

# **Detecting Financial Fraud Using Machine Learning**

**Omee Ghori and Ashwin Parihar**

Dept. of Computer Engineering and Information Technology

P P Savani University, Surat, India, Surat, India

omeeghori34@gmail.com and ashwin.parihar@ppsru.ac.in

**Abstract:** *With the increasing use of online banking and mobile wallets, the number of transactions that are made electronically has risen. The aim of this study is to create a machine learning system that will help detect fraudulent activities through transaction analysis. For this purpose, the authors have used the following machine learning techniques – Logistic Regression, Decision Tree, Random Forest, Gradient Boosting and Naïve Bayes.*

*It learns from this dataset which consists of transactions in financial terms. There is some pre-processing that they have done in their dataset. They also considered measures such as accuracy, precision, recall, F1 score and confusion matrix while checking the effectiveness of the system for fraud detection. As far as results are concerned, Random Forest outperformed other methods in the test for accuracy with 99.20% score. This means that Random Forest can be used effectively for fraud detection. Conclusion The study concludes that machine learning is quite effective in enhancing fraud detection process..*

**Keywords:** Financial Fraud Detection, Machine Learning, Random Forest, Transaction Analysis, Data Preprocessing, Classification

## **I. INTRODUCTION**

Financial fraud is becoming a major problem due to the rapid development and use of digital financial systems. Financial fraud mainly involves various types of illegal activities related to the manipulation of financial transactions to achieve personal and organizational benefits[2]. Financial fraud mainly includes credit card fraud, identity theft, online payment system fraud, money laundering, and unauthorized financial transactions.

In order to counter the limitations mentioned above, machine learning methods have emerged as useful techniques for detecting financial fraud.

Machine learning models have the ability to handle a large volume of transactions and detect new patterns among the transactions, which could be an indication of financial fraud[5]. Machine learning helps in building fraud detection models capable of recognizing patterns from transactional data. Supervised learning approaches for example logistic regression, decision tree, random forest, and Gradient Boosting remain the most general machine learning algorithms applied in financial fraud detection. These algorithms have been used to classify transactions as legitimate or fraudulent based on the training data. Ensemble learning approaches such as Random Forest have been found to perform better in financial fraud detection than other machine learning approaches[6]. This is because the Random Forest approach has the capability to handle complex patterns and avoid over-fitting[14].

The main aim of the research in the proposed study remains toward grow a financial fraud detection scheme by machine learning approaches. The proposed system will use machine learning algorithms to analyse the attributes of the transactions such as the type of the transactions, the amount in the transactions, the balance in that account of this sender, and these balance in the account of the receiver. The machine learning algorithms drive be evaluated by dissimilar limits such as accuracy, precision, recall, F1-score, also confusion matrix[7].

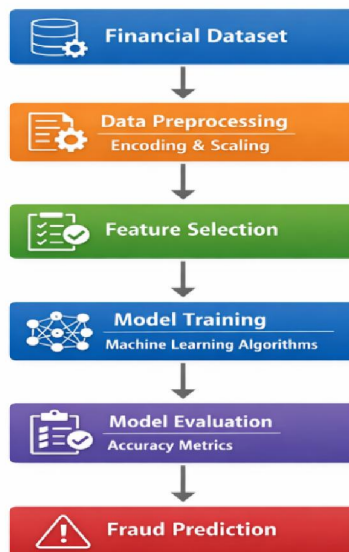


## II. LITERATURE REVIEW

Some researchers consume employed many machine learning techniques used to fraud detection purposes[2]. An approach of one rule-based machine learning model has been proposed used for detecting fraudulent financial activities using patterns of transactions and anomaly detection techniques[7]. Statistical and machine learning techniques have been employed for detecting financial statement fraud. The results showed that machine learning methods were more effective than traditional statistical methods[3].

A literature review was conducted on intelligent fraud detection methods. The results showed that data mining and machine learning methods were more effective for detecting fraudulent financial statements[5]. Several researchers have used collective learning methods, for example random forest as well as gradient boosting used to improving the performance from fraud detection system[13] [14]. Machine learning methods take remained castoff for enhancing fraud prevention trendy financial transactions. Machine learning methods have been cast-off for detecting suspicious behavioral patterns[11]. Artificial intelligence methods have been used for resolving several problems associated with finance. Artificial intelligence methods have been used for predictive analytics, fraud detection, and managing risks[4]. Deep learning devices take been used in detecting financial fraud. Deep learning methods consume exposed talented results designed for detecting financial fraud. Deep learning methods consume exposed hopeful marks of their skill towards learn complex patterns from large dataset. Adaptive machine learning models have been proposed to identify fraud activities in a changing financial environment[10]. After the literature review, the thing stands evident that machine learning systems enhance the accuracy of detecting fraud activities.

### System Architecture



**Fig 1.**The above figure shows the process that is The rapid advancement of Data Mining and Machine Learning has significantly influenced multiple domains, including agriculture and financial fraud detection. These technologies enable intelligent decision-making through pattern recognition, predictive analytics, and anomaly detection.

In the domain of financial fraud detection, early foundational work by Bhattacharyya et al. [1] and Ngai et al. [2] demonstrated the effectiveness of data mining techniques in identifying fraudulent transactions. Similarly, Ravisankar et al. [3] explored feature selection methods for detecting financial statement fraud. Comprehensive surveys by Abdallah et al. [4], [10] and West & Bhattacharya [5] highlighted the evolution of fraud detection systems, emphasizing the importance of hybrid and intelligent models.



Anomaly detection plays a central role in fraud identification, as discussed by Chandola et al. [7], who provided a detailed survey of anomaly detection techniques. Further improvements in fraud detection accuracy were achieved through probabilistic calibration and handling of imbalanced datasets, as shown by Dal Pozzolo et al. [6] and Bahnsen et al. [8]. More recent work by Carcillo et al. [9] demonstrated the effectiveness of combining supervised and unsupervised learning approaches for credit card fraud detection. Additionally, Randhawa et al. [11] applied machine learning techniques to improve fraud detection performance in real-world datasets.

Core machine learning methodologies such as supervised learning [12], ensemble models like Random Forest [14], and boosting techniques such as XGBoost [13] have been widely adopted due to their scalability and predictive power. These methods are grounded in fundamental data mining principles outlined by Han et al. [15].

Parallel to financial applications, significant research has been conducted in the field of smart agriculture. Patel et al. [16] proposed a Python-based approach for paddy leaf disease detection using image processing techniques. Similarly, Chauhan et al. [24] and Purani et al. [25] introduced innovative diagnostic methods that integrate computational intelligence with traditional plant pathology.

The integration of Internet of Things has further enhanced agricultural monitoring systems. Mehta et al. [18] reviewed IoT-based solutions for real-time disease detection in rice crops, while Sinha et al. [26] developed a smart agriculture system using MQTT protocol for efficient communication. Singh & Sharma [23] proposed a novel architecture for monitoring and predicting rice plant diseases, demonstrating the effectiveness of hybrid AI models.

Supporting these applications, big data analytics plays a crucial role in handling large-scale agricultural and financial datasets. Singh [19] and Shrivastava & Singh [22] discussed various aspects of big data processing, while Singh [20] highlighted critical privacy concerns associated with large datasets. Additionally, predictive analytics techniques have been applied in diverse domains, such as gaming performance prediction by Singh et al. [21], showcasing the versatility of machine learning models.

Recent studies, including Sharma et al. [17] and Navadiya & Singh [17], emphasize the importance of integrating AI, IoT, and image processing techniques for developing efficient and scalable solutions. Overall, the literature indicates a strong convergence of intelligent technologies across domains, enabling improved accuracy, automation, and real-time decision-making.

### III. METHODOLOGY

The proposed financial fraud detection system is developed through the application of a financial fraud detection scheme using the structured pipeline of machine learning. The planned pipeline of machine learning is the process through which the data is collected, preprocessed, and finally the model is developed and the fraud is predicted. All the steps have an significant part to show in the development of the model, and the proposed methodology is focused on the analysis of financial transactional data.

#### Data Collection

The first stage in this proposed system is to gather the data set for financial transactions, which includes detailed information regarding various kinds of operations in finance. It is to be noted that the data set contains different attributes with respect to the transaction, such as the step of that transaction, these type of the contract, the amount of the transaction, the balance of the sender, the balance of the receiver, etc. These attributes help the machine learning algorithm understand the behavioural aspects of the transactions, whether they are legitimate or not. The attributes that are generally present in the data set are: Step – This represents the time units of the transactions. Type – This field indicates the kind of transaction, which can be a transfer, payment, cash-out, or debit. Amount – This field indicates the amount of money in the transaction. Old Balance Origin (oldbalanceOrg) – This field shows the balance in the sender's account before the transaction. New Balance Origin (newbalanceOrig) – This field indicates the balance in the sender's account later the transaction. Old Balance Destination (oldbalanceDest) – This field indicates the stability in the



receiver's account already the transaction. New Balance Destination (newbalanceDest) – This field indicates these balance for this receiver's account afterward the transaction.

isFlaggedFraud – This field indicates whether the transaction is flagged as suspicious or not. isFraud – This field indicates whether the transaction remains fraud or not, which is the target variable.

The dataset used in this research has 16,426 transactions with 11 attributes, which are enough information for machine learning models.

### Data Preprocessing

Data preprocessing is an central part of machine learning systems. In most cases, financial data contains extraneous details that are not understandable by machine learning algorithms. In this study, different data preprocessing methods are used. Irrelevant data such as the account numbers of the sender and receiver are removed because they are not significant in fraud detection. They may interfere with the model. Then, categorical data such as transaction type is changed to numerical data using label encoding. Machine learning algorithms work with numerical data. Therefore, clear-cut data must be converted appropriately. Next, we use feature scaling with Normal Scaler on our data. This is done to ensure that our data is standardized, such that to to each feature is climbed thus that it takes a mean of zero and a normal nonconformity of single. This is done so that features with large values are not dominant over features with lower values during the training of the model. This is especially important in algorithms such as Logistic Regression, which remain affected by feature greatness. Then we use a train-test split on our data. In this study, 80% of the data is castoff in training the model, though 20% is used in evaluating the act of the model.

### Model Training

After the data has been cleaned, several machine learning models are skilled toward notice fraudulent transaction. By using several models, it's possible to comparison the act of the model act determine the best algorithm used for the detection of fraud. The study uses the following models:

#### Logistic Regression:

Logistic regression is a supervised learning algorithm that may be used for binary classification problems. It calculates the probability that a particular transaction is fraudulent by applying the logistic function.

#### Decision Tree:

This decision tree is one classification algorithm that ripping the data then creates branches built on the features. It creates rules those can be used for determine whether a transaction is legitimate or not.

#### Random Forest:

Random forest is any collective learning algorithm that uses many Decision Trees in conjunction with to each other. It is used to recover the accuracy of the model and reduce overfitting.

#### Gradient Boosting:

Gradient Boosting is an ensemble method where several weak classifiers are connected in a sequence. The classifiers improve upon the previous one by focusing on the errors of the previous classifier.

#### Naive Bayes:

Naive Bayes is a probabilistic classifier based on Bayes' theorem. It accepts freedom of features and determines the probability of a transaction being fraudulent based on prior probabilities.

By employing several classifiers, the system will be able to compare the effectiveness of each classifier in identifying fraud patterns in financial transaction data.

### Model Evaluation

performance of the models in detection fraudulent transactions container stay gauged by using various evaluation parameters. Here are the parameters:



**Accuracy:**

At most machine learning tasks, accuracy is known a usually castoff metrical that reflects the amount of properly classified examples ended the total number of examples. It offers a overall knowledge of just how near the model's calculations are to the actual values: But, in the context of credit card fraud detection - anywhere the dataset is very unnecessary - accuracy can be deceptive. A model can attain high accuracy levels just by identifying all the non-fraudulent transactions correctly, yet it can still make unwell in detecting fraudulent transactions. In this regard, precision, recall, and F1 score are equally important measures for assessing the actual performance of a model.

**Precision:**

Precision is the proportion of the actual number of cases where the model is right, to the total number of cases where the model has projected positively. It is the measure of the reliability of the model's predictions. High precision means the model is right when it predicts fraud.

**Recall:**

Recall, also known as compassion or the true positive amount, is the amount of actual fraud cases properly detected in the model. Recall is defined as: A recall of 1 means that the model detected altogether actual fraud cases by no false negatives. In fraud detection, maximizing recall is particularly important because failure toward detect fraudulent transactions is often costly.

**F1-score:**

These harmonic mean of precision and recall. this balances precision and recall, which makes it good to use after there are both false positive also false negatives.

**Confusion Matrix:**

A confusion matrix is basically used near control whether the model is good at classifying fraud or is simply identifying regular transactions. It is divided into four parts, like true positive, true positive , true negative, and false negative. True positive is when a fraud is identified correctly; popular other words, when the model is correct in identifying a fraud as a fraud.

Then there is true negative, which is pretty much the opposite of true positive; in other words, when a regular transaction is identified correctly, there is no problem there. False positive is when a regular transaction is identified as a fraud incorrectly.

False negative is probably the worst part because a real fraud is identified incorrectly by the model. Sometimes it feels like these errors can mess up the whole system, but yeah, that what they mean overall.

Once the presentation of the models is gauged using the parameters above, the best performing model with the best accuracy is selected as the final fraud detection model. Out of the models trained using the above parameters, the Random Forest variant remained found to have the top accuracy.

**Fraud Prediction**

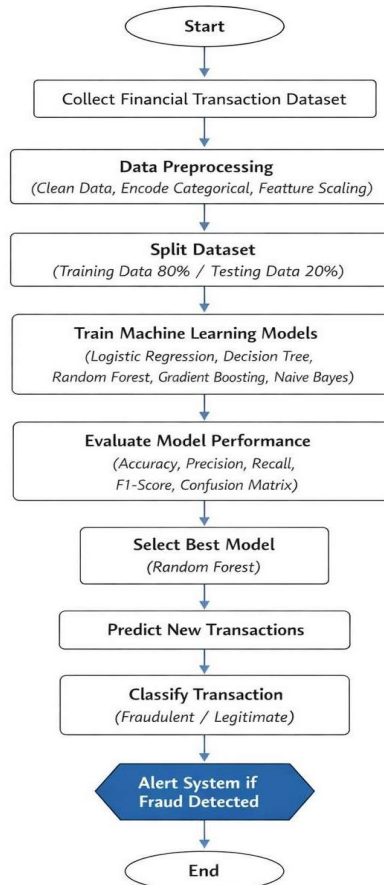
Once the presentation of the models is gauged using the limits above, the best performing model by the best accuracy is nominated as the final fraud detection model. Out of the models trained using the above parameters, the Random Forest variant remained found to have the greatest accuracy.

The performance of the trained model can then be used to assess new transactions by considering the features of the transactions such as the amount involved in the transactions, the balance involved in the transactions, etc., and then classifying the transactions as fraudulent or normal.

This way, the system can be used to integrate with the financial system and assess the transactions in real-time to identify any fraudulent transactions.



**Flowchart of Fraud Detection System**



**Fig 2.** The first step is to obtain the financial transactions dataset. The dataset is then preprocessed, which involves data cleaning, categorical data encoding, and feature scaling. Once the data is preprocessed, the dataset is split into training and testing sets, where 80% is for training, while 20% is for testing.

The next step involves fitting a series of machine learning algorithms, including Logistic Regression, Decision Tree, Random Forest, Gradient Boosting, and Naive Bayes. Once the algorithms are fitted, their performances are evaluated based on accuracy, precision, recall, F1-score, and confusion matrix.

Finally, the algorithm that performed the best is selected (Random Forest), and it is used to make predictions on new transactions.

**IV. IMPLEMENTATION**

The system is created using Python and Scikit-learn libraries. The basic steps include loading the data set, encoding the variables if necessary, and then splitting the data set into training and test circles. Many models are trained by means of the data set and compared with each other to select the best one. Finally, the best model is used to make the prediction of the fraudulent transaction or not. Between very the models tested, the Random Forest algorithm gave the best results.



**Table 1:** Dataset Information

Parameter	Value
Total Transactions	16,426
Total Features	11
Training Data	80%
Testing Data	20%
Test Samples	3,286

Data that has been selected for use in this experiment involves 16,426 financial transaction records, which have 11 attributes each, describing the properties of the financial transaction. Attributes enable algorithms used in machine learning techniques to identify patterns in data.

The data set is split into two portions that will serve as training data and testing data. The portion that serves as the training data includes 80% of the data set, which is to be used by algorithms in identifying patterns from the data. Testing data involve 20% of the data set. A total of 3,286 financial transactions are selected from the entire data set to serve as the testing data. We will use the data set in testing the effectiveness of machine learning algorithms on the test data. Through this kind of test, we can be able to find out the effectiveness of the algorithms in determining whether the transactions are fraudulent or genuine.

#### V. EXPERIMENTAL RESULTS

Model	Accuracy
Logistic regression	0.8959
Decision tress	0.9914
Random forest	0.9920
Gradient boosting	0.9902
Naive Bayes	0.5626

Some machine learning methods were used to detect any transaction that is considered fraud during financial processes. The performance evaluation of the methods was done in terms of accuracy, which shows the percentage of correct detection.

The Logistic Regression Accuracy Score is 0.8959. This means that while Logistic Regression is good at predicting the data, Logistic Regression cannot deal with the complex relationships within the dataset. On the other hand, the Decision Tree Accuracy Score is exceptionally high, with an accuracy of 0.9914.4. The best model among those studied has become the Random Forest algorithm, because the value of its accuracy rate is equal to 0.9920.

This algorithm involves the creation of the ensemble of several decision trees aimed at improving the precision of predictions. Also, such a model as Gradient Boosting can be referred to as accurate one when it comes to the prediction of test data, because its accuracy equals 0.9902.ssOn the other hand, there was also the model with the lowest level of accuracy, which is equal to 0.5626, and this is Naive Bayes model, which proves that the model does not suit the provided data set because of its assumption of independence between variables.

Considering the above-mentioned data, we may suggest that the Random Forest model should be applied in detecting frauds.



## VI. CONCLUSION

The detection of financial fraud has turned into a highly significant task in today's digital financial world. The emergence of online transactions, digital banking, and electronic payment systems has made the fraudsters very sophisticated, making it hard to detect the fraud by means of the traditional approach of rules-based detection. The conventional method of detection relies on rules, which is not efficient in identifying these difficulties of fraud.

That results have shown which an performance of the collective methods was better than the statistical models. The Random Forest classifier performed better among all the algorithms, achieving an accuracy of around 99.20%.

If the performance of the classifier is considered in terms of precision, recall, F1 score, also confusion matrix, it can be understood that the Random Forest classifier performs exceptionally well popular distinguishing between genuine then fraudulent transactions. Considering the accuracy of the classifier, it can be understood that the system performs well in identifying fraud patterns in the financial transactions data set.

In the present study, we propose a system that uses the machine learning-based approach to determine financial frauds by taking the challenges head-on. The approach is based on the idea of going deeper into the financial information by applying various supervised learning algorithms to detect financial frauds. We tested various systems such as per logistic regression, decision Tree, random Forest, gradient boosting, also naive bayes toward determine the potential of the algorithms to detect financial frauds.

The framework that is developed for the purpose of fraud detection can be highly useful for banks, financial institutions, as well as payment service providers in the fight against fraud. By integrating the machine learning models with the transactions that are happening in the financial sector, the fraud rates can be reduced, and the platforms that are used for dealing with the digital money can be made more secure. This also allows real-time analysis of the transactions that are happening.

Although the current methods have shown high accuracy and efficiency in the results produced, there is still room for improvement. It is possible that future research will involve a application of deep learning techniques such as per a application for nervous networks to fraud detection. Additionally, the application of real-time data streams then the concept of adaptive learning may be useful in the detection of fraud in the ever-changing financial location.

## REFERENCES

- [1]. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.
- A. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Systems*, vol. 50, no. 3, pp. 559–569, 2011.
- [2]. P. Ravisankar, V. Ravi, G. R. Rao, and I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques," *Decision Support Systems*, vol. 50, no. 2, pp. 491–500, 2011.
- A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90–113, 2016.
- [3]. J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," *Computers & Security*, vol. 57, pp. 47–66, 2016.
- [4]. S. S. Dal Pozzolo et al., "Calibrating probability with undersampling for unbalanced classification," *IEEE Symposium Series on Computational Intelligence*, 2015.
- [5]. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, 2009.
- [6]. D. Bahnsen et al., "Improving credit card fraud detection with calibrated probabilities," *SIAM International Conference on Data Mining*, 2014.
- A. Carcillo et al., "Combining unsupervised and supervised learning in credit card fraud detection," *Information Sciences*, vol. 557, pp. 317–331, 2021.



- [7]. M. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system using machine learning approaches," *International Journal of Computer Applications*, vol. 165, no. 9, pp. 15–20, 2017.
- [8]. K. Randhawa et al., "Credit card fraud detection using machine learning techniques," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 5, pp. 24–32, 2018.
- [9]. S. B. Kotsiantis, "Supervised machine learning: A review of classification techniques," *Informatica*, vol. 31, no. 3, pp. 249–268, 2007.
- [10]. T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," *ACM SIGKDD*, 2016.
- [11]. L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
- [12]. J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed., Morgan Kaufmann, 2012.
- [13]. Patel, E. J., Singh, S., & Awasthi, R. K. (2025). Python-based detection of paddy leaf diseases: A computational approach. *International Journal of Computer Science Trends and Technology (IJCSST)*.
- [14]. Navadiya, K., & Singh, S. (2025). A review on future extraction of images using different methods. *International Journal of Advanced Research in Science, Communication and Technology*.
- [15]. Mehta, M. H., Singh, S., & Awasthi, R. K. (2025). A review of IoT-based technologies for identification and monitoring of rice crop diseases. *International Journal of Latest Technology in Engineering, Management & Applied Science*.
- [16]. Singh, S. (2020). Handling different aspects of big data: A review article. *Solid State Technology*, 63(6), 13117–13122.
- [17]. Singh, A. K. S. (2017). The analysis of the privacy issues in big data: A review. *International Journal of Recent Trends in Engineering & Research (IJRTER)*, 3.
- [18]. Singh, R., Chawda, R. K., & Singh, S. (2021). Analytics on Player Unknown's Battlegrounds player placement prediction using machine learning. *International Journal of Creative Research Thoughts (IJCRT)*, 9(5), 313–320.
- [19]. Shrivastava, A. K., & Singh, S. (2016). Big data analytics: A review. *International Journal of Computer Science and Technology*, 7(3), 92–95.
- [20]. Goyal, D. P., Roy, S., & Singh, S. (1982). Production of heavy clusters in interactions at  $\geq 1000$  GeV. *Physical Review D*, 26(11), 3273.
- [21]. Sharma, R. K., Sethi, S., & Singh, S. (2025). Tech-driven strategies for paddy disease prevention and crop health optimization. *International Journal of Advanced Research in Science, Communication and Technology*.
- [22]. Chauhan, A., & Parihar, A., & Singh, S. (2025). From leaves to lab: Innovative methods in plant disease diagnosis. *International Journal of Engineering in Computer Science*, 7(1), 219–226.
- [23]. Singh, S., & Sharma, A. (2021). The novel architecture for monitoring and prediction of rice plant diseases. *International Journal of Advanced Research in Engineering and Technology*, 12(3).
- [24]. Purani, D., & Singh, S. (2025). Innovations in plant disease diagnosis: Bridging nature and technology. *International Journal of Research Publication and Reviews*, 6(6), 10693–10701.
- [25]. Sinha, M., Chawda, R. K., & Singh, S. (2021). Smart agriculture using Internet of Things and based MQTT protocol. *International Journal of Creative Research Thoughts (IJCRT)*, 9(5), 273–276.
- [26]. Goyal, D. P., Singh, S., & Arya, N. S. (1984). Characteristics of intermediate-energy nucleons emitted from 50 GeV  $\pi^-$  interactions. *Il Nuovo Cimento A*, 79(4), 419–427.
- [27]. Awasthi, R. K., & Singh, S. (2023). An overview of machine learning methods for the detection of diseases in rice plants in agricultural research.
- [28]. Goyal, D. P., Singh, K. Y., Singh, S., & Arya, N. S. (1986). Comparative study of various methods of primary energy estimation in nucleon-nucleon interactions. *Nuclear Instruments and Methods in Physics Research Section A*.



- [29]. Mills, E., Nachega, J., & Singh, S. Adherence to antiretroviral therapy in Africa versus North America: A comparative meta-analysis. JAMA.
- [30]. Singh, M. K. N. M. S. (2025). A review on future extraction of images using different methods. International Journal of Advanced Research in Science, Communication and Technology.
- [31]. Srivastava, D. K. T. M. H. P. D. S. K. M. S. S. M. S. S. M. S. C. M. M. S. K. S. D. S. (2024). AI based humanoid device for objects identification. Indian Patent No. 431745-001.
- [32]. Kumar, R., Singh, S. P., Rajput, R., & Gupta, M. K. Designing of laboratory-based demand side management in the smart grid prospective. Solid State Technology, 63(4), 1805–1828.

