# ijRASET

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

www.ijraset.com

Call: ○ 08813907089     |     E-mail ID: ijraset@gmail.com

# Credit Card Fraud Detection Using Machine Learning: A Review

Mehvish[1], Satish Saini[2], Ravinder Pal Singh[3]

[1]*M. Tech Scholar, Department of Electronics and Communication, RIMT University, Punjab, India*
[2]*Professor and HOD, Department of Electrical Engineering, RIMT University, Punjab, India*
[3]*Technical Head, Department of Research Innovation and Incubation RIMT University, Punjab, India*

*Abstract: Emerging technology has brought about transformative changes across various vital industries such as healthcare, finance, manufacturing, transportation, and e-commerce. Among these sectors, the financial industry, in particular, has experienced significant positive shifts due to technological advancements. Banking services have embraced digitization and the evolution of e-commerce, resulting in a notable growth in the utilization of credit cards. However, with these advancements comes a challenge: an increase in fraudulent activities. This challenge has prompted the financial industry to take proactive measures to ensure the security and effectiveness of its operations. The surge in credit card usage has unfortunately attracted a higher number of fraudulent actors, leading to several predicaments for the banking sector. Amidst these challenges, financial institutions are committed to safeguarding credit card transactions and providing secure e-banking services to their clients. To address this, they are actively engaged in the development of more sophisticated fraud detection techniques. These techniques aim to not only identify a broader range of fraudulent transactions but also to enhance the overall effectiveness of fraud prevention systems and fraud detection systems. This article aims to provide a comprehensive overview of the key elements that constitute effective fraud detection, along with a deep dive into the current systems and methodologies in place. By shedding light on the prevalent challenges and complexities associated with fraudulent activities in the banking industry, the article also underscores the vital role that machine learning techniques play in the realm of solutions. In essence, this article seeks to showcase the positive trajectory of the financial industry's response to emerging challenges, highlighting its commitment to leveraging cutting-edge technology to ensure secure and seamless banking experiences for all clients.*
*Keywords: Machine learning techniques; credit card fraud detection; legitimate transaction; financial institutions; digitalization; e-commerce*

## I.     INTRODUCTION

Big Data technology have played a significant role in modernizing a number of important fields, including healthcare, finance, manufacturing, transport, and e-commerce, in the quickly changing financial sector environment. The banking sector stands out among these industries as a key participant impacted by the digitalization of services and the increase in e-commerce transactions. Significant issues have arisen in the banking industry, notably in Fraud Control Systems, as a result of the rising use of credit cards and the growth in fraudsters. Strong fraud detection methods that can secure credit card transactions and safeguard the openness of online payments are therefore urgently needed. In this article, we will go into the fundamentals of fraud detection, investigate current fraud detection technologies, discuss the difficulties the banking industry faces, and concentrate on machine learning-based solutions now available.

The financial system must be protected from harmful activity by fraud detection and prevention systems (FDS and FPS). Traditional rule-based systems alone, however, are no longer sufficient to fight the constantly changing threat landscape as fraudsters grow more skilled at hiding their actions. The pressing necessity for financial institutions to improve their fraud detection skills has resulted in an increased dependence on cutting-edge technology like machine learning.

In this article, we'll examine the foundational elements of fraud detection, look at current fraud detection technologies, discuss the difficulties the banking industry faces, and concentrate on machine learning-based solutions now in use. We'll look at how machine learning has revolutionized the battle against financial fraud with its capacity to analyze massive volumes of data, unearth hidden patterns, and react to changing fraud trends. Banks want to strengthen credit card transactions and assure the efficiency and safety of their e-banking services by utilizing the power of sophisticated analytics and artificial intelligence, giving clients trust and preserving the integrity of the financial ecosystem.

In addition, we will examine how data privacy and regulatory compliance relate to fraud detection. For financial institutions, finding the ideal balance between effective fraud prevention and consumer privacy protection continues to be of utmost importance. Financial institutions must traverse a difficult terrain to ensure their fraud detection operations comply with legal and ethical standards as governments pass strict data protection regulations and customers demand more open data management.

Financial institutions can provide a safe and secure environment for credit card transactions and e-banking services in a world that is becoming more and more digital by being on the cutting edge of technical developments and encouraging a proactive and cooperative reaction to new dangers.

## II. FUNDAMENTAL ASPECTS OF FRAUD DETECTION

Fraud detection is the process of locating and stopping unlawful transactions, dishonest behaviour, and fraudulent activity inside a financial system. It entails sorting through enormous volumes of data in real-time to identify trustworthy transactions from shady ones. Important components of fraud detection include.

A credit card serves as a financial tool issued to clients, commonly allowing them to make purchases up to a predetermined credit limit or to access cash advances. One of the key benefits of credit cards is that they grant cardholders the convenience of time, permitting them to settle their dues at a later date by carrying the debt forward to the subsequent payment cycle.

Credit cards, unfortunately, present a lucrative target for fraudulent activities. Exploiting vulnerabilities, significant sums can be swiftly and discreetly siphoned off without the card owner's knowledge. The complexity lies in the fact that fraudsters often endeavor to make their illicit transactions appear genuine, making the detection of fraud a formidable challenge.
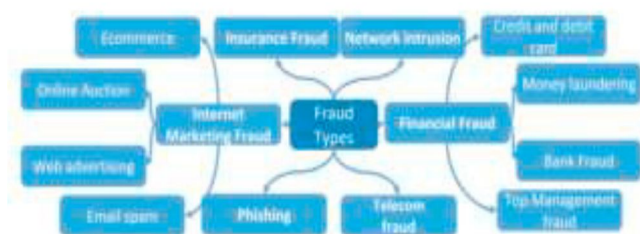


Figure 1 Types of Fraud

Scams have garnered significant attention worldwide in recent years, with credit card thefts being a prominent concern. The prevalence of such incidents has led to a heightened awareness among the general population. A notable advancement in technology has been the transition from traditional magnetic stripe cards to EMV smart cards, which store data on integrated circuits. This innovation has notably enhanced the security of on-card payments. However, challenges persist, particularly in the realm of card-not-present (CNP) fraud, where rates remain elevated.

A pivotal study conducted by the US Payments Forum in 2017 underscores the evolving nature of fraud tactics. With the bolstered security of chip cards, criminals have shifted their focus towards CNP transactions, resulting in a rise in reported CNP fraud instances. Despite advancements in technology, the potential for illicit card usage by criminals remains a concern. In response, a range of machine learning algorithms has emerged as a viable solution. To effectively combat fraud, a diverse array of supervised and semi-supervised machine learning techniques is employed. However, our particular focus revolves around addressing three crucial challenges inherent in the card fraud dataset: the imbalanced class distribution, the presence of both labeled and unlabeled samples, and the necessity to efficiently process a substantial volume of transactions.

To facilitate real-time fraud detection within dynamic datasets, an array of supervised machine learning methods comes into play. This repertoire includes Decision Trees, Naive Bayes Classification, Least Squares Regression, Logistic Regression, and Support Vector Machines (SVM). Moreover, to capture the intricate behavioral patterns of both ordinary and atypical transactions, two separate approaches are employed: CART-based and Random-tree-based random forests. While Random Forest demonstrates its prowess on smaller datasets, it encounters difficulties when grappling with imbalanced data distributions.

The impending undertaking is directed at mitigating these challenges by elevating the capabilities of the random forest methodology itself. Ongoing research delves into the exploration of meta-classifiers and meta-learning strategies, with a specific focus on navigating the complexities of highly skewed credit card fraud data. The overarching goal is to assess the performance of Logistic Regression, K-Nearest Neighbors, and Naive Bayes within the specific context of credit card fraud detection.

However, it's important to note that relying solely on supervised learning techniques for fraud detection may not yield consistent success. To address this limitation, alternative approaches are explored. Notably, a model utilizing Restricted Boltzmann Machine (RBM) and Deep Autoencoder (DAE) is developed. This model is adept at learning regular transaction patterns and identifying anomalies. Additionally, a hybrid technique merging Adaboost and Majority Voting procedures has been devised, showcasing the industry's commitment to innovative solutions in the ongoing battle against fraud.

### A. Financial Fraud Detection

Financial fraud is a concept that encompasses instances where individuals manipulate others into providing money or valuable financial assets [3]. The repercussions of such fraud are far-reaching, often involving hackers and data breaches that compromise consumer personal information and sensitive data held by financial institutions. This breach of security can lead to substantial financial losses and a tarnished reputation for the affected institution [11]. While various industries grapple with the impact of financial fraud, the banking sector is notably vulnerable. Within the realm of banking, fraud can take on different forms [6][12]:

1) Money laundering entails the illicit practice of disguising funds acquired through unlawful activities as originating from legitimate sources. Mortgage fraud, on the other hand, pertains to deceptive practices employed to secure a mortgage loan. It typically occurs when a prospective homebuyer manipulates essential information during the qualification process to obtain a mortgage for property acquisition.
2) Another prominent facet is credit card fraud, encompassing illicit activities executed during credit card transactions. This form of fraud can manifest in diverse ways, including the misplacement or theft of credit cards, as well as the illicit acquisition of private credit card information—commonly referred to as card-not-present fraud.

### B. Credit Card Fraud Detection

The detection of credit card fraud has become a critical component of financial fraud prevention due to the substantial increase in financial losses incurred. Various defensive measures, including the utilization of Fraud Prevention Systems (FPSs), have been implemented to combat ongoing credit card scams. However, the efficacy of these measures falls short in mitigating the detrimental impacts of such fraud. Consequently, it has been established that an alternative type of Fraud Detection System (FDS) holds more promise for effectively identifying credit card transaction fraud. Nevertheless, the development of a potent FDS encounters several challenges, resulting in adverse outcomes such as high rates of false alarms, sluggish detection processes, and compromised detection accuracy. To streamline transaction processing and reduce processing time, strategies like dimensionality reduction (e.g., PCA) are employed to pinpoint pertinent features. Additionally, numerosity reduction methods aggregate credit card transactions.

1) *Velocity Challenge:* Real-time detection becomes a necessity when crafting an online CCFDS founded on big data technology. In response, alternative algorithms are harnessed to equip CCFDS with accurate online detection capabilities. Techniques such as the BOAT (Bootstrapped Optimistic method for Tree Construction) method and the Self-Organization Map (SOM) approach curtail training time while maintaining efficacy.
2) *Volatility Challenge:* The dynamic nature of cardholders' behaviors, influenced by an array of factors, poses a challenge to ensuring their accuracy. The Credit Card FDS must be adaptive and agile in the face of ever-evolving fraudulent tactics.
3) *Value Challenge:* The imbalanced nature of credit card transactions, where legitimate transactions overwhelmingly outnumber fraudulent ones, distorts class distribution and data balance. Supervised approaches, impacted the most by this imbalance, tend to favor the majority class (legitimate transactions) in their predictions, thereby neglecting the minority class (fraudulent transactions).
4) *Variety Challenge:* Credit card data originates in diverse formats and sizes, stored across a multitude of database structures utilized by financial institutions. This diversity also mirrors the array of strategies fraudsters employ to perpetrate fraudulent activities.

### III. EXISTING SOLUTIONS

### A. Credit Card Fraud Detection Process

Creating a dependable credit card fraud detection system involves a sequence of essential steps:

1) *Parameterization Stage:* The initial step encompasses collecting credit card transaction data and seamlessly integrating it into the designated database system. Further, this data undergoes preprocessing to ensure its alignment with the predetermined format, minimizing any discrepancies.

2) *Training Stage:* This pivotal phase involves constructing and refining the fraud detection system's model. To suit the unique attributes of the data, an assortment of machine learning algorithms and data mining methodologies can be employed. This adaptability allows for optimal model development.

3) *Detection Stage:* With the completion of the training stage and the availability of the model, the detection phase ensues. The model's efficacy is rigorously evaluated using diverse criteria, enabling the identification of the technique exhibiting the highest detection rates. This evaluation ensures the system's proficiency in identifying instances of credit card fraud.
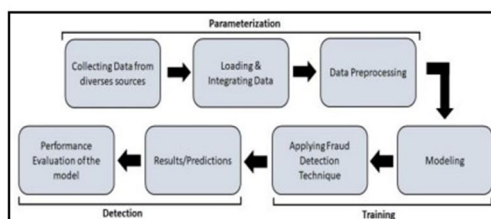


Figure 2 Process of detecting credit card frauds (Parameterization, Training, and Detection

We aim to conduct several comparative studies that analyse a range of research articles within the realm of credit card fraud detection. These studies will focus on evaluating different machine learning approaches utilized in the modelling and training stages of the process.

B. *Existing Solutions Based on Machine Learning Techniques*

1) *Supervised Learning:* When historical data containing labeled samples of fraudulent and genuine transactions is available, supervised learning is a commonly utilized method in fraud detection. The fundamental goal is to create a prediction model that, using the patterns identified from the labeled data, can correctly categorize fresh, unseen transactions as either fraudulent or lawful. Researchers used supervised learning methods to detect credit card theft in a study that was published in the "Journal of Computational Science" (Chen et al., 2018) [4]. They made use of a labeled dataset of previous credit card transactions, where each transaction was classified as either legal or fraudulent. The researchers conducted experiments using various supervised learning techniques, including logistic regression, decision trees, and support vector machines (SVM). Notably, their findings highlighted the exceptional performance of SVM, boasting an impressive accuracy rate surpassing 95%. This outcome proved to be particularly significant in accurately detecting instances of fraudulent transactions. Capitalizing on this heightened accuracy, the financial institution was empowered to swiftly respond and curtail further losses. The model's proficiency in recognizing patterns associated with credit card theft enabled proactive intervention, reinforcing the institution's ability to safeguard its assets.

2) *Preparation of Data:* The labeled dataset comprises of transactions with matching labels indicating whether each transaction is real or fraudulent, together with accompanying variables (such as transaction amount, location, time, user behavior, etc.).

3) *Model Training:* To discover the connections between the characteristics and the target labels, supervised learning methods such as logistic regression, support vector machines (SVM), decision trees, or random forests are trained on the labeled dataset.

## IV. TYPES OF MACHINE LEARNING APPROACHES

A. *Unsupervised Learning*

When labeled data is limited or nonexistent, unsupervised learning is appropriate for fraud detection. Identifying anomalies or outliers in transaction data is the main goal of unsupervised learning in this situation, supposing that fraudulent transactions are uncommon and considerably different from normal ones. In a research paper published in the "IEEE Transactions on Dependable and Secure Computing" (Akhtar et al., 2019) [5], the authors introduced an innovative approach rooted in unsupervised learning. Their primary objective was to detect irregularities within real-time payment transactions.

To achieve this, they harnessed a substantial dataset of payment transaction records obtained from an e-commerce platform. Employing a density-based clustering technique, specifically DBSCAN (Density-Based Spatial Clustering of Applications with Noise), the researchers sought out peculiar patterns within the data. Notably, this approach proved highly effective in identifying transactions that deviated significantly from the established patterns of legitimate transactions, particularly those associated with fraudulent activities.

A distinct characteristic of their method is that it relies solely on the inherent features of the dataset, without the need for labeled data. This innovative strategy aligns with the broader trend of harnessing the power of unsupervised learning to address complex challenges in anomaly detection.

Model Training: To discover patterns and structures in the data that significantly depart from the norm, unsupervised learning algorithms are used, such as clustering methods (e.g., k-means) or density-based approaches (e.g., DBSCAN).

Transactions that significantly deviate from the expected behavior are detected as anomalies and are hence thought to be potentially fraudulent.

## B. Semi-Supervised Learning

A hybrid method called semi-supervised learning makes use of both labeled and unlabeled data. Semi-supervised learning can increase the accuracy of fraud detection and adapt to new fraud trends by mixing components of both supervised and unsupervised learning. A semi-supervised learning-based fraud detection system for mobile banking transactions was proposed in a research paper published in the journal "Expert Systems with Applications" (Nigam et al., 2020) [6].

In this investigation, the researchers paired a larger amount of unlabeled data with a smaller group of fraudulent transactions that had been identified as such. They employed a semi-supervised learning strategy that combined an autoencoder, a kind of neural network used for unsupervised feature learning, with a supervised classifier.

The outcomes demonstrated that the hybrid model outperformed conventional supervised or unsupervised approaches alone in terms of fraud detection performance. The model successfully identified both established fraud patterns and newly emergent fraud behaviors, demonstrating how semi-supervised learning may increase the accuracy of fraud detection..

1) *Data Preparation:* The algorithm uses a small portion of labeled data and a more extensive set of unlabeled data.
2) *Model Training:* The model learns from the labeled data to understand known patterns of fraud, and it leverages the unlabeled data to identify anomalies and potential novel fraud patterns.
3) *Anomaly Detection:* By combining information from labeled and unlabeled data, the model can provide more accurate fraud predictions.

## C. Ensemble Methods

When compared to individual models, ensemble approaches are more accurate and resilient since they integrate numerous models to make group judgments. A framework for ensemble learning was suggested in a paper that was published in the "International Journal of Intelligent Systems and Applications" (Liu et al., 2017) [7] for the identification of credit card fraud.

To create an ensemble model, the researchers merged a number of base classifiers, including gradient boosting machines, random forests, and decision trees. Each classifier cast a vote on whether a transaction was fraudulent or valid, and they combined the results using a voting method.

While retaining a high detection rate for fraudulent transactions, the ensemble model considerably decreased the percentage of false positives. The ensemble technique effectively tackled the challenges posed by class imbalance and intricate fraud patterns. This achievement was made possible through the utilization of a diverse range of base classifiers.

The process of model construction involved training multiple distinct models, such as decision trees, neural networks, and logistic regression, using the same dataset.

In the subsequent step of combining forecasts, each model independently predicted the legitimacy or fraudulent nature of a transaction.

To arrive at a conclusive decision, the forecasts from the various models were merged through methods like voting or weighted averaging. This aggregation process contributes to a more robust and accurate determination.

## D. Deep Learning

Deep learning utilizes artificial neural networks with multiple layers (deep architectures) to extract intricate features from vast datasets. Within this context, the authors of a study published in "Neurocomputing" (Liang et al., 2020) [8] proposed a novel approach based on deep learning to detect fraudulent online banking activities.

Their methodology revolved around harnessing a deep convolutional neural network (CNN) to autonomously capture features from transaction data, encompassing attributes like timestamps, geographical locations, and transaction amounts. By doing so, the CNN constructed hierarchical representations of these attributes, enabling the discernment of complex patterns linked to fraudulent behavior.

Noteworthy aspects of their approach include:

1) *Outperforming Conventional Methods:* The deep learning model exhibited superior performance compared to traditional machine learning techniques when handling intricate and high-dimensional data. It demonstrated remarkable accuracy and robustness in identifying instances of fraud.

2) *Automated Feature Extraction:* Deep learning models possess the capability to autonomously learn pertinent features from the data, thereby alleviating the reliance on manual feature engineering.

3) *Model Training:* It's worth noting that training deep learning models typically necessitates a substantial amount of data and computational resources, highlighting the resource-intensive nature of this approach.

4) *Hierarchical Representation:* The deep architecture allows the model to capture hierarchical representations of fraud patterns, leading to more sophisticated fraud detection

Table 1 Comparative analysis with results and limitations of the literature

| Ref. | Paper Title (Year) | Purpose / Results | Limitations |
|---|---|---|---|
| [10] | Data Analytics Predictive Modeling for Credit Card Fraud Detection (2018) | Compared to other approaches, random forest offers the highest accuracy and precision.. | Trees used in RF have limited memory. |
| [11] | Machine Learning Algorithm Performance Evaluation for Credit Card Anaysis and Fraud Detection (2020) | Unsupervised approaches outperform conventional strategies for addressing dataset skewness, such as Isolation Forest and Local Outlier Factor. | The research should concentrate on resampling methods that lower high imbalance rates. |
| [12] | Machine Learning Methods for Detecting Credit Card Fraud (2019) | By using feature selection PCA (Principal Component Analysis) and oversampling SMOTE (Synthetic Minority Over-sampling) approaches, the Random Forest algorithm performs effectively.. | Working with classical algorithms makes more sense when there isn't much data, but when there is more data that might cause problems, more complex approaches are required.. |
| [13] | Convolutional Neural Networks for Credit Card Fraud Detection (2016) | The model that performs best is the convolutional neural network (CNN). | The findings from the suggested technique are the best, however future methods should concentrate on solving the problem of severely unbalanced data. |
| [14] | Credit Card Fraud Detection Using Selected Machine Learning Algorithms (2019) | In this study, the statistical and incremental learning methodologies were utilized to detect credit card transaction frauds. | Particularly for the dataset given, the statistic learning technique cannot be viewed as a long-term solution.. |
| [15] | Deep Learning, Logistic Regression, and Gradient Boosted Trees for Credit Card Fraud Analysis (2017) | We noticed that Deep Neural Network (NN) is the best machine learning algorithm after analyzing the prediction performance of 3 different methods.. | There are some drawbacks, including the low predictive power of logistic regression, the substantial amount of data required for GBT, and the difficulty in feature selection for NN.. |
| [16] | An Effective Method for Detecting Credit Card Fraud Using Machine Learning Methodologies (2018) | Logistic Regression and Decision Tree are best algorithms. | Hence, the machine learning models used in this work ignore the other performance metrics. |
| [17] | A Comparison of Machine Learning Techniques for Detecting Credit Card Fraud Based on Time Variance (2018) | In order to identify performance discrepancies, this study compares 10 machine learning algorithms without and with the "Time" attribute. | The study should concentrate on finding a more effective solution to the severe data imbalance issue. |

## V.    CONCLUSION

Machine learning approaches have revolutionized fraud detection in the banking sector. Each technique brings its strengths and challenges to the table, offering a variety of ways to address the complexities of identifying fraudulent transactions. Financial institutions can benefit from adopting a combination of these approaches, leveraging the power of supervised learning for known fraud patterns, unsupervised learning for novel fraud detection, semi-supervised learning to improve accuracy, ensemble methods for robust predictions, and deep learning for handling complex data structures.

By harnessing the potential of machine learning in fraud detection, banks and financial institutions can create secure and efficient environments for credit card transactions and e-banking services, instilling trust in their customers and safeguarding the integrity of their financial systems.

## REFERENCES

[1] Iwasokun GB, Omomule TG, Akinyede RO. Encryption and tokenization-based system for credit card information security. Int J Cyber Sec Digital Forensics. 2018;7(3):283–93.

[2] Burkov A. The hundred-page machine learning book. 2019;1:3–5.

[3] Maniraj SP, Saini A, Ahmed S, Sarkar D. Credit card fraud detection using machine learning and data science. Int J Eng Res 2019; 8(09).

[4] Dornadula VN, Geetha S. Credit card fraud detection using machine learning algorithms. Proc Comput Sci. 2019;165:631–41.

[5] Thennakoon, Anuruddha, et al. Real-time credit card fraud detection using machine learning. In: 2019 9th international conference on cloud computing, data science & engineering (Confuence). IEEE; 2019.

[6] Robles-Velasco A, Cortés P, Muñuzuri J, Onieva L. Prediction of pipe failures in water supply networks using logistic regression and support vector classifcation. Reliab Eng Syst Saf. 2020;196:106754.

[7] Liang J, Qin Z, Xiao S, Ou L, Lin X. Efcient and secure decision tree classifcation for cloud-assisted online diagnosis services. IEEE Trans Dependable Secure Comput. 2019;18(4):1632–44.

[8] Ghiasi MM, Zendehboudi S. Application of decision tree-based ensemble learning in the classifcation of breast cancer. Comput in Biology and Medicine. 2021;128:104089.

[9] Lingjun H, Levine RA, Fan J, Beemer J, Stronach J. Random forest as a predictive analytics alternative to regression in institutional research. Pract Assess Res Eval. 2020;23(1):1.

[10] Breiman L. Random forests. Mach Learn. 2001;45(1):5–32.

[11] Ning B, Junwei W, Feng H. Spam message classifcation based on the Naive Bayes classifcation algorithm. IAENG Int J Comput Sci. 2019;46(1):46–53.

[12] Katare D, El-Sharkawy M. Embedded system enabled vehicle collision detection: an ANN classifer. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC); 2019. p. 0284–0289.

[13] Campus K. Credit card fraud detection using machine learning models and collating machine learning models. Int J Pure Appl Math. 2018;118(20):825–38.

[14] Varmedja D, Karanovic M, Sladojevic S, Arsenovic M, Anderla A. Credit card fraud detection-machine learning methods. In: 18th international symposium INFOTEH-JAHORINA (INFOTEH); 2019. p. 1-5.

[15] Khatri S, Arora A, Agrawal AP. Supervised machine learning algorithms for credit card fraud detection: a comparison. In: 10th international conference on cloud computing, data science & engineering (Confuence); 2020. p. 680-683.

[16] Awoyemi JO, Adetunmbi AO, Oluwadare SA. Credit card fraud detection using machine learning techniques: a comparative analysis. In: International conference on computer networks and Information (ICCNI); 2017. p. 1-9.

[17] Seera M, Lim CP, Kumar A, Dhamotharan L, Tan KH. An intelligent payment card fraud detection system. Ann Oper Res 2021;1–23.

[18] Guo S, Liu Y, Chen R, Sun X, Wang X. X, Improved SMOTE algorithm to deal with imbalanced activity classes in smart homes. Neural Process Lett. 2019;50(2):1503–26

# INTERNATIONAL JOURNAL
# FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 ⓦ (24*7 Support on Whatsapp)