iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75014

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

Fraud Detection in Credit Card Payments and Payment Gateways Using Machine Learning

Dhanashree Patil[1], Atharv Bandewar2, Bhavesh Chaure[3], Shubham Adhav[4], Abhijeet Date3
Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India

Abstract: ***Credit card fraud has become a very common problem in the modern economy, especially with the rise of online transactions. This paper investigates advanced machine learning techniques for fraud detection, using models such as Random Forest, Gradient Boosting, Support Vector Machines (SVM), and Long Short-Term Memory Networks (LSTM). A hybrid ensemble model is also proposed to enhance the accuracy of detection while reducing false positives and negatives. The experimental results have proven the efficiency of these models, and the hybrid model performed better. [1] [2]***
Keywords: Credit Card Fraud Detection, Machine Learning, Hybrid Models.

I. INTRODUCTION

Credit cards have been highly valued as a mode of paying for online transactions in the modern economy. The use of a credit card implies that users make purchases on a line of credit rather than their personal bank deposits. This offers immediate, short-term credit during transactions. Credit card fraud has increased despite the benefits of electronic payments, driven by changing technologies. [3] There are banks that are financial institutions offering savings and investment facilities. Credit card fraud is described as a criminal act committed with dishonest intent, and for financial advantage, without the cardholder's consent or knowledge. Credit card fraud refers to an unlawful use of a credit card whereby another person than the account owner uses the credit card without the card owner's permission. Credit cards are those methods with which consumers can buy both brick-and-mortar and shopping online goods and services. Offline transactions are also weak points in which a card is scanned or inserted through the point of sale of the merchant, but nothing can be stopped even if the card is already stolen. Another weakness is online transactions since unauthorized payments can frequently be made by attackers when they have minimal information. Credit card fraud detection includes the tracking of user activities to note suspicious behavior. Effective techniques of prevention need to be put into practice to deal with the issue. Frauds were to be reduced through technology, that is, the combination of machine learning and data science with significant help in sorting and flagging suspicious activities. Sorting out the fraudulent transactions was difficult but needed. The NCRB Report 2020 reflected a rise of 225% in cases of debit and credit card fraud compared to those in 2019. Also, the more organizations value online banking, the more than 40% of respondents stated in 2022 that their institution best emphasized fraud prevention. [4]

A. Types of Credit Card Fraud

Today, the withdrawal, deposits, and purchases are done in real-time. The Association of Certified Fraud Examiners defines fraud as "any act or intent committed with the goal of depriving a person, organization, or business of property or money through deception or other unfair means." Credit card fraud is quite common. Such credit card fraud includes the following:

1) POS Fraud: In this method, small skimming devices are secretly attached on the terminals of a POS system. At the time of swipe, they capture all card data and store them. Most such fraud cases involve a dishonest trader sharing or facilitating such stolen information. [5]
2) Skimming: Skimming is one where a device called a "skimmer" is employed. The skimmer reads and records information lodged within the magnetic strip as the card is swiped through the skimmer and stores it, and then writes this information onto the magnetic strip of a blank card. Once done, there comes an exact clone of the original. [6
3) Phishing: In phishing, the scam targets the cardholder. He or she receives an email purporting to come from the bank or any other financial institution he or she has accounts with. When he clicks on the link, the cardholder gets redirected to another website asking him for his personal details. The URL is usually very authentic and makes most of the target victims fall into its trap. [7]

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

II. METHODOLOGY

All There are several algorithms of machine learning that have been applied for the purpose of efficient fraudulent transaction detection. Each of them has its own strengths in identifying various complex patterns and anomalies. Some of the algorithms used in this study include XGBoost, LSTM, Random Forest, SVM, and the hybrid model

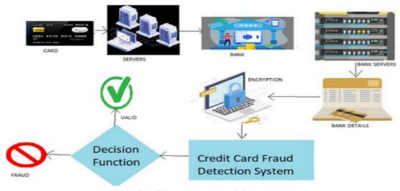


Fig 2: System Architecture

A. XGBoost (Extreme Gradient Boosting)

XGBoost is the optimized version of gradient boosting mainly for the sake of efficiency and speed implemented in C++. This is an ensemble method that constructs decision trees to predict target variables, thereby proving effective for classification and regression tasks. Essentially, each tree in the sequence learns from the errors of the previous one by updating the weights of the wrongly predicted instances to create an even stronger predictive model at each step of iteration. XGBoost accepts missing values. It can be regularized. This model is majorly accuracy-based; thus, it is one of the main chosen algorithms for difficult datasets, such as fraud detection.

Mathematically, XGBoost minimizes the following objective function containing loss and regularization terms:

$$\text{Objective} = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k)$$

where $l\{y,y'\}$ is the loss function measuring the difference between actual and predicted values, and $\Omega(f)$ is the regularization term to prevent overfitting. [13]

B. LSTM (Long Short-Term Memory Networks)

LSTM is one type of Recurrent Neural Networks (RNN) that proves effective on data based on temporal dependencies such as sequences of transactions over time. In contrast to the traditional RNNs, LSTM networks eliminate problems of vanishing and exploding gradients, which makes it an ideal choice to handle long-term dependencies. An LSTM network includes memory cells with input, output, and forget gates controlling information flow in terms of retaining crucial details while discarding unwanted information. Such architecture makes LSTM capable of pattern recognition over time; hence, it is beneficial in identifying fraudulent transactions that could follow some temporal patterns.

Equations for operation of LSTM cell: The cell is operated using the following equations where σ\sigmaσ is the sigmoid function, ht is the cell's hidden state, and Ct is the cell state.

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)$$

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$$

$$C_t = f_t * C_{t-1} + i_t * \tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$$

$$h_t = o_t * \tanh(C_t)$$

C. Random Forest

Random Forest is an ensemble learning method based on the idea that many decision trees built from training data combined to make a prediction lead to higher accuracy along with lower variance. Here, at each node of this tree, a random subset of features is used, and building trees only on a randomly sampled subset of the overall training sample helps prevent overfitting. Random Forest does excellently well both in classification and regression; moreover, it is robust to outliers and noise, which makes it particularly good for datasets with highly heterogeneous attributes, such as transaction data.

There is a summary of the Random Forest algorithm as given below:

1) Randomly selects subsets of the dataset for each tree.
2) Construct the decision tree based on those subsets, assuming just random subsets of features.
3) Aggregate the predictions made by all the trees to produce the final output, usually in the form of majority voting if it's classification and averaging for regression.

©IJRASET: All Rights are Reserved

D. SVM (Support Vector Machine)

SVM is a learning algorithm that can be used in the framework of supervised machine learning to categorize data as either belonging to one of two classes. In SVM, the primary task is finding the optimal hyperplane that totally separates the points of different classes. SVM is particularly useful for datasets where there are clear margins between the classes. In fraud detection, SVM would classify transactions as either fraudulent or legitimate by mapping to higher dimensions of space to locate the best decision boundary.

Mathematically, the SVM algorithm finds this hyperplane by solving

$$\min \frac{1}{2}||w||^2$$

subject to the constraint:

$$y_i(w \cdot x_i + b) \geq 1 \quad \forall i$$

where *w* is the normal vector to the hyperplane, and *b* is the bias term. The algorithm maximizes the margin between the classes, helping to create a robust boundary for classification.

E. HYBRID MODEL (Ensemble Learning)

Ensemble learning is a type of machine learning wherein the predictive strengths of many models are amalgamated to improve overall performance. The ensemble methods aggregate the predictions of different models in such a way that eliminates the weakness of each particular model, thereby improving accurateness, robustness, and generalization capability. Some popular ensemble strategies are bagging, boosting, and stacking.

F. Overview of Stacking

Stacking or stacked generalization is an ensemble method whereby one trains many base models or level-0 models and, according to their predictions, generates predictions with the help of a second model, which could be called a meta-model or level-1 model. The primary advantage provided by stacking arises when the base models have complementary strengths; it uses these diverse perspectives in the production of a more accurate and reliable prediction.

1) The base models are the simplest layers of models that learn independently from the training data. The choice of such models is not limited; most common choices include classifiers like Decision Trees, Support Vector Machines (SVM), Neural Networks, and many others. As a part of this study, Random Forest, Gradient Boosting, and SVM are employed as the base models.

2) Meta-Model: In this approach, the meta-model learns to predict the final output given the predictions of base models. It is often found using something very simple, such as Logistic Regression, as it learns from the outputs of already sophisticated models. The meta-model seeks patterns and corrects errors that other models may commit to make better predictions on the final level.

III. RESULT AND DISCUSSION

A. Results

1) Data Preprocessing

- The missing values are handled by removing rows with nulls.
- Categorical features such as "category," "job," and "merchant" were encoded using a label for compatibility with models.
- The target variable, is_fraud, was cleaned for non-numeric characters. Dropping rows with parsing errors in column dob has been also applied.
- Feature scaling rescales the input variables for standardization.

2) Model Performance:

In training, these models were exposed to an 80-20 train-test split.

- SVM led to a classical accuracy of around 86.64%
- Gradient Boosting had a proficiency rate of 97.6%.
- In Random Forest, the model has obtained the precision of 96.95%.
- The LSTM model was tuned with extra layers, dropout, and epochs, and it reached 91.4% accuracy. [5] [12]

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. Discussion

1) Comparison of Model Effectiveness:

- SVM is good at those scenarios where they could get linear and moderately nonlinear separability. However, SVM might be even less adequate in extremely complicated fraud detection applications in its simpler boundary structure.
- Competitive accuracies were achieved by Gradient Boosting and Random Forest, though the latter did better because it was immune to overfitting on structured data.
- After optimization, LSTM performed significantly better with potential sequential patterns or temporal relationships being the key to this dataset.

2) Impact of Hyperparameter Tuning

- Complexity and regularization in sequence-based models It increased the number of layers and dropout rate within an LSTM, which improves its prediction power.
- Similar to model tuning, optimization of parameters- choice of kernel in SVM or tree depth in Random Forest, among others-can be undertaken to further enhance the performance of this model.

3) Limitations

- Preprocessing may reduce the richness of the dataset and let the data become potentially biased through dropping rows that include missing values.
- So, the performance of the LSTM model is such that it shows us that there do exist patterns somewhere lurking in sequence data, but simultaneously, this demanding requirement for intense computational power may not scale accordingly.

IV. FOR HYBRID MODEL

Accuracy was used as the primary measure of assessment for individual models such as Random Forest, Gradient Boosting, and SVM besides the stacked hybrid model. The following results were obtained:

A. Individual Model Performance

1) Random Forest: Accuracy stood at 97.65%. It has the ensemble property, which makes it effectively capture complex and subtle patterns with agility in data, hence highly useful in the detection of the nature of fraud within any given transaction.

2) Gradient Boosting: The model had a slightly better accuracy, which is 97.68%. Since an error correction based on the previous stages helps Gradient Boosting to be highly accurate, sometimes overfitting tuning might become necessary.

3) Support Vector Machine (SVM): It could attain an accuracy of 95.12%. SVM does very well in finding decision boundaries but ensemble methods topped the list as they utilized higher diversity of predictions.

While the individual and specifically the Random Forest, Gradient Boosting models did extremely well, there were minor differences in the models where the prediction results were concerned. This is what precipitated the need for using stacking since it was a way through which one could benefit from each model's strength differently.

B. Stacked Hybrid Model Performance

1) The stacked model achieved an accuracy of 97.85% versus the independent models and performed better than each of the individual models. While this may seem like a minor improvement, in fraud detection, even tiny improvements in the accuracy of a model can decrease the number of undetected fraudulent transactions that slip through the cracks.

2) To capture any patterns that individual models might not recognize, the logistic regression meta-model could learn from the predictions of base models combining them as meta-features. This results in a reduction of both bias and variance, and the final model is more robust. [14]

C. Interpretation of Results

1) Complementary strengths: The individual models used different perspectives; the Random Forest captured the interactions and importance of variables which were not necessarily linear in nature. The Gradient Boosting focused much more on correcting the misclassifications. The SVM produced a strong boundary description. With the balanced strengths of the individual models, the weaknesses of the stacked model are catered to.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

2) Better Robustness: The higher accuracy of the stacked model also indicates that this model would actually be able to handle the kind of variability and imbalance in such datasets, where fraud is obviously outpaced by legitimate transactions. Overfitting, which is much more potential in more complex models, was also reduced by stacking.

In practice, this means stacking turns out to be a very reliable fraud detection framework, which is particularly important in applications like real-time fraud detection. False positives, or legitimate transactions being flagged as fraud, and false negatives, or frauds which escaped undetected, play a crucial role in keeping customer confidence intact and minimizing loss.

V. LIMITATIONS AND CONSIDERATIONS

The stacked model, although it improves accuracy slightly, is computationally more intensive in that training would require multiple base models and meta-feature generation.

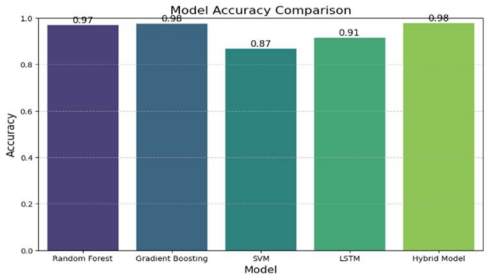
The performance level of the stacked model depends a lot on the base models as well as on the meta-model chosen. This provides scopes for further research in future where other models such as neural networks or alternative meta-models could be used to enhance the performance even more

A. Performance Table

Table 1

Model	Accuracy (%)
Support Vector Machine (SVM)	86.64%
Gradient Boosting	97.6%
Random Forest	96.95%
LSTM	91.4%
HYBRID MODEL	97.85%

B. Model Accuracy Comparison for Different Algorithms



The bar chart you've provided compares the accuracies of four different machine learning models: SVM, Gradient Boosting, Random Forest, and LSTM. Here is a detailed interpretation of the chart's content:

1) X-axis: Represents the model types, specifically:
- SVM (Support Vector Machine)
- Gradient Boosting
- Random Forest
- LSTM (Long Short-Term Memory network)

2) Y-axis: Represents the accuracy of each model, ranging from 0 to 1 (or 0% to 100%).

3) Observations:
- Gradient Boosting and Random Forest models have the highest accuracy, with values close to or at 1.0, indicating they performed very well in this specific task or dataset.
- LSTM also achieved high accuracy, slightly below Gradient Boosting and Random Forest, but still high.
- SVM has the lowest accuracy among the four models, but it's still fairly high, suggesting it also performed reasonably well on the task.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Applications

1) Banks and credit card companies can apply them to monitor it in real-time, flagging suspicious transactions that are helping to prevent fraud losses and protect clients' assets.
2) E-commerce Platforms: Online retailers will be able to incorporate the model into payment systems in an effort to detect abnormal purchase behaviors thus protecting them from hijacking online transactions.
3) Payment Gateways: Through fraud detection models, it can avoid unauthorized access and fraudulent transactions across numerous payment gateways, which can help gain back confidence with security.
4) Insurance Companies: Similar fraud detection models on insurance claims could be very useful for avoiding financial losses through fraudulent claims by identifying suspicious patterns.
5) Telecom Operators: It identifies the abnormal usage or fraud in the customer account, SIM swap and data usage without permission, and these are very imperative in the current telecom market to have high customer satisfaction

D. Benefits

1) High Accuracy and Low False Positives: The ensemble and hybrid models have shown a high degree of accuracy, with lower false positives compared to other models, which may be disruptive to legal transactions. This increases customer satisfaction and minimises delays in operations.
2) Real-Time Detection: Such models support near-real-time processing of transaction data so that suspicious activities can be responded to immediately, thus preventing potential losses in terms of financial transactions.
3) Adaptability to Emerging Fraud Tactics: Hybrid machine learning models can adjust to newly emerging patterns of fraud in real-time, ensuring long-term strength and flexibility.
4) Cost-Effectiveness in Fraud Management: Automated fraud detection helps reduce instances of a person spending hours and hours monitoring data, as the machine does it for them. This helps reduce the costs of an organization while keeping the security intact.
5) The risk of fraud is reduced along with secure transactions of the organization. Customer loyalty and confidence in service can be increased through this, which is necessary for users of any competitive market.

Such applications and advantages indicate the importance of advanced fraud detection in securing the financial activity and the protection of customers along with the operational efficiency in various business sectors.

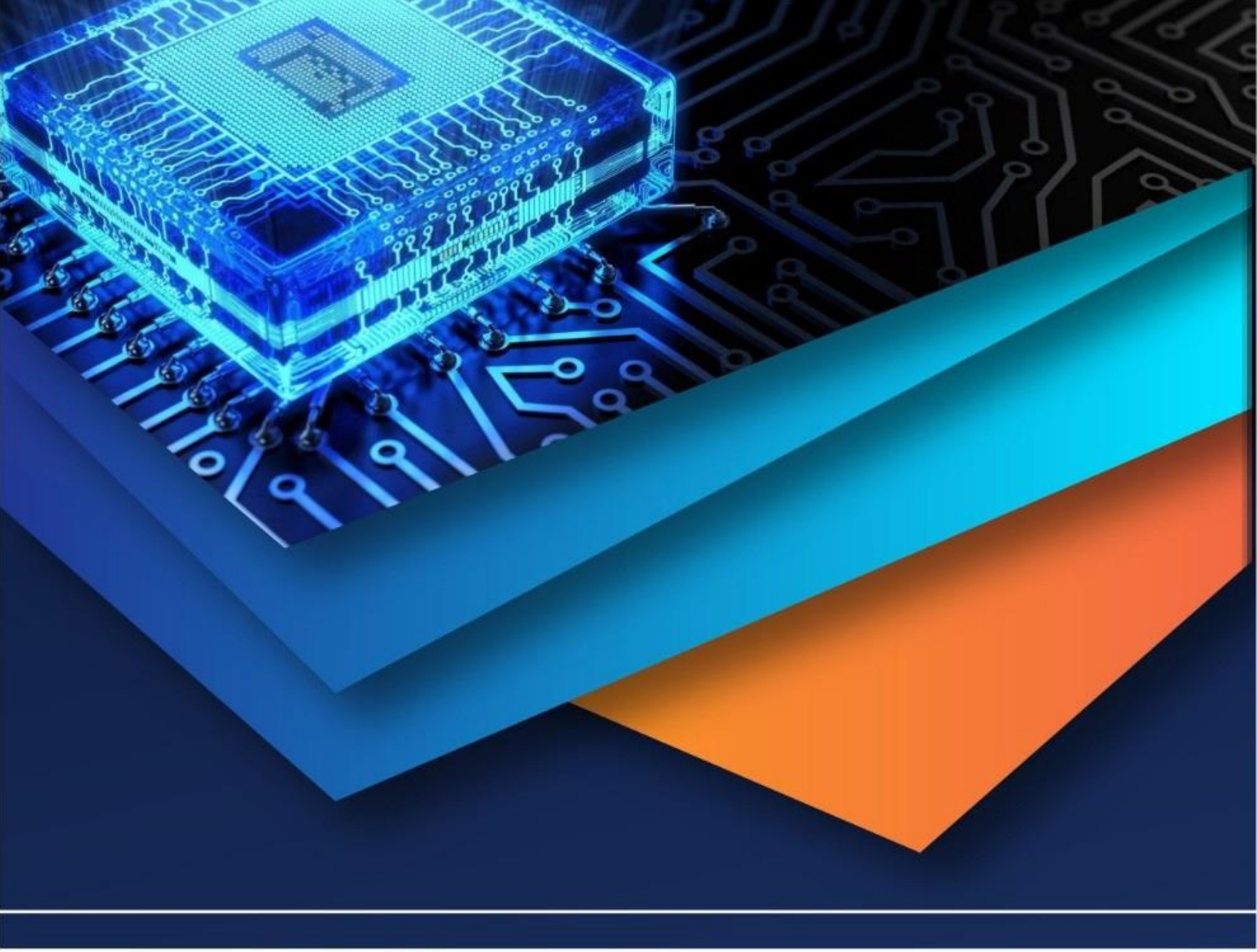
REFERENCES

[1] S. B. E. D. Y. Sahin, ""A cost-sensitive decision tree approach for fraud detection"," Expert Syst. Appl., vol. 40, pp. 5916-5923, 2013.
[2] C. Y. W. L. M. L. Y. Li, " "A principle component analysis-based random forest with the potential nearest neighbor method for automobile insurance fraud identification"," Appl. Soft Comput...
[3] S. P. S. Subudhi, ""Use of optimized Fuzzy C-Means clustering and supervised classifiers for automobile insurance fraud detection"," J. King Saud Univ.-Comput. Inf. Sci.
[4] A. A. A. A. O. Adewumi, ""A survey of machine learning and nature inspired based credit card fraud detection techniques"," Int. J. Syst. Assurance Eng. Manage., vol. 8, no. 2, pp. 937-953, 2017.
[5] A. K. S. S. A. M. A. Srivastava, ""Credit card fraud detection using hidden Markov model"," IEEE Trans. Depend. Sec. Comput, vol. 5, no. 1, pp. 37-48,, 2008.
[6] M. S. J. T. Quah, ""Real-time credit card fraud detection using computational intelligence"," Expert Syst. Appl., vol. 35, pp. 1721-1732, 2008.
[7] S. J. K. T. J. C. W. S. Bhattacharyya, " "Data mining for credit card fraud: A comparative study"," Decision Support Syst., vol. 50, no. 3, pp. 602-613, 2011.
[8] M. K. A. N. S. Halvaiee, " "A novel model for credit card fraud detection using artificial immune systems"," Appl. Soft Comput.,, vol. 24, pp. 40-49, 2014.
[9] A. K. S. S. A. K. M. S. Panigrahi, ""Credit card fraud detection: A fusion approach using Dempster– Shafer theory and Bayesian learning"," Inf. Fusion, vol. 10, no. 4, pp. 354-363, 2009.
[10] E. D. N. Mahmoudi, ""Detecting credit card fraud by modified fisher discriminant analysis"," Expert Syst. Appl., vol. 42, no. 5, pp. 2510-2516, 2015.
[11] M. A. V. L. C. J. M. S. D. Sánchez, " "Association rules applied to credit card fraud detection"," Expert Syst. Appl.,, vol. 36, no. 2, pp. 3630-3640, 2009.
[12] M. H. O. E. Duman, " "Detecting credit card fraud by genetic algorithm and scatter search"," Expert Syst. Appl., vol. 38, no. 10, pp. 13057-13063, 2011.
[13] V. R. G. R. R. I. B. P. Ravisankar, ""Detection of financial statement fraud and feature selection using data mining techniques"," Decision Support Syst , vol. 50, no. 2, pp. 491-500, 2011.
[14] C. S. Y. M. E. Kirkos, " "Data mining techniques for the detection of fraudulent financial statements"," Expert Syst. Appl., vol. 32, no. 4, pp. 995-1003, 2007.
[15] S. B. Y. F. H. Glancy, " "A computational model for financial reporting fraud detection"," Decision Support Syst., vol. 50, no. 3, pp. 595-601, 2011.
[16] M. B. D. E. A. S. T. C. I. T. Christou, ""Detecting fraud in online games of chance and lotteries"," Expert Syst. Appl., vol. 38, no. 10, pp. 13158-13169, 2011.
[17] C.-F. Tsai, ""Combining cluster analysis with classifier ensembles to predict financial distress"," Inf. Fusion, vol. 16, pp. 46-58, 2014.
[18] D. J. C. J. Y. Z. F. H. Chen, ""Application of random forest rough set theory decision tree and neural network to detect financial statement fraud—Taking corporate governance into consideration"," Proc. Int. Conf. Intell. Comput, pp. 221- 234, 2014.
[19] C. P. L. K. S. T. W. S. L. M. Seera, ""Classification of transcranial Doppler signals using individual and ensemble recurrent neural networks"," Neurocomputing, vol. 249, pp. 337-344, 2017.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[20] K. S.-M. V. L. R. G. C. Phua, "Resilient identity crime detection"," IEEE Trans. Knowl. Data Eng., vol. 24, no. 3, pp. 533-546, 2012.
[21] M. W. Powers, ""Evaluation: From precision recall and F measure to ROC informedness markednes and correlation"," J. Mach. Learn. Technol., vol. 2, no. 1, pp. 37-63, 2011.
[22] C. K. L. M. S. C. P. L. A. K. N. K. Randhawa, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," IEEE Access, vol. 6, pp. 14277- 14284, 2018.
[23] B. P. S. R. S. Lubna Shaikh, ""Credit Card Fraud Detection Using Machine Learning Algorithms"," 2023

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)