

Credit Card Fraud Detection

Soudari Sudheshna¹, Barmavath Srikanth², Maraju Manikanta Chary³

Department of Computer Science and Engineering, Anurag University, India.

Corresponding author's email: soudari555shna@gmail.com

Abstract. The main aim of this project is to detect fraudulent credit card transactions by utilizing credit card details. As financial transactions grow in volume and complexity, it becomes increasingly critical for credit card companies to identify fraudulent activities to protect customers from unauthorized charges. Although instances of fraud are relatively infrequent, they present substantial financial risks to both consumers and financial institutions. This research employs three machine learning techniques—One-Class SVM, Local Outlier Factor, and Isolation Forest—to analyse transaction data in real-time, addressing the challenges posed by imbalanced datasets and the sophistication of fraud schemes. By implementing a comprehensive detection system using these models on a credit card transaction dataset, the study aims to enhance the accuracy of fraud detection and provide timely alerts to prevent financial losses. Key results indicate that the proposed methodology significantly improves the identification of fraudulent transactions, ultimately leading to more secure credit card usage for consumers. The conclusions drawn from this research emphasize the necessity for ongoing innovation in fraud detection methodologies to keep pace with the ever- changing landscape of financial fraud.

Keywords. Credit card fraud detection, machine learning, One-Class SVM, Local Outlier Factor, Isolation Forest.

1 INTRODUCTION

Credit card fraud has become a critical issue as the use of credit cards in everyday transactions grows. Traditional fraud detection systems, such as rule-based methods and statistical models, have struggled to keep up with the evolving tactics of fraudsters [1][2]. These methods often fail to accurately detect emerging fraud patterns, leading to both false positives and false negatives, which undermine the effectiveness of fraud prevention strategies [3][4]. In response to these challenges, researchers have turned to machine learning (ML) techniques to develop more robust fraud detection frameworks. ML methods, such as supervised and unsupervised learning models, offer the ability to adapt to new fraud schemes, improving the accuracy of detection and reducing the risk of financial losses [5][6].

Recent studies demonstrate that integrating ML models like One-Class SVM, Local Outlier Factor, and Isolation Forest into fraud detection systems can significantly enhance performance metrics, such as precision, recall, and overall detection accuracy [7][8]. One-Class SVM effectively isolates outliers in transaction data, while Local Outlier Factor identifies unusual transactions by comparing them to local clusters of data points [9][10]. Isolation Forest, a highly efficient anomaly detection method, partitions the data into isolation trees, making it easier to identify fraudulent transactions [11][12].

These ML approaches not only increase detection accuracy but also reduce the operational burden on financial institutions, allowing them to shift focus from reactive to preventive strategies [13][14]. Studies reveal that ML-based systems can adapt to constantly changing fraud patterns, ensuring continuous protection against new forms of fraud [15][16]. By addressing the limitations of traditional methods, this research

provides valuable insights into developing adaptive fraud detection systems that increase consumer trust and reduce financial risks for institutions [17][18].

Ultimately, the implementation of advanced ML techniques can create a more secure environment for digital transactions, bolstering the financial industry's efforts to safeguard consumer transactions [19][20].



This research contributes to ongoing efforts to enhance credit card security, demonstrating the applicability of innovative machine learning models in safeguarding consumer transactions. The objective of this work is to develop a machine learning-based framework that improves the detection of fraudulent transactions, thereby reducing the financial risks associated with credit card fraud. By addressing existing challenges in fraud detection and highlighting the importance of adaptive systems, this research aims to contribute valuable insights and solutions to the field. Ultimately, implementing these advanced techniques can lead to increased trust among consumers, reduced losses for financial institutions, and a more secure environment for digital transactions.

2 RESEARCH METHODOLOGY

This section outlines the methodology used for the credit card fraud detection project, detailing data preprocessing, feature selection, model training, and evaluation.

2.1 Dataset

The dataset used in this project comprises credit card transaction records, sourced from Kaggle. It contains anonymized features related to transaction details, which underwent Principal Component Analysis (PCA) for dimensionality reduction. PCA was employed to transform the high-dimensional data into fewer components while retaining the most significant information. This not only reduced the complexity of the dataset but also improved computational efficiency and model performance by focusing on the features that are most relevant to fraud detection.

2.2 Data Preprocessing

To prepare the dataset for model training, the following preprocessing steps were applied:

- Data Cleaning:
 - Duplicates were identified and removed to ensure the dataset contained unique transactions.
 - Missing Values: Although the dataset did not have missing values, handling potential missing data is a crucial step in real-world scenarios to ensure model robustness.
- Normalization:
 - Min-Max Scaling was applied to normalize the features. This scaling technique ensures that all features are within a uniform range, typically between 0 and 1, which helps prevent any particular feature from dominating others due to varying scales. This step is especially important when dealing with distance-based algorithms like One-Class SVM and Local Outlier Factor.

2.3 Feature Selection

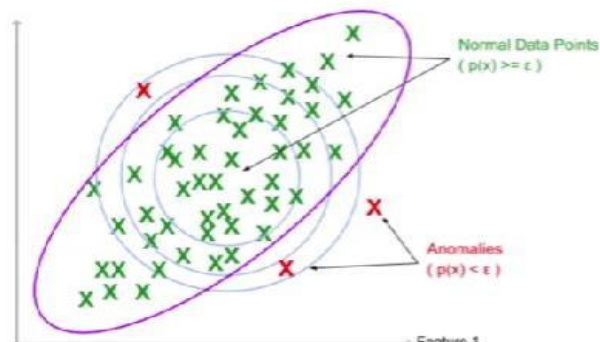
To ensure the model utilizes the most relevant features, various feature selection techniques were employed:

- **Correlation Analysis:**
 - The relationship between features was analyzed using a correlation matrix. This step helped in identifying and removing highly correlated features that provide redundant information, ensuring a more generalized model and reducing multicollinearity issues.
- **Feature Importance:**
 - Recursive Feature Elimination (RFE) was used to systematically identify and retain the most important features. RFE works by recursively considering smaller sets of features and eliminating the least significant features, which ultimately improved the model's efficiency in detecting fraudulent transactions.

2.4 Machine Learning Algorithms

Three machine learning algorithms were implemented, each specifically suited for anomaly detection:

1. **Isolation Forest:**
 - This is a tree-based algorithm particularly well-suited for **anomaly detection** in high-dimensional datasets. It works by isolating observations by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of the selected feature. The idea is that anomalies are few and different, and they are isolated quickly by this random process.
2. **One-Class SVM:**
 - This algorithm fits a **boundary around normal transactions** in the feature space and classifies points lying outside this boundary as anomalies. It is highly effective for **unsupervised anomaly detection**, as it only requires data from the normal class to learn and identify potential outliers, which in this case are fraudulent transactions.



3. **Local Outlier Factor (LOF):**
 - LOF calculates the **local density** deviation of a given data point with respect to its neighbours. It is useful in identifying **local anomalies** where the density of fraudulent transactions is considerably different from normal ones, making it a powerful algorithm for outlier detection in fraud detection systems.

2.5 Model Training and Evaluation

The models were trained using **stratified k-fold cross-validation** to ensure balanced representation of both fraud and non-fraud classes during training and validation. The following evaluation metrics were used to assess the model performance:

- **Accuracy:** Overall correctness of the model, measuring how well the model predicts both fraudulent and legitimate transactions.

- **Precision:** The proportion of correctly identified frauds out of all instances predicted as fraud. A high precision value indicates fewer false positives.
- **Recall:** The proportion of actual frauds that were correctly identified. High recall ensures that most fraudulent transactions are detected.
- **F1 Score:** The harmonic mean of precision and recall, providing a balanced measure of a model's performance.
- **ROC-AUC:** This metric evaluates the model's ability to distinguish between fraudulent and non-fraudulent transactions across all classification thresholds. A higher AUC indicates a better-performing model.

2.6 Implementation

The project was implemented using **Python**, leveraging the **PyCaret** library for efficient model training and hyperparameter tuning. PyCaret offers an easy-to-use interface for comparing multiple models, tuning hyperparameters, and evaluating models based on various metrics.

Key Python libraries used include:

- **Pandas** for data manipulation and preprocessing.
- **Scikit-learn** for feature scaling and implementation of algorithms.
- **Matplotlib** and **Seaborn** for data visualization.

PyCaret's **anomaly detection module** was utilized to streamline the process of training and evaluating the machine learning models. It also facilitated the process of fine-tuning hyperparameters to improve model accuracy and performance.

2.7 Model Deployment

The best-performing model, based on evaluation metrics, was deployed using **Streamlit**, a Python-based framework that allows the creation of interactive web applications. The deployed application offers **real-time fraud predictions**, where users can input transaction data, and the system classifies the transaction as either normal or fraudulent.

Key features of the deployed model include:

- **Real-time fraud detection:** Users can upload new transaction data, and the model provides instant feedback on whether the transaction is suspicious.
- **Continuous Monitoring and Retraining:** As part of future plans, the application will include mechanisms for **continuous monitoring** of incoming transactions and **retraining** the model as new fraud patterns emerge, ensuring the system stays up-to-date and adapts to new fraud techniques.

3 THEORY AND CALCULATION

In fraud detection, anomaly detection plays a pivotal role in identifying rare fraudulent transactions among a large volume of legitimate ones. Traditional rule-based systems struggle with evolving fraud tactics, which is why this project uses advanced machine learning algorithms such as Isolation Forest, One-Class SVM, and Local Outlier Factor (LOF). These models detect outliers by identifying unusual transaction patterns, providing a more dynamic and adaptive approach to fraud detection. Isolation Forest isolates anomalies based on their distinct behaviour, One-Class SVM defines a boundary for normal transactions, and LOF detects anomalies based on local density deviations. This foundation enhances real-time detection accuracy, offering a more efficient solution for financial security.

Calculation

This project leverages PyCaret, an open-source low-code machine learning library, to facilitate model development and optimization. The workflow involves:

- **Data Preparation:** Cleaning and preprocessing the dataset.
- **Model Implementation:** Deploying selected algorithms for fraud detection.

- **Performance Evaluation:** Evaluating models based on accuracy, precision, recall, and F1- score.

3.1 Mathematical Expressions and Symbols

In credit card fraud detection, algorithms like One-Class SVM and Isolation Forest use mathematical models to identify anomalies.

- **Recall**

Recall is defined as the ratio of correctly predicted positive observations to the all actual positives:

$$\text{Recall} = \frac{TP}{TP+FN}$$

Where:

TP = True Positives, FN = False Negatives

- **Precision**

Precision is defined as the ratio of correctly predicted positive observations to the total predicted positives:

$$\text{Precision} = \frac{TP}{TP+FP}$$

Where:

FP = False Positives

- For **One-Class SVM**, the optimization problem is defined as:

$$\min + \sum_{w=1}^p \frac{1}{2} (\|w\|^2)$$

subject to:

$$(w \cdot \phi(x_i)) \geq \rho - \xi_i \forall i$$

where w is the weight vector, $\phi(x_i)$ is the mapped input data, ρ is the threshold, and ξ_i are slack variables

- For **Isolation Forest**, the anomaly score $s(x)$ for a data point xxx is:

$$s(x) = 2^{-E(h(x))/C(n)}$$

where $E(h(x))$ is the average path length of the point xxx , and $C(n)$ is the average path length in a binary search tree for a dataset of size n

These formulas guide the detection of fraudulent transactions.

4 RESULTS AND DISCUSSION

In credit card fraud detection, we implemented three machine learning algorithms:


Isolation Forest, One-Class SVM, and Local Outlier Factor.

Credit Card Fraud Detection ⇄

Upload the transaction CSV file for fraud detection:

The file should contain the following columns: Time , V1 to V28 , Amount .

Choose a CSV file



Drag and drop file here
Limit 200MB per file • CSV

Browse files

Figure 1. Uploading the Document.

The high recall indicates that the models successfully identified fraudulent activities, crucial for minimizing financial losses. However, optimizing precision remains a challenge, highlighting the need for further refinement.

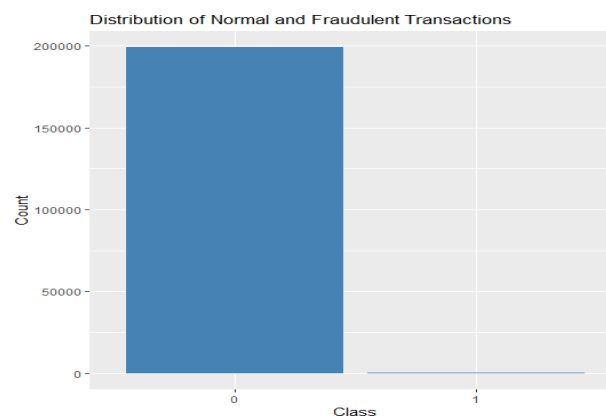


Figure 2. Bar Graph (Normal vs Fraud Transaction)

Fraudulent transactions: 2

Legitimate transactions: 23

Figure 2. Prediction Result

Overall, the results demonstrate the efficacy of advanced machine learning techniques in enhancing fraud detection, emphasizing their role in improving security in financial transactions.

4.1 Preparation of Figures and Tables

4.1.1 Formatting Tables

The table outlines key activities in the credit card fraud detection process, including dataset uploads, model predictions, and results analysis. Each entry lists estimated completion times and their significance for effective fraud detection, emphasizing the importance of timely execution for optimal outcomes. Formatting requirement has been summarized in the Table 1.

Table 1: Activity Breakdown and Estimated Duration for Credit Card Fraud Detection.

Activity	Description	Estimated Time to Complete	Impact on Learning Process
Dataset Upload	Users or admins upload transaction data for analysis.	2-3 minutes	Initial engagement, sets the foundation for analysis.
Data Exploration	Users explore data characteristics, such as transaction patterns and anomalies.	3-5 minutes	Increases understanding of data, influencing preprocessing.
Feature Engineering	Identification and creation of relevant features for model training, including transaction amounts, merchant categories, etc.	5-10 minutes	Enhances model performance, leading to better fraud detection
Model Training	The machine learning model is trained on the processed data to identify fraudulent behaviour.	30-60 minutes	Higher accuracy improves fraud detection capabilities.
Hyperparameter Tuning	Adjust the model's hyperparameters to optimize performance and minimize overfitting.	10-20 minutes	Fine-tuning enhances model efficiency, improving fraud detection and reducing false positives.
Prediction and Validation	The model predicts potential fraudulent transactions, which are validated against known outcomes.	10-15 minutes	Validated predictions enhance trust in the model's effectiveness.
Result Analysis	Users analyse prediction results and make decisions based on flagged transactions.	10-20 minutes	Informative insights lead to actionable strategies for fraud prevention.
Model Deployment	Deploy the trained model into a web application for real-time fraud detection.	20-30 minutes	Deployment enables continuous monitoring, improving user engagement and system utility.
Model Retraining	Periodic retraining of the model with new transaction data to maintain accuracy.	10-15 minutes	Keeps the model up-to-date, adapting to evolving fraud patterns for sustained performance.

5 CONCLUSIONS

The project effectively showcases the use of PyCaret, a low-code machine learning library, to develop and optimize advanced credit card fraud detection models. By employing its automated machine learning pipeline, the project enhances model accuracy and adaptability, crucial for addressing evolving fraudulent tactics. PyCaret simplifies the machine learning process, enabling financial institutions to implement effective fraud detection without extensive coding knowledge. This adaptability allows models to quickly learn from new transaction patterns, reducing false positives and missed fraud cases.

While recognizing the need for continuous model updates to keep pace with changing fraud behaviours, the findings emphasize the importance of innovative solutions in the financial sector. Future research may explore integrating additional data sources and hybrid modelling techniques to strengthen fraud detection systems further. Overall, this work highlights the critical role of advanced machine learning in enhancing fraud detection efforts, fostering trust and security in financial transactions.

6 DECLARATIONS

6.1 Study Limitations

This study is limited by the use of a PCA-reduced dataset of credit card transactions, which may exclude critical features that could enhance model performance. This reduction can lead to a narrower understanding of the data, potentially impacting the predictive accuracy of the employed machine learning algorithms.

6.2 Acknowledgements

We would like to acknowledge the contributions of our peers and mentors who provided invaluable support and feedback throughout this project. Their expertise and insights enriched our research and helped us effectively navigate challenges. We appreciate their dedication to reviewing our work, which enhanced its quality and rigor, motivating us to expand our understanding and achieve our goals.

6.3 Funding source

None

REFERENCES

1. Murthy, G., and R. Shankar. "Composite Fermions." (1998): 254-306.
2. Mahalakshmi, A., Goud, N. S., & Murthy, G. V. (2018). A survey on phishing and its detection techniques based on support vector method (Svm) and software defined networking (sdn). *International Journal of Engineering and Advanced Technology*, 8(2), 498-503.
3. Murthy, G., & Shankar, R. (2002). Semiconductors II-Surfaces, interfaces, microstructures, and related topics-Hamiltonian theory of the fractional quantum Hall effect: Effect of Landau level mixing. *Physical Review-Section B-Condensed Matter*, 65(24), 245309-245309.
4. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2014). Optimal placement of DG in distribution system to mitigate power quality disturbances. *International Journal of Electrical and Computer Engineering*, 7(2), 266-271.
5. Muraleedharan, K., Raghavan, R., Murthy, G. V. K., Murthy, V. S. S., Swamy, K. G., & Prasanna, T. (1989). An investigation on the outbreaks of pox in buffaloes in Karnataka.
6. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2012). Reliability improvement of radial distribution system with distributed generation. *International Journal of Engineering Science and Technology (IJEEST)*, 4(09), 4003-4011.
7. Gowda, B. M. V., Murthy, G. V. K., Upadhye, A. S., & Raghavan, R. (1996). Serotypes of Escherichia coli from pathological conditions in poultry and their antibiogram.
8. Balasubbareddy, M., Murthy, G. V. K., & Kumar, K. S. (2021). Performance evaluation of different structures of power system stabilizers. *International Journal of Electrical and Computer Engineering (IJECE)*, 11(1), 114-123.
9. Murthy, G. V. K., & Sivanagaraju, S. (2012). S. Satyana rayana, B. Hanumantha Rao," Voltage stability index of radial distribution networks with distributed generation,". *Int. J. Electr. Eng*, 5(6), 791-803.

10. Anuja, P. S., Kiran, V. U., Kalavathi, C., Murthy, G. N., & Kumari, G. S. (2015). Design of elliptical patch antenna with single & double U-slot for wireless applications: a comparative approach. *International Journal of Computer Science and Network Security (IJCSNS)*, 15(2), 60.
11. Siva Prasad, B. V. V., Mandapati, S., Kumar Ramasamy, L., Boddu, R., Reddy, P., & Suresh Kumar, B. (2023). Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc networks. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, 64(3), 658-671.
12. Siva Prasad, B. V. V., Sucharitha, G., Venkatesan, K. G. S., Patnala, T. R., Murari, T., & Karanam, S. R. (2022). Optimisation of the execution time using hadoop-based parallel machine learning on computing clusters. In *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021* (pp. 233-244). Singapore: Springer Nature Singapore.
13. Prasad, B. V., & Ali, S. S. (2017). Software-defined networking based secure routing in mobile ad hoc network. *International Journal of Engineering & Technology*, 7(1.2), 229.
14. Elechi, P., & Onu, K. E. (2022). Unmanned Aerial Vehicle Cellular Communication Operating in Non-terrestrial Networks. In *Unmanned Aerial Vehicle Cellular Communications* (pp. 225-251). Cham: Springer International Publishing.
15. Prasad, B. V. V. S., Mandapati, S., Haritha, B., & Begum, M. J. (2020, August). Enhanced Security for the authentication of Digital Signature from the key generated by the CSTRNG method. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1088-1093). IEEE.
16. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Veeneetha, S. V., Srivalli, N., ... & Sahitya, D. (2022, November). Prediction of Flight-fare using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 134-138). IEEE.
17. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Bhargavi, P. J., Alekhya, A., ... & Nandini, K. (2022, November). Cardiovascular Disease Prediction using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 60-66). IEEE.
18. Mukiri, R. R., Kumar, B. S., & Prasad, B. V. V. (2019, February). Effective Data Collaborative Strain Using RecTree Algorithm. In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM)*, Amity University Rajasthan, Jaipur-India.
19. Rao, B. T., Prasad, B. V. V. S., & Peram, S. R. (2019). Elegant Energy Competent Lighting in Green Buildings Based on Energetic Power Control Using IoT Design. In *Smart Intelligent Computing and Applications: Proceedings of the Second International Conference on SCI 2018, Volume 1* (pp. 247-257). Springer Singapore.
20. Someswar, G. M., & Prasad, B. V. V. S. (2017, October). USVGM protocol with two layer architecture for efficient network management in MANET'S. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 738-741). IEEE.
21. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, 13(2), 2749-2757.
22. Balram, G., Poornachandrarao, N., Ganesh, D., Nagesh, B., Basi, R. A., & Kumar, M. S. (2024, September). Application of Machine Learning Techniques for Heavy Rainfall Prediction using Satellite Data. In *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1081-1087). IEEE.
23. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
24. KATIKA, R., & BALRAM, G. (2013). Video Multicasting Framework for Extended Wireless Mesh Networks Environment. *pp-427-434, IJSRET*, 2(7).
25. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, 7(2), 01-12.
26. Prasad, P. S., & Rao, S. K. M. (2017). A Survey on Performance Analysis of Manets Under Security Attacks. *network*, 6(7).
27. Reddy, P. R. S., & Ravindranath, K. (2024). Enhancing Secure and Reliable Data Transfer through Robust Integrity. *Journal of Electrical Systems*, 20(1s), 900-910.
28. REDDY, P. R. S., & RAVINDRANATH, K. (2022). A HYBRID VERIFIED RE-ENCRYPTION INVOLVED PROXY SERVER TO ORGANIZE THE GROUP DYNAMICS: SHARING AND REVOCATION. *Journal of Theoretical and Applied Information Technology*, 100(13).
29. Reddy, P. R. S., Ram, V. S. S., Greshma, V., & Kumar, K. S. Prediction of Heart Healthiness.
30. Reddy, P. R. S., Reddy, A. M., & Ujwala, B. IDENTITY PRESERVING IN DYNAMIC GROUPS FOR DATA SHARING AND AUDITING IN CLOUD.

31. Madhuri, K., Viswanath, N. K., & Gayatri, P. U. (2016, November). Performance evaluation of AODV under Black hole attack in MANET using NS2. In *2016 international conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-3). IEEE.
32. Kooroor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
33. Rao, N. R., Kooroor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7 S).
34. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, 255.
35. DASTAGIRIAH, D. (2024). A SYSTEM FOR ANALYSING CALL DROP DYNAMICS IN THE TELECOM INDUSTRY USING MACHINE LEARNING AND FEATURE SELECTION. *Journal of Theoretical and Applied Information Technology*, *102*(22).
36. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiriah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
37. Sudhakar, R. V., Dastagiriah, C., Patterm, S., & Bhukya, S. (2024). Multi-Objective Reinforcement Learning Based Algorithm for Dynamic Workflow Scheduling in Cloud Computing. *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, *12*(3), 640-649.
38. PushpaRani, K., Roja, G., Anusha, R., Dastagiriah, C., Srilatha, B., & Manjusha, B. (2024, June). Geological Information Extraction from Satellite Imagery Using Deep Learning. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.
39. Sravan, K., Rao, L. G., Ramineni, K., Rachapalli, A., & Mohmmad, S. (2024). Analyze the Quality of Wine Based on Machine Learning Approach Check for updates. *Data Science and Applications: Proceedings of ICDSA 2023, Volume 3*, 820, 351.
40. Chandhar, K., Ramineni, K., Ramakrishna, E., Ramana, T. V., Sandeep, A., & Kalyan, K. (2023, December). Enhancing Crop Yield Prediction in India: A Comparative Analysis of Machine Learning Models. In *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)* (pp. 1-4). IEEE.
41. Ramineni, K., Shankar, K., Shabana, Mahender, A., & Mohmmad, S. (2023, June). Detecting of Tree Cutting Sound in the Forest by Machine Learning Intelligence. In *International Conference on Power Engineering and Intelligent Systems (PEIS)* (pp. 303-314). Singapore: Springer Nature Singapore.
42. Ashok, J., RAMINENI, K., & Rajan, E. G. (2010). BEYOND INFORMATION RETRIEVAL: A SURVEY. *Journal of Theoretical & Applied Information Technology*, *15*.
43. Sekhar, P. R., & Sujatha, B. (2020, July). A literature review on feature selection using evolutionary algorithms. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-8). IEEE.
44. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng.*, *11*, 503-512.
45. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*(Special Issue 1).
46. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
47. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, *17*(4), 1265-1282.
48. Amarnadh, V., & Moparthi, N. R. (2024). Prediction and assessment of credit risk using an adaptive Binarized spiking marine predators' neural network in financial sector. *Multimedia Tools and Applications*, *83*(16), 48761-48797.
49. Amarnadh, V., & Moparthi, N. R. (2024). Range control-based class imbalance and optimized granular elastic net regression feature selection for credit risk assessment. *Knowledge and Information Systems*, 1-30.
50. Amarnadh, V., & Akhila, M. (2019, May). RETRACTED: Big Data Analytics in E-Commerce User Interest Patterns. In *Journal of Physics: Conference Series* (Vol. 1228, No. 1, p. 012052). IOP Publishing.
51. Selvan, M. Arul, and S. Miruna Joe Amali. "RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE." (2024).
52. Selvan, M. Arul. "Fire Management System For Industrial Safety Applications." (2023).

53. Selvan, M. A. (2023). A PBL REPORT FOR CONTAINMENT ZONE ALERTING APPLICATION.
54. Selvan, M. A. (2023). CONTAINMENT ZONE ALERTING APPLICATION A PROJECT BASED LEARNING REPORT.
55. Selvan, M. A. (2021). Robust Cyber Attack Detection with Support Vector Machines: Tackling Both Established and Novel Threats.
56. Selvan, M. A. (2023). INDUSTRY-SPECIFIC INTELLIGENT FIRE MANAGEMENT SYSTEM.
57. Selvan, M. Arul. "PHISHING CONTENT CLASSIFICATION USING DYNAMIC WEIGHTING AND GENETIC RANKING OPTIMIZATION ALGORITHM." (2024).
58. Selvan, M. Arul. "Innovative Approaches in Cardiovascular Disease Prediction Through Machine Learning Optimization." (2024).
59. Reddy, B. R., & Adilakshmi, T. (2023). Proof-of-Work for Merkle based Access Tree in Patient Centric Data. *structure*, 14(1).
60. Reddy, B. R., Adilakshmi, T., & Kumar, C. P. (2020). Access Control Methods in Cloud Enabled the Cloud-Enabled Internet of Things. In *Managing Security Services in Heterogenous Networks* (pp. 1-17). CRC Press.
61. Reddy, M. B. R., Akhil, V., Preetham, G. S., & Poojitha, P. S. (2019). Profile Identification through Face Recognition.
62. Meghanareddy, K., Reddy, R., & Murthy, V. A Privacy Preserving Multi Owner Secure Search in Cloud Computing.
63. Kumar, R. V., Reddy, B. R., & Battula, S. K. (2012). EFFICIENT USAGE OF INFRASTRUCTURE CLOUDS.
64. Aydın, Ö., Karaarslan, E., & Gökçe Narin, N. (2023). Artificial intelligence, vr, ar and metaverse technologies for human resources management. *VR, AR and Metaverse Technologies for Human Resources Management (June 15, 2023)*.
65. Dutta, P. K., Naskar, M. K., & Mishra, O. P. (2012). Test of strain behavior model with radon anomaly in seismogenic area: A Bayesian melding approach. *International Journal of Geosciences*, 3(01), 126.
66. Dutta, P. K., Mallikarjuna, K., & Satish, A. (2017, September). Sensor based solar tracker system using electronic circuits for moisture detection and auto-irrigation. In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)* (pp. 1475-1478). IEEE.
67. Dutta, P. K., Mishra, O. P., & Naskar, M. K. (2013). A review of operational earthquake forecasting methodologies using linguistic fuzzy rule-based models from imprecise data with weighted regression approach.
68. Lokhande, M., Kalpanadevi, D., Kate, V., Tripathi, A. K., & Bethapudi, P. (2023). Study of Computer Vision Applications in Healthcare Industry 4.0. In *Healthcare Industry 4.0* (pp. 151-166). CRC Press.
69. Tripathi, A. K., Soni, R., & Verma, S. (2022). A review on ethnopharmacological applications, pharmacological activities, and bioactive compounds of *Mimosa pudica* (linn.). *Research Journal of Pharmacy and Technology*, 15(9), 4293-4299.
70. Mishra, S., Grewal, J., Wal, P., Bhivshet, G. U., Tripathi, A. K., & Walia, V. (2024). Therapeutic potential of vasopressin in the treatment of neurological disorders. *Peptides*, 174, 171166.
71. Koliqi, R., Fathima, A., Tripathi, A. K., Sohi, N., Jesudasan, R. E., & Mahapatra, C. (2023). Innovative and Effective Machine Learning-Based Method to Analyze Alcoholic Brain Activity with Nonlinear Dynamics and Electroencephalography Data. *SN Computer Science*, 5(1), 113.
72. Tripathi, A. K., Diwedi, P., Kumar, N., Yadav, B. K., & Rathod, D. (2022). *Trigonella Foenum Grecum* L. Seed (Fenugreek) Pharmacological Effects on Cardiovascular and Stress Associated Disease. *NeuroQuantology*, 20(8), 4599.
73. Biswas, D., Sharma, G., Pandey, A., Tripathi, A. K., Pandey, A., & Sahu, P. & Chauhan, P. (2022). Magnetic Nanosphere: Promising approach to deliver the drug to the site of action. *NeuroQuantology*, 20(11), 4038.
74. Parganiha, R., Tripathi, A., Prathyusha, S., Baghel, P., Lanjhiyana, S., & Lanjhiyana, S. & Sarkar, D. (2022). A review of plants for hepatic disorders. *J. Complement. Med. Res*, 13(46), 10-5455.
75. Tripathi, A. K., Dwivedi, C. P., Bansal, P., Pradhan, D. K., Parganiha, R., & Sahu, D. An Ethnoveterinary Important Plant Terminalia Arjuna. *International Journal of Health Sciences*, (II), 10601-10607.
76. Babbar, R., Kaur, A., Vanya, Arora, R., Gupta, J. K., Wal, P., ... & Behl, T. (2024). Impact of Bioactive Compounds in the Management of Various Inflammatory Diseases. *Current Pharmaceutical Design*, 30(24), 1880-1893.
77. Parganiha, R., Tripathi, A., Prathyusha, S., Baghel, P., Lanjhiyana, S., Lanjhiyana, S., ... & Sarkar, D. (2022). A review of plants for hepatic disorders. *J. Complement. Med. Res*, 13(46), 10-5455.
78. Sahu, A., Mishra, S., Wal, P., Debnath, B., Chouhan, D., Gunjal, S. D., & Tripathi, A. K. (2024). Novel Quinoline-Based RAF Inhibitors: A Comprehensive Review on Synthesis, SAR and Molecular Docking Studies. *ChemistrySelect*, 9(23), e202400347.
79. Habeeb, M., Vengateswaran, H. T., Tripathi, A. K., Kumbhar, S. T., & You, H. W. (2024). Enhancing

- biomedical imaging: the role of nanoparticle-based contrast agents. *Biomedical Microdevices*, 26(4), 1-18.
80. Sinha, S., Tripathi, A. K., Pandey, A., Naik, P., Pandey, A., & Verma, V. S. (2024). Self-Assembled PEGylated Micelles for Precise and Targeted Drug Delivery: Current Challenges and Future Directions. *Biocatalysis and Agricultural Biotechnology*, 103296.
 81. Sahu, P., Sharma, G., Verma, V. S., Mishra, A., Deshmukh, N., Pandey, A., ... & Chauhan, P. (2022). Statistical optimization of microwave assisted acrylamide grafting of *Linum usitatissimum* Gum. *NeuroQuantology*, 20(11), 4008.
 82. Tripathi, A. K., Sharma, N., Mishra, J., Bisoi, D., Mohapatra, N., Muztaba, M. M., ... & TarakaRamarao, C. (2023). EVALUATION OF ANTI-INFLAMMATORY ACTIVITY OF PLANT EXTRACT OF *CORDIA DICHOTOMA* LEAVES ON CARRAGEENAN-INDUCED PAW EDEMA IN ALBINO WISTER RATS AND ITS PHYTOCHEMICAL ANALYSIS. *Ann. For. Res*, 66(1), 803-818.
 83. Vasista, T. G. K. (2017). Towards innovative methods of construction cost management and control. *Civ Eng Urban Plan: Int J*, 4, 15-24.
 84. Vasista, T. G. K. (2012). Quality Management System for Contemporary Public Administration: A case study of e-Governance. *Journal of Public Administration and Governance*, 2(4), 164-177.
 85. Vasista, T. G. (2018). SaaS Based E-Court Applications in E-Governance in India. *International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT) Vol*, 9.
 86. Al Sudairi, M. A. T., & Vasista, T. G. (2013). Achieving process standardization in digital society with 'ASCP model'. *Journal of Supply Chain and Customer Relationship Management*, 2013, 1.
 87. Vasista, T. G. K., & AlAbdullatif, A. M. (2017). Role of electronic customer relationship management in demand chain management: A predictive analytic approach. *International Journal of Information Systems and Supply Chain Management (IJISSCM)*, 10(1), 53-67.
 88. Vasista, T. G., & AlSudairi, M. A. T. (2018). Managing through computer aided quality control in oil & natural gas industry project sites. *Journal of Advanced Research in Dynamical and Control Systems*, 10(4), 896-905.
 89. Algharabat, R. S., Zamil, A. M., & Vasista, T. G. K. (2015). The influence of retailer enterprise marketing information system on bullwhip effect. *International Journal of Business and Management*, 10(3), 237.
 90. AlSudairi, M. A., & Vasista, T. G. K. (2012). Design of strategic business model for electronic enterprise in digital society. *International Journal of Digital Society*, 3(3-4), 690-697.
 91. AlSudairi, M. A., & Vasista, T. G. K. (2012, June). Model for value creation and action generation of an electronic enterprise in a knowledge based economy. In *International Conference on Information Society (i-Society 2012)* (pp. 174-180). IEEE.
 92. Vasista, T. G., & Zamil, A. M. (2023). Role of metaverse in the fourth industrial revolution for providing customer experiences. In *How the Metaverse Will Reshape Business and Sustainability* (pp. 155-169). Singapore: Springer Nature Singapore.
 93. Hsu, H. Y., Hwang, M. H., & Chiu, Y. S. P. (2021). Development of a strategic framework for sustainable supply chain management. *AIMS Environmental Science*, (6).
 94. AlSudairi, M., Vasista, T. G., Zamil, A. M., & Algharabat, R. S. (2012). Mitigating the Bullwhip Effect with eWord Of Mouth: eBusiness Intelligence Perspective. *International Journal of Managing Value and Supply Chains*, 3(4), 27.
 95. Vasista, T. G. K., & AlSudairi, M. A. (2013). Service-oriented architecture (SOA) and semantic web services for web portal integration. In *Advances in Computing and Information Technology: Proceedings of the Second International Conference on Advances in Computing and Information Technology (ACITY) July 13-15, 2012, Chennai, India-Volume 2* (pp. 253-261). Berlin, Heidelberg: Springer Berlin Heidelberg.
 96. AlSudairi, M. A., & Tatapudi, G. (2014). Social innovation: Can it be a strategy for influencing GCC public welfare?. *Innovation*, 16(2), 273-282.
 97. Bhat, S. (2015). Technology for Chemical Industry Mixing and Processing. *Technology*, 2(2).
 98. Bhat, S. (2024). Building Thermal Comforts with Various HVAC Systems and Optimum Conditions.
 99. Bhat, S. (2020). Enhancing Data Centre Energy Efficiency with Modelling and Optimisation of End-To-End Cooling.
 100. Bhat, S. (2016). Improving Data Centre Energy Efficiency with End-To-End Cooling Modelling and Optimisation.
 101. Bhat, S. (2015). Deep Reinforcement Learning for Energy-Saving Thermal Comfort Management in Intelligent Structures.
 102. Bhat, S. (2015). Design and Function of a Gas Turbine Range Extender for Hybrid Vehicles.
 103. Bhat, S. (2023). Discovering the Attractiveness of Hydrogen-Fuelled Gas Turbines in Future Energy Systems.
 104. Bhat, S. (2019). Data Centre Cooling Technology's Effect on Turbo-Mode Efficiency.

105. Bhat, S. (2018). The Impact of Data Centre Cooling Technology on Turbo-Mode Efficiency.
106. Arora, P., & Bhardwaj, S. (2021). Methods for Threat and Risk Assessment and Mitigation to Improve Security in the Automotive Sector. *Methods*, 8(2).
107. Arora, P., & Bhardwaj, S. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems.
108. Arora, P., & Bhardwaj, S. (2019). The Suitability of Different Cybersecurity Services to Stop Smart Home Attacks.
109. Arora, P., & Bhardwaj, S. (2017). A Very Safe and Effective Way to Protect Privacy in Cloud Data Storage Configurations.
110. Kumar, T. V. (2024). A Comparison of SQL and NO-SQL Database Management Systems for Unstructured Data.
111. Kumar, T. V. (2024). A Comprehensive Empirical Study Determining Practitioners' Views on Docker Development Difficulties: Stack Overflow Analysis.
112. Kumar, T. V. (2024). Developments and Uses of Generative Artificial Intelligence and Present Experimental Data on the Impact on Productivity Applying Artificial Intelligence that is Generative.
113. Kumar, T. V. (2024). A New Framework and Performance Assessment Method for Distributed Deep Neural Network Based Middleware for Cyberattack Detection in the Smart IoT Ecosystem.
114. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
115. Sharma, S., & Dutta, N. (2016). Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
116. Sakshi, S. (2023). Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications.
117. Madar, B., Kumar, G. K., & Ramakrishna, C. (2017). Captcha breaking using segmentation and morphological operations. *International Journal of Computer Applications*, 166(4), 34-38.
118. Naik, R., Rao, P. R., & Madar, B. (2016). Cleaning of sensitive data in the cloud using Monitoring as a service. *International Journal of Computing*, 5(3).
119. Rani, M. S., & Dorthi, K. (2022, June). An Empirical Study on Package Query Processing System using Parallel Processing Mechanisms. In *2022 7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 1571-1575). IEEE.
120. Reddy, T., Prasad, T. S. D., Swetha, S., Nirmala, G., & Ram, P. (2018). A study on antiplatelets and anticoagulants utilisation in a tertiary care hospital. *International Journal of Pharmaceutical and Clinical Research*, 10, 155-161.
121. Shakeel, M., Rao, C. L., Prasad, T. S., Alam, T., Rawat, N., & Kavitha, R. (2023, May). An examination of cybersecurity threats and authentication systems. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2727-2731). IEEE.
122. Teegala, S. P., Vijai, C., Nagpal, A., Anuradha, R., Aljbori, A., & Swathi, B. (2023, December). Enhanced Authentication Methods for Access and Control Management in Cloud Computing. In *2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)* (Vol. 10, pp. 1673-1677). IEEE.
123. Teegala, S. P., & Rao, C. G. (2022, March). A Novel Authentication Mechanism for SecureData Access based on Encryption Key Sharing for Cloud Web Application. In *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)* (Vol. 1, pp. 1890-1897). IEEE.
124. Viswanatha, V., Ramachandra, A. C., Prasanna, R. R., Kakarla, P. C., Simha, P. V., & Mohan, N. (2022). *Implementation of Tiny Machine Learning Models on Arduino 33-BLE for Gesture and Speech Recognition* (No. 8495). EasyChair.
125. Prasanna, R., Kakarla, P. C., PJ, V. S., & Mohan, N. (2022). Implementation of tiny machine learning models on arduino 33 ble for gesture and speech recognition. *arXiv preprint arXiv:2207.12866*.
126. AC, R., Chowdary Kakarla, P., Simha PJ, V., & Mohan, N. (2022). Implementation of Tiny Machine Learning Models on Arduino 33-BLE for Gesture and Speech Recognition. AC, R., Chowdary Kakarla, P., Simha PJ, V., & Mohan, N. (2022). Implementation of Tiny Machine Learning Models on Arduino 33-BLE for Gesture and Speech Recognition.
127. Pabba, C., & Kumar, P. (2022). An intelligent system for monitoring students' engagement in large classroom teaching through facial expression recognition. *Expert Systems*, 39(1), e12839.
128. Pabba, C., Bhardwaj, V., & Kumar, P. (2024). A visual intelligent system for students' behavior classification using body pose and facial features in a smart classroom. *Multimedia Tools and Applications*, 83(12), 36975-37005.
129. Reddy, A. S., Chakradhar, P., & Santosh, T. (2018). Demand forecasting and demand supply management of vegetables in India: a review and prospect. *Int J Comput Technol*, 17(1), 7170-7178.
130. Pabba, C., & Kumar, P. (2024). A vision-based multi-cues approach for individual students' and overall class engagement monitoring in smart classroom environments. *Multimedia Tools and Applications*, 83(17), 52621-52652.

131. Nagaraj, P., Banala, R., & Prasad, A. K. (2021, August). Real time face recognition using effective supervised machine learning algorithms. In *Journal of Physics: Conference Series* (Vol. 1998, No. 1, p. 012007). IOP Publishing.
132. Nagaraj, P., Prasad, A. K., Narsimha, V. B., & Sujatha, B. (2022). Swine flu Detection and Location using Machine Learning Techniques and GIS. *International Journal of Advanced Computer Science and Applications*, 13(9).
133. Nagaraj, P., Phebe, G. S., & Singh, A. (2021, November). A Novel Technique to Classify Face Mask for Human Safety. In *2021 Sixth International Conference on Image Information Processing (ICIIP)* (Vol. 6, pp. 235-239). IEEE.
134. Nagaraj, P., Prasad, D. A. K., Dass, D. M. V., & Kumar, K. R. (2022). Swine Flu Hotspot Prediction In Regions Based on Dynamic Hotspot Detection Algorithm. *Journal of Theoretical and Applied Information Technology (JATIT)*, 30.
135. Priyanka, J. H., & Parveen, N. (2022). Online employment portal architecture based on expert system. *Indones. J. Electr. Eng. Comput. Sci*, 25(3), 1731-1735.
136. Priyanka, J. H., & Parveen, N. (2024). DeepSkillNER: an automatic screening and ranking of resumes using hybrid deep learning and enhanced spectral clustering approach. *Multimedia Tools and Applications*, 83(16), 47503-47530.
137. Jammalamadaka, S. B., Duvvuri, B. K., Jammalamadaka, K. S., & Priyanka, J. H. (2019). Automating WEB interface in relation to user behaviour. In *First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018* (pp. 91-102). Springer Singapore.
138. Sathish, S., Thangavel, K., & Boopathi, S. (2011). Comparative analysis of DSR, FSR and ZRP routing protocols in MANET. In *International Conference on Information and Network Technology IPCSIT vol* (Vol. 4).
139. Sathish, S., Thangavel, K., & Boopathi, S. (2010). Performance analysis of DSR, AODV, FSR and ZRP routing protocols in MANET. *MES Journal of Technology and Management*, 57-61.
140. Murali, V., & Boopathi, S. (2014). A Comparative Analysis of Various Segmentation Techniques in Brain Tumor Image. *International Journal of Application or Innovation in Engineering & Management (IJAIEEM)*, ISSN, 2319-4847.
141. Balaraju, J., & Prasada Rao, P. V. R. D. (2019). Designing authentication for Hadoop Cluster using DNA algorithm. *Int. J. Recent. Technol. Eng. (IJRTE)*, 8(3).
142. Balaraju, J., & Prasada Rao, P. V. R. D. (2020). Innovative secure authentication interface for Hadoop cluster using DNA cryptography: A practical study. In *Soft Computing and Signal Processing: Proceedings of 2nd ICSCSP 2019 2* (pp. 17-29). Springer Singapore.
143. Balaraju, J., & Prasada Rao, P. V. R. D. (2018). Recent advances in big data storage and security schemas of HDFS: a survey. *Journal of Engineering Technology. Special Issue (Emerging Trends in Engineering Technology)*, 118(24), 132-138.
144. Balaraju, J., & Prasada Rao, P. V. R. D. (2020). Investigation and finding a DNA cryptography layer for securing data in Hadoop cluster. *Int. J. Advance Soft Comput. Appl*, 12(3).