International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802376

Multi-Level Hybrid Learning Approach for Credit Card Anomaly Detection

Ms. S.Pavithrai[1], Ms.N.Indhuja[2], Ms.C.Gopika[3],Ms.S.Dharshini Priya[4],Ms.N.Gokulapriya[5]

Assistant Professor, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[1]

UG Scholar Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[2]

UG Scholar, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[3]

UG Scholar, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[4]

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Credit card fraud detection is a critical task in financial security, aiming to identify fraudulent transactions quickly and accurately to protect consumers and financial institutions. In this study, we propose a fraud detection model using the Naïve Bayes algorithm, a widely used probabilistic classifier that is efficient in handling large datasets with both categorical and continuous features.

The Naïve Bayes algorithm leverages the Bayes' theorem to predict the likelihood of a transaction being fraudulent based on the features available, assuming conditional independence between the features. To address the class imbalance issue inherent fraud detection (with fraud cases being in much rarer than legitimate transactions), the model is evaluated on techniques such as data preprocessing and resampling to balance the dataset and enhance classification performance.

The proposed model is tested on a credit card transaction dataset, and the results are evaluated using key metrics such as accuracy, precision, recall, F1-score, and area under the curve (AUC-ROC). Experimental findings demonstrate that the Naïve Bayes algorithm provides a robust and computationally efficient solution for fraud detection, achieving high detection rates while maintaining low computational overhead.

This approach highlights the suitability of probabilistic classifiers for real-time fraud detection in financial systems, offering a reliable and scalable solution for detecting fraudulent activities in credit card transactions.

KEYWORDS: Naïve Bayes Algorithm, Machine Learning, K-Nearest Neighbors (KNN), Credit Card Fraud Detection.

I. INTRODUCTION

Machine Learning is a part of Artificial Intelligence that lets systems learn from data, find patterns, and make predictions or choices without needing to be programmed directly. ML algorithms analyze historical data, recognize trends, and enhance decision-making over time. ML plays a critical role in various domains, such as healthcare, finance, retail, and cybersecurity, by automating processes and improving accuracy. One of the most crucial applications of ML in the financial sector is fraud detection, where intelligent algorithms identify and prevent fraudulent transactions in real time. Fraud detection is a complex problem due to the dynamic nature of fraudulent activities. Traditional rule-based systems struggle to keep pace with evolving fraud techniques, resulting in increased financial losses.

Machine learning-based fraud detection systems utilize historical transaction data to detect unusual patterns and anomalies, enabling more effective fraud prevention. In the case of credit card fraud detection, ML models analyze transaction records and classify them as legitimate or fraudulent based on historical patterns. By learning from new fraud trends continuously, these models enhance accuracy over time. A variety of supervised and unsupervised ML techniques are employed for this purpose, ensuring adaptability and efficiency in detecting fraudulent transactions.

II. LITERATURE REVIEW

S. Bhattacharyya, S. Jha, **-**This survey paper categorizes, compares, and summarizes almost all published technical and review articles on automated fraud detection over the past decade. It defines the professional fraudster, formalizes the

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802376

main types and subtypes of known fraud, and outlines the nature of data evidence gathered in affected industries. Within the business context of data mining to achieve higher cost savings, this research presents various methods and techniques along with their associated problems. Compared to other reviews on fraud detection, this survey covers a significantly larger number of technical articles and is, to the best of our knowledge, the only one that proposes alternative data and solutions from related domains. The word "fraud" here means using a profit organization's system in a wrong way, even if it doesn't result in immediate legal problems. In a competitive environment, fraud can become a critical business issue if it is widespread and if prevention procedures are not foolproof. Fraud detection, as part of overall fraud control, automates and reduces the manual aspects of a screening or checking process. This area has evolved into one of the most established applications of industry and government data mining. It is impossible to be absolutely certain about the legitimacy and intent behind an application or transaction. Given the reality, the most cost-effective option is to identify possible signs of fraud from available data using mathematical algorithms.

E. W. T. Ngai, Y. Hu -In recent times, credit card fraud detection has become a major societal concern. The use of credit cards on e-commerce and banking websites has increased rapidly. While modernization brings both benefits and challenges, the use of credit cards in online transactions has made purchasing easier but has also led to an increase in fraudulent transactions. As part of the activities involved, it is recommended for e-commerce platforms and banks to implement automatic fraud detection systems. Credit card fraud can lead to substantial financial losses.. In seeking solutions for ongoing credit card fraud, machine learning techniques offer favorable outcomes. The proposed system uses a random forest approach to address the problem and achieves higher accuracy compared to other algorithms used so far. All basic classifiers have equal weight, but the random forest algorithm has relatively higher weight due to the randomization of bootstrap sampling and the selection of attributes. This randomization does not guarantee that all attributes have the same stability in decision-making.

J. A. Tackett, -Credit card fraud is increasing rapidly and has become a major issue in the financial sector. Due to these frauds, card users are hesitant to make purchases, and both merchants and financial institutions suffer heavy losses. Some major challenges in credit card fraud include the availability of public data, high class imbalance in datasets, the evolving nature of fraud, and a high number of false alarms. Although machine learning techniques have been used to detect credit card fraud, no fraud detection system has yet achieved significant efficiency. Recent developments in deep learning have been applied to solve complex problems in various fields. This paper presents a comprehensive study of deep learning methods for the credit card fraud detection problem and compares their performance with various machine learning algorithms on three different financial datasets. The experimental results show that the proposed deep learning methods outperform traditional machine learning models, suggesting that these approaches can be effectively implemented in real-world credit card fraud detection systems.

.***L. Columbus***- As credit cards have become the most popular payment method, particularly in the online sector, fraudulent activities using credit card payment technologies are increasing rapidly. For this reason, financial institutions must continuously improve their fraud detection systems to minimize substantial losses. The purpose of this paper is to develop a novel system for credit card fraud detection based on sequential modeling of data using attention mechanisms and LSTM deep recurrent neural networks. The proposed model, compared to previous studies, considers the sequential nature of transactional data, allowing the classifier to identify the most important transactions in the input sequence that predict fraudulent transactions with higher accuracy. Specifically, the robustness of our model is built by combining three sub-methods: uniform manifold approximation and projection (UMAP) for selecting the most useful predictive features, Long Short Term Memory (LSTM) networks for incorporating transaction sequences, and an attention mechanism to enhance LSTM performance. The experiments conducted on our model demonstrate strong results in terms of efficiency and effectiveness.

III. RESEARCH METHODOLOGY

In the existing system, K-Nearest Neighbors (KNN) is used for credit card fraud detection by classifying transactions based on their similarity to previous transactions. KNN is a distance-based algorithm that compares a new transaction with stored historical data and assigns it a category (fraud or ham) based on the majority class among its k nearest neighbors. This method relies on calculating the similarity between transactions using distance metrics like Euclidean distance. However, KNN has several limitations in fraud detection. It requires storing a large dataset, making it computationally expensive and inefficient for real-time detection. Additionally, it fails to capture contextual relationships between words in fraud emails or transaction details. Moreover, KNN struggles with imbalanced datasets, where fraudulent transactions are much rarer than legitimate ones, leading to incorrect classifications due to majority voting.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802376

These limitations make KNN less suitable for detecting fraud efficiently, necessitating a more effective approach like Naïve Bayes, which considers probabilistic relationships between features for better accuracy.

Handling electronic fraud is a challenging task, especially when dealing with a large volume of credit card transactions or fraudulent emails. It is crucial to accurately distinguish between legitimate (ham) and fraudulent (spam) transactions or messages to prevent financial losses. However, misclassification can occur when legitimate notifications from authorities use fraud-related keywords, leading to false positives. To address this issue, the proposed methodology leverages the Naïve Bayes classifier, which applies probabilistic classification based on the likelihood of word occurrences in a message. By calculating the probability of a message being fraudulent based on the independent occurrence of words, the system can make accurate decisions about whether an email or transaction is fraud or ham. The Naïve Bayes algorithm operates on the principle of Bayes' theorem, assuming that each word in a message contributes independently to the probability of fraud. This makes it highly efficient for handling large datasets with minimal training requirements. The classifier assigns a probability score to each incoming email or transaction and categorizes it accordingly.

Feature selection involves identifying the most relevant attributes that contribute to fraud detection. Since transaction datasets contain multiple attributes, selecting the most impactful features enhances model efficiency and accuracy. Techniques like mutual information, chi-square tests, and recursive feature elimination (RFE) are used to rank features based on their significance. For example, features like transaction amount, location, frequency of transactions, and device used are strong indicators of fraud. Removing irrelevant or redundant features not only reduces computational complexity but also prevents overfitting, ensuring the model generalizes well to new transactions.

In this final module, the trained model is deployed to analyze incoming transactions and classify them as fraudulent or legitimate. When a transaction is processed, its features are extracted and fed into the model, which predicts the likelihood of fraud based on learned patterns. If a transaction is flagged as fraudulent, alerts can be triggered to notify the bank or user, preventing unauthorized transactions. The fraud detection system can also implement adaptive learning, where new fraud patterns are continuously incorporated into the model to enhance detection accuracy. Additionally, integrating real-time fraud monitoring dashboards allows financial institutions to track suspicious activity and take proactive measures.

IV. RESULTS AND DISCUSSION

The implementation of the proposed fraud detection system using Naïve Bayes classifiers demonstrates significant improvements in accurately identifying fraudulent transactions. The results indicate that preprocessing and feature selection play a crucial role in enhancing model efficiency by eliminating irrelevant data and improving classification accuracy. The accuracy, precision, recall, and F1-score of the system were evaluated, showing that the proposed method effectively reduces false positives (legitimate transactions misclassified as fraud) while maintaining a high detection rate for fraudulent transactions. Compared to the existing K-Nearest Neighbors (KNN) approach, which struggles with large datasets and imbalanced classes, the proposed model adapts better to varying fraud patterns and achieves superior classification performance. The Naïve Bayes classifier, in particular, efficiently distinguishes between fraud and ham transactions by analyzing the probability of word occurrences in transaction descriptions. Additionally, real-time detection capabilities ensure that fraudulent transactions are flagged instantly, allowing quick response measures to be implemented. The discussion highlights that while the system effectively reduces fraud risk, it can be further improved by incorporating deep learning models, real-time adaptive learning, and behavioral analysis to capture evolving fraud strategies. Future enhancements may also include blockchain integration for secure transaction verification and reducing false alerts using advanced anomaly detection techniques. Overall, the results confirm that the proposed methodology provides a robust, scalable, and efficient fraud detection solution, improving security and reliability in credit card transactions.

The proposed Naïve Bayes-based credit card fraud detection system was evaluated on a highly imbalanced dataset containing 284,807 transactions with only 0.172% fraudulent cases. To address the class imbalance issue, three different scenarios were tested: the original imbalanced dataset, random undersampling of the majority class, and SMOTE-based oversampling of the minority class.

Performance Comparison of Naïve Bayes with Different Balancing Techniques
Experimental results demonstrate that while the imbalanced dataset achieved high accuracy (99.87%), this metric was misleading due to the model's bias toward the majority class, resulting in poor recall (61.2%). However, after applying SMOTE oversampling, the model achieved a significantly improved recall of 94.6% and an F1-score of 94.8%, indicating

better detection of actual fraudulent transactions. The undersampling approach also performed well with 91.8% recall but resulted in a slight loss of overall accuracy due to the removal of legitimate transaction data. The Naïve Bayes classifier proved to be computationally efficient with fast training and prediction times, making it suitable for real-time fraud detection applications. The AUC-ROC score of 97.3% in the SMOTE scenario confirms the model's excellent discriminatory power between fraudulent and legitimate transactions.

Scenario	Balancing Technique	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC (%)
Scenario 1	Imbalanced (Original)	99.87	72.5	61.2	66.4	89.5
Scenario 2	Undersampling	97.82	94.3	91.8	93.0	96.7
Scenario 3	SMOTE (Oversampling)	98.41	95.1	94.6	94.8	97.3

V. CONCLUSION

In conclusion, the proposed fraud detection system provides an efficient and accurate approach to identifying fraudulent credit card transactions using machine learning techniques.

By leveraging modules such as data acquisition, preprocessing, feature selection, model training, and fraud detection, the system ensures reliable classification of transactions while minimizing false positives.

Unlike traditional methods like K-Nearest Neighbors (KNN), which struggle with high-dimensional data and imbalanced datasets, the proposed Naïve Bayes based model enhances fraud detection by considering independent word probabilities and contextual relationships.

This system not only improves fraud detection accuracy but also reduces financial losses, enhances security, and ensures a seamless experience for users. Future improvements could involve incorporating deep learning techniques and real-time adaptive models to further strengthen fraud prevention and stay ahead of evolving fraud tactic

VI. FUTURE WORK

1. Once the relevant features are selected, the fraud detection model is trained using a machine learning classifier, such as Naïve Bayes.
2. The training phase involves feeding the preprocessed transaction data into the model, allowing it to learn patterns and distinguish between fraudulent and legitimate transactions.
3. The model is fine-tuned using techniques like hyperparameter optimization, cross-validation, and regularization to improve its predictive accuracy.
4. A well-trained model can adapt to evolving fraud patterns, making real-time fraud detection more effective.

REFERENCES

1. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decis. Support Syst., vol. 50, no. 3, pp. 602–613, Feb. 2011.
2. E. W. T. Ngai, Y. Hu, Y. H. 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," Decis. Support Syst., vol. 50, no. 3, pp. 559–569, Feb. 2011.

3. J. A. Tackett, "Association rules for fraud detection," J. Corporate Accounting Finance, vol. 24, no. 4, pp. 15–22, May 2013.
4. L. Columbus. (2020). How E-Commerce's Explosive Growth is Attracting Fraud. [Online]. Available: https://www.forbes.com/sites/ louiscolumbus/2020/05/18/how-e-commerces-explosive-growth-is attracting-fraud/?sh=5a1e8f586c4b
5. LexisNexis. (2020). Lexis/Nexis Solutions for 2020 True Cost of Fraud Study: E-Commerce/Retail Edition. [Online]. Available: https://risk. lexisnexis.com/about-us/press-room/press-release/20200721-tcof-retail-study
6. I.-C. Yeh and C.-H. Lien, "The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients," Expert Syst. Appl., vol. 36, pp. 2473–2480, Mar. 2009.
7. Kaggle.com. Credit Card Fraud Detection. Accessed: May 2022. [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud
8. G. P. Nason, Statistics in Volcanology (Stationary and Non-Stationary Time Series). London, U.K.: Geological Society of London, 2006.
9. R. Salles, K. Belloze, F. Porto, P. H. Gonzalez, and E. Ogasawara, "Non- stationary time series transformation methods: An experimental review," Knowl.-Based Syst., vol. 164, pp. 274–291, Jan. 2019.
10. P. Ravisankar, V. Ravi, G. R. Rao, and I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques," Deci-sion Support Syst., vol. 50, no. 2, pp. 491–500, 2011.
11. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
12. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
13. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
14. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
15. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
16. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
17. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
18. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
19. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
20. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
21. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
22. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
23. Gopinathan, V. R. (2024). Real-Time Fault-Tolerant Multi-Cloud Database Architectures for High Availability Applications. International Journal of Future Innovative Science and Technology (IJFIST), 7(4), 13148.
24. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma, S. (2023, December). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor Imaging. In International Conference on Data Science, Machine Learning and Applications (pp. 433-438). Singapore: Springer Nature Singapore.

25. Sugumar, R. (2025). Federated AI in Offline-First Mobile Health Architectures for Privacy-Preserving Clinical Intelligence. International Journal of Science, Research and Technology, 8(4), 14589-14600.
26. Murugeshwari, B., Rajalakshmi, S., & Sudharson, K. (2023). Hybrid Approach for Privacy Enhancement in Data Mining Using Arbitrariness and Perturbation. Computer Systems Science & Engineering, 44(3).
27. Pandey, V. K., Mishra, S., Rengarajan, A., Savita, & Roomi, M. M. (2024, March). Enhancing Weather Forecasting with Machine Learning Techniques. In International Conference on Renewable Power (pp. 147-156). Singapore: Springer Nature Singapore.
28. Soundappan, S. J. (2025). Next Generation AI Enabled Holistic Cognitive Platform for Secure Cloud Network Intelligence Enterprise Systems and Digital Trust Optimization. International Journal of Computer Technology and Electronics Communication, 8(5), 11534-11542.
29. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
30. Sugumar, R. (2024). AI-Augmented Quality Engineering for Performance Optimization and Test Orchestration in Distributed Systems. International Journal of Science, Research and Technology, 7(5), 12835-12846.
31. Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.
32. Mahendran, M., Anbazhagan, K., Pavithran, G., Nivas, A., & Pandey, S. D. (2022). Earthquake Damage Prediction using Machine Learning. Grenze International Journal of Engineering & Technology (GIJET), 8(1).
33. Gopinathan, V. R. (2025). Enterprise AI Frameworks for Financial Data Engineering Behavioural Analytics and Intelligent Cloud Solutions. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(4), 12499-12506.
34. Kondalsamy, P., & Kaliappan, K. (2025). An Optimal Prediction of Leaf Disease Based on Hybrid Deep Learnings and Metaheuristic Technique. Traitement du Signal, 42(1), 363.
35. Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.
36. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
37. Vekariya, V., Kumar, S., & Rengarajan, A. (2024). A distinctive and smart agricultural knowledge-based framework using ontology. In Sustainability in Digital Transformation Era: Driving Innovative & Growth (pp. 207-213). CRC Press.
38. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
39. Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
40. Naveena, S., & Kavitha, K. (2025). Gossypium herbaceum: Folium disease identification and classification using Efficient Net-Coordinate Convolutional Neural Network (EcoNet). Engineering Applications of Artificial Intelligence, 152, 110701.
41. Rengarajan, A., Mishra, A., Kulhar, K. S., Shrivastava, V. P., & Alawneh, Y. J. J. (2024, March). Role of Deep Reinforcement Learning in Mitigating Cyber Security Issues: A Review. In International Conference on Renewable Power (pp. 37-48). Singapore: Springer Nature Singapore.
42. Achari, A. P. S. K., & Sugumar, R. (2024, November). Performance analysis and determination of accuracy using machine learning techniques for naive bayes and random forest. In AIP Conference Proceedings (Vol. 3193, No. 1, p. 020199). AIP Publishing LLC.
43. Mathew, A., & Alex, H. (2022). Detect & protect-medical device cybersecurity. Curr. Overview Sci. Technol. Res, 1, 60-68.
44. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
45. Anbazhagan, K. (2024). Trustworthy and Adaptive AI Systems for Enterprise Analytics Cybersecurity and Decision Optimization Using API-First and Cloud-Native Architectures. International Journal of Technology, Management and Humanities, 10(03), 65-74.
46. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
47. Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". International Journal of Engineering Trends and Technology, 70(3), 284-294.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802376

48. Karthika, K., Anusha, K., Kavitha, K., Harshadha, R., Dharshini, D. S., & Sundhar, N. A. (2025, April). Frequency Reconfigurable Antenna using Advanced Materials: A Study. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.
49. Thavamani, C., & Rengarajan, A. (2024). Clustering related behaviour of users by the use of partitioning and parallel transaction reduction algorithm. International Journal of Advanced Intelligence Paradigms, 29(2-3), 122-132.
50. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
51. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338-356.
52. SakthiPreetha, A., Kavitha, K., Karthika, K., & Manohari, R. G. (2025, April). A Novel Metasurface-Embedded Antenna for WBAN Communications. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-4). IEEE.
53. Murugeshwari, B., Selvaraj, D., Sudharson, K., & Radhika, S. (2023). Data Mining with Privacy Protection Using Precise Elliptical Curve Cryptography. Intelligent Automation & Soft Computing, 35(1).
54. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
55. Anbazhagan, K., Kumar, R., Thilagavathy, R., & Anuradha, D. (2024, March). Shortest Job First with Gateway-based Resource Management Strategy for Fog Enabled Cloud Computing. In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-6). IEEE.
56. Kannadhasan, S., Vasuki, S., Kavitha, K., Karthikeyan, P., & Usha, S. G. A. (Eds.). (2025, April). Preface: Role of Artificial Intelligence and IoT in Engineering, Technology & Science [ICRAETS 2024]. In AIP Conference Proceedings (Vol. 3258, No. 1, p. 010001). AIP Publishing LLC.
57. Dhinakaran, D., Prathap, P. J., Selvaraj, D., Kumar, D. A., & Murugeshwari, B. (2022). Mining privacy-preserving association rules based on parallel processing in cloud computing. International Journal of Engineering Trends and Technology, 70(3), 284-294.