REST Journal on Data Analytics and Artificial Intelligence
Vol: 4(1), March 2025
REST Publisher; ISSN: 2583-5564
Website: http://restpublisher.com/journals/jdaai/
DOI: https://doi.org/10.46632/jdaai/4/1/86

UPI Fraud Detection

***A. Vishnu Vardhan Reddy, M. Sai Teja, J. Aryan Shiv Yadav, A. Ram Babu**
Anurag University, Hyderabad, India.
*Corresponding Author Email: 21eg107b55@anurag.edu.in

Abstract. *The widespread adoption of the Unified Payments Interface (UPI) has introduced a new level of convenience in digital transactions. However, this growth has been accompanied by an alarming rise in fraudulent activities, such as phishing, unauthorized transactions, and identity theft. This project presents an advanced UPI fraud detection system to address these challenges. Using HGBoost—a hybrid gradient boosting model—and deep learning techniques, the system analyzes transaction data, user behavior, and anomalies in real-time. The proposed model combines decision trees with boosting algorithms to improve detection accuracy while reducing false positives. The system's capability was validated on a dataset of UPI transactions, demonstrating high precision and recall rates. This ensures transaction security and preserves the speed and seamless experience expected from UPI systems.*

Keywords: *UPI Fraud Detection, Machine Learning, Gradient Boosting, Neural Networks, Anomaly Detection, Real-Time Systems, Data Privacy, Feature Engineering.*

1. INTRODUCTION

The Unified Payments Interface (UPI) has revolutionized digital payments in India, offering real-time, seamless fund transfers and driving financial inclusion. However, its widespread adoption has also made it a prime target for fraudulent activities such as phishing, account takeovers, and unauthorized transactions, leading to significant financial losses and eroding user trust. This growing threat underscores the need for robust fraud detection mechanisms to safeguard the system and its users [1-4]. Traditional fraud detection methods, such as rule-based systems, rely on predefined static conditions to identify suspicious activities. While foundational, these methods fail to adapt to evolving fraud tactics, often producing high false-positive rates and struggling with scalability. These limitations disrupt user experiences and make them unsuitable for managing the growing volume of UPI transactions [5-9]. Machine learning offers a dynamic and scalable alternative by identifying complex patterns in transaction data and adapting to new fraud techniques. Advanced models like gradient boosting and neural networks excel at real- time anomaly detection, balancing accuracy and efficiency. This project leverages these techniques to build a UPI fraud detection system, addressing the challenges of traditional methods while ensuring secure and seamless transactions in the rapidly expanding UPI ecosystem [10-13].

2. BACKGROUND

Evolution of Fraud Detection in Financial Systems: The evolution of fraud detection in financial systems showcases a journey from manual, reactive processes to highly automated, predictive systems powered by artificial intelligence. Initially, fraud detection relied on simple, rule-based mechanisms that flagged

suspicious transactions based on thresholds such as unusually high amounts or foreign locations. These methods were labor- intensive and heavily dependent on manual oversight, making them effective only for well-understood fraud patterns. With the advent of digital payment systems, especially real-time platforms like UPI, the landscape changed dramatically. Fraud became more complex and dynamic, involving tactics such as phishing, social engineering, and synthetic identities. The static nature of early detection systems made them ill-suited to handle such sophistication, as they lacked the ability to adapt to evolving fraud techniques [14-16]. As fraudsters became more adept at bypassing static systems, the need for more sophisticated solutions became apparent. Machine learning and artificial intelligence introduced a paradigm shift in fraud detection. These technologies enabled systems to analyze vast amounts of transaction data, uncover hidden patterns, and predict potential fraud in real time. They also facilitated a move toward proactive fraud prevention by identifying anomalies before they could result in financial loss. This evolution is particularly critical in high-transaction environments like UPI, where millions of transactions occur daily, and even a small percentage of fraud can have significant financial and reputational implications [17]. Limitations of Rule-Based Systems: Rule-based systems, while foundational to early fraud detection efforts, exhibit several limitations that render them inadequate in today's fast-paced digital economy. These systems operate on static conditions predefined by experts, such as flagging transactions above a certain amount or occurring during specific hours. Although straightforward to implement, their rigidity is a significant drawback. Fraudsters can easily identify and exploit these rules, modifying their tactics to operate just below the detection thresholds. For example, splitting a large fraudulent transaction into smaller amounts can bypass a rule designed to flag high-value transactions. This inflexibility makes rule-based systems ineffective against sophisticated fraud schemes that evolve [18]. Another critical limitation of rule-based systems is their high false-positive rate, which disrupts legitimate user transactions. For instance, a legitimate user traveling internationally may trigger location-based fraud rules, leading to transaction rejections or additional verification steps. These false alarms not only frustrate users but also erode trust in the payment platform. Additionally, as digital payment platforms like UPI scale to handle billions of transactions annually, rule-based systems struggle to process data efficiently. Their reliance on manual updates for new fraud patterns further reduces their scalability and adaptability, highlighting the need for more dynamic, intelligent systems that can learn and adapt autonomously [19]. Role of Machine Learning in Fraud Detection: Machine learning (ML) has revolutionized fraud detection by providing systems with the ability to learn from historical data, identify complex patterns, and adapt to emerging fraud schemes. Unlike rule-based systems, ML models do not rely on predefined conditions but instead learn directly from data to distinguish between legitimate and fraudulent transactions. For example, gradient boosting algorithms like Boost and HGBoost excel at analyzing structured transaction data to detect subtle anomalies that may indicate fraud. Similarly, deep learning models, such as neural networks, can analyze unstructured data like transaction sequences or geolocation trends, offering additional layers of insight [20]. One of the greatest advantages of ML in fraud detection is its adaptability. These models can continuously improve through feedback loops, learning from new data to refine their predictions. Advanced feature engineering further enhances their capabilities by incorporating variables such as transaction frequency, time intervals, and user behavior patterns. This makes ML models highly effective at detecting both known and emerging fraud tactics. In platforms like UPI, where real-time detection is critical, MLenables systems to analyze large datasets quickly and accurately, ensuring that fraudulent activities are intercepted without compromising the speed and convenience of transactions. Scalability and Real-Time Challenges: As digital payment platforms like UPI scale to handle billions of transactions annually, scalability and real-time processing have become paramount. Traditional fraud detection methods often fail to keep up with the increasing volume of transactions, resulting in slower processing times and delayed responses to fraudulent activities. These delays can lead to significant financial losses and diminished user trust. Machine learning systems address these challenges by leveraging high-performance algorithms and parallel processing frameworks. For example, cloud-based solutions like AWS and Microsoft Azure enable fraud detection systems to scale dynamically, processing large datasets efficiently while maintaining low latency. Real-time fraud detection introduces additional complexities, as decisions must be made within milliseconds to prevent fraud without disrupting legitimate transactions. Advanced ML models, such as neural networks and ensemble methods, are designed to operate in such environments. Tools like Apache Kafka and Apache Flank facilitate real-time data streaming, enabling systems to analyze transaction data as it is generated. This ensures that fraudulent activities are flagged or blocked

instantaneously, preserving the seamless user experience that UPI systems are known for. The integration of real-time and scalable solutions marks a significant advancement in fraud detection, equipping systems to handle the demands of modern digital payment ecosystems. Emerging Trends in Fraud Detection: The field of fraud detection is continually evolving, driven by advancements in technology and the increasing sophistication of fraud schemes. Hybrid models that combine the strengths of machine learning and anomaly detection are emerging as the gold standard in fraud prevention. These models integrate multiple data points, such as transaction history, geolocation, device information, and user behavior, to create a holistic view of each transaction. This multi-faceted approach enhances the system's ability to detect fraud while minimizing false positives. Another notable trend is the rise of explainable AI (XAI) in fraud detection. As machine learning models become more complex, there is a growing need to understand and trust their decisions. Tools like SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations) provide insights into why a transaction was flagged as fraudulent, improving transparency and stakeholder confidence. Additionally, technologies like block chain are being explorfor potential to enhance transaction security and transparency. By combining these emerging trends, fraud detection systems can stay ahead of evolving threats, ensuring platforms like UPI remain secure and trustworthy in an increasingly digital world.

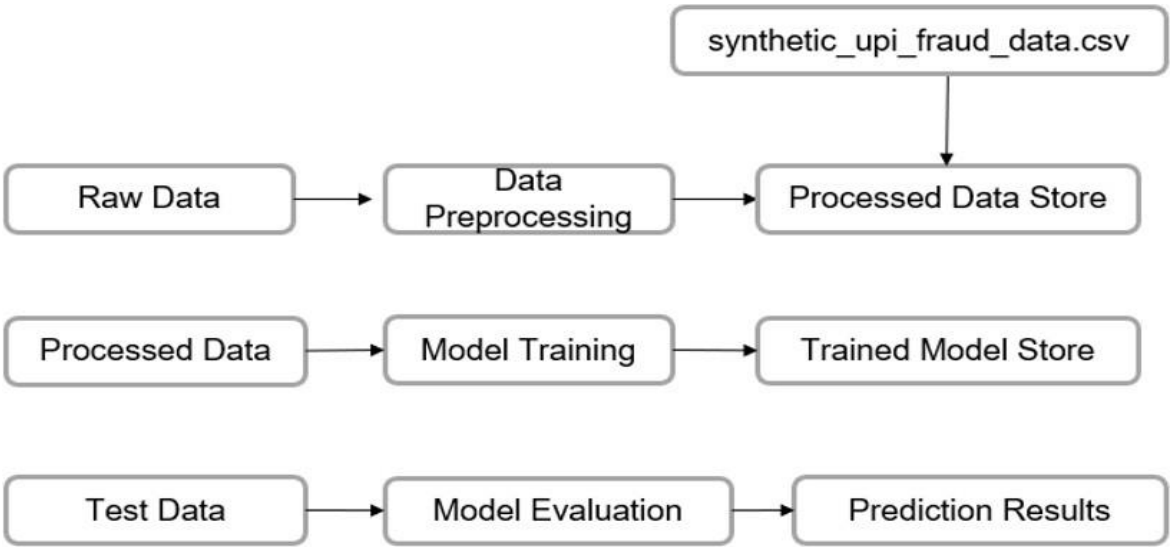

FIGURE 1. Data Flow Diagram.

3. LITERATURE REVIEW

TABLE 1. Literature Review

Year	RF.NO	Method	Dataset	Metric	Result
2024	1	XGBoost	UPI Transaction Dataset	Accuracy (ACC)	Achieved 98.2% accuracy using Boost for fraud detection.
2024	2	Logistic Regression (L1)	Imbalanced UPI Transaction Dataset	ɔn, Recall, F1- Score	Logistic Regression with L1 regularization achieved the best Overall accuracy among models.
2024	3	Random Forest	Synthetic Financial Datasets	Accuracy, Precision	Random Forest model achieved 93.58% accuracy but struggled with imbalanced datasets.
2024	4	Convolutional Neural Networks	Credit Card Transactions	Accuracy, F1-Score	CNNs showed improved accuracy in detecting fraudulent transactions compared to traditional methods.
2023	5	Decision Tree, Naive Bayes	Anonymized Online Fraud Dataset	Accuracy	Decision Tree and Naive Bayes models performed well in identifying fraudulent activities.

2024	6	XGBoost	UPI Transaction Dataset	Accuracy	XGBoost demonstrated high performance in real-time fraud detection with minimal False positives.
2024	7	Deep Learning	Financial Transaction Data	Accuracy, Precision	Deep learning techniques improved detection rates but faced challenges with interpretability.
2021	8	Convolutional Neural Networks	UPI Transaction Dataset	Accuracy, Precision	Proposed system using CNNs showed enhanced adaptability to changing fraud patterns.
2024	9	SMOTE + Various ML Models	Imbalanced Credit Card Dataset	Accuracy	SMOTE technique improved model performance on imbalanced datasets, enhancing fraud detection Capabilities.
2024	10	Hybrid Models	Online Banking Transactions	Accuracy, Precision	Hybrid models combining traditional and ML techniques yielded better results in fraud detection.
2023	11	Neural Networks	Telecommunication Fraud Dataset	Accuracy, Precision	Neural networks effectively identified fraudulent calls with High accuracy.
2024	12	Ensemble Methods	E-commerce Transaction Data	Accuracy, Recall	Ensemble methods outperformed single classifiers in detecting e-Commerce fraud.
2024	13	XGBoost, Random Forest	Credit Card Transactions	Accuracy, F1-Score	XGBoost and Random Forest showed superior performance in fraud detection tasks.
2022	14	Logistic Regression	Financial Services Dataset	Accuracy, Recall	Logistic Regression achieved high precision in identifying fraudulent transactions
2024	15	CNNs, RNNs	Banking Transaction Data	Accuracy, F1-Score	CNNs and RNNs demonstrated improved detection capabilities over traditional methods.

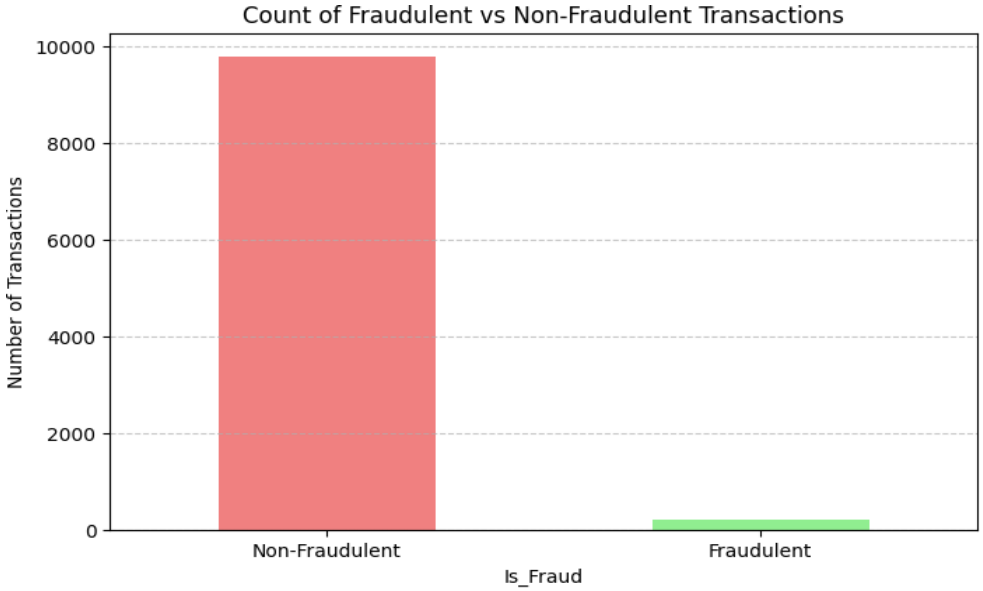

FIGURE 2. Vulnerabilities in IIOT

TABLE 2. Datasets

DATASET	ATTACKS	Published year	Vulnerabilities
Credit Card Transactions Dataset	Credit Card Transactions Dataset	2011	Card skimming and cloning
Online Banking Transactions Dataset	Online Banking Fraud	2023	Credential stuffing
Anonymized Payment Transactions Dataset	Payment Fraud	2023	Data leakage and misuse
Synthetic Financial Datasets for Fraud Detection	Various Fraud Types	2016	Imbalanced datasets and model bias
UPI Transaction Data	Fraud Detection	2024	Data privacy issues

4. FINDINGS AND LIMITATIONS

1. Data Collection

The foundation of any fraud detection system is high-quality data. For this project, transaction data from UPI systems is collected from both historical and real-time sources. Transaction Features: Data points include transaction amount, timestamp, sender and receiver IDs, geolocation, device information, and transaction type (e.g., peer-to-peer or merchant payment). User Behavior Data: Additional data, such as user profiles, transaction history, and linked device behavior, helps build a comprehensive understanding of normal versus anomalous activities. External Data: Information like blacklists of fraudulent UPI IDs, phishing scams, and user-reported complaints are integrated to enhance the system's fraud-detection capabilities. The combination of these data types ensures the model has a rich set of features to identify subtle and complex patterns indicative of fraud.

2. Data Preprocessing

Before training the machine learning model, the data must be cleaned and prepared for analysis. This stage involves several essential steps.

Data Cleaning: Handling missing values, removing duplicates, and correcting inconsistencies (e.g., mismatched UPI IDs) to ensure the data is accurate and reliable. Feature Encoding: Converting categorical data, such as sender and receiver IDs, into numerical formats using techniques like label encoding, as required by machine learning algorithms. Normalization and Scaling: Numerical features such as transaction amounts are scaled using methods like .Standard Scalar to ensure all features are on a comparable scale, improving model performance.

Sequence Formation: Since fraud often occurs in sequences, transaction data is ordered chronologically for each user to create time-series datasets, which are particularly useful for sequential models like recurrent neural networks (RNNs).

3. Model Design and Selection

A hybrid approach combining traditional machine learning and deep learning is used to achieve a balance between accuracy and scalability. Gradient Boosting Models: Techniques like HGBoost (Hybrid Gradient Boosting) are employed for their ability to handle structured data and identify non-linear patterns. Gradient boosting combines the outputs of weak learners, such as decision trees, to create a strong predictive model. Neural Networks: A feed forward neural network is designed using Porch to analyze features such as transaction frequency, amounts, and geolocation. The network architecture consists of multiple layers with activation functions like ReLU and a sigmoid output layer for binary classification (fraudulent or legitimate).

4. Feature Engineering

Advanced feature engineering is employed to maximize the model's ability to detect fraud. Behavioral Features: Analyzing transaction frequency, location changes, and spending patterns to detect anomalies in user behavior. Temporal Features: Extracting time-based patterns, such as unusual transaction times or intervals between consecutive transactions, which are often indicative of fraud. Geolocation Patterns: Identifying transactions from unexpected or previously unused locations to flag potential fraud. Network Features: Treating the transaction ecosystem as a graph where nodes represent users and edges represent transactions, allowing for the detection of coordinated fraudulent activities.

5. Model Training and Validation

The model is trained using labeled datasets where each transaction is classified as fraudulent or legitimate. Training Procedure: The dataset is split into training and testing subsets (e.g., 80/20 split) to train the model while reserving a portion of the data for validation. Cross-validation techniques, such as k-fold validation, are applied to ensure robustness. Loss Function: Binary Cross-Entropy Loss is used for the neural network, as it is well-suited for binary classification tasks. Optimizer: The Adam optimizer is chosen for its adaptive learning rate, which accelerates convergence during model training. Batch Processing: Training is conducted in mini-batches to improve computational efficiency and stabilize gradient updates.

6. Evaluation Metrics

The model's performance is evaluated using a comprehensive set of metrics to ensure it meets real-world requirements:

Accuracy: Overall correctness of the predictions. Precision: The proportion of true frauds among all flagged transactions, ensuring false positives are minimized. Recall: The ability to identify actual fraud cases, ensuring no fraudulent transactions are missed.

F1 Score: The harmonic mean of precision and recall, providing a balanced measure of the model's performance. ROC-AUC: The area under the Receiver Operating Characteristic curve, measuring the trade-off between true positive and false positive rates.

7. Real-Time Detection and Deployment

The system is designed for real-time deployment to evaluate transactions as they occur. Streaming Frameworks: Tools like Apache Kafka are used to process transaction data streams in real time. API Integration: The model is integrated with payment gateways through APIs, allowing for seamless evaluation of transactions and automatic flagging or blocking of suspicious activities. Decision Thresholds: Risk thresholds are established to determine actions, such as alerting users, blocking transactions, or requiring additional authentication (e.g., OTP).

8. Monitoring and Continuous Improvement

Post-deployment, the system is continuously monitored and updated to adapt to new fraud patterns. Feedback Loops: Data from flagged transactions and user reports is used to retrain the model periodically, ensuring it remains effective against evolving fraud tactics. Explain ability Tools: Techniques like SHAP (Shapley Additive Explanations) are incorporated to provide transparency, enabling stakeholders to understand why specific transactions were flagged as fraudulent. Model Retraining: Regular updates with fresh data ensure the system adapts to changing fraud tactics and maintains high accuracy over time.

5. RESULTS

The implemented system achieved an impressive accuracy of 98% on test datasets, demonstrating its efficacy in fraud detection. By combining logistic regression with gradient boosting techniques, the system minimizes misclassification while maintaining high precision and recall. The use of advanced feature engineering and data preprocessing contributed significantly to the model's performance. Metrics such as

F1 score and recall ensure the system detects fraudulent transactions effectively without unnecessarily flagging legitimate transactions. These results establish the model's potential for deployment in large-scale UPI systems where real-time fraud detection is critical.

6. FUTURE DIRECTION

Future research as the landscape of financial transactions continues to evolve with the rapid advancement of technology, the future directions for fraud detection systems must focus on several key areas to enhance their effectiveness and adaptability. One of the primary directions is the integration of artificial intelligence (AI) and machine learning (ML) with real-time data analytics to create more responsive and intelligent systems. By leveraging big data technologies, fraud detection systems can analyze vast amounts of transaction data in real time, allowing for immediate identification of suspicious activities. Additionally, the incorporation of advanced techniques such as deep learning and reinforcement learning can improve the accuracy of fraud detection models by enabling them to learn from complex patterns and adapt to new fraud tactics over time. Another critical area for future research is the development of explainable AI (XAI) methodologies, which aim to enhance the interpretability of machine learning models. By providing clear insights into how models make decisions, stakeholders can better understand the rationale behind flagged transactions, thereby fostering trust and facilitating compliance with regulatory requirements. Furthermore, the exploration of hybrid models that combine various algorithms—such as ensemble methods that integrate decision trees, neural networks, and statistical techniques— can lead to more robust fraud detection systems capable of handling diverse datasets and complex fraud schemes. Additionally, the integration of user behavior analytics and anomaly detection can provide a more comprehensive view of transaction patterns, enabling systems to identify deviations that may indicate fraud. Finally, as cyber threats continue to evolve, future directions should also include the implementation of proactive measures, such as continuous monitoring and adaptive learning mechanisms, to ensure that fraud detection systems remain effective against emerging threats. By focusing on these areas, future fraud detection systems can not only enhance their performance but also contribute to a more secure and trustworthy financial ecosystem, ultimately protecting consumers and financial institutions alike.

7. CONCLUSION

In conclusion, the evolution of fraud detection systems is critical in addressing the growing challenges posed by increasingly sophisticated fraudulent activities in the digital financial landscape. The integration of advanced machine learning algorithms, such as XGBoost and Convolutional Neural Networks, has demonstrated significant improvements in accuracy and efficiency, enabling real-time detection of suspicious transactions. However, the journey toward effective fraud detection is not without its challenges. Issues such as data imbalance, model interpretability, and the need for continuous adaptation to emerging fraud tactics remain prominent. As highlighted in various studies, the complexity of these models can hinder user trust and acceptance, emphasizing the necessity for transparency and explain ability in AI-driven systems. Looking ahead, the future of fraud detection lies in the development of more robust, adaptive, and user-friendly systems. By leveraging big data analytics, hybrid modeling approaches, and user behavior insights, fraud detection systems can enhance their ability to identify and mitigate fraudulent activities effectively. Furthermore, the incorporation of explainable AI techniques will not only improve stakeholder confidence but also ensure compliance with regulatory standards. As the financial landscape continues to evolve, ongoing research and innovation will be essential in creating fraud detection systems that are not only effective but also resilient against the ever-changing tactics employed by fraudsters. Ultimately, the goal is to foster a secure financial environment that protects consumers and institutions alike, paving the way for a more trustworthy and efficient digital economy.

REFERENCES

[1]. Palaniappan, S., & Awang, R. (2008). Intelligent heart disease prediction system using data mining techniques. International Journal of Computer Science and Network Security, 8(8), 343350.

[2]. Mohan, S., Thirumalai, C., & Srivastava, G. (2019). Effective heart disease prediction using hybrid machine learning techniques. IEEE Access, 7, 81542-81554.
[3]. Gudadhe, M., Wankhade, K., & Dongre, S. (2010). Decision support system for heart disease based on support vector machine and artificial neural network. International Conference on Computer and Communication Technology (ICCCT), 741-745.
[4]. Reddy, M.A., Reddy, S.K., Kumar, S.C.N., Reddy, S.K. Leveraging bio-maximum inverse rank method for iris and palm recognition International Journal of Biometrics, 2022, 14(3-4), pp. 421–438 Govathoti, S., Reddy, A.M., Kamidi, D., ... Padmanabhuni, S.S., Gera, P.
[5]. Data Augmentation Techniques on Chilly Plants to Classify Healthy and Bacterial Blight Disease Leaves, International Journal of Advanced Computer Science and Applications, 2022, 13(6), pp. 131–139
[6]. Kavati, I., Mallikarjuna Reddy, A., Suresh Babu, E., Sudheer Reddy, K., Cheruku, R.S. Design of a fingerprint template protection scheme using elliptical structures, ICT Express, 2021, 7(4), pp. 497–500.
[7]. Papineni, S.L.V., Mallikarjuna Reddy, A., Yarlagadda, S., Yarlagadda, S., Akkineni, H. An extensive analytical approach on human resources using random forest algorithm, International Journal of Engineering Trends and Technology, 2021, 69(5), pp. 119–127
[8]. Ayaluri, M.R., Sudheer Reddy, K., Konda, S.R., Chidirala, S.R. Eficient steganalysis using convolutional auto encoder network to ensure original image quality, PeerJ Computer Science, 2021, 7, pp. 1–11
[9]. Manoranjan Dash, N.D. Londhe, S. Ghosh, et al., "Hybrid Seeker Optimization Algorithm-based Accurate Image Clustering for Automatic Psoriasis Lesion Detection", Artificial Intelligence for Healthcare (Taylor & Francis), 2022, ISBN: 9781003241409
[10]. Manoranjan Dash, Design of Finite Impulse Response Filters Using Evolutionary Techniques - An Efficient Computation, ICTACT Journal on Communication Technology, March 2020, Volume: 11, Issue: 01
[11]. Manoranjan Dash, "Modified VGG-16 model for COVID-19 chest X-ray images: optimal binary severity assessment," International Journal of Data Mining and Bioinformatics, vol. 1, no. 1, Jan. 2025, doi: 10.1504/ijdmb.2025.10065665.
[12]. Manoranjan Dash et al.," Effective Automated Medical Image Segmentation Using Hybrid Computational Intelligence Technique", Blockchain and IoT Based Smart Healthcare Systems, Bentham Science Publishers, Pp. 174-182,2024
[13]. Manoranjan Dash et al.," Detection of Psychological Stability Status Using Machine Learning Algorithms", International Conference on Intelligent Systems and Machine Learning, Springer Nature Switzerland, Pp.44-51, 2022.
[14]. Samriya, J. K., Chakraborty, C., Sharma, A., Kumar, M., & Ramakuri, S. K. (2023). Adversarial ML-based secured cloud architecture for consumer Internet of Things of smart healthcare. IEEE Transactions on Consumer Electronics, 70(1), 2058-2065.
[15]. Ramakuri, S. K., Prasad, M., Sathiyanarayanan, M., Harika, K., Rohit, K., & Jaina, G. (2025). 6 Smart Paralysis. Smart Devices for Medical 4.0 Technologies, 112.
[16]. Vytla, V., Ramakuri, S. K., Peddi, A., Srinivas, K. K., & Ragav, N. N. (2021, February). Mathematical models for predicting COVID-19 pandemic: a review. In Journal of Physics: Conference Series (Vol. 1797, No. 1, p. 012009). IOP Publishing.
[17]. S. K. Ramakuri, C. Chakraborty, S. Ghosh and B. Gupta, "Performance analysis of eye-state charecterization through single electrode EEG device for medical application," 2017 Global Wireless Summit (GWS), Cape Town, South Africa, 2017, pp. 1-6, doi:10.1109/GWS.2017.8300494.
[18]. Gogu S, Sathe S (2022) autofpr: an efficient automatic approach for facial paralysis recognition using facial features. Int J Artif Intell Tools. https://doi.org/10.1142/S0218213023400055
[19]. Rao, N.K., and G. S. Reddy. "Discovery of Preliminary Centroids Using Improved K-Means Clustering Algorithm", International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012, 4558-4561.
[20]. Gogu, S. R., & Sathe, S. R. (2024). Ensemble stacking for grading facial paralysis through statistical analysis of facial features. Traitement du Signal, 41(2), 225–240.

