



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

Credit Card Fraud Detection Using an Enhanced Artificial Neural Network with Regularization Techniques

Harshit Dhote

Electronics and Electrical

Email ID -harshitdhote02@gmail.com

Shri Vaishnav Institute of Technology and Science (SVITS) Indore

Mihir Paul

LNCT Excellence Bhopal

Email ID - mihirpaul2005@gmail.com

Abstract

Credit card fraud detection remains a critical challenge due to the highly imbalanced nature of transaction data, evolving fraud patterns, and the need for real-time decision-making. Recent research demonstrates that ensemble learning techniques, such as bagging and boosting, significantly improve detection accuracy while reducing false positive rates by effectively handling class imbalance. In parallel, advanced deep learning architectures, including Convolution Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown strong potential in capturing complex spatial and temporal patterns within transaction data. Anomaly detection methods further enhance fraud detection capabilities by identifying irregular transaction behaviors and minimizing false negatives. This study highlights the importance of integrating ensemble learning, deep learning, and anomaly detection approaches to develop robust and adaptive fraud detection systems. Additionally, incorporating auxiliary data sources such as user behavior, geo-location information, and device fingerprints provides richer contextual insights, leading to improved prediction performance. The development of real-time fraud detection models is emphasized as a crucial research direction to prevent financial losses through timely intervention.

Keywords-Fraud Detection, Financial Transactions, Ensemble Learning, Bagging and Boosting, Deep Learning, PCA, Convolutional Neural Networks (CNN).

Introduction

Credit card fraud involves the unauthorized use of an individual's credit card or the theft of credit card information to obtain financial benefits. Fraudulent activities can take several forms. One common type is counterfeit card fraud, where criminals steal card details and create fake cards with duplicated card numbers and PINs. Another prevalent category is card-not-present (CNP) fraud, which occurs when stolen card information is used for online or telephone



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

transactions without the physical presence of the card . Additional forms of credit card fraud include identity theft, where personal information is misused to open new credit card accounts, and skimming fraud, where criminals install malicious devices on legitimate card readers to capture card details.[1]

In recent years, there has been significant interest in applying machine learning techniques to credit card fraud detection. Fraud has become a growing concern for financial institutions worldwide, as it results in substantial financial losses for cardholders, banks, and merchants who are responsible for reimbursing unauthorised transactions. Beyond financial losses, credit card fraud can erode trust in the banking system, potentially reducing consumer confidence, spending, and overall economic stability.

The consequences of credit card fraud extend beyond monetary loss. Victims often suffer emotional distress, damage to credit histories, and long-term financial complications. Banks and financial institutions also incur additional costs related to refunding fraudulent transactions and implementing advanced security mechanisms to prevent future fraud. Moreover, the societal impact of credit card fraud is widespread, as its ripple effects influence the broader economy and affect individuals beyond the immediate victims.

Detecting credit card fraud remains challenging due to the evolving tactics and technologies used by fraudsters, the increasing complexity of transaction data, and the growing volume of online and electronic payments. Distinguishing fraudulent transactions from legitimate ones has become increasingly difficult, particularly as fraud patterns continuously change. To address these challenges, financial institutions have adopted machine learning and statistical models capable of analyzing large datasets, identifying hidden patterns, and detecting suspicious activities in real time.[2]

A- Machine Learning Models

Supervised learning is a machine learning approach in which models are trained using labelled datasets to predict outcomes for unseen data. It is commonly applied to tasks such as classification, regression, and recommendation systems. In credit card fraud detection, supervised learning algorithms are trained on historical transaction data labelled as either genuine or fraudulent. Commonly used supervised learning techniques include Logistic Regression, Support Vector Machines (SVM), Decision Trees, Random Forest, Naïve Bayes, and K-Nearest Neighbour (KNN).

1) Logistic Regression

Logistic regression is a statistical method used to estimate the probability of a binary outcome, such as whether a transaction is fraudulent or legitimate, based on one or more independent variables. These variables may include transaction amount, frequency, and time of



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

occurrence. The model maps input features to a probability value between 0 and 1 using the logistic (sigmoid) function :

$$Z(p)=1+e^{-z}, z=p+x_1+x_2+\dots+x_n$$

where p represents the probability of fraud and z is the linear combination of input features.

Several studies have demonstrated the effectiveness of logistic regression in fraud detection. Minastireanu and Mesnita compared multiple machine learning techniques across financial and e-commerce domains and found logistic regression to offer high accuracy and efficient handling of complex datasets. Maranzato applied logistic regression to extract correlated features from transaction data to flag suspicious transactions, while Luo and Wan used the model to identify characteristics of fraudulent accounts in e-business environments.[3]

Logistic regression is valued for its simplicity, interpretability, and ease of training. However, its assumption of linearity and sensitivity to imbalanced datasets can make it prone to overfitting if not carefully managed.

2) Decision Trees

Decision trees are supervised learning algorithms used for both classification and regression tasks. They employ a hierarchical tree structure consisting of a root node, internal decision nodes, and leaf nodes. Each split in the tree is based on information gain, guiding the decision process toward the most informative features.

Dhankhad et al. applied a decision tree classifier to an imbalanced credit card transaction dataset and achieved an accuracy of 91% in detecting fraudulent transactions. proposed a hybrid decision tree model that combined Hunt's and Luhn's algorithms to improve the detection of inconsistencies in customer data.

Decision trees are easy to interpret and robust against overfitting; however, their performance may degrade on complex or highly imbalanced datasets. To overcome these limitations, researchers have explored ensemble and sampling techniques. Zareapoor and Amsolmoali employed bagging with decision trees, while Ahsan et al. applied oversampling techniques to handle data imbalance. These studies confirm the effectiveness of decision trees for fraud detection, although further improvements are still required [6].

3) Random Forest (RF)

Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve classification accuracy. Each tree is trained on a random subset of the data, and the



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

final decision is made by aggregating the predictions of all trees. This approach generally outperforms single decision tree models and is widely used in classification tasks .

Lin and Jiang integrated an autoencoder with a probabilistic random forest model to enhance fraud detection without requiring traditional sampling techniques. Pozzolo [proposed a weight-sensitive random forest model for real-time fraud detection using streaming financial data and demonstrated improved performance in handling class imbalance and delayed transaction verification. Saheed et al. compared Random Forest with SVM and Naïve Bayes using a Genetic Algorithm for feature selection and found Random Forest to be the most effective predictor.

Despite its strengths, Random Forest has certain limitations, including higher computational cost, slower convergence, and reduced interpretability compared to individual decision trees . Nevertheless, it remains one of the most powerful techniques for credit card fraud detection.

4) Support Vector Machines (SVM)

Support Vector Machines are supervised learning algorithms used for classification, regression, and outlier detection. SVMs work by constructing a hyperplane that maximises the margin between different classes, enabling effective separation of fraudulent and legitimate transactions.

Compared SVM and Random Forest algorithms for fraud detection and reported an accuracy of 84.1% using SVM. Bin et al. [46] proposed a hybrid CNN–SVM model that combined deep learning with SVM to identify fraud patterns in real-world transaction data. Their results demonstrated that SVM-based hybrid models are effective in capturing complex fraud behaviours.

B- Deep Learning Models

VGG16

VGG16 is a deep Convolutional Neural Network (CNN) architecture introduced by the Visual Geometry Group (VGG) at the University of Oxford. It consists of 16 weight layers, including 13 convolutional layers and 3 fully connected layers. The network uses small 3×3 convolution filters stacked sequentially, along with ReLU activation and max-pooling layers to capture hierarchical image features. VGG16 is widely used in image classification and feature extraction tasks due to its simple and uniform architecture, although it requires high computational resources and memory because of its large number of parameters. [7]



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**



Fig. 1 Vgg16 Layer Architecture

VGG19

VGG19 is an extension of the VGG16 architecture with 19 weight layers, comprising 16 convolutional layers and 3 fully connected layers. By increasing the network depth, VGG19 is capable of learning more complex and fine-grained image representations. Similar to VGG16, it employs small 3×3 convolution kernels and max-pooling layers. While VGG19 often achieves slightly improved accuracy over VGG16, it also introduces higher computational complexity and increased training time, making it less efficient for real-time applications.[8]

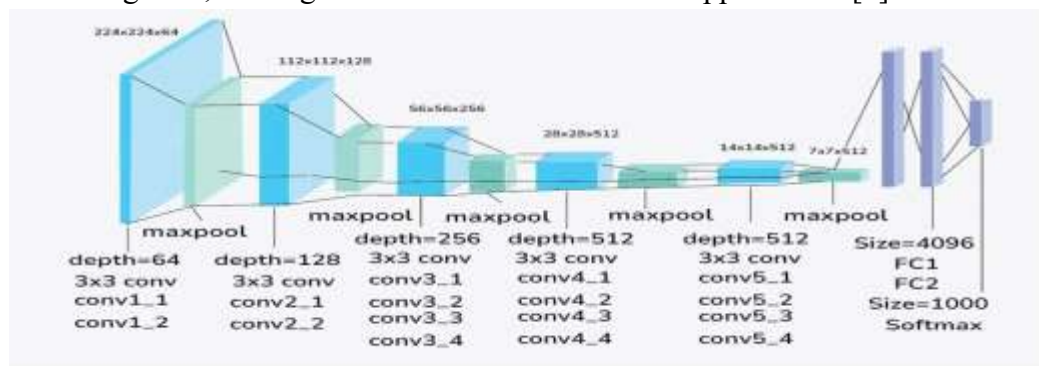


Fig.2 VGG 19 Layer Architecture

ResNet50

(Residual Network with 50 layers) addresses the limitations of very deep networks by introducing residual learning through shortcut (skip) connections. These connections allow gradients to flow directly through the network, mitigating the vanishing gradient problem and enabling the training of much deeper architectures. ResNet50 consists of 50 layers and uses bottleneck residual blocks with 1×1, 3×3, and 1×1 convolution layers. Compared to VGG architectures, ResNet50 achieves higher accuracy with fewer parameters and is more



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

computationally efficient, making it well-suited for large-scale image recognition and transfer learning applications.[8]

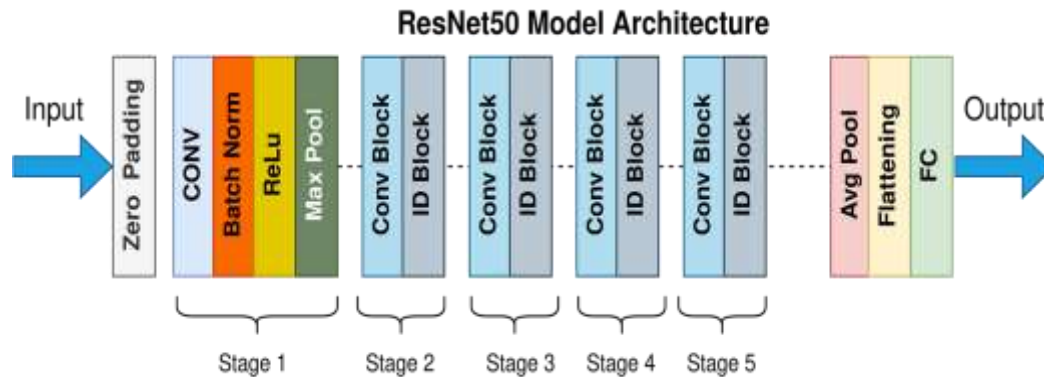
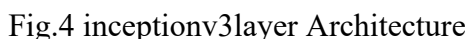


Fig.3 ResNet50 model

InceptionV3

First presented the “creative” horizontal. In his 2014 paper *Going Deeper with Convolutions*: The goal of start-up model is to function as a “multi-feature explorer” by calculating 1×1 , 3×3 , or 5×5 , in the same model of the network- these filter results are applied according to the dimensions of the channel. To improve the capacity of deep neural networks before use, the most direct way is to increase the depth of the network. However, as the depth of the network width increases, there are too many internal dimensions, which results in more resource consumption. Therefore, in order to overcome these problems, Szegedy et al first introduced the Inception model into the Google Net architecture. And completed an impressive performance and read record as the winner of the Image Net ILSVRC Challenge. The first model consists of an upper water-supply layer and a corresponding plate. The sizes of the mixed layers were 1×1 , 3×3 , and 5×5 which were combined. Between two matching 1×1 layers, the maximum reduction is used to reduce the dimensionality and a tandem filter is required to combine the different layers. In addition, by removing the 5×5 convolutions and introducing two 3×3 convolutions to modify the initial model change, it was widely used in later network configurations [9].



The Mobile Net model is built on a tangible deep convolution, a type of broken convolution that converts a regular convolution to a deep complexity and a one-to-one complexity termed an effective convolution point. Convolution filters each communication channel in Mobile Nets using a single filter. After that, the wise complexity performs a one-to-one convolution to combine the deep convolution advances. Traditional convolution not only filters use, but combines the use of a series of new products in one process. The single column divides it into two layers, one for filtering and one for mixing. This deletion has an effect on the calculation of the calculation and the size of the model.[10]



One of the recent breakthroughs in neural networks for the recognition of visual objects is referred to as DenseNet. DenseNet is quite similar to ResNet, although there are a few key distinctions between the two DenseNet adds (.) its own output to the output of the layer that came before it, while ResNet uses an additive method (+) that joins the identity of the layer that



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

came before it with the identity of the layer that will come after it. Using composite function action, an output from a lower layer can be used as an input for a higher layer. When the action is done on a layer, this can happen. The different parts of this combined method are called the convolution layer, the pooling layer, the batch normalisation, and the non-linear activation layer. Because of these links, the network has an absolute maximum of $L(L+1)/2$ direct connections. The number of levels in the architecture is denoted by the letter L . The DenseNet has several versions, such as DenseNet-121, DenseNet-160, DenseNet-201, etc. The number in the digits shows how many levels are in the neural network.[11].

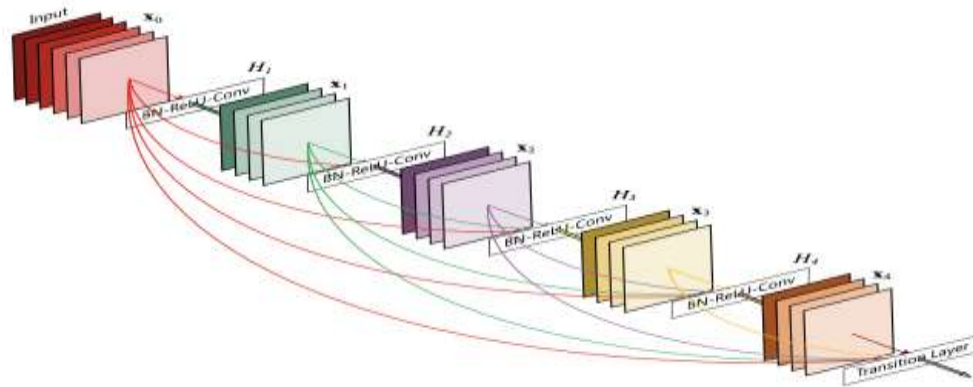


Fig.6 DenseNet Layer Architecture

GoogLeNet

The convolutional neural network known as Google Net consists of a total of 22 layers. You can load a network that has already been trained. The data set that was used to train it can be either ImageNet or Places365. The network that was trained on ImageNet can divide images into 1,000 different types of objects. In these groups, you can find things like a computer, a mouse, a pencil, and a wide range of animals. The Inception architecture is the foundation for the GoogLeNet variety of convolutional neural network that Google developed. It does this through the utilization of Inception modules, which provide the network the ability to select from a number of different convolutional filter sizes in each block. These modules are layered one atop the other in an Inception network, which also includes some max-pooling layers with stride 2 now and then to reduce the resolution of the grid by one half.[12]



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

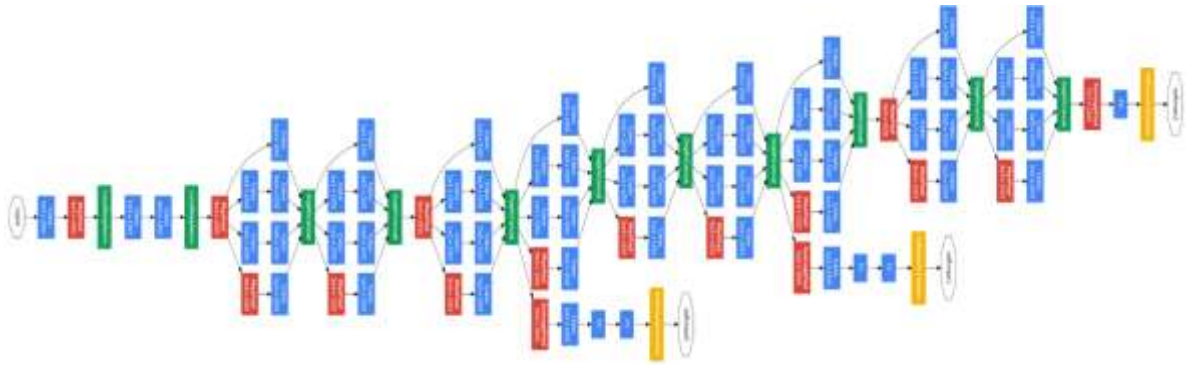


Fig.7 GoogLeNet Layer Architecture

Data Pre-Processing Techniques

Data preparation is a critical stage in data mining and machine learning, as the effectiveness of any predictive model largely depends on the quality of the input data. Data pre-processing involves the cleaning and transformation of acquired data to convert raw information into a suitable format for analysis. However, collected log data are often noisy, incomplete, and of poor quality, which can negatively affect the performance of data mining algorithms. Consequently, the reliability of machine learning models is highly dependent on the quality of the training data used. Data pre-processing enhances the suitability of raw data by collecting, integrating, cleaning, transforming, reducing, and discretising it, thereby improving its quality and usability. It is widely acknowledged that effective data pre-processing significantly impacts the performance and outcomes of machine learning tasks. [13]

C- Data Cleaning and Transformation

Data cleaning and transformation represent the initial steps in the data pre-processing pipeline for credit card fraud detection. Data cleaning focuses on identifying, correcting, and eliminating errors, inconsistencies, and missing values to ensure data accuracy, completeness, and consistency. The primary objective of this step is to improve overall data quality. Cleaned and well-structured data provide reliable inputs for machine learning models, leading to improved prediction accuracy and robustness.

Data transformation involves converting cleaned raw data into formats that are more suitable for analysis and visualisation. Common transformation techniques include scaling, normalisation, and encoding of categorical variables. These mathematical transformations ensure that data attributes are represented in compatible ranges and structures, allowing learning algorithms to process them effectively. Overall, data transformation aligns the dataset with analytical requirements, enhancing model performance and interpretability.[14]

Feature Selection and Extraction



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

Feature selection and extraction are essential components of data pre-processing that aim to improve model efficiency, accuracy, and interpretability. Feature selection focuses on identifying the most relevant attributes within a dataset while eliminating redundant or irrelevant features, thereby reducing dimensionality. By simplifying the dataset, classification models become more efficient and less prone to overfitting. Additionally, feature selection enhances model interpretability by retaining only meaningful features that contribute significantly to prediction outcomes.

Feature extraction, on the other hand, involves creating new features by transforming or combining existing attributes to better represent the underlying patterns in the data. Both feature selection and extraction help reduce the overall dimensionality of the dataset, improve computational efficiency, and enhance the generalisation capability of machine learning models[15]

Handling Imbalanced Datasets

An imbalanced dataset refers to a situation where class distributions are uneven, with one class significantly outnumbering the other. In such datasets, the majority class typically represents legitimate transactions, while the minority class corresponds to fraudulent transactions. The imbalance rate, defined as the ratio between the number of majority and minority class samples, is commonly used to quantify this disparity. Imbalanced datasets pose significant challenges for machine learning models, as they tend to bias predictions toward the majority class.

This issue is particularly critical in credit card fraud detection, where fraudulent transactions constitute a very small proportion of total transactions. Traditional machine learning algorithms often struggle to correctly identify minority class instances, leading to high false-negative rates. Therefore, addressing data imbalance through appropriate pre-processing techniques is essential to improve fraud detection accuracy and ensure reliable model performance

D- Feature normalization and scaling.

If the goal is for all the numbers in your dataset to be on the same scale, it's necessary to normalize and standardize them. In this part we will discuss advanced methods of data transformation and data scaling which should enable more accurate and effective analysis. Properly normalized and scaled data may be beneficial to data processing procedures, particularly those necessary to the complex machine learning models.[16]

Min-Max Scaling: It is normally fed with a value of 0-1 and the values are rescaled.

Z-Score Standardization: Moves the data into the normal distribution with some modifications made with regard to standard deviation of that data and the mean.



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

Feature Engineering and Selection

Efficient data pre-processing is the cornerstone of enabling data scientists to enhance predictive power of their models with the help of feature engineering and feature selection. This section delves into cutting-edge methods for developing new features and identifying the most significant ones.

Dimensionality Reduction: Keeping only the most important data by reducing the number of variables being considered.

Interaction Features: Building additional characteristics to depict interdependencies among variables in order to capture more intricate relationships. When developing efficient models, it is essential to transform and choose features that will have a direct impact on their learning and prediction capabilities. [16]

Dimensionality Reduction

The main goal of dimensionality reduction is to cut down on the amount of features in a dataset while maintaining all the critical information.[17] To put it another way, it keeps the most important parts of high-dimensional data while moving it to a lower-dimensional space. shows in Figure 3

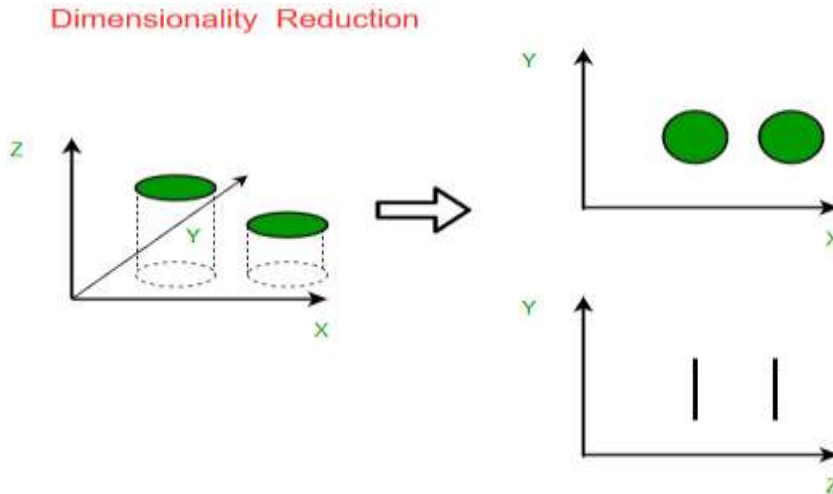


Figure 3-dimension reduction

Principal Component Analysis

The mapping from higher-dimensional to lower-dimensional data must be performed under the constraint that the variance of the lower-dimensional data must be greatest for the mapping to be successful.



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

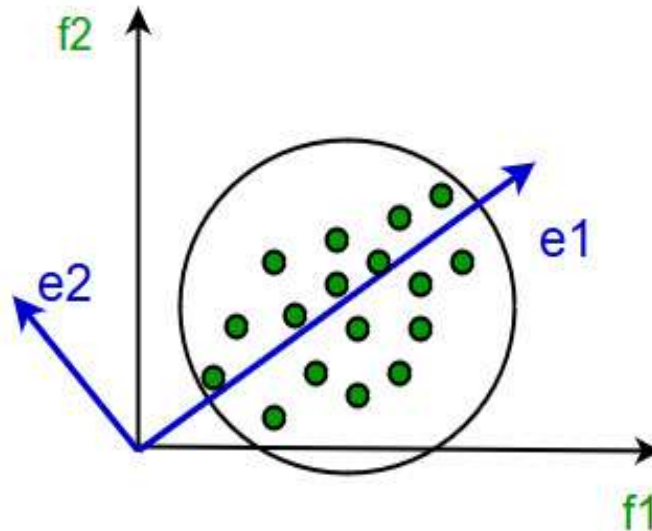


Figure 2 Principal Component Analysis structure

DATASET DESCRIPTION

E- Evaluation Metrics

Evaluation metrics play a crucial role in assessing the effectiveness of machine learning models for credit card fraud detection. Due to the highly imbalanced nature of fraud datasets, selecting appropriate performance metrics is essential to ensure reliable and meaningful evaluation.

Accuracy and Error Rates

Accuracy is one of the most commonly used metrics to evaluate the performance of machine learning models. It is defined as the ratio of correctly predicted transactions to the total number of transactions [18-19]: Although accuracy is simple to compute and interpret, it can be misleading in the context of credit card fraud detection, where non-fraudulent transactions significantly outnumber fraudulent ones. In such imbalanced datasets, a model can achieve high accuracy by classifying all transactions as legitimate, despite failing to identify fraud cases. Consequently, accuracy alone cannot serve as a reliable indicator of a model's fraud detection capability.

To overcome this limitation, error rates such as false positive rate (FPR) **and** false negative rate (FNR) **must** also be considered. The false positive rate refers to the proportion of legitimate transactions incorrectly classified as fraudulent, while the false negative rate represents the proportion of fraudulent transactions misclassified as legitimate. These error rates are particularly critical in credit card fraud detection. False positives can inconvenience genuine



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

customers by blocking legitimate transactions, whereas false negatives are more severe as they allow fraudulent transactions to go undetected, resulting in financial losses for both individuals and financial institutions.[20]

Precision, Recall, and F1-Score

Precision, recall, and F1-score are widely adopted metrics for evaluating fraud detection systems, particularly when dealing with imbalanced datasets. **Precision** is defined as the ratio of true positive predictions to the total number of predicted positives. It indicates how accurately the model identifies fraudulent transactions and reflects the likelihood of false alarms. A higher precision value suggests fewer false positives.

Recall, also known as sensitivity, is calculated as the ratio of true positives to the total number of actual fraudulent transactions in the dataset. Recall measures the model's ability to detect fraud cases correctly, and a higher recall value corresponds to fewer false negatives.

The **F1-score** combines precision and recall into a single metric by computing their harmonic mean. This metric provides a balanced evaluation of the model's performance, particularly when precision and recall trade-offs exist. The F1-score is especially useful in fraud detection scenarios where both minimizing false positives and detecting fraudulent transactions accurately are equally important.[21]

CONCLUSION

This study addressed the growing challenge of fraud detection in financial transactions by exploring intelligent, data-driven approaches capable of handling large-scale, highly imbalanced datasets and evolving fraud patterns. Traditional rule-based and signature-based methods were found to be inadequate due to their limited adaptability and high false-positive rates. To overcome these limitations, the research focused on machine learning and deep learning techniques that can automatically learn complex patterns from transactional data.

The experimental analysis demonstrated that baseline machine learning models such as Logistic Regression, Random Forest, and Support Vector Machine provide reliable fraud detection performance when evaluated using robust metrics including accuracy, F1-score, ROC-AUC, and PR-AUC. Furthermore, the integration of ensemble learning through a stacked model improved overall detection capability by effectively combining the strengths of individual classifiers.

The study also highlighted the importance of explainability and model robustness for real-world deployment. By incorporating advanced neural network architectures and regularization techniques such as Batch Normalization and Dropout, the proposed approach enhances generalization performance and adaptability to changing fraud behaviors. Overall, the findings confirm that intelligent and scalable fraud detection frameworks are essential for securing modern financial systems and supporting timely, data-driven decision-making. This research



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

provides a strong foundation for future work aimed at developing real-time, explainable, and highly accurate fraud detection solutions.

Future Directions and Research Opportunities

Future research in credit card fraud detection can benefit significantly from the adoption of ensemble learning techniques, which have been shown to enhance prediction accuracy while reducing false positive rates. Methods such as bagging and boosting demonstrate strong performance in fraud detection tasks and help mitigate the effects of class imbalance, where fraudulent transactions represent only a small fraction of the dataset.

In addition to ensemble approaches, exploring advanced deep learning architectures, including Recurrent Neural Networks (RNNs) and Convolution Neural Networks (CNNs), presents promising opportunities for capturing complex temporal and spatial patterns in transaction data. Furthermore, anomaly detection algorithms can be employed to identify unusual or suspicious transaction patterns, thereby strengthening fraud detection capabilities while minimizing false negatives. Integrating ensemble learning, deep learning, and anomaly detection techniques is likely to further improve the effectiveness of machine learning-based fraud detection systems.

Another important research direction involves incorporating additional data sources beyond traditional transactional attributes. Supplementary information such as user behaviour patterns, geo-location data, and device fingerprints can provide richer contextual insights into transaction behaviour, thereby enhancing detection accuracy. Additionally, the development of real-time fraud detection systems remains a critical area of focus. Financial institutions must design models capable of analysing transactions within extremely short time frames to detect fraudulent activities promptly and prevent substantial financial losses.

Ethical considerations also play a vital role in the deployment of machine learning-based fraud detection systems. Protecting user privacy and securing sensitive financial data are paramount concerns. Despite these challenges, recent advancements in ensemble learning, deep learning architectures, and anomaly detection algorithms have demonstrated substantial potential in improving both the precision and efficiency of fraud detection systems.

A promising direction for future work will involve the implementation of an Artificial Neural Network (ANN) enhanced with Batch Normalization and Dropout layers to further improve fraud detection performance. The proposed ANN architecture will consist of multiple dense layers with neuron configurations of $256 \rightarrow 128 \rightarrow 64 \rightarrow 32$, each employing ReLU activation functions to effectively capture non-linear patterns in transaction data. Batch Normalization will be applied to stabilize and accelerate the training process by normalizing the inputs of each layer, while Dropout with a rate of 0.3 will be incorporated to randomly deactivate neurons during



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

training, thereby reducing overfitting and enhancing generalization capability.

References

1. H. K. Prakosa and N. Rokhman, "Anomaly detection in hospital claims using K-Means and linear regression," *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, vol. 15, no. 4, p. 391, Oct. 2021, doi: 10.22146/IJCCS.68160.
2. M. Carminati, A. Baggio, F. Maggi, U. Spagnolini, and S. Zanero, "FraudBuster: Temporal analysis and detection of advanced financial frauds," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, LNCS, vol. 10885, pp. 211–233, 2018, doi: 10.1007/978-3-319-93411-2_10.
3. Sadgali, N. Sael, and F. Benabbou, "Performance of machine learning techniques in the detection of financial frauds," *Procedia Computer Science*, vol. 148, pp. 45–54, Jan. 2019, doi: 10.1016/J.PROCS.2019.01.007.
4. F. Alharbi *et al.*, "A brief review of acoustic and vibration signal-based fault detection for belt conveyor idlers using machine learning models," *Sensors*, vol. 23, no. 4, Feb. 2023, doi: 10.3390/S23041902.
5. P. Freitas de Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, "An efficient intrusion prevention system for CAN: Hindering cyber-attacks with a low-cost platform," *IEEE Access*, vol. 9, pp. 166855–166869, 2021, doi: 10.1109/ACCESS.2021.3136147.
6. S. P. Devika, K. S. Nisarga, G. P. Rao, S. B. Chandini, and N. Rajkumar, "A research on credit card fraudulent detection system," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 2, pp. 5029–5032, Jul. 2019, doi: 10.35940/IJRTE.B1083.078219.
7. Pumsirirat A and Yan L, "Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine", *International Journal of advanced computer science and applications*, vol.9, no.1, pp.18-25, January 2018.
8. Omariba Z B, Masese N B, Wanyembi G, "Security and privacy of electronic banking" *International Journal of Computer Science Issues (IJCSI)*, vol.9, no.4, pp.432, July 2012.
9. A. Dal Pozzolo, G. Boracchi, O. Caen, C. Alippi, G. Bontempi Credit card fraud detection: A realistic modeling and a novel learning strategy *IEEE Transactions on Neural Networks and Learning Systems*, 29 (8) (2017), pp. 3784-3797
10. S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. S. Hacid An experimental study with imbalanced classification approaches for credit card fraud detection *IEEE Access*, 7 (2019), pp. 93010-93022



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

11. E. Strelcenia, S. Prakoonwit Improving classification performance in credit card fraud detection by using new data augmentation AI, 4 (1) (2023), pp. 172-198
12. A. Wahid, M. Msahli, A. Bifet, G. Memmi NFA: A neural factorization autoencoder based online telephony fraud detection Digital Communications and Networks (2023) 10.1016/j.dcan.2023.03.002
13. Omariba Z B, Masese N B, Wanyembi G, “Security and privacy of electronic banking”, International Journal of Computer Science Issues (IJCSI), vol.9, no.4, pp.432, July 2012.
14. S. P. Maniraj, A. Saini, S. Ahmed, and S. D. Sarkar, “Credit card fraud detection using machine learning and data science,” *International Journal of Engineering Research and Technology (IJERT)*, vol. 8, no. 9, Sep. 2019, doi: 10.17577/IJERTV8IS090031.
15. Trivedi, M. Monik, and M. Mridushi, “Credit card fraud detection,” *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, vol. 5, no. 1, pp. 39–42, Jan. 2016, doi: 10.17148/IJARCCE.2016.5109.
16. Singh P and Singh M, “Fraud detection by monitoring customer behavior and activities”, International Journal of Computer Applications, vol.111, pp.11, January 2015M. Elnour, N. Meskin, K. Khan, and R. Jain, “A dual isolation-forests-based attack detection framework for industrial control systems,” *IEEE Access*, vol. 8, pp. 36639–36651, 2020, doi: 10.1109/ACCESS.2020.2975066.
17. X. Shu, S. Zhang, Y. Li, and M. Chen, “An anomaly detection method based on random convolutional kernel and isolation forest for equipment state monitoring,” *Eksploatacja i Niezawodność – Maintenance and Reliability*, vol. 24, no. 4, pp. 758–770, 2022, doi: 10.17531/EIN.2022.4.16.
18. C. Xiong *et al.*, “Construct and validate a predictive model for surgical site infection after posterior lumbar interbody fusion based on machine learning algorithm,” *Computational and Mathematical Methods in Medicine*, vol. 2022, 2022, doi: 10.1155/2022/2697841.
19. Gianini G, Fossi L G, Mio C, Caelen O, Brunie L, Damiani E, “Managing a pool of rules for credit card fraud detection by a Game Theory based approach”, *Future Generation Computer Systems*, vol.102, pp.549-61, January 2020.