were used, 284807 Transactions generated: Provable 268103 , trend: then off balance with cheats Achieved a record 0.329% (Fig. 5). By preprocessing the credit card records with the Destroyed + ENN calculation, we find that the initial phase (IL) and final phase (FL) of the AIFD model are improved by slightly longer introduction time (IET/s) and final phase got it. Phase slip in time (FET /S).

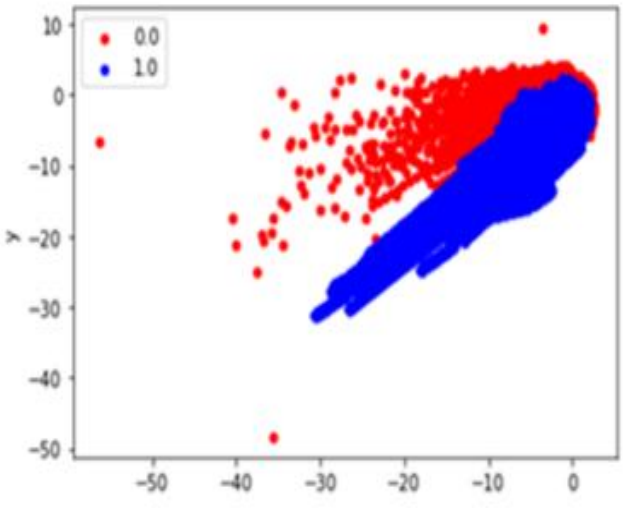


Figure 5. Credit Card (SMOTE ENN) dataset

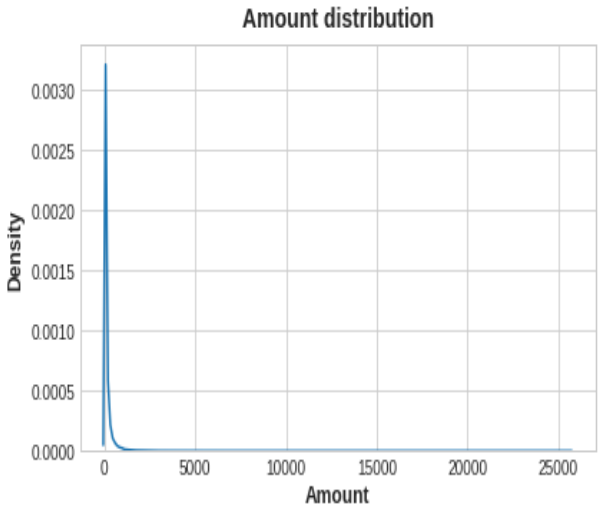
4. Results and Discussion

Step 1: Collect Records and Data

The dataset contains his Visa exchanges performed by a Mauritian cardholder. This dataset contains his 492 fakes from his 284,807 trades made in the last two days. The dataset is highly skewed, with all the same positive strata (fakes) accounting for only 0.172 percent. The important parts determined by PCA are the highlights V1, V2...V28. The main items that have not changed in the PCA are times and totals. Mark the number of seconds that have passed between each exchange in the record and the primary exchange and store it in the Time field. Exchange totals are specified in the "Total" element and can be used for child expense topics, etc. Highlight the response variable named "class". Value is 1 if blackmail exists, 0 if blackmail does not exist.

Step2 – Data pre-processing

1. Check Duplicate values in pandas data frame and found 8063 duplicate data, all related to non fraudolent transacti ons. I will drop them.
2. Amount Distribution



Box Cox and Log Transformation on Amount

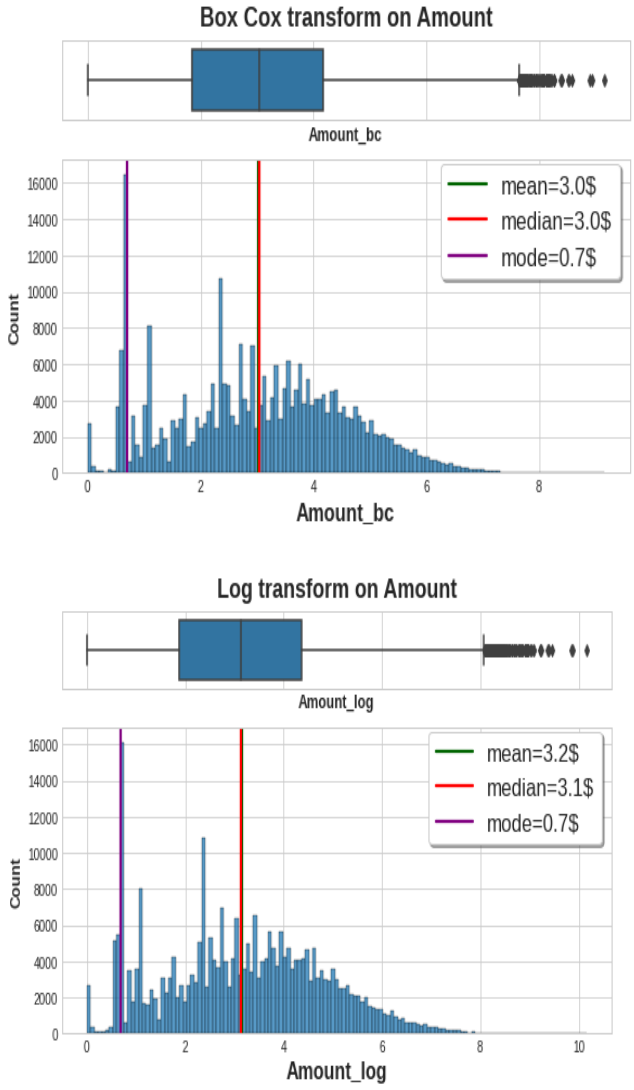


Table 1 is shown the simulation parameter of different ML algorithm. Table 1 is representing in four machine learning algorithm for recall, precision, F1 Score and accuracy. Naïve Bayes gives a recall of 84.6%, a precision of 78%, a F1-score of 69.9%, an accuracy of 97.7%, Logistic regression gives a recall of 61.2%, a precision of 82.1%, a F1-score of 70.1%, an accuracy of 98.8%, K-NN gives a recall of 70.4%, a precision of 86.1%, a F1-score of 77.5%, an accuracy of 98.8% and proposed ENN-DNN gives a recall of 75.7%, a precision of 83.7%, a F1-score of 79.5%, and an accuracy of 99.9%.

Table 1. Simulation Result for Different Technique

Results	Naïve Bayes	Logistic Regression	K-NN	Proposed ENN-DNN Technique
Recall	84.6%	61.2%	70.4%	75.7%
Precision	78%	82.1%	86.1%	93.7%
F1 Score	69.9%	70.1%	77.5%	91.6%
Accuracy	97.6%	98.8%	98.8%	99.3%

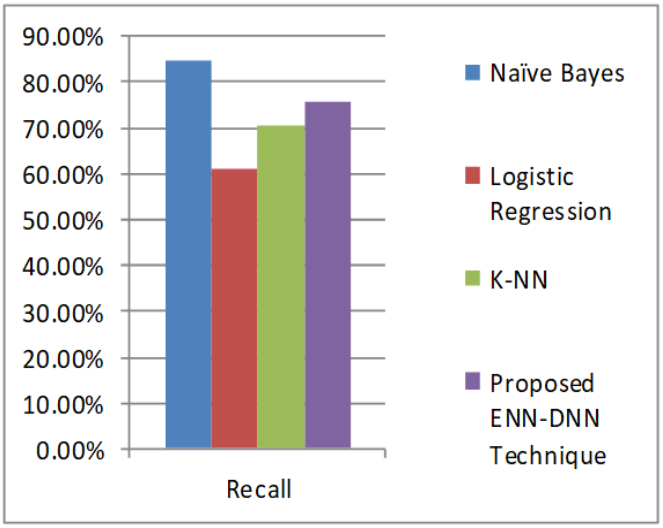


Figure 6. Graphical Represent of Recall

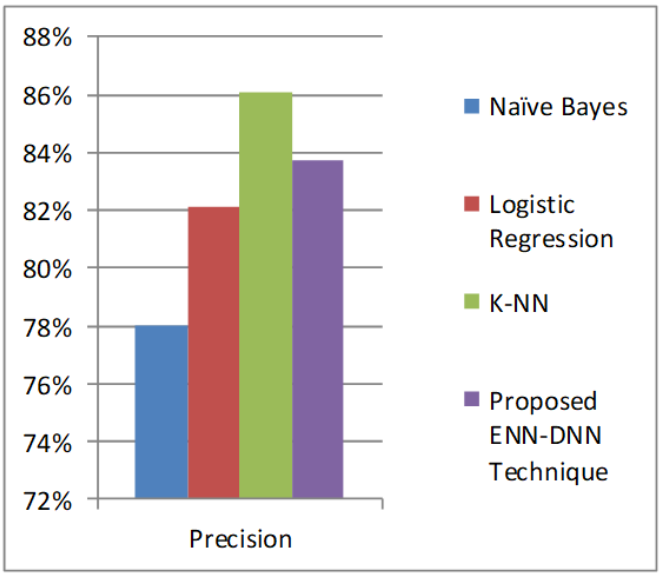


Figure 7. Graphical Represent of Precision

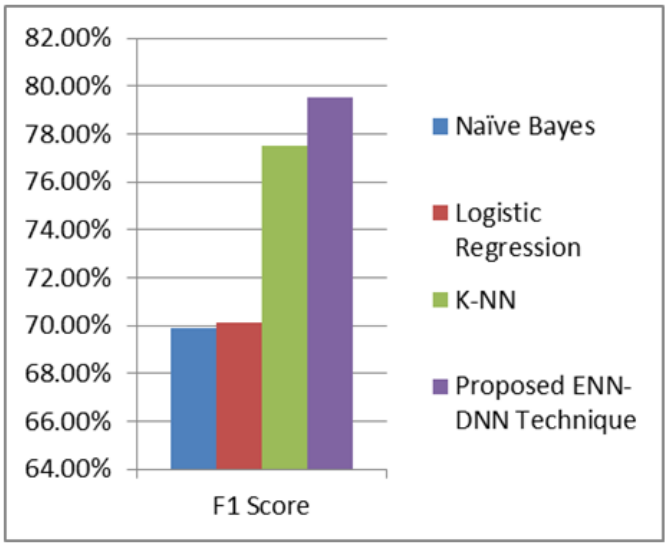


Figure 8. Graphical Represent of Recall

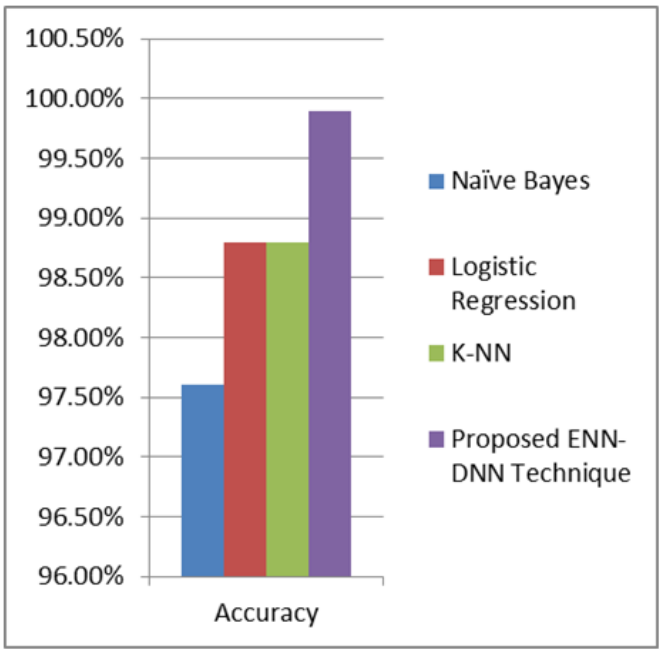


Figure 9. Graphical Represent of Accuracy

Table 2 is shows the comparison result for previous and proposed ENN-DNN technique. The previous technique is credit card data applied for CNN-SVM technique. The proposed technique is 27.8% improvement accuracy compared to previous CNN-SVM and 7.8% improvement accuracy compared previous CNN-SVM. The bar graph of the training and testing accuracy is shown in figure 10.

Table 2. Comparison Result

Results	Previous Technique	Proposed ENN-DNN Technique
Recall	90.34%	75.7%
Precision	90.50%	93.7%
F1 Score	90.41%	91.6%
Accuracy	91.08%	99.3%

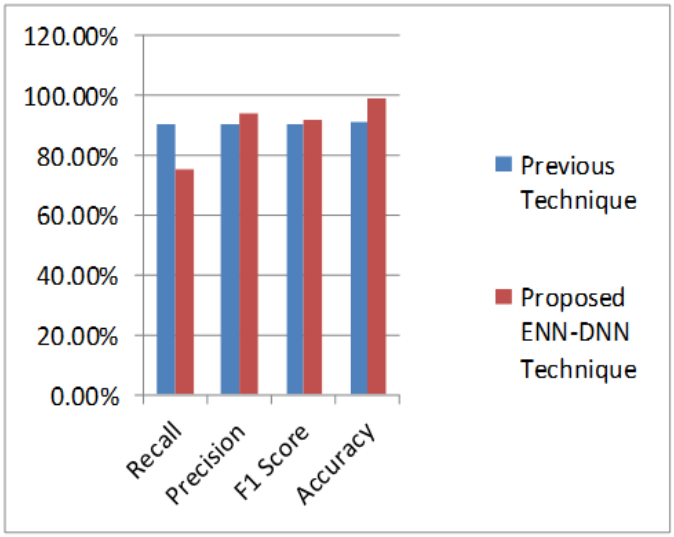


Figure 10. Graphical Represent of Accuracy

5. Conclusion and Future Scope

Electronic payment has two options users either choose online or offline. In virtual payment, user have to give information such as account holder name, PIN, card number and expiration date. A card and PIN are required for actual instalment payments. Online instalment offers a variety of options, so the customer uses different types of instalment instruments such as his Visa, check card, net banking, e-wallet, UPI, etc. Mastercard is the best-known and most attractive electronic payment method for online purchases. Recently, the use of online instalment components has increased. Charge cards can be used online or offline. From the simple analysis report, the most intended payment method for hacker is credit card.

Today, for the business companies or banking sectors the Credit Card Fraud become one of the biggest issues that requires more safety and security. As technologies are increasing, facilities are increasing with that other hand Credit card fraud scams are also rising. Consumers wants secure channel to complete the transaction. There are many different types of credit card frauds and we can detect the fraud transaction by available different fraud detection techniques.

References

[1] Tesfahun Berhane , Tamiru Melese, Assaye Walelign, and Abdu Mohammed, "A Hybrid Convolutional Neural Network and Support Vector Machine-Based Credit Card Fraud Detection Model", Mathematical Problems in Engineering (SCI), Hindawi, pp.**1-10**, **2023.**

[2] Ibomoiye Domor Mienye and Yanxia Sun, "A Machine Learning Method with Hybrid Feature Selection for Improved Credit Card Fraud Detection", Applied Science, **2023.**

[3] Vipul Jain, H Kavitha and S Mohana Kumar, "Credit Card Fraud Detection Web Application using Streamlit and Machine Learning", International Conference on Data Science and Information System (ICDSIS), IEEE **2022.**

[4] Yathartha Singh, Kiran Singh and Vivek Singh Chauhan, "Fraud Detection Techniques for Credit Card Transactions", 3rd International Conference on Intelligent Engineering and Management (ICIEM), IEEE **2022.**

[5] J. Leach and U. Tayasivam, "Optimizing data evaluation metrics for fraud detection using machine learning," International Journal of Mathematics and Computer Science, Vol.**16**, Issue.8, pp.**52–59, 2022.**

[6] R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," Human-Centric Intelligent Systems, Vol.**2**, Issue.**1-2**, pp.**55–68, 2022.**

[7] V. Plakandaras, P. Gogas, T. Papadimitriou, and I. Tsamardinos, "Credit card fraud detection with automated machine learning systems," Applied Artifcial Intelligence, vol. 36, no. 1, Article ID 2086354, **2022.**

[8] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, "Credit card fraud detection using a new hybrid machine learnig Architecture", Mathematics, Vol.**10**, Issue.**9**, pp.**1480, 2022.**

[9] S. Al-Faqir and O. Ouda, "Credit card frauds scoring model based on deep learning ensemble," Journal of Teoretical and Applied Information Technology, Vol.**100**, Issue.**14, 2022.**

[10] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," IEEE Access, Vol.**10**, pp.**39700–39715, 2022.**

[11] F. Itoo and S. Singh "Comparison and analysis of logistic regression Naïve Bayes and KNN machine learning algorithms for credit card fraud detection" International Journal of Information Technology Vol.**13**, Issue.**4**, pp.**1503-1511 2021.**

[12] E. S. C. R. S K Saddam Hussain "Fraud Detection in Credit Card Transactions Using SVM and Random Forest Algorithms" IEEE Xplore **2021.**

[13] E. Ileberi Y. Sun and Z. Wang "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost" IEEE Vol.**9**, Issue.**5**, pp.**165286-165294 2021.**

[14] D. Tanouz R. R. Subramanian and D. Eswar "Credit Card Fraud Detection Using Machine Learning" IEEE **2021.**

[15] S. Khatri A. Arora and A. P. Agrawal "Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison" IEEE **2020.**

