International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902015

Credit Card Fraud Detection System Using Machine Learning

Mandati Sindhu, Gujja Srisailam, Ganji Vijay, Katika Komala, Jadav Sanjana,

A. Jitendra Alaparthi, Dr. D. Prasad Dharnasi

UG, Student, CSE, Holy Mary Institute of Technology and Science, Hyderabad, TS, India

UG, Student, CSE, Holy Mary Institute of Technology and Science, Hyderabad, TS, India

UG, Student, CSE, Holy Mary Institute of Technology and Science, Hyderabad, TS, India

UG, Student, CSE, Holy Mary Institute of Technology and Science, Hyderabad, TS, India

UG, Student, CSE, Holy Mary Institute of Technology and Science, Hyderabad, TS, India

Associate Professor, Department of Computer Science and engineering, Holy Mary Institute of Technology &Science, Telangana, India

Professor, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India

Publication History: Received: 23.02.2026; Revised: 10.03.2026; Accepted: 13.03. 2026; Published: 18.03.2026.

ABSTRACT: The rapid growth of online payment systems has made credit cards a widely used more of digital transactions. Along with this growth, incidents of credit card fraud have increased, leading to financial losses for banks and reduced confidence among customers. Conventional fraud detection approaches are mostly based on predefined rules, which are often ineffective in identifying newly emerging fraud patterns, particularly when fraudulent transactions form only a small portion of the overall data. To address this challenge, this study applies machine learning techniques for identifying fraudulent credit card transactions. A major issue in this domain is the highly imbalanced nature of transaction data, where legitimate transaction significantly outnumber fraudulent ones. To reduce the impact of data imbalance, the Synthetic Minority Over-Sampling Technique (SMOTE) is used to generate additional fraud samples and enhance model training. Multiple machine learning classifiers are developed to learn transaction patterns and distinguish between genuine and fraudulent activities. Model performance is assessed using recall, F1-Score, and the Area under the Precision-Recall Curve (AUPRC), as these metrics provide a more reliable evaluation for imbalanced datasets. Experimental analysis indicates that the Random Forest classifier outperforms other models, achieving an accuracy of 99.95%. The findings demonstrate that machine learning-based approaches can significantly enhance fraud detection systems and support effective real-time monitoring of credit card transactions.

KEYWORDS: Credit Card Fraud Detection, Machine Learning, SMOTE, Random Forest, Imbalanced data

I. INTRODUCTION

The widespread use of digital payment platforms has increased credit card transactions across various sectors. While this has sped up transactions and made them more convenient, it has also raised the risk of fraud. Manually monitoring such a large volume of transactions is unrealistic, making automated detection techniques essential. These systems identify unusual transaction behaviour by examining historical data patterns.

Fraud detection is particularly challenging because there are very few instances of fraud compared to legitimate transactions. This difference impacts the effectiveness of traditional detection methods. Additionally, fraud strategies change over time, which decreases the reliability of static rules. The proposed work focuses on using machine learning techniques to improve classification accuracy while addressing class imbalance. SMOTE balances the dataset, and multiple models are tested to find the most dependable solution for credit card fraud detection.

Literature Survey: Initial studies on credit card fraud detection mainly used fixed rules and basic statistical checks to identify suspicious transactions [1]. These systems depended on conditions such as transaction limits, unusual spending behaviour, or location mismatch. Although such approaches were easy to deploy, they were not effective in real-world environments where fraud patterns change frequently. As transaction volumes increased, these traditional methods produced many incorrect alerts and required continuous manual updates, reducing their usefulness in modern financial systems.

Later research introduced machine learning-based solutions to improve fraud detection performance [2]. These approaches learn patterns directly from historical transaction data and are capable of identifying abnormal behaviour more effectively than rule-based systems. However, many studies pointed out that fraud detection data is highly imbalanced [3], with fraudulent transactions occurring far less frequently than normal ones. To overcome this challenge, researchers explored data balancing strategies and evaluation techniques better suited for rare event detection. Recent literature emphasizes the importance of using metrics such as Precision, Recall, and F1-Score instead of accuracy to properly assess fraud detection models under imbalanced conditions [4]. Several studies have applied oversampling techniques such as SMOTE to address class imbalance and improve fraud detection performance.

II. PROBLEM STATEMENT

The increasing use of credit cards for digital payments and online transactions has made financial activities faster and more convenient. At the same time, this has increased the risk of unauthorized transactions and fraud. Credit card fraud leads to financial loss for banks and customers and creates concerns about transaction security. As the number of transactions processed each day continues to grow, identifying fraudulent activity quickly and accurately has become a major challenge for financial systems.

Fraud detection is difficult because fraudulent transactions occur very rarely compared to legitimate transactions, resulting in highly imbalanced data. In addition, fraud techniques change over time, making traditional detection methods less effective. Many existing systems generate a large number of false alerts, which can block genuine customer transactions and reduce user trust. Therefore, there is a need for an automated fraud detection system that can effectively handle imbalanced data, accurately classify transactions as Fraud or Normal, and reduce false positives while operating efficiently on large-scale transaction data. Therefore, this study applies SMOTE to balance the dataset and evaluates multiple machine learning models to identify the most effective approach for fraud detection.

III. METHODOLOGY

1. Study Design
This work uses an experimental research method based on machine learning techniques. The main goal is to build a classification system that can automatically identify fraudulent credit card transactions by learning pattern from previously recorded transaction data.
2. Dataset collection
The transaction data in this study comes from a publicly available credit card fraud dataset. The dataset includes only numerical features that have been anonymized to protect customer privacy. Each transaction record has a class label indicating whether the transaction is genuine or fraudulent.
3. Nature of the data
A significant challenge with the dataset is its highly imbalanced nature. Fraudulent transactions make up a very small portion of the overall data, while normal transactions dominate the dataset. This imbalance makes fraud detection difficult because traditional models usually favour the majority class.
4. Proposed System Framework
The proposed system follows a step-by-step process. First, the transaction data is cleaned and prepared for analysis. Then, the data imbalance is addressed using the Synthetic Minority Over-sampling Technique (SMOTE). After balancing, machine learning models are trained and tested. Finally, the best-performing model is used to predict whether a transaction is fraudulent or legitimate.

System architecture

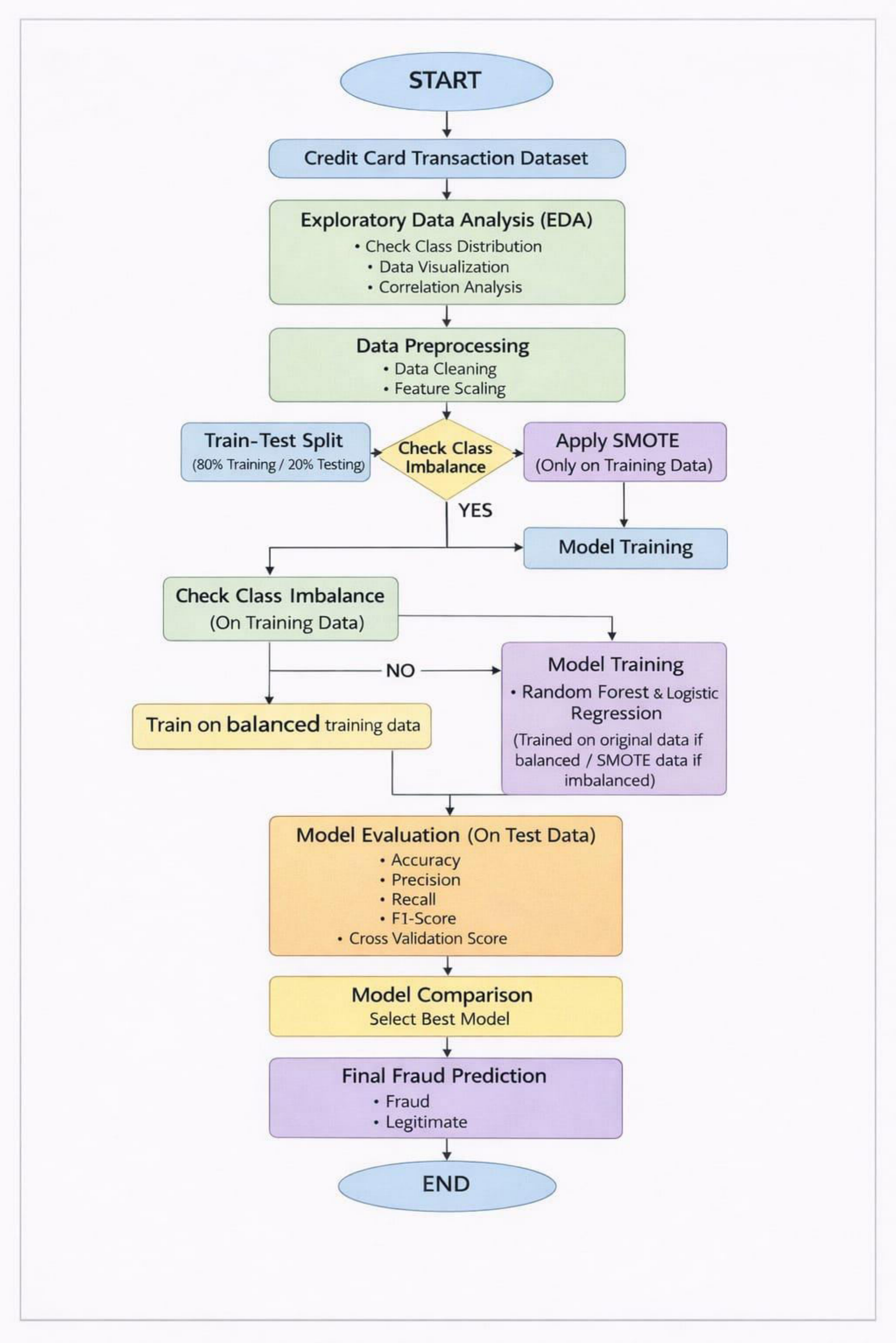

Figure 1: System Architecture of the Proposed Fraud Detection System

This system architecture illustrates the end-to-end workflow of the proposed credit card fraud detection system using machine learning techniques. The transaction dataset is first pre-processed to ensure data quality. Class imbalance present in the dataset is addressed using the Synthetic Minority Over-sampling Technique (SMOTE), which is applied only to the training data. Machine learning models such as Logistic Regression and Random Forest are then trained and evaluated using appropriate performance metrics. Finally, the best-performing model is selected to predict whether a given credit card transaction is fraudulent or legitimate.

5. Data Preparation

Before applying machine, learning algorithms preprocessing is done to improve data reliability. Duplicate records are removed, missing values are addressed, and feature scaling is applied where necessary. The dataset is then split into input features and output labels. SMOTE is applied only to the training data to enhance the model's ability to learn fraud patterns.

6. Model Training

The pre-processed dataset is divided into training and testing sets. Logistic Regression and Random Forest algorithms are implemented using the training data. These models analyse transaction attributes and learn to classify transaction as fraud or non-fraud.

7.Performance Assessment

Model performance is evaluated using multiple metrics to ensure a reliable assessment. Accuracy measures overall correctness, while precision and recall evaluate fraud detection capability. The F1-Score balances precision and recall results. A confusion matrix is also created to show correct and incorrect predictions.

IV. RESULTS AND DISCUSSION

This section evaluates the performance of Logistic Regression, Decision Tree and Random Forest models for credit card fraud detection. The models are assessed using Accuracy, Recall, and F1-score metrics.

- Real-Time Fraud Prediction Process

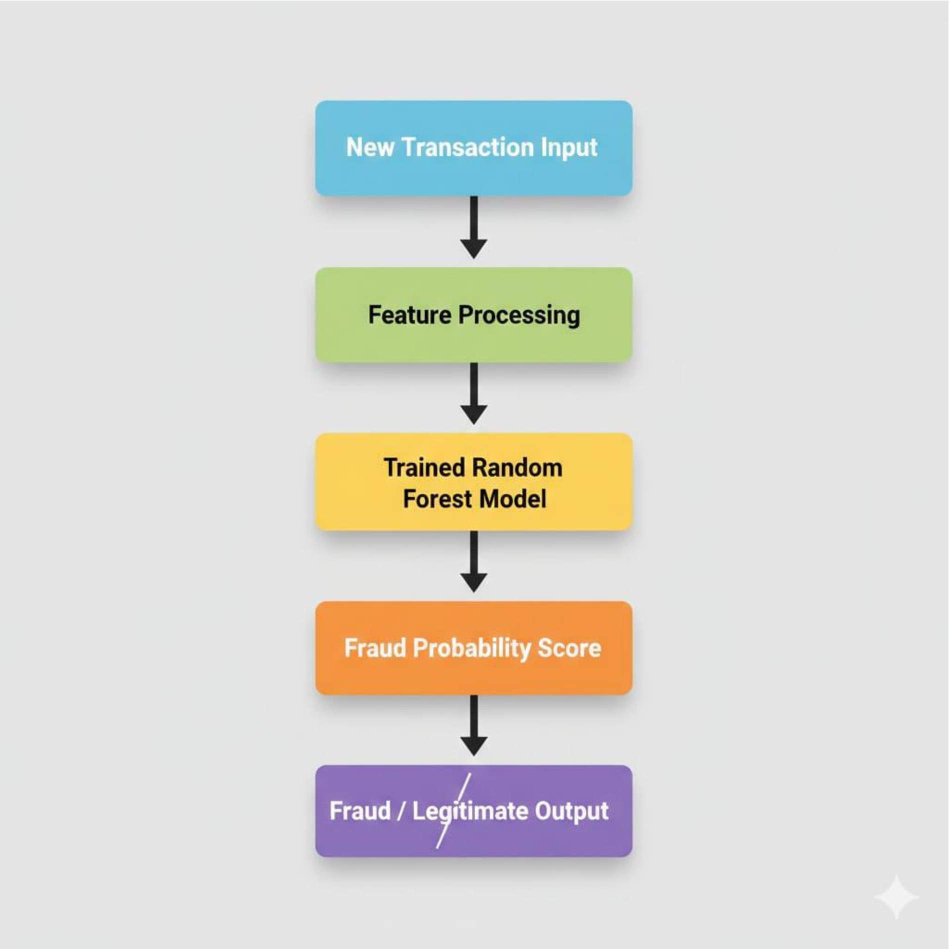

Figure 2: Probability flow diagram

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902015

Figure 2 shows the real-time fraud prediction workflow. Incoming transaction data is first pre-processed and then evaluated by the trained Random Forest model. This produces a fraud classification and an associated probability score to help make risk-based decisions.

- **Model Accuracy Comparison**

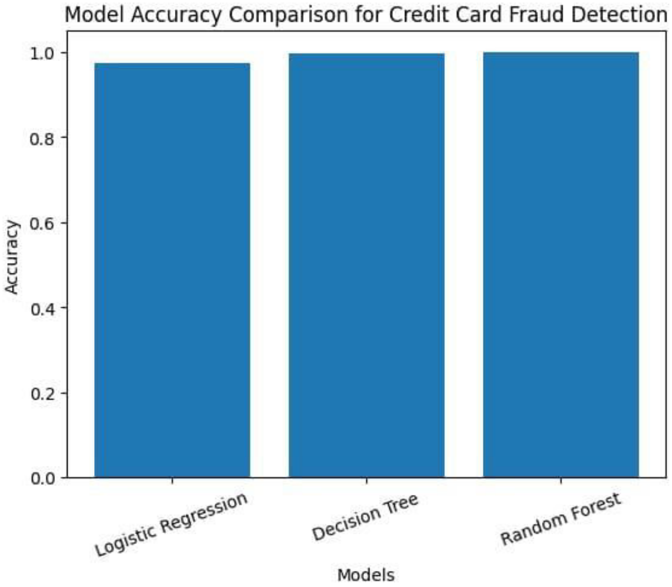

Figure 3: Model Accuracy Comparison

Figure 3 displays the accuracy values of all models Random Forest has the highest accuracy at 99.95%. Decision Tree achieves an accuracy of 99.76%. Logistic Regression has an accuracy of 97.41%, Although Random Forest demonstrates superior accuracy, accuracy alone is not a reliable metric for fraud detection tasks because the dataset is highly imbalanced. Therefore, additional performance metrics such as recall and F1-Score are considered to ensure a more comprehensive evaluation of the final model.

- **Recall Comparison**

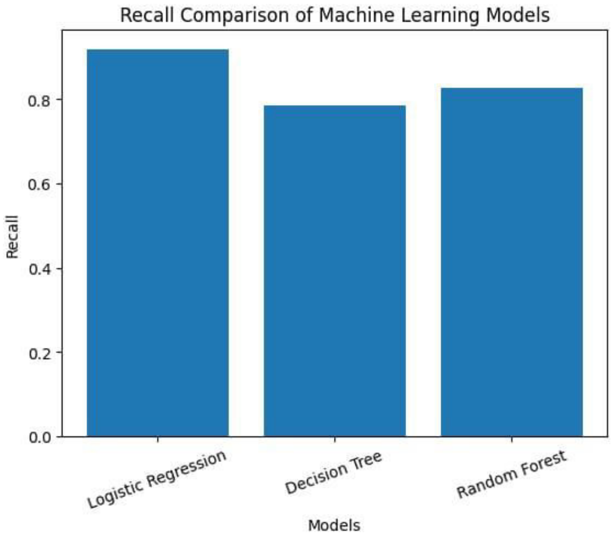

Figure 4: Recall Comparison

Figure 4 shows the recall values. Logistic Regression identifies more fraud cases, leading to a high recall. However, it also makes many incorrect predictions, which weakens its overall performance. Random forest delivers better and more stable results.

- **F1-Score Comparison**

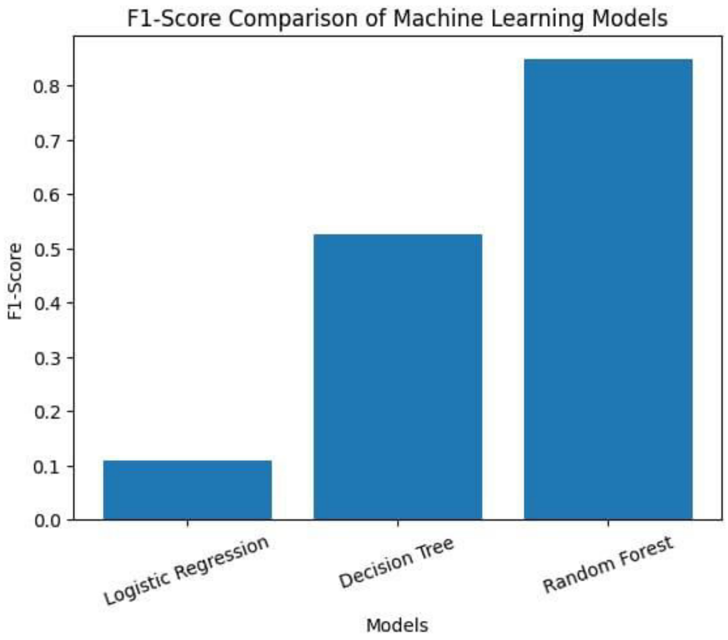

Figure 5: F1-score Comparison of Machine Learning Models

Figure 5 compares the F1-score. Random Forest achieves the highest F1-Score of 0.8482. Decision Tree earns a score of 0.5256. Logistic Regression has a very low value of 0.1089. Based on these values, Random Forest is the best model. Relying on accuracy alone is not enough for fraud detection because of the limited amount of fraud data. Recall and F1-Score provide a clearer picture of model performance. From all results, Random Forest is selected as the final model for this project

V. CONCLUSION

The increasing use of digital payment systems has made credit card fraud a critical problem that affects both users and financial institutions. This project focused on designing a fraud detection system using machine learning techniques to identify suspicious credit card transactions. To overcome the challenge of data imbalance, preprocessing steps and the Synthetic Minority Over-sampling Technique (SMOTE) were applied, which helped improve the learning capability of the models. Multiple machine learning algorithms, including Logistic Regression, Decision Tree and Random Forest algorithms were implemented and evaluated. Their performance was examined using evaluation metrics such as accuracy, precision, recall, F1-score and the confusion matrix. The results demonstrate that machine learning models are capable of detecting fraudulent transactions with improved reliability and can contribute to strengthening the security of credit card-based payment systems. The developed system also provides fraud probability scores for each transaction, enabling risk-based classification and real-time decision making.

VI. FUTURE SCOPE

In future work, deep learning techniques and real-time streaming data can be incorporated to further enhance fraud detection performance. The system can also be integrated with banking applications for automated transaction monitoring.

REFERENCES

1. Dharnasi, P. (2025). A multi-domain AI framework for enterprise agility integrating retail analytics with SAP modernization and secure financial intelligence. *International Journal of Humanities and Information Technology*, 7(4), 61–66.
2. Nithin, A., Harish, B., Prashanth, B., Shirisha, C. H., Raviteja, C. H., Prasad, D., & Saravanan, M. (2026). One stop personalized career and educational advisor. *International Journal of Engineering & Extended Technologies Research*, 8(2), 542–550.
3. Singh, K., Amrutha Varshini, G., Karthikeya, M., Manideep, G., Sarvanan, M., & Dharnasi, P. (2026). Automatic brand logo detection using deep learning. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(1), 126–130.
4. Gogada, S., Gopichand, K., Reddy, K. C., Keerthana, G., Nithish Kumar, M., Shivalingam, N., & Dharnasi, P. (2026). Cloud computing/deep learning customer churn prediction for SaaS platforms. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(1), 74–78.
5. Naresh, D., Anand, P., Harish, M., Vamshi, A., Kethan, A., Nirmala, B., & Saravanan, M. (2026). Face recognition door lock system with IoT & AI. *International Journal of Computer Technology and Electronics Communication*, 9(2), 526–534.
6. Tirupalli, S. R., Munduri, S. K., Sangaraju, V., Yeruva, S. D., Saravanan, M., & Dharnasi, P. (2026). Blockchain integration with cloud storage for secure and transparent file management. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(1), 79–86.
7. Basha, S. A., Krishna, V. S. B., Shanker, S. S., Sravya, R., Shivalingam, N., & Dharnasi, P. (2026). AI-powered price prediction for agriculture markets. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(2), 512–515.
8. Varshini, M., Chandrapathi, M., Manirekha, G., Balaraju, M., Afraz, M., Sarvanan, M., & Dharnasi, P. (2026). ATM access using card scanner and face recognition with AIML. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(1), 113–118.
9. Akula, A., Budha, G., Bingi, G., Chanda, U., Borra, A. R., Yadav, D. B., & Saravanan, M. (2026). Emotion recognition from facial expressions using CNNs. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(1), 120–125.
10. Chandu, S., Goutham, T., Badrinath, P., Prashanth Reddy, V., Yadav, D. B., & Dharnas, P. (2026). Biometric authentication using IoT devices powered by deep learning and encrypted verification. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(1), 87–92.
11. Priya, B. A., Gayathri, D., Maheshwari, B., Nikhitha, C., Sravanam, D., Yadav, D. B., & Saravanan, M. (2026). Fake news detection using natural language processing. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 498–505.
12. Keerthana, L. M., Mounika, G., Abhinaya, K., Zakeer, M., Chowdary, K. M., Bhagyaraj, K., & Prasad, D. (2026). Floods and landslide prediction using machine learning. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(1), 125–129.
13. Bhagyasri, Y., Bhargavi, P., Akshaya, T., Pavansai, S., Dharnasi, P., & Jitendra, A. (2026). IoT based security & smart home intrusion prevention system. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 457–462.
14. Rachana, P., Kalyan, P. P., Kumar, T. S., Reddy, P. M., Rohan, P., Saravanan, M., & Dharnasi, P. (2026). Secure chat application with end-to-end encryption using deep learning. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 472–478.
15. Akshaya, N., Balaji, Y., Chennarao, J., Sathwik, P., & Dharnasi, P. (2026). Diabetic retinopathy diagnosis with deep learning. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(2), 506–512.
16. Kumar, A. S., Saravanan, M., Joshna, N., & Seshadri, G. (2019). Contingency analysis of fault and minimization of power system outage using fuzzy controller. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 4111–4115.
17. Vishwanath, M. Y., Ganapathi, K., Krupa, K. D., Bharat Kumar, K. L. N., Reddy, K. S., Saravanan, M., & Dharnasi, P. (2026). Online election system to avoid fraud voting by using cybersecurity techniques with the help of ML techniques. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 516–526.
18. Amitha, K., Ram Manohar Reddy, M., Yashwanth, K., Shylaja, K., Rahul Reddy, M., Srinu, B., & Dharnasi, P. (2026). AI empowered security monitoring system with the help of deployed ML models. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(1), 69–73.

19. Rupika, M., Nandini, G., Mythri, M., Vasu, K., Abhiram, M., Shivalingam, N., & Dharnasi, P. (2026). Electronic gadget addiction prediction using machine learning. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(2), 500–505.
20. Dadigari, M., Appikatla, S., Gandhala, Y., Bollu, S., Macha, K., & Saravanan, M. (2026). Bitcoin price prediction with ML through blockchain technology. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(1), 130–136.
21. Saravanan, M., & Sivakumaran, T. S. (2016). Three phase dual input direct matrix converter for integration of two AC sources from wind turbines. *Circuits and Systems*, 7, 3807–3817.
22. Chinthala, S., Erla, P. K., Dongari, A., Bantu, A., Chityala, S. G., & Saravanan, M. S. (2026). Food recognition and calorie estimation using machine learning. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(2), 480–488.
23. Yadamakanti, S., Mahesh, Y., Rathnam, S. A., Praveen, V., Jitendra, A., & Dharnasi, P. (2026). Unified payments interface fraud detection using machine learning. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 488–497.
24. Feroz, A., Pranay, D., Srikar Sai Raj, B., Harsha Vardhan, C., Rohith Raja, B., Nirmala, B., & Dharnasi, P. (2026). Blockchain and machine learning combined secured voting system. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(1), 119–124.
25. Rakesh, V., Vinay Kumar, M., Bharath Patel, P., Varun Raj, B., Saravanan, M., & Dharnasi, P. (2026). IoT-based gas leakage detector with SMS alert. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 449–456.
26. Varsha, P., Chary, P. K., Sathvik, P., Varma, N. V., Rahul, S., Saravanam, M., & Dharnasi, P. (2026). IoT-based fire alarm and location tracking system. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(2), 528–532.
27. Krishna, G., Rajesh, B., Dinesh, B., Sravani, B., Rajesh, G., Dharnasi, P., & Sarvanan, M. (2026). Smart agriculture system using IoT with help of AI techniques. *International Journal of Computer Technology and Electronics Communication*, 9(2), 479–487.
28. Reddy, N. H. V., Reddy, N. T., Bharath, M., Hemanth, N., Dharnasi, D. P., Nirmala, B., & Jitendra, A. (2026). AI based learning assistant using machine learning. *International Journal of Engineering & Extended Technologies Research*, 8(2), 495–504.
29. Chinthamalla, N., Anumula, G., Banja, N., Chelluboina, L., Dangeti, S., Jitendra, A., & Saravanan, M. (2026). IoT-based vehicle tracking with accident alert system. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(2), 486–494.
30. Nagamani, K., Laxmikala, K., Sreeram, K., Eshwar, K., Jitendra, A., & Dharnasi, P. (2026). Disaster management and earthquake prediction system using machine learning. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(2), 495–499.
31. Pavan Kumar, T., Abhishek Goud, T., Yogesh, S., Manikanta, V., Dinesh, P., Srinu, B., & Dharnasi, P. (2026). Smart attendance system using facial recognition for staff using AI/ML. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(2), 513–519. https://doi.org/10.15662/IJRPETM.2026.0902005
32. Sanjay, P., Vardhan, Y. H., Raja, S. Y., Krishna, V. M., Nirmala, B., & Dharnasi, P. (2026). Disaster management and earthquake tsunami prediction system using machine learning and deep learning. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(2), 516–522.
33. Vangara, N., Bhargavi, P., Chandu, R., Bhavani, V., Yadav, D. B., & Dharnasi, P. (2026). Machine learning based intrusion detection system using supervised and unsupervised learning. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(2), 505–511.
34. Harish, G., Venkatesh, M., Venkatesh, M., Sandeep, G., Mustaffa, M., Sarvanan, M., Dharnasi, D. P., & Alaparth, A. J. (2026). Heart disease prediction using ML and pandas. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 506–515.
35. Prasad, E. D., Sahithi, B., Jyoshnavi, C., Swathi, D., Arun Kumar, T., Dharnasi, P., & Saravanan, M. (2026). A technology driven solution for food and hunger management. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 440–448.
36. Chanamalla, B., Murali, V. N., Suresh, B., Deepak, M. S., Zakriya, M., Yadav, D. B., & Saravanan, M. (2026). AI-driven multi-agent shopping system through e-commerce system. *International Journal of Computer Technology and Electronics Communication (IJCTEC)*, 9(2), 463–470.
37. Keerthana, L. M., Mounika, G., Abhinaya, K., Zakeer, M., Chowdary, K. M., Bhagyaraj, K., & Prasad, D. (2026). Floods and landslide prediction using machine learning. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(1), 125–129.

38. Kumar, A. S., Saravanan, M., Joshna, N., & Seshadri, G. (2019). Contingency analysis of fault and minimization of power system outage using fuzzy controller. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 4111–4115.
39. Prasad, K., Rakesh, K., Vishnu, G., Raju, G., Vardhan, K., Sarvanan, M., Dharnasi, D. P., & Alaparth, A. J. (2026). Handwritten character recognition using neural networks. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(2), 532–541.
40. Thotla, S. B., Vyshnavi, S., Anusha, P., Vinisha, R., Mahesh, S., Yadav, D. B., & Dharnasi, P. (2026). Traffic congestion prediction using real time data by using deep learning techniques. *International Journal of Engineering & Extended Technologies Research*, 8(2), 489–494.